



Panduan Pengguna

AWS Security Hub



AWS Security Hub : Panduan Pengguna

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Merek dagang dan tampilan dagang Amazon tidak boleh digunakan sehubungan dengan produk atau layanan apa pun yang bukan milik Amazon, dengan cara apa pun yang dapat menyebabkan kebingungan di antara pelanggan, atau dengan cara apa pun yang merendahkan atau mendiskreditkan Amazon. Semua merek dagang lain yang tidak dimiliki oleh Amazon merupakan hak milik masing-masing pemiliknya, yang mungkin atau tidak terafiliasi, terkait dengan, atau disponsori oleh Amazon.

Table of Contents

Apa itu AWS Security Hub?	1
Fitur	1
Integrasi	2
Wilayah AWS didukung untuk pratinjau publik	2
Aksesibilitas	4
Harga	4
Memulai	4
Mengaktifkan Security Hub	5
Rekomendasi	14
Konsep	16
Temuan OCSF	17
Temuan cakupan	18
Temuan cakupan untuk Security Hub CSPM	18
Temuan cakupan untuk GuardDuty	18
Temuan cakupan untuk Amazon Inspector	19
Temuan cakupan untuk Macie	19
Temuan paparan	20
Sumber daya yang didukung	20
Sifat yang didukung	21
Menghasilkan temuan paparan	22
Menentukan tingkat keparahan temuan eksposur	27
Meninjau temuan paparan	28
Memulihkan temuan paparan	30
Temuan urutan serangan	88
Meninjau temuan urutan serangan	89
Remediasi temuan urutan serangan	90
Aturan otomatisasi	90
Penyempurnaan Utama	91
Integrasi Eksternal	91
Kriteria yang didukung OCSF	91
Bidang OCSF untuk AutomationRulesFindingFieldsUpdate	92
Integrasi pihak ketiga	92
Buat kunci KMS	92
Jira Cloud	96

ServiceNow	100
Dasbor	103
Widget ringkasan eksposur	104
Widget ringkasan ancaman	104
Widget cakupan keamanan	104
Melihat detail tentang sumber daya di Security Hub	105
Grafik jalur serangan potensial	106
Menonaktifkan Security Hub	107
Apa itu AWS Security Hub CSPM?	108
Manfaat CSPM Security Hub	109
Mengakses Security Hub CSPM	110
Layanan terkait	111
Security Hub CSPM uji coba gratis, penggunaan, dan harga	111
Melihat detail penggunaan dan perkiraan biaya	112
Detail harga	112
Konsep CSPM Security Hub	113
Mengaktifkan Security Hub CSPM	119
Memverifikasi izin yang diperlukan	119
Mengaktifkan CSPM Security Hub dengan Integrasi Organizations	119
Konfigurasi pusat	120
Mengaktifkan Security Hub CSPM secara manual	121
Skrip pengaktifan multi-akun	123
Langkah selanjutnya: Manajemen dan integrasi postur	123
Konfigurasi AWS Config untuk Security Hub CSPM	124
Pertimbangan sebelum mengaktifkan dan mengonfigurasi AWS Config	124
Merekam sumber daya di AWS Config	125
Cara untuk mengaktifkan dan mengonfigurasi AWS Config	127
Kontrol Config.1	128
Menghasilkan aturan terkait layanan	128
Pertimbangan biaya	129
Konfigurasi lokal	129
Konfigurasi pusat	130
Manfaat menggunakan konfigurasi pusat	131
Kapan menggunakan konfigurasi pusat?	132
Istilah dan konsep konfigurasi pusat	132
Mengaktifkan konfigurasi pusat	138

Dikelola secara terpusat versus dikelola sendiri	144
Cara kerja kebijakan konfigurasi	148
Membuat dan mengaitkan kebijakan konfigurasi	154
Meninjau status dan detail kebijakan konfigurasi	160
Memperbarui kebijakan konfigurasi	164
Menghapus kebijakan konfigurasi	169
Memutuskan konfigurasi	171
Konfigurasi dalam konteks	173
Menonaktifkan konfigurasi pusat	174
Mengelola Security Hub CSPM untuk beberapa akun	178
Mengelola akun dengan AWS Organizations	178
Mengelola akun secara manual dengan undangan	179
Rekomendasi untuk lingkungan multi-akun	180
Jumlah maksimum akun anggota	180
Membuat hubungan administrator-anggota	180
Mengkoordinasikan akun administrator di seluruh layanan	181
Mengelola akun dengan AWS Organizations	182
Berintegrasi dengan AWS Organizations	183
Mengaktifkan CSPM Security Hub secara otomatis di akun baru	192
Mengaktifkan CSPM Security Hub secara manual di akun baru	194
Memutuskan akun anggota organisasi	196
Mengelola akun dengan undangan	198
Menambahkan dan mengundang akun anggota	200
Menanggapi undangan	203
Memutuskan akun anggota	207
Menghapus akun anggota	208
Memutuskan hubungan dari akun administrator	210
Transisi ke AWS Organizations	211
Tindakan yang diizinkan oleh administrator dan akun anggota	213
Pengaruh tindakan akun pada data CSPM	219
Security Hub CSPM dinonaktifkan	219
Akun anggota dipisahkan dari akun administrator	220
Akun anggota dihapus dari organisasi	220
Akun ditangguhkan	220
Akun ditutup	221
Menggabungkan data CSPM di seluruh Wilayah	223

Jenis data yang dikumpulkan	224
Agregasi untuk akun administrator dan anggota	226
Konfigurasi dan agregasi pusat	227
Mengaktifkan agregasi	228
Meninjau pengaturan agregasi	230
Memperbarui pengaturan agregasi	231
Menghentikan agregasi	233
Menghapus agregator temuan (konsol)	234
Standar CSPM	236
Referensi standar	237
AWS Praktik Terbaik Keamanan Dasar	239
AWS Penandaan Sumber Daya	255
Tolok Ukur AWS Yayasan CIS	262
NIST SP 800-53 Revisi 5	278
NIST SP 800-171 Revisi 2	295
PCI DSS	300
Standar yang dikelola layanan	310
Mengaktifkan standar	324
Mengaktifkan standar di beberapa akun dan Wilayah AWS	325
Mengaktifkan standar dalam satu akun dan Wilayah AWS	326
Memeriksa status standar	328
Meninjau detail standar	331
Memahami skor keamanan standar	331
Meninjau kontrol untuk standar	332
Mematikan standar yang diaktifkan secara otomatis	334
Menonaktifkan standar	335
Menonaktifkan standar di beberapa akun dan Wilayah AWS	336
Menonaktifkan standar dalam satu akun dan Wilayah AWS	337
Kontrol CSPM	339
Tampilan kontrol terkonsolidasi	339
Skor keamanan ringkasan untuk kontrol	340
Referensi kontrol	341
Ubah log untuk kontrol	455
Akun AWS kontrol	526
AWS Amplify kontrol	528
Kontrol Amazon API Gateway	531

AWS AppConfig kontrol	537
AppFlow Kontrol Amazon	543
AWS App Runner kontrol	545
AWS AppSync kontrol	548
Kontrol Amazon Athena	552
AWS Backup kontrol	557
AWS Batch kontrol	565
AWS Certificate Manager kontrol	571
AWS CloudFormation kontrol	575
CloudFront Kontrol Amazon	578
AWS CloudTrail kontrol	588
CloudWatch Kontrol Amazon	599
AWS CodeArtifact kontrol	645
AWS CodeBuild kontrol	647
Kontrol Amazon CodeGuru Profiler	652
Kontrol Amazon CodeGuru Reviewer	654
Kontrol Amazon Cognito	656
AWS Config kontrol	657
Kontrol Amazon Connect	660
Kontrol Firehose Data Amazon	662
AWS DataSync kontrol	663
Kontrol Detektif Amazon	665
AWS DMS kontrol	667
Kontrol Amazon DocumentDB	681
Kontrol Amazon DynamoDB	686
EC2 Kontrol Amazon	693
Kontrol EC2 Auto Scaling Amazon	769
Kontrol ECR Amazon	777
Kontrol Amazon ECS	782
Kontrol Amazon EFS	796
Kontrol Amazon EKS	803
ElastiCache Kontrol Amazon	809
AWS Elastic Beanstalk kontrol	815
Elastic Load Balancing	819
Kontrol Elasticsearch	834
Kontrol EMR Amazon	843

EventBridge Kontrol Amazon	847
Kontrol Amazon Fraud Detector	850
FSx Kontrol Amazon	857
AWS Global Accelerator kontrol	862
AWS Glue kontrol	864
GuardDuty Kontrol Amazon	867
AWS Identity and Access Management kontrol	881
Kontrol Amazon Inspector	917
AWS IoT kontrol	921
AWS Kontrol IoT Events	930
AWS Kontrol IoT SiteWise	935
AWS Kontrol IoT TwinMaker	943
AWS Kontrol Nirkabel IoT	949
Kontrol Amazon IVS	953
Kontrol Amazon Keyspaces	958
Kontrol Amazon Kinesis	959
AWS KMS kontrol	963
AWS Lambda kontrol	969
Kontrol Amazon Macie	975
Kontrol MSK Amazon	976
Kontrol Amazon MQ	979
Kontrol Amazon Neptune	984
AWS Network Firewall kontrol	991
Kontrol OpenSearch Layanan Amazon	1001
AWS Private CA kontrol	1011
Kontrol Amazon RDS	1014
Kontrol Amazon Redshift	1056
Kontrol Amazon Redshift	1073
Amazon Route 53 kontrol	1080
Kontrol Amazon S3	1082
Kontrol Amazon SageMaker AI	1106
AWS Secrets Manager kontrol	1114
AWS Service Catalog kontrol	1120
Kontrol Layanan Email Sederhana Amazon	1121
Kontrol Amazon SNS	1124
Kontrol Amazon SQS	1129

AWS Step Functions kontrol	1132
AWS Systems Manager kontrol	1135
AWS Transfer Family kontrol	1141
AWS WAF kontrol	1150
WorkSpaces Kontrol Amazon	1157
Izin untuk mengonfigurasi kontrol	1159
Mengaktifkan kontrol	1160
Mengaktifkan kontrol lintas standar	1161
Mengaktifkan kontrol dalam standar tertentu	1164
Mengaktifkan kontrol baru secara otomatis	1167
Menonaktifkan kontrol	1169
Menonaktifkan kontrol lintas standar	1170
Menonaktifkan kontrol dalam standar tertentu	1173
Kontrol yang disarankan untuk menonaktifkan	1175
Pemeriksaan dan skor keamanan	1180
AWS Config Sumber daya yang diperlukan untuk temuan kontrol	1181
Jadwal untuk menjalankan pemeriksaan keamanan	1232
Menghasilkan dan memperbarui temuan kontrol	1234
Status kepatuhan dan status kontrol	1249
Menghitung skor keamanan	1251
Kategori kontrol	1254
Identifikasi	1254
Lindungi	1255
Mendeteksi	1256
Menanggapi	1257
Memulihkan	1257
Meninjau detail kontrol	1258
Melihat detail untuk kontrol	1259
Kontrol penyaringan dan penyortiran	1260
Parameter kontrol	1262
Pengaruh memodifikasi nilai parameter kontrol	1263
Kontrol yang mendukung parameter kustom	1264
Meninjau nilai parameter kontrol saat ini	1264
Menyesuaikan parameter kontrol	1267
Kembali ke parameter kontrol default	1271
Memeriksa status perubahan parameter kontrol	1275

Meninjau dan mengelola temuan kontrol	1276
Memfilter dan menyortir temuan kontrol	1277
Sampel temuan kontrol	1278
Integrasi CSPM	1303
Meninjau daftar integrasi	1303
Mengaktifkan aliran temuan dari integrasi	1305
Menonaktifkan aliran temuan dari integrasi	1306
Melihat temuan dari integrasi	1307
Layanan AWS integrasi	1308
Ikhtisar integrasi AWS layanan dengan Security Hub CSPM	1308
AWS layanan yang mengirimkan temuan ke Security Hub CSPM	1309
AWS layanan yang menerima temuan dari Security Hub CSPM	1326
Integrasi pihak ketiga	1329
Ikhtisar integrasi pihak ketiga dengan Security Hub CSPM	1329
Integrasi pihak ketiga yang mengirimkan temuan ke Security Hub CSPM	1339
Integrasi pihak ketiga yang menerima temuan dari Security Hub CSPM	1356
Integrasi pihak ketiga yang mengirimkan temuan ke dan menerima temuan dari Security Hub CSPM	1362
Integrasi produk khusus	1364
Persyaratan dan rekomendasi untuk integrasi produk khusus	1364
Memperbarui temuan dari produk khusus	1365
Contoh integrasi kustom	1366
Temuan CSPM	1367
BatchImportFindings untuk menemukan penyedia	1369
Prasyarat untuk menggunakan BatchImportFindings	1369
Menentukan apakah akan membuat atau memperbarui temuan	1369
Pembatasan untuk menemukan pembaruan dengan BatchImportFindings	1370
Memperbarui temuan dengan FindingProviderFields	1370
BatchUpdateFindings untuk pelanggan	1372
Bidang yang tersedia untuk BatchUpdateFindings	1373
Mengkonfigurasi akses ke BatchUpdateFindings	1373
Meninjau detail dan riwayat penemuan	1376
Meninjau detail dan riwayat penemuan	1378
Memfilter temuan	1381
Filter default pada daftar pencarian	1381
Petunjuk untuk menambahkan filter	1382

Temuan pengelompokan	1383
Mengatur status alur kerja temuan	1384
Mengatur status alur kerja temuan	1386
Mengirim temuan ke tindakan khusus	1387
Menemukan format: ASFF	1388
ASFF dan konsolidasi	1468
Atribut ASFF tingkat atas yang diperlukan	1528
Atribut ASFF tingkat atas opsional	1539
ResourcesObjek ASFF	1560
Wawasan CSPM	1684
Meninjau dan bertindak berdasarkan wawasan	1685
Melihat dan mengambil tindakan pada hasil wawasan	1685
Melihat dan mengambil tindakan atas temuan hasil wawasan (konsol)	1687
Wawasan terkelola	1688
Wawasan khusus	1699
Membuat wawasan khusus	1700
Mengedit wawasan khusus	1703
Menghapus wawasan khusus	1705
Otomatisasi CSPM	1707
Aturan otomatisasi	1708
Mendefinisikan kriteria aturan dan tindakan aturan	1708
Kriteria aturan dan tindakan aturan yang tersedia	1709
Temuan yang dievaluasi oleh aturan otomatisasi	1715
Cara kerja urutan aturan	1716
Membuat aturan otomatisasi	1717
Melihat aturan otomatisasi	1721
Mengedit aturan otomatisasi	1722
Urutan aturan pengeditan	1724
Menghapus atau menonaktifkan aturan otomatisasi	1725
Contoh aturan otomatisasi	1727
Respon dan remediasi otomatis	1734
EventBridge jenis acara	1735
EventBridge format acara	1737
Mengkonfigurasi aturan EventBridge	1740
Mengkonfigurasi dan menggunakan tindakan kustom	1745
Dasbor CSPM	1751

Widget ringkasan risiko	1751
Widget ringkasan ancaman	1751
Widget cakupan keamanan	1752
Widget yang tersedia untuk dasbor Ringkasan	1752
Widget ditampilkan secara default	1752
Widget tersembunyi secara default	1754
Memfilter dasbor Ringkasan	1755
Membuat dan menyimpan set filter	1757
Memperbarui atau menghapus set filter	1757
Menyesuaikan dasbor Ringkasan	1758
Batas CSPM regional	1759
Pembatasan agregasi Lintas Wilayah	1759
Ketersediaan integrasi menurut Wilayah	1759
Integrasi yang didukung di Wilayah Tiongkok (Beijing) dan Tiongkok (Ningxia)	1759
Integrasi yang didukung di Wilayah AWS GovCloud (AS-Timur) dan AWS GovCloud (AS-Barat)	1760
Ketersediaan standar menurut Wilayah	1762
Ketersediaan kontrol berdasarkan Wilayah	1762
Batas regional pada kontrol CSPM	1762
AS Timur (Virginia Utara)	1764
AS Timur (Ohio)	1764
AS Barat (California Utara)	1766
AS Barat (Oregon)	1768
Afrika (Cape Town)	1769
Asia Pasifik (Hong Kong)	1773
Asia Pasifik (Hyderabad)	1775
Asia Pasifik (Jakarta)	1783
Asia Pasifik (Malaysia)	1788
Asia Pasifik (Melbourne)	1802
Asia Pasifik (Mumbai)	1811
Asia Pasifik (Osaka)	1812
Asia Pasifik (Seoul)	1817
Asia Pasifik (Singapura)	1818
Asia Pasifik (Sydney)	1820
Asia Pasifik (Thailand)	1821
Asia Pasifik (Tokyo)	1837

Kanada (Pusat)	1838
Kanada Barat (Calgary)	1840
Tiongkok (Beijing)	1853
Tiongkok (Ningxia)	1862
Eropa (Frankfurt)	1870
Eropa (Irlandia)	1872
Eropa (London)	1873
Eropa (Milan)	1874
Eropa (Paris)	1878
Eropa (Spanyol)	1880
Eropa (Stockholm)	1888
Eropa (Zürich)	1890
Israel (Tel Aviv)	1897
Meksiko (Tengah)	1906
Timur Tengah (Bahrain)	1922
Timur Tengah (UEA)	1926
Amerika Selatan (Sao Paulo)	1933
AWS GovCloud (AS-Timur)	1935
AWS GovCloud (AS-Barat)	1944
Membuat sumber daya CSPM dengan CloudFormation	1954
CSPM dan template Security Hub AWS CloudFormation	1954
Pelajari lebih lanjut tentang AWS CloudFormation	1955
Berlangganan pengumuman CSPM	1956
Format pesan Amazon SNS	1962
Menonaktifkan CSPM Security Hub	1964
Keamanan	1967
Perlindungan data	1967
Manajemen identitas dan akses	1969
Audiens	1969
Mengautentikasi dengan identitas	1970
Mengelola akses menggunakan kebijakan	1974
Bagaimana Security Hub bekerja dengan IAM	1976
Contoh kebijakan berbasis identitas	1984
Peran terkait layanan	1991
AWS kebijakan terkelola	1994
Pemecahan Masalah	2012

Validasi kepatuhan	2016
Ketahanan	2017
Keamanan infrastruktur	2017
Titik akhir VPC (AWS PrivateLink)	2018
Pertimbangan untuk titik akhir VPC Security Hub	2018
Membuat VPC endpoint antarmuka untuk Security Hub	2018
Membuat kebijakan VPC endpoint untuk Security Hub	2019
Subnet bersama	2019
Mencatat panggilan API	2020
Informasi CSPM Security Hub di CloudTrail	2020
Contoh: Entri file log CSPM Security Hub	2021
Pemberian tag pada sumber daya	2023
Menandai dasar-dasar	2023
Menggunakan tag dalam kebijakan IAM	2025
Menambahkan tanda	2026
Mengedit tag untuk sumber daya	2028
Meninjau tag	2030
Menghapus tanda	2033
Kuota	2036
Kuota maksimum	2036
Nilai kuota	2036
Riwayat dokumen	2037
.....	mmcxv

Apa itu AWS Security Hub?

Note

Security Hub dalam rilis pratinjau dan dapat berubah sewaktu-waktu.

AWS Security Hub adalah solusi keamanan cloud terpadu yang memprioritaskan masalah keamanan kritis Anda dan membantu Anda merespons dalam skala besar. Security Hub mendeteksi masalah keamanan dengan secara otomatis menghubungkan dan memperkaya sinyal keamanan dari berbagai sumber, seperti manajemen postur, manajemen kerentanan (Amazon Inspector), data sensitif (Macie), dan deteksi ancaman (). GuardDuty Hal ini memungkinkan tim keamanan untuk memprioritaskan risiko aktif di lingkungan cloud mereka melalui analisis otomatis dan wawasan kontekstual. Melalui visualisasi intuitif, Security Hub mengubah sinyal keamanan yang kompleks menjadi wawasan yang dapat ditindaklanjuti, yang memungkinkan Anda membuat keputusan berdasarkan informasi tentang keamanan dengan cepat. Security Hub juga menyertakan alur kerja respons otomatis untuk membantu Anda memulihkan risiko, meningkatkan produktivitas tim, dan meminimalkan gangguan operasional.

Fitur

Solusi keamanan terpadu

Dapatkan visibilitas yang lebih luas di seluruh lingkungan cloud Anda melalui manajemen terpusat dalam solusi keamanan cloud terpadu.

Wawasan keamanan yang dapat ditindaklanjuti

Dapatkan wawasan keamanan yang dapat ditindaklanjuti melalui analitik lanjutan untuk mempelajari risiko keamanan yang terkait dengan lingkungan Anda.

Mengurangi waktu respons

Merampingkan waktu respons dengan alur kerja otomatis dan sistem tiket terintegrasi.

Temuan paparan

Security Hub menghubungkan temuan dari pemeriksaan kontrol CSPM Security Hub, Amazon Inspector, dan lainnya Layanan AWS untuk mendeteksi eksposur yang terkait dengan sumber daya. AWS

Temuan diformat dalam Open Cybersecurity Schema Framework (OCSF)

Security Hub menghasilkan temuan di OCSF dan menerima temuan di OCSF dari Security Hub CSPM dan lainnya: Layanan AWS

- Amazon GuardDuty
- Amazon Macie
- Amazon Inspector

Dasbor

Konsol Security Hub memberikan pandangan komprehensif tentang eksposur, ancaman, cakupan keamanan, dan sumber daya Anda serta visualisasi interaktif yang disebut grafik jalur serangan, yang menunjukkan bagaimana penyerang potensial dapat mengakses dan mengendalikan sumber daya yang terkait dengan temuan eksposur.

Integrasi dengan produk pihak ketiga

Anda dapat meningkatkan postur keamanan Anda dengan integrasi Security Hub. Misalnya, jika Anda menggunakan Jira Cloud atau ServiceNow ITSM, Anda dapat menggunakan fitur ini untuk membuat tiket dari temuan.

Integrasi

Security Hub terintegrasi dengan yang berikut Layanan AWS ini.

- AWS Security Hub Manajemen Postur Keamanan Cloud (CSPM)
- Amazon GuardDuty
- Amazon Inspector
- Amazon Macie

Wilayah AWS didukung untuk pratinjau publik

Security Hub mendukung hal berikut Wilayah AWS untuk rilis pratinjau publik ini.

- Asia Pasifik (Tokyo)
- Asia Pasifik (Seoul)
- Asia Pasifik (Osaka)
- Asia Pasifik (Mumbai)
- Asia Pasifik (Singapura)
- Asia Pacific (Sydney)
- Kanada (Pusat)
- Eropa (Frankfurt)
- Eropa (Stockholm)
- Eropa (Irlandia)
- AS Barat (California Utara)
- AS Barat (Oregon)
- Eropa (London)
- Eropa (Paris)
- Amerika Selatan (São Paulo)
- AS Timur (Virginia Utara)
- AS Timur (Ohio)

Berikut ini adalah opt-in Wilayah AWS, yang mengharuskan Anda mengaktifkannya sebelum Anda dapat mengaksesnya.

- Afrika (Cape Town)
- Asia Pasifik (Hong Kong)
- Asia Pasifik (Jakarta)
- Eropa (Milan)
- Timur Tengah (Bahrain)

Untuk informasi tentang hal ini Wilayah AWS, lihat [Status keikutsertaan](#) di Panduan Pengguna Wilayah AWS dan Availability Zones.

Aksesibilitas

Security Hub tersedia dalam Wilayah AWS daftar di atas. Anda dapat mengaktifkan Security Hub untuk setiap akun atau akun di organisasi Anda. Anda dapat mengakses Security Hub melalui hal-hal berikut:

Konsol Security Hub

Konsol Security Hub adalah antarmuka berbasis browser yang dapat Anda gunakan untuk membuat dan mengelola AWS sumber daya. Di konsol ini, Anda dapat mengakses akun, data, dan sumber daya Anda.

Security Hub API

Security Hub API memberi Anda akses terprogram ke akun, data, dan sumber daya Anda. Anda dapat mengirim permintaan HTTPS langsung ke Security Hub.

AWS CLI

[Dengan AWS CLI, Anda dapat menjalankan perintah di baris perintah sistem Anda untuk melakukan tugas dan membangun skrip yang melakukan tugas.](#) Dalam beberapa kasus, AWS CLI dapat lebih berguna daripada konsol Security Hub.

AWS SDKs

[AWS SDKs](#) terdiri dari pustaka dan kode sampel untuk berbagai bahasa dan platform pemrograman (C ++, Go, Java, .NET, dan Python). Mereka menyediakan akses terprogram ke Security Hub dan lainnya Layanan AWS dalam bahasa pilihan Anda dan dapat membantu Anda mengelola tugas seperti mengelola kesalahan, menandatangani permintaan, dan mencoba ulang permintaan.

Harga

Tidak ada biaya untuk menggunakan Security Hub. Security Hub gratis selama pratinjau publik ini.

Memulai dengan Security Hub

Note

Security Hub dalam rilis pratinjau dan dapat berubah sewaktu-waktu.

Topik di bagian ini menjelaskan cara memulai dengan Security Hub.

Mengaktifkan Security Hub

Note

Security Hub dalam rilis pratinjau dan dapat berubah sewaktu-waktu.

Anda dapat mengaktifkan Security Hub untuk apa pun Akun AWS. Prosedur dalam topik ini menjelaskan cara mengaktifkan Security Hub dari akun manajemen AWS organisasi, akun administrator yang didelegasikan, dan akun mandiri.

Note

Setelah mengaktifkan Security Hub, eksposur di lingkungan Anda akan segera dianalisis. Namun, Anda dapat menunggu hingga 6 jam untuk menerima temuan eksposur untuk sumber daya.

Aktifkan Security Hub untuk suatu organisasi

Prosedur di bagian ini menjelaskan cara mengaktifkan Security Hub untuk akun manajemen AWS organisasi. Prosedur ini mengasumsikan Anda telah menetapkan administrator yang didelegasikan untuk Security Hub CSPM dan menyertakan langkah di mana Anda dapat menetapkan administrator yang didelegasikan untuk organisasi Anda di Security Hub. Untuk informasi selengkapnya tentang menyetel administrator yang didelegasikan di Security Hub, lihat [Menyetel akun administrator yang didelegasikan di Security Hub](#).

Jika Anda memutuskan untuk menetapkan administrator yang didelegasikan untuk Security Hub selama pengaktifan, Anda harus [membuat kebijakan sumber daya di AWS Organizations konsol yang](#) memungkinkan administrator yang didelegasikan untuk melakukan tindakan atas nama organisasi Anda. Anda dapat menggunakan contoh kebijakan sumber daya berikut untuk akun administrator yang didelegasikan.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
```

```
"Sid": "Statement",
"Effect": "Allow",
"Principal": {
  "AWS": "arn:aws:iam::delegated-administrator-account-id:root"
},
"Action": [
  "organizations:AttachPolicy",
  "organizations:CreatePolicy",
  "organizations:DetachPolicy",
  "organizations>DeletePolicy",
  "organizations:UpdatePolicy",
  "organizations:ListPolicies",
  "organizations:ListPoliciesForTarget",
  "organizations:ListTargetsForPolicy",
  "organizations:DescribePolicy",
  "organizations:DescribeEffectivePolicy",
  "organizations:DisablePolicyType",
  "organizations:EnablePolicyType"
],
"Resource": "*"
}
]
```

Jika Anda tidak menetapkan administrator yang didelegasikan, Anda dapat mengatur administrator yang didelegasikan nanti. Untuk selengkapnya, lihat [Menyetel akun administrator yang didelegasikan di Security Hub](#). Topik ini mencakup prosedur yang menjelaskan cara menyetel administrator yang didelegasikan untuk organisasi Anda dari halaman Umum di konsol Security Hub.

Prosedur berikut menjelaskan cara menyetel akun administrator yang didelegasikan untuk organisasi Anda di Security Hub.

Untuk mengaktifkan Security Hub untuk akun manajemen AWS organisasi

1. Masuk ke AWS akun Anda dengan kredensi akun manajemen AWS organisasi Anda. Buka konsol Security Hub di <https://console.aws.amazon.com/securityhub/v2/home>.
2. Dari beranda Security Hub, pilih Security Hub. Pilih Mulai.
3. (Opsional) Untuk akun administrator yang didelegasikan, tetapkan administrator yang didelegasikan berdasarkan opsi yang disediakan. Sebagai praktik terbaik, kami merekomendasikan untuk menggunakan administrator yang didelegasikan yang sama di seluruh layanan keamanan untuk tata kelola yang konsisten. Untuk informasi selengkapnya

tentang menyetel akun administrator yang didelegasikan, lihat [Menyetel akun administrator yang didelegasikan di Security Hub](#).

4. (Opsional) Untuk mengaktifkan Akun, pilih kotak untuk mengaktifkan Security Hub untuk AWS akun Anda.
5. Pilih Salin dan lampirkan untuk membuka pengaturan organisasi. Di konsol Organizations, pilih Delegasi di bawah Administrator yang didelegasikan untuk AWS Organizations, dan tempel kebijakan sumber daya. Pilih Buat Kebijakan.
6. Buka konsol Security Hub. Pilih Konfigurasi

Saat Anda mengaktifkan Security Hub, peran terkait layanan yang disebut [AWSServiceRoleForSecurityHubV2](#) dibuat di akun Anda, dan perekam terkait layanan ditambahkan ke akun Anda. Perekam terkait layanan adalah jenis AWS Config perekam yang dikelola oleh AWS layanan yang dapat merekam data konfigurasi pada sumber daya khusus layanan. Dengan perekam terkait layanan, Security Hub memungkinkan pendekatan berbasis peristiwa untuk mendapatkan item konfigurasi sumber daya yang diperlukan untuk cakupan analisis eksposur. Perekam terkait layanan dikonfigurasi per Akun AWS dan Wilayah AWS.

 Note

Jika Anda menetapkan administrator yang didelegasikan, administrator yang didelegasikan dapat membuat dan menerapkan kebijakan yang memungkinkannya mengaktifkan dan menonaktifkan akun anggota untuk Security Hub. Untuk selengkapnya, lihat [Membuat kebijakan sebagai administrator yang didelegasikan untuk mengelola akun anggota](#).

Aktifkan Security Hub untuk administrator yang didelegasikan

Jika akun manajemen AWS organisasi menetapkan administrator yang didelegasikan untuk organisasinya, administrator yang didelegasikan harus mengaktifkan Security Hub untuk akunnya. Prosedur berikut harus diselesaikan oleh administrator yang didelegasikan, tetapi hanya jika administrator yang didelegasikan belum mengaktifkan Security Hub untuk akun mereka. Untuk informasi tentang menyetel administrator yang didelegasikan, lihat [Menyetel akun administrator yang didelegasikan di Security Hub](#).

Untuk mengaktifkan Security Hub untuk akun administrator yang didelegasikan

1. [Masuk ke AWS akun Anda dengan kredensi administrator yang didelegasikan, dan buka konsol Security Hub di v2/home. https://console.aws.amazon.com/securityhub/](https://console.aws.amazon.com/securityhub/)
2. Dari beranda Security Hub, pilih Security Hub, lalu pilih Memulai.
3. Pilih Aktifkan.
4. (Opsional) Untuk Tag, tentukan apakah akan menambahkan pasangan nilai kunci ke pengaturan akun.
5. Pilih Buka Security Hub.

Saat Anda mengaktifkan Security Hub, peran terkait layanan yang disebut [AWSServiceRoleForSecurityHubV2](#) dibuat di akun Anda, dan perekam terkait layanan ditambahkan ke akun Anda. Perekam terkait layanan adalah jenis AWS Config perekam yang dikelola oleh AWS layanan yang dapat merekam data konfigurasi pada sumber daya khusus layanan. Dengan perekam terkait layanan, Security Hub memungkinkan pendekatan berbasis peristiwa untuk mendapatkan item konfigurasi sumber daya yang diperlukan untuk cakupan analisis eksposur. Perekam terkait layanan dikonfigurasi per Akun AWS dan Wilayah AWS.

 Note

Sebagai administrator yang didelegasikan untuk organisasi, Anda dapat membuat dan menerapkan kebijakan yang memungkinkan Anda mengaktifkan dan menonaktifkan akun anggota untuk Security Hub. Untuk selengkapnya, lihat [Membuat kebijakan sebagai administrator yang didelegasikan untuk mengelola akun anggota](#).

Aktifkan Security Hub untuk akun mandiri

Prosedur berikut menjelaskan cara mengaktifkan Security Hub untuk akun mandiri. Ada dua jenis akun mandiri yang dapat mengaktifkan Security Hub: Akun AWS bukan di dalam organisasi dan Akun AWS bagian dalam organisasi. Akun AWS Bagian dalam AWS organisasi dapat berupa Akun AWS tempat administrator yang didelegasikan melampirkan AWS Organizations kebijakan ke. Akun AWS Untuk informasi selengkapnya, lihat [kebijakan Security Hub](#) di Panduan AWS Organizations Pengguna.

Untuk mengaktifkan Security Hub untuk akun mandiri

1. [Masuk ke AWS akun Anda dengan kredensi Anda, dan buka konsol Security Hub di https://console.aws.amazon.com/securityhub/v2/home](https://console.aws.amazon.com/securityhub/v2/home).
2. Dari beranda Security Hub, pilih Security Hub, lalu pilih Memulai.
3. Pilih Aktifkan.

Saat Anda mengaktifkan Security Hub, peran terkait layanan yang disebut [AWSServiceRoleForSecurityHubV2](#) dibuat di akun Anda, dan perekam terkait layanan ditambahkan ke akun Anda. Perekam terkait layanan adalah jenis AWS Config perekam yang dikelola oleh AWS layanan yang dapat merekam data konfigurasi pada sumber daya khusus layanan. Dengan perekam terkait layanan, Security Hub memungkinkan pendekatan berbasis peristiwa untuk mendapatkan item konfigurasi sumber daya yang diperlukan untuk cakupan analisis eksposur. Perekam terkait layanan dikonfigurasi per Akun AWS dan Wilayah AWS.

Menyetel akun administrator yang didelegasikan di Security Hub

 Note

Security Hub dalam rilis pratinjau dan dapat berubah sewaktu-waktu.

Dari akun manajemen AWS organisasi, Anda dapat mengatur administrator yang didelegasikan untuk organisasi Anda. Sebagai praktik terbaik, kami merekomendasikan penggunaan administrator yang didelegasikan yang sama di seluruh layanan keamanan untuk tata kelola yang konsisten. Prosedur di bagian ini menjelaskan cara menetapkan administrator yang didelegasikan untuk organisasi Anda dengan dua cara. Cara pertama adalah untuk akun manajemen AWS organisasi yang belum menetapkan administrator yang didelegasikan di Security Hub CSPM. Cara kedua adalah untuk akun manajemen AWS organisasi yang mengaktifkan Security Hub tetapi melewatkan pengaturan administrator yang didelegasikan selama pengaktifan.

Pertimbangan

Anda mungkin menemukan skenario di mana Anda ingin menetapkan administrator yang didelegasikan untuk Security Hub yang berbeda dari administrator yang didelegasikan untuk Security Hub CSPM. Jika Anda memiliki administrator yang didelegasikan yang disiapkan di Security Hub CSPM, pertimbangkan hal berikut:

- Jika akun manajemen AWS organisasi disetel sebagai administrator yang didelegasikan untuk CSPM Security Hub, Anda tidak dapat menetapkan akun ini sebagai administrator yang didelegasikan untuk Security Hub. Namun, Anda dapat menunjuk orang lain Akun AWS di organisasi sebagai administrator yang didelegasikan untuk Security Hub. Untuk tata kelola yang konsisten di seluruh layanan keamanan, sebaiknya gunakan akun yang sama (selain akun manajemen AWS organisasi) sebagai administrator yang didelegasikan untuk Security Hub CSPM dan Security Hub.
- Jika akun selain akun manajemen AWS organisasi ditetapkan sebagai administrator yang didelegasikan untuk CSPM Security Hub, akun ini akan menjadi administrator yang didelegasikan di Security Hub secara otomatis. Dalam skenario ini, Security Hub hanya mengizinkan khusus ini Akun AWS untuk berfungsi sebagai administrator yang didelegasikan.

 Note

Jika Anda menggunakan akun selain akun manajemen organisasi sebagai administrator yang didelegasikan CSPM Security Hub, menghapusnya melalui konsol CSPM Security Hub atau AWS Organizations API juga akan menghapusnya dari Security Hub. Demikian pula, jika Anda menghapus administrator yang didelegasikan Security Hub melalui konsol Security Hub atau AWS Organizations API, administrator tersebut akan dihapus dari Security Hub CSPM. Ketika administrator yang didelegasikan dihapus dari Security Hub CSPM, Konfigurasi Pusat akan secara otomatis memilih keluar.

Prosedur berikut mengasumsikan Anda belum menetapkan administrator yang didelegasikan untuk Security Hub CSPM dan menetapkan administrator yang didelegasikan untuk Security Hub.

Untuk menetapkan administrator yang didelegasikan di Security Hub

1. [Masuk ke AWS akun Anda dengan kredensial akun manajemen organisasi Anda, dan buka konsol Security Hub di https://console.aws.amazon.com/securityhub/v2/home.](https://console.aws.amazon.com/securityhub/v2/home)
2. Dari beranda Security Hub, pilih Security Hub, lalu pilih Memulai.
3. Di Administrator yang didelegasikan, pilih Konfigurasi. Di jendela pop-up, masukkan Akun AWS nomor 12 digit untuk Akun AWS yang Anda inginkan, atau pilih akun yang disarankan (jika Anda menggunakan administrator yang didelegasikan di layanan keamanan lain) untuk ditetapkan sebagai administrator yang didelegasikan untuk organisasi Anda. Pilih Simpan.

4. (Opsional) Untuk mengaktifkan Akun, pilih kotak untuk mengaktifkan Security Hub untuk Anda Akun AWS.
5. Pilih Salin dan lampirkan untuk membuka pengaturan organisasi. Di konsol Organizations, pilih Delegasi di bawah Administrator yang didelegasikan untuk AWS Organizations, dan tempel kebijakan sumber daya. Pilih Buat Kebijakan.
6. Buka konsol Security Hub. Pilih Konfigurasi

 Note

Setelah Anda menetapkan administrator yang didelegasikan, akun tersebut harus [mengaktifkan Security Hub](#) dan mengonfigurasi kebijakan untuk menerima temuan dari akun anggotanya.

Prosedur berikut mengasumsikan Anda mengaktifkan Security Hub tetapi melewati pengaturan administrator yang didelegasikan selama pengaktifan. Anda dapat mengatur administrator yang didelegasikan di konsol Security Hub dari halaman Umum.

Untuk menetapkan administrator yang didelegasikan di konsol Security Hub dari halaman Umum

1. [Masuk ke AWS akun Anda dengan kredensial akun manajemen organisasi Anda, dan buka konsol Security Hub di https://console.aws.amazon.com/securityhub/v2/home.](https://console.aws.amazon.com/securityhub/v2/home)
2. Dari panel navigasi, pilih Umum.
3. Di Administrator yang didelegasikan, pilih Konfigurasi. Di jendela pop-up, masukkan Akun AWS nomor 12 digit untuk yang ingin Anda tetapkan sebagai administrator Akun AWS yang didelegasikan untuk organisasi Anda. Atau pilih yang disarankan Akun AWS jika Anda menetapkan administrator yang didelegasikan di layanan AWS keamanan lainnya. Pilih Simpan.

Setelah menyelesaikan prosedur ini, Anda harus menyalin pernyataan kebijakan delegasi untuk Security Hub dan melampirkannya ke administrator yang didelegasikan untuk AWS Organizations kebijakan, sehingga administrator yang didelegasikan untuk Security Hub dapat melakukan tindakan di Security Hub. Tanpa pernyataan kebijakan ini, administrator yang didelegasikan tidak dapat mengonfigurasi Security Hub untuk organisasi Anda. Untuk informasi selengkapnya, lihat [Melampirkan pernyataan kebijakan delegasi untuk Security Hub](#).

Melampirkan pernyataan kebijakan delegasi untuk Security Hub

Dari akun manajemen organisasi, Anda harus menyalin pernyataan kebijakan delegasi untuk Security Hub dan melampirkannya ke administrator yang didelegasikan untuk AWS Organizations kebijakan, sehingga administrator yang didelegasikan untuk Security Hub dapat melakukan tindakan di Security Hub. Tanpa pernyataan kebijakan ini, administrator yang didelegasikan tidak dapat mengonfigurasi Security Hub untuk organisasi Anda. Anda dapat menyalin kebijakan ini dari halaman Umum di konsol Security Hub. Saat melakukannya, Anda akan diarahkan ke halaman Pengaturan di AWS Organizations konsol tempat Anda dapat mengedit administrator yang didelegasikan untuk AWS Organizations kebijakan. Topik ini menjelaskan cara menyalin kebijakan di Security Hub. Untuk informasi tentang cara memperbarui administrator yang didelegasikan untuk AWS Organizations kebijakan, lihat [Memperbarui kebijakan delegasi berbasis sumber daya](#) dengan di Panduan Pengguna. AWS Organizations

Untuk melampirkan pernyataan kebijakan delegasi untuk Security Hub

1. [Masuk ke AWS akun Anda dengan kredensial akun manajemen organisasi Anda, dan buka konsol Security Hub di https://console.aws.amazon.com/securityhub/ v2/home.](https://console.aws.amazon.com/securityhub/ v2/home)
2. Dari panel navigasi, pilih Umum.
3. Dalam pernyataan kebijakan delegasi untuk Security Hub, pilih Salin dan lampirkan. Anda diarahkan ke halaman Pengaturan di AWS Organizations mana Anda dapat mengedit administrator yang didelegasikan untuk AWS Organizations kebijakan untuk menyertakan pernyataan kebijakan delegasi. Jika Anda ingin melihat pernyataan kebijakan sebelum menyalinnya, pilih Detail kebijakan.

Note

Jika Anda menetapkan administrator yang didelegasikan, administrator yang didelegasikan dapat membuat dan menerapkan kebijakan yang memungkinkannya mengaktifkan dan menonaktifkan akun member. Prosedur dalam topik berikut menjelaskan cara menetapkan kebijakan ini.

Membuat kebijakan sebagai administrator yang didelegasikan untuk mengelola akun anggota

Sebagai administrator yang didelegasikan untuk organisasi, Anda dapat membuat dan menerapkan kebijakan yang memungkinkan Anda mengaktifkan dan menonaktifkan akun anggota. Anda dapat mengakses semua kebijakan yang dikonfigurasi dari layar Konfigurasi konsol Security Hub. Prosedur berikut menjelaskan cara membuat kebijakan ini.

Note

Langkah 6. adalah langkah opsional di mana Anda dapat menjelaskan bagaimana kebijakan ini berinteraksi dengan kebijakan induk. Untuk informasi tentang pewarisan kebijakan, lihat [Memahami pewarisan kebijakan pengelolaan di Panduan Pengguna AWS Organizations](#)

Untuk membuat kebijakan yang memungkinkan Anda mengaktifkan dan menonaktifkan akun anggota

1. [Masuk menggunakan kredensial Anda, dan buka konsol Security Hub di https://console.aws.amazon.com/securityhub/v2/home?wilayah=us-timur-1](https://console.aws.amazon.com/securityhub/v2/home?wilayah=us-timur-1).
2. Dari panel navigasi, pilih Pengaturan, lalu pilih Konfigurasi.
3. Pilih Buat kebijakan.
4. Untuk Detail, masukkan nama untuk kebijakan dan tentukan apakah akan memasukkan deskripsi opsional untuk kebijakan tersebut.
5. Untuk Wilayah, pilih Aktifkan semua Wilayah, Nonaktifkan semua Wilayah, atau Tentukan Wilayah. Jika Anda memilih Aktifkan semua Wilayah, Anda dapat menentukan apakah akan mengaktifkan Wilayah baru secara otomatis. Jika Anda memilih Nonaktifkan semua Wilayah, Anda dapat menentukan apakah akan menonaktifkan Wilayah baru secara otomatis. Jika Anda memilih, Tentukan Wilayah, Anda harus memilih Wilayah mana yang ingin Anda aktifkan dan nonaktifkan.
6. (Opsional) Untuk pengaturan lanjutan, silakan merujuk ke [panduan](#) dari AWS Organizations.
7. (Opsional) Untuk Tag, tentukan apakah akan menambahkan pasangan nilai kunci ke kebijakan. Anda dapat menambahkan hingga 50 tanda.
8. Pilih Berikutnya.
9. Tinjau perubahan Anda, lalu pilih Terapkan. Akun target Anda dikonfigurasi berdasarkan kebijakan. Untuk melihat kebijakan efektif di tingkat akun, Anda dapat meninjau tab Organisasi di halaman Konfigurasi tempat Anda dapat memilih akun.

Menghapus akun administrator yang didelegasikan di Security Hub

Note

Security Hub dalam rilis pratinjau dan dapat berubah sewaktu-waktu.

Anda dapat menghapus akun administrator yang didelegasikan di konsol Security Hub kapan saja. Namun, tindakan ini tidak hanya menghapus administrator yang didelegasikan dari Security Hub, tetapi juga Security Hub CSPM. Kami menyarankan hanya melakukan tindakan ini ketika Anda telah mengkonfirmasi operasi ini dengan akun keamanan Anda.

Note

Jika Anda menggunakan akun selain akun manajemen organisasi sebagai administrator yang didelegasikan CSPM Security Hub, menghapusnya melalui Konsol CSPM atau AWS Organizations API juga akan menghapusnya dari Security Hub.

Demikian pula, jika Anda menghapus administrator yang didelegasikan Security Hub melalui Security Hub Console atau AWS Organizations API, itu juga akan dihapus dari Security Hub CSPM. Ketika administrator yang didelegasikan dihapus dari CSPM, Konfigurasi Pusat akan secara otomatis memilih keluar.

Untuk menghapus akun administrator yang didelegasikan

1. [Masuk ke AWS akun Anda dengan kredensi akun manajemen organisasi Anda, dan buka konsol Security Hub di `https://console.aws.amazon.com/securityhub/v2/home?wilayah=us-timur-1`.](https://console.aws.amazon.com/securityhub/v2/home?wilayah=us-timur-1)
2. Dari panel navigasi, pilih Umum.
3. Di Adminsitrator yang didelegasikan, pilih Hapus administrator yang didelegasikan. Di jendela pop-up, masukkan konfirmasi, dan pilih Hapus.

Rekomendasi Security Hub

Note

Security Hub dalam rilis pratinjau dan dapat berubah sewaktu-waktu.

Layanan keamanan berikut AWS mengirimkan temuan ke Security Hub dalam format OCSF. Setelah Anda mengaktifkan Security Hub, sebaiknya aktifkan ini Layanan AWS untuk keamanan tambahan.

Security Hub CSPM

Saat Anda [mengaktifkan Security Hub CSPM](#), Anda mendapatkan pandangan komprehensif tentang status keamanan Anda. AWS Ini membantu Anda menilai lingkungan Anda terhadap standar industri keamanan dan praktik terbaik. Meskipun Anda dapat memulai dengan Security Hub tanpa mengaktifkan Security Hub CSPM, sebaiknya aktifkan Security Hub CSPM karena Security Hub menghubungkan sinyal keamanan dari Security Hub CSPM untuk meningkatkan manajemen postur tubuh Anda.

Jika Anda [mengaktifkan Security Hub CSPM](#), kami juga menyarankan untuk [mengaktifkan standar Praktik Terbaik Keamanan AWS Dasar](#) untuk akun Anda. Standar ini terdiri dari serangkaian kontrol yang mendeteksi kapan Anda Akun AWS dan sumber daya menyimpang dari praktik terbaik keamanan. Saat Anda mengaktifkan standar Praktik Terbaik Keamanan AWS Dasar untuk akun Anda, AWS Security Hub Cloud Security Posture Management (CSPM) secara otomatis mengaktifkan semua kontrolnya, termasuk kontrol untuk jenis sumber daya berikut:

- Kontrol akun
- Kontrol DynamoDB
- EC2 Kontrol Amazon
- Kontrol IAM
- AWS Lambda kontrol
- Kontrol Amazon RDS
- Kontrol Amazon S3

Anda dapat menonaktifkan salah satu kontrol dalam daftar ini. Namun, jika Anda menonaktifkan salah satu kontrol ini, Anda tidak dapat menerima temuan eksposur untuk sumber daya yang didukung. Untuk informasi tentang kontrol yang berlaku pada standar Praktik Terbaik Keamanan AWS Dasar, lihat standar Praktik [Terbaik Keamanan AWS Dasar v1.0.0 \(FSBP\)](#).

GuardDuty

Saat [mengaktifkan GuardDuty](#), Anda dapat melihat semua ancaman dan temuan cakupan keamanan di dasbor konsol Security Hub. Jika Anda mengaktifkan GuardDuty, GuardDuty secara otomatis mulai mengirim data ke Security Hub dalam format OCSF.

Amazon Inspector

Saat [mengaktifkan Amazon Inspector](#), Anda dapat melihat semua eksposur dan temuan cakupan keamanan di dasbor konsol Security Hub. Jika Anda mengaktifkan Amazon Inspector, Amazon Inspector secara otomatis mulai mengirim data ke Security Hub dalam format OCSF.

Kami merekomendasikan untuk mengaktifkan EC2 pemindaian Amazon dan pemindaian standar Lambda. Saat Anda mengaktifkan EC2 pemindaian Amazon, Amazon Inspector memindai instans EC2 Amazon di akun Anda untuk mengetahui kerentanan paket dan masalah jangkauan jaringan. Saat Anda mengaktifkan pemindaian standar Lambda, Amazon Inspector memindai fungsi Lambda untuk kerentanan perangkat lunak dalam dependensi paket. Untuk informasi selengkapnya, lihat [Mengaktifkan jenis pemindaian](#) di Panduan Pengguna Amazon Inspector.

Macie

Saat [mengaktifkan Macie](#), Anda dapat mendeteksi eksposur tambahan untuk bucket Amazon S3 Anda. Sebaiknya konfigurasi [penemuan data sensitif otomatis](#), sehingga Macie dapat mengevaluasi inventaris bucket Amazon S3 Anda setiap hari.

Konsep Security Hub

Note

Security Hub dalam rilis pratinjau dan dapat berubah sewaktu-waktu.

Istilah dan konsep berikut akan membantu Anda memahami cara mengelola temuan eksposur.

Eksposur

Skenario keamanan potensial di akun Anda yang mungkin disebabkan oleh kerentanan, sumber daya yang dapat dieksploitasi, atau kesalahan konfigurasi.

Temuan eksposur

Jenis temuan yang menggambarkan paparan yang ada di lingkungan Anda. Temuan eksposur mencakup sifat dan sinyal. Sinyal dapat mencakup satu atau lebih jenis sifat eksposur. Security Hub menghasilkan temuan eksposur ketika sinyal dari Security Hub CSPM mengontrol temuan atau lainnya Layanan AWS, seperti Amazon Inspector, menunjukkan adanya eksposur. Sumber

daya dapat memiliki paling banyak satu temuan eksposur. Security Hub menghasilkan temuan eksposur saat sumber daya diekspos. Jika sumber daya tidak memiliki sifat eksposur atau memiliki sifat yang tidak mencukupi, Security Hub tidak menghasilkan temuan eksposur untuk sumber daya tersebut.

Sinyal

Temuan yang berkontribusi pada temuan eksposur. Sinyal dapat disebut sebagai temuan yang berkontribusi. Sinyal dapat berasal dari Security Hub CSPM,, atau lainnya AWS Config Layanan AWS, seperti Amazon Inspector.

Sifat

Deviasi keamanan yang menghasilkan temuan eksposur. Jenis sifat termasuk Misconfiguration, Reachability, Sensitive Data, dan Vulnerability. Suatu sifat dikaitkan dengan satu sinyal, dan sinyal dapat mengandung banyak sifat. Misalnya, kontrol CSPM Security Hub menunjukkan kebijakan yang dikelola pelanggan memungkinkan kontrol akses administratif. Sinyal ini mengandung sifat salah konfigurasi.

Temuan OCSF di Security Hub

Note

Security Hub dalam rilis pratinjau dan dapat berubah sewaktu-waktu.

Semua temuan di Security Hub diformat dalam Open Cybersecurity Schema Framework (OCSF). Security Hub menganggap temuan `activity_name != Close` sebagai temuan aktif. Temuan aktif dihapus secara otomatis jika tidak diperbarui dalam 90 hari. Security Hub menganggap temuan `Activity_name = Close` sebagai temuan tertutup. Temuan tertutup akan dihapus secara otomatis jika tidak diperbarui dalam 14 hari. Security Hub menentukan kapan sebuah temuan diperbarui menggunakan nilai temuan `terbaru.modified_time_dt`. Di akhir periode retensi temuan, Security Hub menghapus temuan secara permanen. Mencari penyedia dapat mengubah nilai `finding.info.modified_time_dt` bidang ketika mereka memperbarui temuan. Untuk informasi tentang `Activity_name` nilai lainnya, lihat [Temuan Kerentanan](#) dalam skema OCSF.

Temuan cakupan di Security Hub

Note

Security Hub dalam rilis pratinjau dan dapat berubah sewaktu-waktu.

Temuan cakupan untuk Security Hub memberikan visibilitas ke mana fitur AWS keamanan diaktifkan dan di mana mungkin ada celah dalam cakupan dalam akun mandiri atau di seluruh lingkungan organisasi AWS. Mengaktifkan fitur keamanan tambahan akan meningkatkan kemampuan deteksi Security Hub. Temuan Cakupan mengevaluasi fitur CSPM Amazon Inspector, Macie, dan Security Hub yang GuardDuty diaktifkan untuk akun. Temuan ini muncul sebagai widget di dasbor Security Hub dengan kemampuan untuk menelusuri tampilan yang lebih rinci dengan kemampuan keamanan tertentu. Untuk administrator yang didelegasikan, widget ini menunjukkan rincian cakupan di semua akun yang diaktifkan Security Hub.

Batasan

- Untuk akun anggota, informasi cakupan dikumpulkan di seluruh tautan Wilayah AWS, tetapi hanya untuk akun anggota tersebut.
- Informasi cakupan tidak ditampilkan untuk akun yang tidak terhubung ke Security Hub
- Cakupan hanya menunjukkan jika Layanan AWS diaktifkan, bukan apakah fitur tertentu dalam AWS layanan diaktifkan.

Temuan cakupan untuk Security Hub CSPM

Temuan Cakupan CSPM Security Hub menilai apakah standar keamanan manajemen postur yang memenuhi syarat diaktifkan di akun. Mengaktifkan Security Hub CSPM Standard akan memenuhi syarat, dengan pengecualian AWS Control Tower dan standar Resource Tagging.

Diperlukan waktu hingga 24 jam untuk mendeteksi standar yang diaktifkan secara default saat mengaktifkan Security Hub CSPM.

Temuan cakupan untuk GuardDuty

GuardDuty Temuan cakupan menilai GuardDuty apakah diaktifkan dan GuardDuty fitur mana yang diaktifkan dalam Akun AWS:

- Perlindungan Malware untuk Amazon EC2 - Memindai EC2 instans Amazon untuk mencari potensi malware
- Perlindungan Amazon EKS - Memantau log audit Kubernetes untuk ancaman di kluster Amazon EKS
- Perlindungan Lambda - Menganalisis pemanggilan fungsi Lambda untuk potensi ancaman
- Perlindungan Amazon S3 - Menganalisis peristiwa data untuk potensi ancaman terhadap bucket Amazon S3
- Amazon RDS Protection - Monitor ancaman terhadap basis data Amazon RDS
- Runtime Monitoring - Menyediakan pemantauan real-time perilaku runtime di instans Amazon EC2

Diperlukan waktu hingga 24 jam untuk pembaruan GuardDuty cakupan agar tercermin di semua akun anggota dalam suatu organisasi.

Temuan cakupan untuk Amazon Inspector

Temuan Cakupan Amazon Inspector menilai apakah Amazon Inspector diaktifkan dan fitur mana yang diaktifkan di akun:

- EC2 Pemindaian Amazon - Memindai EC2 instans Amazon untuk mencari kerentanan
- Amazon ECR Scanning - Memindai gambar kontainer di Amazon ECR untuk kerentanan
- Pemindaian Standar Lambda - Memindai fungsi Lambda untuk kerentanan
- Pemindaian Kode Lambda - Memindai fungsi kode Lambda untuk kerentanan kode
- Amazon Inspector Code Security - Memindai kode sumber aplikasi pihak pertama, dependensi aplikasi pihak ketiga, dan Infrastruktur sebagai Kode untuk kerentanan

Temuan cakupan untuk Macie

Temuan Cakupan Macie adalah penilaian yang menunjukkan apakah Macie diaktifkan di seluruh Akun AWS

Diperlukan waktu hingga 24 jam untuk pembaruan penemuan data sensitif otomatis Macie untuk mencerminkan semua akun anggota dalam suatu organisasi.

Temuan paparan di Security Hub

Note

Security Hub dalam rilis pratinjau dan dapat berubah sewaktu-waktu.

Security Hub menghubungkan temuan dari pemeriksaan kontrol CSPM Security Hub dan lainnya Layanan AWS, seperti Amazon Inspector, untuk mendeteksi eksposur yang terkait dengan sumber daya. AWS Temuan eksposur adalah jenis temuan yang menggambarkan paparan potensial di lingkungan Anda karena kerentanan, sumber daya yang dapat dieksploitasi, atau kesalahan konfigurasi. Dengan memprioritaskan dan menyelesaikan eksposur Anda yang paling kritis, Anda dapat mencegah potensi serangan terhadap lingkungan Anda. Anda dapat mengakses temuan eksposur di konsol Security Hub dan secara terprogram dengan operasi Security Hub CSPM dan Security Hub API.

Jenis sumber daya yang didukung untuk temuan eksposur di Security Hub

Note

Security Hub dalam rilis pratinjau dan dapat berubah sewaktu-waktu.

Security Hub menghasilkan temuan eksposur untuk jenis AWS sumber daya berikut:

- `AWS::DynamoDB::Table`
- `AWS::EC2::Instance`
- `AWS::ECS::Service`
- `AWS::EKS::Cluster`
- `AWS::IAM::User`
- `AWS::Lambda::Function`
- `AWS::RDS::DBInstance`
- `AWS::S3::Bucket`

Security Hub menghasilkan satu temuan eksposur per sumber daya. Jika sumber daya tidak memiliki sifat eksposur atau memiliki sifat yang tidak mencukupi, Security Hub tidak menghasilkan temuan eksposur untuk sumber daya tersebut.

Jenis sifat yang didukung di Security Hub

Note

Security Hub dalam rilis pratinjau dan dapat berubah sewaktu-waktu.

Security Hub menghasilkan temuan eksposur ketika AWS Security Hub Cloud Security Posture Management (CSPM) mengontrol temuan dan temuan yang dihasilkan oleh pendukung lain Layanan AWS, seperti Amazon Inspector, mengandung sifat eksposur untuk sumber daya. Tabel berikut memberikan informasi tentang jenis sifat yang didukung.

Jenis sifat	Deskripsi	Sumber	Sumber daya yang terkena dampak
Kesalahan konfigurasi	Menunjukkan sumber daya yang salah dikonfigurasi.	Temuan kontrol CSPM Security Hub.	Semua jenis sumber daya.
Keterjangkauan	Menunjukkan jalur jaringan terbuka ke sumber daya.	Temuan kontrol CSPM Security Hub dan temuan jangkauan jaringan Amazon Inspector.	EC2 Contoh Amazon
Data Sensitif	Menunjukkan bahwa sumber daya berisi data sensitif.	Temuan data sensitif Macie.	Bucket Amazon S3
Kerentanan	Menunjukkan bahwa sumber daya diekspos ke Common Vulnerabilities and Exposure (CVEs).	Temuan kerentanan paket Amazon Inspector.	EC2 Instans Amazon, layanan Amazon ECS, kluster

Jenis sifat	Deskripsi	Sumber	Sumber daya yang terkena dampak
			Amazon EKS, dan fungsi Lambda

Setiap sifat dapat dikaitkan dengan beberapa judul yang memberikan detail tentang paparan yang memengaruhi sumber daya. Misalnya, Anda mungkin melihat judul Exploit Available untuk sifat Kerentanan dalam detail untuk temuan EC2 eksposur.

Menghasilkan temuan paparan

Note

Security Hub dalam rilis pratinjau dan dapat berubah sewaktu-waktu.

Security Hub menghasilkan temuan eksposur setiap 6 jam. Selama setiap periode 6 jam, Security Hub mempertimbangkan sifat eksposur yang tersedia untuk sumber daya. Ini menghasilkan paling banyak satu temuan eksposur per ID sumber daya. Keunikan temuan ditentukan oleh ID,, jenis Wilayah AWS, dan akun. Ini berarti Anda dapat memiliki dua sumber daya dengan ID yang sama, tetapi sumber daya akan menjadi jenis sumber daya yang berbeda. Temuan eksposur ini menggabungkan semua sifat eksposur yang berlaku yang berlaku untuk sumber daya.

Jika sumber daya tidak memiliki sifat eksposur atau memiliki sifat yang tidak mencukupi, Security Hub tidak menghasilkan temuan eksposur untuk sumber daya tersebut. Security Hub tidak mempublikasikan temuan eksposur untuk jenis sumber daya yang tidak mendukung temuan eksposur. Ketika sumber daya memiliki jumlah dan kombinasi sifat yang signifikan, Security Hub menghasilkan temuan eksposur. Jumlah dan kombinasi sifat juga menentukan tingkat keparahan temuan paparan.

Temuan eksposur sampel

Note

Security Hub dalam rilis pratinjau dan dapat berubah sewaktu-waktu.

Security Hub menormalkan temuan eksposur dalam Open Cybersecurity Schema Framework (OCSF).

Contoh skema OCSF

Dalam skema OCSF sampel berikut, `related_events` parameter berisi detail unik untuk temuan paparan, seperti kontribusi temuan. Temuan yang berkontribusi adalah sifat dan sinyal yang terkait dengan temuan paparan. Satu temuan yang berkontribusi dapat mencakup satu atau lebih sifat. `observablesParameter` mengidentifikasi sumber daya yang terkait dengan temuan yang berkontribusi. Ini bisa berbeda dari `resources` parameter, yang mengidentifikasi sumber daya yang terkait dengan temuan eksposur.

```
{
  "activity_id": 1,
  "activity_name": "Create",
  "category_name": "Findings",
  "category_uid": 2,
  "class_name": "Detection Finding",
  "class_uid": 2004,
  "cloud": {
    "account": {
      "uid": "123456789012",
      "name": "production-application"
    },
    "cloud_partition": "aws",
    "provider": "AWS",
    "region": "us-east-1"
  },
  "finding_info": {
    "analytic": {
      "name": "Exposure",
      "type": "Rule",
      "type_id": 1,
      "uid": "0.0.1"
    },
  },
}
```

```

    "created_time_dt": "2024-11-15T21:39:26.337224100Z",
    "desc": "Publicly invocable Lambda function executed outside of VPC has
vulnerability with known exploit that can be exploited from remote network",
    "finding.info.modified_time_dt": "2024-11-15T21:39:26.337224100Z",
    "related_events_count": 3,
    "related_events": [
      {
        "tags": [
          {
            "name": "Vulnerability",
            "values": [
              "Attack Vector Network",
              "EPSS Level >= High",
              "EPSS Level >= Medium",
              "Exploit Available",
              "No Privileges Required",
              "No User Interaction Required",
              "Vulnerable"
            ]
          }
        ],
        "product": {
          "uid": "arn:aws:securityhub:us-east-1::productv2/aws/inspector"
        },
        "observables": [
          {
            "type": "Resource UID",
            "type_id": 10,
            "value": "arn:aws:lambda:us-east-1:123456789012:application-
function"
          }
        ],
        "type": "Finding",
        "title": "CVE-2023-33246 - org.apache.rocketmq:rocketmq-controller",
        "uid": "arn:aws:inspector2:us-
east-1:123456789012:finding/1234567890abcdef0"
      },
      {
        "tags": [
          {
            "name": "Reachability",
            "values": [
              "Publicly Invocable"
            ]
          }
        ]
      }
    ]
  }
}

```

```

        }
    ],
    "product": {
        "uid": "arn:aws:securityhub:us-east-1::productv2/aws/securityhub"
    },
    "observables": [
        {
            "type": "Resource UID",
            "type_id": 10,
            "value": "arn:aws:lambda:us-east-1:123456789012:application-
function"
        }
    ],
    "type": "Finding",
    "title": "Lambda function policies should prohibit public access",
    "uid": "arn:aws:securityhub:us-east-1:123456789012:security-control/
Lambda.1/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLEaaaaa"
},
{
    "tags": [
        {
            "name": "Misconfiguration",
            "values": [
                "Deployed outside VPC"
            ]
        }
    ],
    "product": {
        "uid": "arn:aws:securityhub:us-east-1::productv2/aws/securityhub"
    },
    "observables": [
        {
            "type": "Resource UID",
            "type_id": 10,
            "value": "arn:aws:lambda:us-east-1:123456789012:application-
function"
        }
    ],
    "type": "Finding",
    "title": "Lambda functions should be in a VPC",
    "uid": "arn:aws:securityhub:us-east-1:123456789012:security-control/
Lambda.3/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
}
],

```

```

    "title": "Publicly invocable Lambda function executed outside of VPC has
vulnerability with known exploit that can be exploited from remote network",
    "types": [
        "Exposure/Potential Impact/Resource Hijacking"
    ],
    "uid": "arn:aws:securityhub:us-
east-1:123456789012:risk:1234f781c7ae7507f01e2fb460f15ca8fe7f9c95e257698a092cb74a4ea84a42"
},
    "metadata": {
        "product": {
            "name": "Security Hub Exposure Analysis",
            "uid": "arn:aws:securityhub:us-east-1::productv2/aws/securityhub-risk",
            "vendor_name": "Amazon"
        },
        "processed_time_dt": "2024-11-15T21:39:58.819Z",
        "profiles": [
            "cloud",
            "datetime"
        ],
        "version": "1.4.0-dev"
    },
    "resources": [
        {
            "cloud_partition": "aws",
            "region": "us-east-1",
            "tags": [
                {
                    "name": "aws:cloudformation:stack-name",
                    "value": "VeepLambdaRule3"
                },
                {
                    "name": "aws:cloudformation:stack-id",
                    "value": "arn:aws:cloudformation:us-east-1:123456789012:stack/
VeepLambdaRule3/a1b2c3d4-5678-90ab-cdef-EXAMPLE22222"
                },
                {
                    "name": "aws:cloudformation:logical-id",
                    "value": "lambdar3function94D10D40"
                }
            ],
            "type": "AwsLambdaFunction",
            "uid": "arn:aws:lambda:us-east-1:123456789012:application-function"
        }
    ],

```

```
{
  "severity": "Critical",
  "severity_id": 5,
  "status": "New",
  "status_id": 1,
  "time": 1731706766337,
  "time_dt": "2024-11-15T21:39:26.337224100Z",
  "type_name": "Detection Finding: Create",
  "type_uid": 200401,
  "vendor_attributes": {
    "severity_id": 5,
    "severity": "Critical"
  }
}
```

Menentukan tingkat keparahan temuan eksposur

Note

Security Hub dalam rilis pratinjau dan dapat berubah sewaktu-waktu.

Security Hub menetapkan setiap eksposur untuk menemukan tingkat keparahan default CRITICAL, HIGH, MEDIUM, atau LOW. Temuan paparan dengan tingkat keparahan INFORMATIONAL tidak dipublikasikan. Security Hub menggunakan beberapa faktor untuk menentukan tingkat keparahan default dari temuan eksposur:

- Kesadaran — Sejauh mana paparan tidak teoritis, tetapi memiliki eksploitasi yang tersedia untuk umum atau otomatis. Ini berlaku untuk temuan paparan untuk EC2 instance dan fungsi Lambda.
- Kemudahan penemuan — Apakah alat otomatis, seperti pemindaian port atau pencarian internet, tersedia untuk menemukan sumber daya yang berisiko.
- Kemudahan eksploitasi — Kemudahan di mana aktor ancaman dapat mengeksploitasi eksposur. Misalnya, jika jalur jaringan terbuka atau metadata yang salah konfigurasi ada, aktor ancaman dapat lebih mudah mengeksploitasi eksposur.
- Kemungkinan eksploitasi — Kemungkinan eksposur akan dieksploitasi dalam 30 hari ke depan. Faktor ini sesuai dengan Exploit Protection Scoring System (EPSS) dan berlaku untuk temuan eksposur untuk EC2 instans Amazon dan fungsi Lambda.

- Dampak — Kerugian jika eksploitasi dilakukan. Misalnya, paparan dapat menyebabkan hilangnya akuntabilitas, hilangnya ketersediaan, hilangnya kerahasiaan dari paparan data, atau hilangnya integritas dari korupsi data.

Meninjau temuan paparan

Note

Security Hub dalam rilis pratinjau dan dapat berubah sewaktu-waktu.

Anda dapat meninjau semua temuan eksposur di konsol AWS Security Hub dan dengan API. Halaman Eksposur di konsol Security Hub menampilkan semua temuan eksposur aktif. Temuan paparan terdaftar dengan mengurangi keparahan. Anda dapat memfilter temuan eksposur Anda dengan menambahkan dan menghapus filter dengan bilah pencarian Tambahkan filter. Anda dapat mengelompokkan temuan eksposur Anda dengan Grup berdasarkan dropdown. Anda juga dapat memfilter temuan eksposur Anda dengan menu Filter cepat.

Detail untuk temuan paparan

Anda dapat melihat banyak detail untuk temuan eksposur. Di konsol Security Hub, detail ini dibagi di antara tab. Tab Ikhtisar menyediakan snapshot dari temuan eksposur. Tab Traits mencantumkan sifat dan sinyal yang terkait dengan temuan eksposur. Tab Sumber Daya memberikan detail tentang sumber daya dan tag sumber daya yang terkait dengan temuan eksposur. Daftar berikut memberikan deskripsi untuk detail pencarian eksposur.

- Menemukan judul — Judul temuan eksposur.
- Tingkat keparahan — Tingkat keparahan temuan paparan. Security Hub menggunakan jumlah dan kombinasi sifat untuk sumber daya untuk menentukan tingkat keparahan temuan eksposur. Tingkat keparahannya bisa CRITICAL, HIGH, MEDIUM, atau LOW. Security Hub tidak mempublikasikan temuan eksposur dengan tingkat keparahan INFORMATIONAL. Anda dapat memperbarui Severity melalui konsol Security Hub atau dengan operasi [BatchUpdateFindingsV2](#) API.
- Deskripsi — Deskripsi temuan eksposur.
- Jenis — Nama jenis pencarian eksposur. Misalnya, namanya mungkin menyerupai sesuatu seperti Exposure/Potential Impact/Resource Hijacking.
- Akun — ID Akun AWS tempat temuan eksposur dihasilkan.

- Usia - Menunjukkan berapa lama temuan eksposur telah aktif.
- Waktu yang dibuat — Stempel waktu yang menunjukkan kapan temuan eksposur dibuat.
- Waktu yang dimodifikasi - Stempel waktu yang menunjukkan kapan temuan eksposur terakhir diperbarui.
- Wilayah — Wilayah AWS Tempat temuan eksposur dihasilkan.
- Nama produk — Nama produk yang menghasilkan temuan eksposur.
- Nama perusahaan — Nama perusahaan yang menghasilkan temuan eksposur.
- Nama aktivitas — Nama kegiatan.
- Status — Status temuan eksposur ini.
- Finding ID — Pengidentifikasi unik yang terkait dengan temuan eksposur.
- Jalur serangan potensial (hanya konsol) — Visualisasi interaktif menunjukkan bagaimana penyerang potensial dapat mengakses dan mengendalikan sumber daya yang terkait dengan temuan eksposur. Untuk informasi selengkapnya, [Melihat eksposur di Security Hub dengan grafik jalur serangan potensial](#).
- Sifat - Mengidentifikasi jenis sifat dan judul sifat yang terkait dengan temuan paparan. Di konsol Security Hub, Anda dapat melihat sifat berdasarkan tipe sifat atau sinyal. Ini membantu Anda menganalisis temuan yang berkontribusi dalam konteks paparan terkait.
- Resources — Mengidentifikasi sumber daya yang terkait dengan temuan eksposur.

Meninjau detail untuk temuan paparan

Note

Security Hub dalam rilis pratinjau dan dapat berubah sewaktu-waktu.

Topik ini menjelaskan cara meninjau detail tentang temuan eksposur di konsol Security Hub dan dengan API.

Meninjau detail untuk temuan eksposur di konsol Security Hub

Untuk melihat detail tentang temuan eksposur di konsol Security Hub

1. [Masuk menggunakan kredensial Anda, dan buka konsol Security Hub di https://console.aws.amazon.com/securityhub/v2/home?wilayah=us-timur-1](https://console.aws.amazon.com/securityhub/v2/home?wilayah=us-timur-1).

2. Dari panel navigasi, pilih Eksposur.
3. Pilih temuan eksposur yang ingin Anda lihat detailnya.

Meninjau detail untuk temuan eksposur dengan API

Anda dapat meninjau temuan eksposur dengan [GetFindingsV2](#) API atau dengan AWS CLI. Anda dapat memfilter hasil dengan `FindingProviderFieldsTypes` parameter dan dengan memberikan nilai filter `Exposure/EC2` jika Anda hanya ingin mengembalikan temuan eksposur untuk EC2 instance. Anda dapat memfilter berdasarkan bidang lain untuk mempersempit hasil.

Perintah contoh

Berikut ini adalah AWS CLI contoh yang mengambil 10 temuan eksposur yang paling baru dihasilkan di akun Anda. Contoh ini diformat untuk Linux, macOS, atau Unix, dan menggunakan karakter garis miring terbalik (`\`) untuk meningkatkan keterbacaan.

```
aws securityhub get-findings-v2 \
    --max-results '10' \
    --filter '{"CompositeFilters": [{"StringFilters":
[{"FieldName": "finding_info.title", "Filter":
{"Value": "GuardDuty", "Comparison": "PREFIX"}]} ]}]'
```

Memulihkan temuan paparan

Note

Security Hub dalam rilis pratinjau dan dapat berubah sewaktu-waktu.

Topik di bagian ini menjelaskan risiko remediasi untuk yang berbeda Layanan AWS.

RemediationBidang [format OCSF](#) berisi dua bidang: `remediation` dan `references`

```
"Remediation": {
  "Recommendation": {
    "remediation": {"desc": "String",
    "references": ["string array"]}
  }
}
```



```
},
```

Note

Panduan remediasi yang disediakan di bagian berikut mungkin memerlukan konsultasi tambahan dalam AWS sumber daya lain.

Memulihkan eksposur untuk tabel DynamoDB

AWS Security Hub dapat menghasilkan temuan eksposur untuk tabel DynamoDB.

Di konsol Security Hub, tabel DynamoDB yang terlibat dalam temuan eksposur dan informasi pengenalannya tercantum di bagian Sumber daya pada detail temuan. Secara terprogram, Anda dapat mengambil detail sumber daya dengan [GetFindingsV2](#) pengoperasian Security Hub API.

Setelah mengidentifikasi sumber daya yang terlibat dalam temuan eksposur, Anda dapat menghapus sumber daya jika Anda tidak membutuhkannya. Menghapus sumber daya yang tidak penting dapat mengurangi profil dan AWS biaya eksposur Anda. Jika sumber daya sangat penting, ikuti langkah-langkah remediasi yang direkomendasikan ini untuk membantu mengurangi risiko. Topik remediasi dibagi berdasarkan jenis sifatnya.

Temuan eksposur tunggal berisi masalah yang diidentifikasi dalam beberapa topik remediasi. Sebaliknya, Anda dapat mengatasi temuan eksposur dan menurunkan tingkat keparahannya dengan hanya membahas satu topik remediasi. Pendekatan Anda terhadap remediasi risiko tergantung pada kebutuhan organisasi dan beban kerja Anda.

Note

Panduan remediasi yang diberikan dalam topik ini mungkin memerlukan konsultasi tambahan dalam AWS sumber daya lain.

Daftar Isi

- [Sifat salah konfigurasi di DynamoDB](#)
 - [Tabel DynamoDB memiliki pemulihan dinonaktifkan point-in-time](#)
 - [Tabel DynamoDB tidak dicakup oleh rencana cadangan](#)
 - [Tabel DynamoDB memiliki perlindungan penghapusan dinonaktifkan](#)

Sifat salah konfigurasi di DynamoDB

Berikut ini menjelaskan sifat kesalahan konfigurasi dan langkah-langkah remediasi untuk tabel DynamoDB.

Tabel DynamoDB memiliki pemulihan dinonaktifkan point-in-time

Aktifkan pemulihan DynamoDB point-in-time

Pemulihan point-in-time DynamoDB menyediakan backup otomatis berkelanjutan untuk data tabel DynamoDB Anda. Untuk informasi tentang cara mengembalikan tabel DynamoDB ke titik waktu, lihat [Memulihkan tabel DynamoDB ke titik waktu dalam Panduan Pengguna Amazon DynamoDB](#).

Tabel DynamoDB tidak dicakup oleh rencana cadangan

AWS Backup menyediakan layanan terpusat untuk mengkonfigurasi, mengelola, dan mengotomatiskan backup di seluruh layanan AWS, termasuk DynamoDB. Tanpa rencana cadangan, tabel Anda tidak memiliki cadangan terjadwal dan otomatis dengan periode retensi yang dapat disesuaikan, menciptakan risiko keamanan yang signifikan. Penyerang dapat merusak atau menghapus data tabel Anda dengan jahat. Tanpa backup yang tepat, Anda mungkin tidak memiliki opsi pemulihan di luar jendela Point-in-Time Pemulihan (jika diaktifkan), berpotensi mengakibatkan kehilangan data permanen. Mengikuti praktik terbaik perlindungan data, kami sarankan untuk menutupi tabel DynamoDB Anda dengan paket cadangan.

Buat rencana cadangan

Sebelum membuat rencana cadangan, tentukan frekuensi cadangan dan periode retensi yang sesuai untuk data Anda. Untuk informasi tentang cara membuat paket cadangan, lihat [Menetapkan sumber daya ke paket cadangan](#) di Panduan Pengguna Amazon DynamoDB.

Tabel DynamoDB memiliki perlindungan penghapusan dinonaktifkan

Perlindungan penghapusan mencegah penghapusan tabel DynamoDB yang tidak disengaja. Saat perlindungan penghapusan dinonaktifkan, tabel DynamoDB rentan terhadap penghapusan yang tidak diinginkan melalui tindakan konsol, panggilan API, perintah CLI, atau proses otomatis. Ini dapat mengekspos AWS lingkungan Anda ke kehilangan data, karena entitas yang tidak sah dengan akses ke AWS lingkungan Anda dapat dengan sengaja menghapus tabel, mengakibatkan gangguan layanan dan kehilangan data permanen. Mengikuti praktik terbaik perlindungan data, sebaiknya aktifkan perlindungan data untuk tabel DynamoDB.

Aktifkan perlindungan penghapusan

Jika Anda mengelola beberapa tabel, pertimbangkan AWS CloudFormation untuk menggunakan untuk memperbarui properti tabel secara massal. Anda dapat memodifikasi AWS CloudFormation template Anda untuk menyertakan `DeletionProtectionEnabled` properti dan memperbarui tumpukan Anda. Setelah menyelesaikan remediasi, verifikasi proteksi penghapusan diaktifkan di menu tarik-turun Info tambahan di tab Pengaturan tabel.

Memulihkan eksposur untuk contoh EC2

AWS Security Hub dapat menghasilkan temuan eksposur untuk instans Amazon Elastic Compute Cloud (EC2).

Pada konsol Security Hub, EC2 instance yang terlibat dalam temuan eksposur dan informasi pengidentifikasinya tercantum di bagian Sumber Daya pada detail temuan. Secara terprogram, Anda dapat mengambil detail sumber daya dengan [GetFindingsV2](#) pengoperasian Security Hub API.

Setelah mengidentifikasi sumber daya yang terlibat dalam temuan eksposur, Anda dapat menghapus sumber daya jika Anda tidak membutuhkannya. Menghapus sumber daya yang tidak penting dapat mengurangi profil dan AWS biaya eksposur Anda. Jika sumber daya sangat penting, ikuti langkah-langkah remediasi yang direkomendasikan ini untuk membantu mengurangi risiko. Topik remediasi dibagi berdasarkan jenis sifatnya.

Temuan eksposur tunggal berisi masalah yang diidentifikasi dalam beberapa topik remediasi. Sebaliknya, Anda dapat mengatasi temuan eksposur dan menurunkan tingkat keparahannya dengan hanya membahas satu topik remediasi. Pendekatan Anda terhadap remediasi risiko tergantung pada kebutuhan organisasi dan beban kerja Anda.

Note

Panduan remediasi yang diberikan dalam topik ini mungkin memerlukan konsultasi tambahan dalam AWS sumber daya lain.

Daftar Isi

- [Sifat salah konfigurasi untuk instance EC2](#)
 - [EC2 Instans ini memungkinkan akses ke IMDS menggunakan versi 1](#)
 - [Peran IAM yang terkait dengan EC2 instans Amazon memiliki kebijakan akses administratif](#)
 - [Peran IAM yang terkait dengan EC2 instans Amazon memiliki kebijakan admin layanan](#)

- [EC2 Instans Amazon memiliki grup keamanan atau ACL jaringan yang memungkinkan akses SSH atau RDP](#)
- [EC2 Instans Amazon memiliki grup keamanan terbuka](#)
- [EC2 Instans Amazon memiliki alamat IP publik](#)
- [Ciri-ciri jangkauan untuk contoh EC2](#)
 - [EC2 Contoh ini dapat dijangkau melalui internet](#)
 - [EC2 Instans Amazon dapat dijangkau dalam VPC Amazon](#)
- [Ciri-ciri kerentanan untuk contoh EC2](#)
 - [EC2 instance memiliki kerentanan perangkat lunak yang dapat dieksploitasi jaringan dengan kemungkinan eksploitasi yang tinggi](#)
 - [EC2 Instans Amazon memiliki kerentanan perangkat lunak](#)

Sifat salah konfigurasi untuk instance EC2

Berikut adalah sifat kesalahan konfigurasi untuk EC2 instance dan langkah-langkah remediasi yang disarankan.

EC2 Instans ini memungkinkan akses ke IMDS menggunakan versi 1

Metadata instans adalah data tentang EC2 instans Amazon yang dapat digunakan aplikasi untuk mengonfigurasi atau mengelola instance yang sedang berjalan. Layanan metadata instans (IMDS) adalah komponen pada instans yang menggunakan kode pada instans untuk mengakses metadata instans dengan aman. Jika IMDS tidak diamankan dengan benar, itu bisa menjadi vektor serangan potensial, karena menyediakan akses ke kredensi sementara dan data konfigurasi sensitif lainnya. IMDSv2 memberikan perlindungan yang lebih kuat terhadap eksploitasi melalui otentikasi berorientasi sesi, membutuhkan token sesi untuk permintaan metadata dan membatasi durasi sesi. Mengikuti prinsip keamanan standar, Anda AWS merekomendasikan agar Anda mengonfigurasi EC2 instans Amazon untuk digunakan IMDSv2 dan dinonaktifkan IMDSv1.

Uji kompatibilitas aplikasi

Sebelum menerapkan IMDSv2, uji instans Anda untuk memastikan kompatibilitasnya dengan IMDSv2. Beberapa aplikasi atau skrip mungkin memerlukan IMDSv1 fungsionalitas inti dan memerlukan konfigurasi tambahan. Untuk informasi selengkapnya tentang alat dan jalur yang direkomendasikan untuk menguji kompatibilitas aplikasi, [Transisi ke penggunaan Layanan Metadata Instans Versi 2 di Panduan Pengguna](#) Amazon Elastic Compute Cloud.

Perbarui contoh untuk digunakan IMDSv2

Ubah instance yang ada untuk digunakan IMDSv2. Untuk informasi selengkapnya, lihat [Memodifikasi opsi metadata instans untuk instans yang ada](#) di Panduan Pengguna Amazon Elastic Compute Cloud.

Menerapkan pembaruan ke instance dalam grup Auto Scaling

Jika instans Anda adalah bagian dari grup Auto Scaling, perbarui template peluncuran atau konfigurasi peluncuran dengan konfigurasi baru, dan lakukan penyegaran instans.

Peran IAM yang terkait dengan EC2 instans Amazon memiliki kebijakan akses administratif

Kebijakan akses administratif memberi EC2 instans Amazon izin Layanan AWS dan sumber daya yang luas. Kebijakan ini biasanya mencakup izin yang tidak diperlukan untuk fungsionalitas misalnya. Memberikan identitas IAM dengan kebijakan akses administratif pada EC2 instans Amazon (bukan set izin minimum yang diperlukan peran yang dilampirkan ke profil instans Anda) dapat meningkatkan cakupan serangan jika EC2 instans Amazon dikompromikan. Jika sebuah instance dikompromikan, penyerang dapat menggunakan izin berlebihan ini untuk bergerak secara lateral di lingkungan Anda, mengakses data, atau memanipulasi sumber daya. Mengikuti prinsip keamanan standar, kami sarankan Anda memberikan hak istimewa paling sedikit, yang berarti Anda hanya memberikan izin yang diperlukan untuk melakukan tugas.

Meninjau dan mengidentifikasi kebijakan administratif

Di dasbor IAM, temukan peran dengan nama peran. Tinjau kebijakan izin yang dilampirkan pada peran IAM. Jika kebijakan tersebut adalah kebijakan AWS terkelola, cari AdministratorAccess atau IAMFullAccess. Jika tidak, dalam dokumen kebijakan, cari pernyataan dengan "Effect": "Allow", "Action": "*", dan "Resource": "*".

Terapkan akses hak akses paling rendah

Ganti kebijakan administratif dengan kebijakan yang hanya memberikan izin khusus yang diperlukan agar instans berfungsi. Untuk informasi selengkapnya tentang praktik terbaik keamanan untuk peran IAM, lihat [Menerapkan izin hak istimewa terkecil](#) dalam praktik terbaik Keamanan di Panduan Pengguna AWS Identity and Access Management. Untuk mengidentifikasi izin yang tidak perlu, Anda dapat menggunakan IAM Access Analyzer untuk memahami cara mengubah kebijakan berdasarkan riwayat akses. Untuk informasi selengkapnya, lihat [Temuan untuk akses eksternal dan tidak terpakai](#) di Panduan AWS Identity and Access Management Pengguna. Atau, Anda dapat membuat peran IAM baru untuk menghindari dampak aplikasi lain menggunakan peran yang ada. Dalam skenario ini, buat peran IAM baru, lalu kaitkan peran IAM baru dengan instance. Untuk petunjuk cara mengganti

peran IAM untuk instance, lihat [Melampirkan peran IAM ke instance](#) di Panduan Pengguna Amazon Elastic Compute Cloud.

Pertimbangan konfigurasi yang aman

Jika izin administratif tingkat layanan diperlukan untuk instans, pertimbangkan untuk menerapkan kontrol keamanan tambahan ini untuk mengurangi risiko:

- Pertimbangan konfigurasi yang aman
 - Otentikasi multi-faktor (MFA) — MFA menambahkan lapisan keamanan tambahan dengan memerlukan bentuk otentikasi tambahan. Ini membantu mencegah akses yang tidak sah bahkan jika kredensialnya dikompromikan. Untuk informasi selengkapnya, lihat [Memerlukan otentikasi multi-faktor \(MFA\) di Panduan Pengguna](#).AWS Identity and Access Management
 - Kondisi IAM - Menyiapkan elemen kondisi memungkinkan Anda membatasi kapan dan bagaimana izin administratif dapat digunakan berdasarkan faktor-faktor seperti IP sumber atau usia MFA. Untuk informasi selengkapnya, lihat [Gunakan ketentuan dalam kebijakan IAM untuk membatasi akses lebih lanjut](#) di AWS Identity and Access Management Panduan Pengguna.
 - Batas izin — Batas izin menetapkan izin maksimum yang dapat dimiliki peran, menyediakan pagar pembatas untuk peran dengan akses administratif. Untuk informasi selengkapnya, lihat [Menggunakan batas izin untuk mendelegasikan manajemen izin dalam akun di Panduan Pengguna](#).AWS Identity and Access Management

Menerapkan pembaruan ke instance dalam grup penskalaan otomatis

Untuk EC2 instans Amazon dalam grup penskalaan AWS otomatis, perbarui templat peluncuran atau konfigurasi peluncuran dengan profil instans baru, dan lakukan penyegaran instans. Untuk informasi tentang memperbarui templat peluncuran, lihat [Memodifikasi templat peluncuran \(mengelola versi templat peluncuran\)](#) di Panduan Pengguna Amazon Elastic Compute Cloud. Untuk informasi selengkapnya, lihat [Menggunakan penyegaran instans untuk memperbarui instance di grup Auto Scaling](#). Untuk informasi selengkapnya tentang penggunaan peran IAM dengan grup Auto Scaling, lihat [peran IAM untuk aplikasi yang berjalan di instans Amazon di Panduan EC2](#) Pengguna Amazon EC2 Auto Scaling.

Peran IAM yang terkait dengan EC2 instans Amazon memiliki kebijakan admin layanan

Kebijakan akses layanan menyediakan EC2 instans Amazon dengan izin luas untuk AWS layanan dan sumber daya. Kebijakan ini biasanya mencakup izin yang tidak diperlukan untuk fungsionalitas

misalnya. Memberikan identitas IAM dengan kebijakan akses administratif pada EC2 instans Amazon, bukan set izin minimum yang dibutuhkan peran yang dilampirkan ke profil instans Anda dapat meningkatkan cakupan serangan jika instance dikompromikan. Mengikuti prinsip keamanan standar, kami menyarankan Anda memberikan hak istimewa paling sedikit, yang berarti Anda hanya memberikan izin yang diperlukan untuk melakukan tugas.

Meninjau dan mengidentifikasi kebijakan administratif

Di dasbor IAM, temukan peran dengan nama peran. Tinjau kebijakan izin yang dilampirkan pada peran IAM. Jika kebijakan tersebut adalah kebijakan AWS terkelola, cari AdministratorAccess atau IAMFullAccess. Jika tidak, dalam dokumen kebijakan, cari pernyataan dengan "Effect": "Allow", "Action": "*", dan "Resource": "*".

Terapkan akses hak akses paling rendah

Ganti kebijakan admin layanan dengan kebijakan yang hanya memberikan izin khusus yang diperlukan agar instance berfungsi. Untuk informasi selengkapnya tentang praktik terbaik keamanan untuk peran IAM, lihat [Menerapkan izin hak istimewa terkecil](#) dalam praktik terbaik Keamanan di Panduan Pengguna AWS Identity and Access Management. Untuk mengidentifikasi izin yang tidak perlu, Anda dapat menggunakan IAM Access Analyzer untuk memahami cara mengubah kebijakan berdasarkan riwayat akses. Untuk informasi selengkapnya, lihat [Temuan untuk akses eksternal dan tidak terpakai](#) di Panduan AWS Identity and Access Management Pengguna. Atau, Anda dapat membuat peran IAM baru untuk menghindari dampak aplikasi lain yang menggunakan peran yang ada. Dalam skenario ini, buat peran IAM baru, lalu kaitkan peran IAM baru dengan instance. Untuk informasi tentang mengganti peran IAM untuk instance, lihat [Melampirkan peran IAM ke instance](#) di Panduan Pengguna Amazon Elastic Compute Cloud.

Pertimbangan konfigurasi yang aman

Jika izin administratif tingkat layanan diperlukan untuk instans, pertimbangkan untuk menerapkan kontrol keamanan tambahan ini untuk mengurangi risiko:

Pertimbangan konfigurasi yang aman

Jika izin administratif tingkat layanan diperlukan untuk instans, pertimbangkan untuk menerapkan kontrol keamanan tambahan ini untuk mengurangi risiko:

- Otentikasi multi-faktor (MFA) — MFA menambahkan lapisan keamanan tambahan dengan memerlukan bentuk otentikasi tambahan. Ini membantu mencegah akses yang tidak sah bahkan

jika kredensialnya dikompromikan. Untuk informasi selengkapnya, lihat [Memerlukan otentikasi multi-faktor \(MFA\) di Panduan Pengguna](#).AWS Identity and Access Management

- Kondisi IAM - Menyiapkan elemen kondisi memungkinkan Anda membatasi kapan dan bagaimana izin administratif dapat digunakan berdasarkan faktor-faktor seperti IP sumber atau usia MFA. Untuk informasi selengkapnya, lihat [Gunakan ketentuan dalam kebijakan IAM untuk membatasi akses lebih lanjut](#) di AWS Identity and Access Management Panduan Pengguna.
- Batas izin — Batas izin menetapkan izin maksimum yang dapat dimiliki peran, menyediakan pagar pembatas untuk peran dengan akses administratif. Untuk informasi selengkapnya, lihat [Mengggunakan batas izin untuk mendelegasikan manajemen izin dalam akun di Panduan Pengguna](#).AWS Identity and Access Management

Menerapkan pembaruan ke instans di grup Auto Scaling

Untuk EC2 instans Amazon dalam grup penskalaan AWS otomatis, perbarui templat peluncuran atau konfigurasi peluncuran dengan profil instans baru, dan lakukan penyegaran instans. Untuk informasi tentang memperbarui templat peluncuran, lihat [Memodifikasi templat peluncuran \(mengelola versi templat peluncuran\)](#) di Panduan Pengguna Amazon Elastic Compute Cloud. Untuk informasi selengkapnya, lihat [Mengggunakan penyegaran instans untuk memperbarui instance di grup Auto Scaling](#). Untuk informasi selengkapnya tentang penggunaan peran IAM dengan grup Auto Scaling, lihat [peran IAM untuk aplikasi yang berjalan di instans Amazon di Panduan EC2](#) Pengguna Amazon EC2 Auto Scaling.

EC2 Instans Amazon memiliki grup keamanan atau ACL jaringan yang memungkinkan akses SSH atau RDP

Protokol akses jarak jauh seperti SSH dan RDP memungkinkan pengguna untuk terhubung dan mengelola instans Amazon EC2 dari lokasi eksternal. Ketika grup keamanan mengizinkan akses tidak terbatas ke protokol ini dari internet, mereka meningkatkan permukaan serangan EC2 instance Amazon Anda dengan mengizinkan akses internet ke instans Anda. Mengikuti prinsip keamanan standar, AWS merekomendasikan Anda membatasi akses jarak jauh ke alamat atau rentang IP tertentu dan tepercaya.

1. Ubah aturan grup keamanan

Batasi akses ke EC2 instans Amazon Anda ke alamat IP tepercaya tertentu. Batasi akses SSH dan RDP ke alamat IP tepercaya tertentu, atau gunakan notasi CIDR untuk menentukan rentang IP (misalnya, 198.168.1.0/24). Untuk mengubah aturan grup keamanan, lihat [Mengonfigurasi aturan grup keamanan](#) di Panduan Pengguna Amazon Elastic Compute Cloud.

EC2 Instans Amazon memiliki grup keamanan terbuka

Grup keamanan bertindak sebagai firewall virtual untuk EC2 instans Amazon Anda untuk mengontrol lalu lintas masuk dan keluar. Grup keamanan terbuka, yang memungkinkan akses tidak terbatas dari alamat IP apa pun, dapat mengekspos instans Anda ke akses yang tidak sah. Mengikuti prinsip keamanan standar, AWS merekomendasikan untuk membatasi akses grup keamanan ke alamat IP dan port tertentu.

Tinjau aturan grup keamanan dan nilai konfigurasi saat ini

Evaluasi port mana yang terbuka dan dapat diakses dari rentang IP yang luas, seperti (0.0.0.0/0 or ::/0). Untuk petunjuk tentang melihat detail grup keamanan, lihat [DescribeSecurityGroups](#) di Asisten Porting untuk Referensi API.NET.

Ubah aturan grup keamanan

Ubah aturan grup keamanan Anda untuk membatasi akses ke alamat atau rentang IP tepercaya tertentu. Saat memperbarui aturan grup keamanan Anda, pertimbangkan untuk memisahkan persyaratan akses untuk segmen jaringan yang berbeda dengan membuat aturan untuk setiap rentang IP sumber yang diperlukan atau membatasi akses ke port tertentu. Untuk mengubah aturan grup keamanan, lihat [Mengonfigurasi aturan grup keamanan](#) di Panduan EC2 Pengguna Amazon.

EC2 Instans Amazon memiliki alamat IP publik

EC2 Instans Amazon dengan alamat IP publik dapat diakses publik dari internet. Sementara alamat IP publik kadang-kadang diperlukan untuk contoh yang menyediakan layanan kepada pelanggan eksternal, ini dapat digunakan sebagai potensi dengan menyerang prinsipal yang tidak sah. Mengikuti prinsip keamanan standar, AWS merekomendasikan agar Anda membatasi paparan sumber daya publik bila memungkinkan.

Pindahkan instance ke subnet pribadi

Jika instans tidak memerlukan akses internet langsung, pertimbangkan untuk memindahkannya ke subnet pribadi dalam VPC Anda. Ini akan menghapus alamat IP publiknya sambil tetap memungkinkannya untuk berkomunikasi dengan sumber daya lain dalam VPC Anda. Untuk informasi selengkapnya, lihat [Bagaimana cara memindahkan EC2 instans Amazon ke subnet lain, Availability Zone, atau VPC?](#) di pusat AWS pengetahuan.

Konfigurasikan instance untuk diluncurkan tanpa alamat IP publik

Jika instance diluncurkan di subnet publik yang tidak memerlukan alamat IP publik, konfigurasi peluncuran dapat dimodifikasi untuk mencegah penetapan otomatis alamat IP publik. Ini dapat dinonaktifkan di tingkat subnet atau saat meluncurkan instance individual. Untuk informasi selengkapnya, lihat [Memodifikasi atribut pengalamatan IP subnet Anda](#) di Panduan Pengguna Amazon Virtual Private Cloud dan [EC2instance alamat IP Amazon Amazon](#) di Panduan Pengguna Amazon Elastic Compute Cloud.

Metode akses alternatif

Pertimbangkan opsi berikut untuk metode akses alternatif:

- Gunakan NAT Gateway untuk konektivitas internet keluar —

Untuk contoh di subnet pribadi yang memerlukan akses ke internet (misalnya, untuk mengunduh pembaruan), pertimbangkan untuk menggunakan NAT Gateway alih-alih menetapkan alamat IP publik. NAT Gateway memungkinkan instance di subnet pribadi untuk memulai koneksi keluar ke internet sambil mencegah koneksi masuk dari internet. Untuk informasi selengkapnya, lihat [gateway NAT di](#) Panduan Pengguna Amazon Virtual Private Cloud.

- Gunakan Elastic Load Balancing — Untuk contoh yang menjalankan aplikasi web, pertimbangkan untuk menggunakan Elastic Load Balancer (LB). LBs dapat dikonfigurasi untuk memungkinkan instance Anda berjalan di subnet pribadi sementara LB berjalan di subnet publik dan menangani lalu lintas internet. Untuk informasi selengkapnya, lihat [Apa itu Elastic Load Balancing?](#) di Panduan Pengguna AWS ELB. Lihat [Subnet penyeimbang beban](#) di Panduan AWS Preskriptif untuk panduan tentang cara memilih strategi lengket untuk LB Anda.

Ciri-ciri jangkauan untuk contoh EC2

Berikut adalah ciri-ciri jangkauan untuk EC2 contoh dan langkah-langkah remediasi yang disarankan.

EC2 Contoh ini dapat dijangkau melalui internet

EC2 Instans Amazon dengan port yang dapat dijangkau dari internet melalui gateway internet (termasuk contoh di belakang Application Load Balancers atau Classic Load Balancers), koneksi peering VPC, atau gateway virtual VPN dapat mengekspos instans Anda ke internet. Mengikuti prinsip keamanan standar, kami merekomendasikan untuk menerapkan kontrol akses jaringan dengan hak istimewa paling rendah dengan membatasi lalu lintas masuk hanya ke sumber dan port yang diperlukan.

Memodifikasi atau menghapus aturan grup keamanan

Di tab Sumber Daya, buka sumber daya untuk Grup EC2 Keamanan Amazon. Tinjau apakah akses internet diperlukan agar instance berfungsi. Ubah atau hapus aturan grup keamanan masuk yang mengizinkan akses tidak terbatas (0.0.0.0/0 atau :/0). Menerapkan aturan yang lebih ketat berdasarkan rentang IP tertentu atau grup keamanan. Jika akses publik terbatas diperlukan, batasi akses ke port dan protokol tertentu yang diperlukan untuk fungsi instans. Untuk petunjuk tentang mengelola aturan grup keamanan, lihat [Mengonfigurasi aturan grup keamanan](#) di Panduan EC2 Pengguna Amazon.

Perbarui jaringan ACLs

Meninjau dan memodifikasi daftar kontrol akses jaringan (ACLs) yang terkait dengan subnet instance. Verifikasi bahwa pengaturan ACL sejajar dengan grup keamanan berubah dan jangan secara tidak sengaja mengizinkan akses publik. Untuk petunjuk tentang memodifikasi jaringan ACLs, lihat [Bekerja dengan jaringan ACLs](#) di Panduan Pengguna Amazon VPC.

Metode akses alternatif

Pertimbangkan opsi berikut untuk metode akses alternatif:

- Gunakan NAT Gateway untuk konektivitas internet keluar — Untuk contoh di subnet pribadi yang memerlukan akses ke internet (misalnya, untuk mengunduh pembaruan), pertimbangkan untuk menggunakan NAT Gateway alih-alih menetapkan alamat IP publik. NAT Gateway memungkinkan instance di subnet pribadi untuk memulai koneksi keluar ke internet sambil mencegah koneksi masuk dari internet.
- Gunakan Systems Manager Session Manager — Session Manager menyediakan akses shell aman ke EC2 instans Amazon Anda tanpa perlu port masuk, mengelola kunci SSH, atau memelihara host bastion.
- Gunakan WAF dan Elastic Load Balancing atau Application Load Balancer — Untuk contoh yang menjalankan aplikasi web, pertimbangkan untuk menggunakan LB yang AWS dikombinasikan dengan Web Application Firewall (WAF). LBs dapat dikonfigurasi untuk memungkinkan instance Anda berjalan di subnet pribadi sementara LB berjalan di subnet publik dan menangani lalu lintas internet. Menambahkan WAF ke penyeimbang beban Anda memberikan perlindungan tambahan terhadap eksploitasi web dan bot.

EC2 Instans Amazon dapat dijangkau dalam VPC Amazon

Amazon Virtual Private Cloud (Amazon VPC) memungkinkan Anda meluncurkan AWS sumber daya di jaringan virtual yang ditentukan. Konfigurasi jaringan Amazon VPC yang memungkinkan akses

tak terbatas antar instance dapat meningkatkan cakupan serangan jika instance dikompromikan. Mengikuti praktik terbaik keamanan, AWS merekomendasikan penerapan segmentasi jaringan dan kontrol akses hak istimewa paling rendah di tingkat subnet dan grup keamanan.

Tinjau pola konektivitas jaringan Amazon VPC

Dalam temuan eksposur, identifikasi ID grup keamanan di ARN. Identifikasi contoh mana yang perlu berkomunikasi satu sama lain dan di port mana. Anda dapat menggunakan Amazon VPC Flow Logs untuk menganalisis pola lalu lintas yang ada di VPC Amazon Anda untuk membantu mengidentifikasi port mana yang sedang digunakan.

Ubah aturan grup keamanan

Ubah aturan grup keamanan Anda untuk membatasi akses ke alamat atau rentang IP tepercaya tertentu. Misalnya, alih-alih mengizinkan semua lalu lintas dari seluruh rentang CIDR VPC (misalnya, 10.0.0.0/16), batasi akses ke grup keamanan atau rentang IP tertentu. Saat memperbarui aturan grup keamanan Anda, pertimbangkan untuk memisahkan persyaratan akses untuk segmen jaringan yang berbeda dengan membuat aturan untuk setiap rentang IP sumber yang diperlukan atau membatasi akses ke port tertentu. Untuk mengubah aturan grup keamanan, lihat [Mengonfigurasi aturan grup keamanan](#) di Panduan EC2 Pengguna Amazon.

Pertimbangkan untuk mengatur sumber daya Amazon VPC Anda ke dalam subnet berdasarkan persyaratan atau fungsi keamanan. Misalnya, tempatkan server web dan server database di subnet terpisah. Untuk informasi selengkapnya, lihat [Subnet untuk VPC Anda](#) di Panduan Pengguna Amazon Virtual Private Cloud.

Konfigurasi jaringan ACLs untuk perlindungan tingkat subnet

Network Access Control Lists (NACLs) menyediakan lapisan keamanan tambahan di tingkat subnet. Tidak seperti kelompok keamanan, NACLs tidak memiliki kewarganegaraan dan memerlukan aturan masuk dan keluar untuk didefinisikan secara eksplisit. Untuk informasi selengkapnya, lihat [Mengontrol lalu lintas subnet dengan daftar kontrol akses jaringan](#) di Panduan Pengguna Amazon Virtual Private Cloud.

Pertimbangan tambahan

Pertimbangkan hal berikut saat membatasi akses ke VPC Amazon Anda

- Transit Gateway atau Amazon VPC Peering dengan perutean terbatas — Jika arsitektur Anda menggunakan beberapa VPCs yang perlu berkomunikasi, pertimbangkan untuk menggunakan Transit Gateway AWS dan Amazon VPC peering untuk menyediakan konektivitas antara Amazon

VPCs sambil memungkinkan Anda mengontrol subnet mana yang dapat berkomunikasi satu sama lain. Untuk informasi selengkapnya, lihat [Memulai menggunakan Gateway Transit VPC Amazon](#) dan koneksi peering [VPC](#).

- Titik akhir layanan dan tautan pribadi - Titik akhir VPC Amazon dapat digunakan untuk menjaga lalu lintas dalam AWS jaringan untuk berkomunikasi AWS dengan sumber daya daripada melalui internet. Ini mengurangi kebutuhan akan konektivitas langsung antara instans yang mengakses layanan yang sama. Untuk informasi tentang titik akhir VPC, lihat [Apa itu titik akhir VPC Amazon?](#) di Panduan Pengguna Amazon Virtual Private Cloud. Untuk konektivitas ke layanan yang dihosting di Amazon lain VPCs, pertimbangkan untuk menggunakan AWS PrivateLink.

Ciri-ciri kerentanan untuk contoh EC2

Berikut adalah ciri-ciri kerentanan untuk EC2 contoh dan langkah-langkah remediasi yang disarankan.

EC2 instance memiliki kerentanan perangkat lunak yang dapat dieksploitasi jaringan dengan kemungkinan eksploitasi yang tinggi

Paket perangkat lunak yang diinstal pada EC2 instance dapat diekspos ke Common Vulnerabilities and Exposures (). CVEs Kritis CVEs menimbulkan risiko keamanan yang signifikan terhadap AWS lingkungan Anda. Prinsipal yang tidak sah dapat mengeksploitasi kerentanan yang belum ditambal ini untuk membahayakan kerahasiaan, integritas, atau ketersediaan data, atau untuk mengakses sistem lain. Kerentanan kritis dengan kemungkinan eksploitasi tinggi mewakili ancaman keamanan langsung, karena kode eksploitasi mungkin sudah tersedia untuk umum dan digunakan secara aktif oleh penyerang atau alat pemindaian otomatis. Kami menyarankan untuk menambal kerentanan ini untuk melindungi instans Anda.

Perbarui instance yang terpengaruh

Tinjau bagian Referensi di tab Kerentanan sifat. Dokumentasi vendor dapat mencakup panduan remediasi khusus. Ikuti remediasi yang sesuai menggunakan pedoman umum ini:

Gunakan Systems Manager Patch Manager untuk menerapkan patch untuk sistem operasi dan aplikasi. Patch Manager membantu Anda memilih dan menerapkan sistem operasi dan patch perangkat lunak secara otomatis pada kelompok besar instance. Jika Patch Manager tidak dikonfigurasi, perbarui sistem operasi secara manual pada setiap instance yang terpengaruh.

Perbarui aplikasi yang terpengaruh ke versi aman terbaru mereka mengikuti prosedur yang direkomendasikan vendor. Untuk mengelola pembaruan aplikasi di beberapa instance,

pertimbangkan untuk menggunakan Manajer Negara Systems Manager untuk menjaga perangkat lunak Anda dalam keadaan konsisten. Jika pembaruan tidak tersedia, pertimbangkan untuk menghapus atau menonaktifkan aplikasi yang rentan hingga tambalan dirilis atau mitigasi lainnya, seperti membatasi akses jaringan ke aplikasi atau menonaktifkan fitur yang rentan.

Ikuti saran remediasi khusus yang disediakan dalam temuan Amazon Inspector. Ini bisa melibatkan perubahan aturan grup keamanan, memodifikasi konfigurasi instance, atau menyesuaikan pengaturan aplikasi.

Periksa apakah instance tersebut merupakan bagian dari Auto Scaling Group. Penambalan penggantian AMI dilakukan pada infrastruktur yang tidak dapat diubah dengan memperbarui ID AMI yang dikonfigurasi untuk menerapkan instans EC2 Amazon baru dalam grup Auto Scaling. Jika Anda menggunakan custom/golden AMI, buat instance dengan AMI baru, lalu sesuaikan instance dan buat AMI emas baru Untuk informasi selengkapnya, lihat [AMI memperbarui patching \(menggunakan patch AMIs untuk grup Auto Scaling\)](#).

Pertimbangan masa depan

Untuk mencegah terjadinya future, pertimbangkan untuk menerapkan program manajemen kerentanan. Amazon Inspector dapat dikonfigurasi untuk memindai instans Anda CVEs secara otomatis. Amazon Inspector juga dapat diintegrasikan dengan Security Hub untuk perbaikan otomatis. Pertimbangkan untuk menerapkan jadwal patching reguler menggunakan Windows Systems Manager Maintenance untuk meminimalkan gangguan pada instans Anda.

EC2 Instans Amazon memiliki kerentanan perangkat lunak

Paket perangkat lunak yang diinstal di Amazon EC2instances dapat terkena Common Vulnerabilities and Exposures (CVEs). Nonkritik CVEs mewakili kelemahan keamanan dengan tingkat keparahan atau eksploitasi yang lebih rendah dibandingkan dengan kritis. CVEs Sementara kerentanan ini menimbulkan risiko yang kurang langsung, penyerang masih dapat mengeksploitasi kerentanan yang belum ditambal ini untuk membahayakan kerahasiaan, integritas, atau ketersediaan data, atau untuk mengakses sistem lain. Mengikuti praktik terbaik keamanan, AWS merekomendasikan untuk menambal kerentanan ini untuk melindungi instance Anda dari serangan.

Perbarui instance yang terpengaruh

Gunakan AWS Systems Manager Patch Manager untuk menerapkan patch untuk sistem operasi. Patch Manager membantu Anda memilih dan menerapkan sistem operasi dan patch perangkat lunak secara otomatis pada kelompok besar instance. Jika Patch Manager tidak dikonfigurasi, perbarui sistem operasi secara manual pada setiap instance yang terpengaruh.

Perbarui aplikasi yang terpengaruh ke versi aman terbaru mereka mengikuti prosedur yang direkomendasikan vendor. Untuk mengelola pembaruan aplikasi di beberapa instance, pertimbangkan untuk menggunakan Manajer Negara AWS Systems Manager untuk menjaga perangkat lunak Anda dalam keadaan konsisten. Jika pembaruan tidak tersedia, pertimbangkan untuk menghapus atau menonaktifkan aplikasi yang rentan hingga tambalan dirilis atau mitigasi lainnya, seperti membatasi akses jaringan ke aplikasi atau menonaktifkan fitur yang rentan.

Ikuti saran remediasi khusus yang disediakan dalam temuan Amazon Inspector. Ini bisa melibatkan perubahan aturan grup keamanan, memodifikasi konfigurasi instance, atau menyesuaikan pengaturan aplikasi.

Periksa apakah instance tersebut merupakan bagian dari Auto Scaling Group. Penambalan penggantian AMI dilakukan pada infrastruktur yang tidak dapat diubah dengan memperbarui ID AMI yang dikonfigurasi untuk menerapkan instans EC2 Amazon baru dalam grup Auto Scaling. Jika Anda menggunakan custom/golden AMI, buat instance dengan AMI baru, lalu sesuaikan instance dan buat AMI emas baru Untuk informasi selengkapnya, lihat [AMI memperbarui patching \(menggunakan patch AMIs untuk grup Auto Scaling\)](#).

Pertimbangan masa depan

Untuk mencegah terjadinya future, pertimbangkan untuk menerapkan program manajemen kerentanan. Amazon Inspector dapat dikonfigurasi untuk memindai instans Anda CVEs secara otomatis. Amazon Inspector juga dapat diintegrasikan dengan Security Hub untuk perbaikan otomatis. Pertimbangkan untuk menerapkan jadwal patching reguler menggunakan Windows Systems Manager Maintenance untuk meminimalkan gangguan pada instans Anda.

Memulihkan eksposur untuk layanan Amazon ECS

AWS Security Hub dapat menghasilkan temuan eksposur untuk layanan Amazon Elastic Container Service (Amazon ECS).

Layanan Amazon ECS yang terlibat dalam temuan eksposur dan informasi mengenalannya tercantum di bagian Sumber Daya dari detail temuan. Anda dapat mengambil detail sumber daya ini di konsol Security Hub atau secara terprogram dengan [GetFindingsV2](#) pengoperasian Security Hub API.

Setelah mengidentifikasi sumber daya yang terlibat dalam temuan eksposur, Anda dapat menghapus sumber daya jika Anda tidak membutuhkannya. Menghapus sumber daya yang tidak penting dapat mengurangi profil dan AWS biaya eksposur Anda. Jika sumber daya sangat penting, ikuti langkah-langkah remediasi yang direkomendasikan ini untuk membantu mengurangi risiko. Topik remediasi dibagi berdasarkan jenis sifatnya.

Temuan eksposur tunggal berisi masalah yang diidentifikasi dalam beberapa topik remediasi. Sebaliknya, Anda dapat mengatasi temuan eksposur dan menurunkan tingkat keparahannya dengan hanya membahas satu topik remediasi. Pendekatan Anda terhadap remediasi risiko tergantung pada kebutuhan organisasi dan beban kerja Anda.

 Note

Panduan remediasi yang diberikan dalam topik ini mungkin memerlukan konsultasi tambahan dalam AWS sumber daya lain.

Daftar Isi

- [Ciri salah konfigurasi untuk layanan Amazon ECS](#)
 - [Layanan Amazon ECS menggunakan definisi tugas yang dikonfigurasi dengan hak istimewa yang ditinggikan](#)
 - [Layanan Amazon ECS memiliki wadah yang dapat mengambil peran IAM](#)
 - [Layanan Amazon ECS menggunakan definisi tugas yang memungkinkan kontainer mengakses sistem file root](#)
 - [Layanan Amazon ECS menggunakan definisi tugas yang dikonfigurasi untuk berbagi namespace proses host](#)
 - [Layanan Amazon ECS menggunakan definisi tugas yang dikonfigurasi dengan kredensial cleartext dalam variabel lingkungan](#)
 - [Layanan Amazon ECS memiliki grup keamanan terbuka](#)
 - [Layanan Amazon ECS memiliki alamat IP publik](#)
 - [Layanan Amazon ECS menggunakan definisi tugas yang dikonfigurasi dengan mode jaringan host diaktifkan](#)
 - [Peran IAM yang terkait dengan layanan Amazon ECS memiliki kebijakan akses administratif](#)
- [Ciri kerentanan untuk layanan Amazon ECS](#)
 - [Layanan Amazon ECS memiliki wadah dengan kerentanan perangkat lunak yang dapat dieksploitasi jaringan dengan kemungkinan eksploitasi yang tinggi](#)
 - [Layanan Amazon ECS memiliki wadah dengan kerentanan perangkat lunak](#)

Ciri salah konfigurasi untuk layanan Amazon ECS

Berikut adalah ciri kesalahan konfigurasi untuk layanan Amazon ECS dan langkah-langkah perbaikan yang disarankan.

Layanan Amazon ECS menggunakan definisi tugas yang dikonfigurasi dengan hak istimewa yang ditinggikan

Kontainer Amazon ECS yang berjalan dengan hak istimewa yang lebih tinggi memiliki kemampuan yang mirip dengan sistem host, berpotensi memungkinkan akses ke sumber daya host dan kontainer lainnya. Konfigurasi ini meningkatkan risiko bahwa kontainer yang dikompromikan dapat digunakan untuk mengakses atau memodifikasi sumber daya di luar cakupan yang dimaksudkan, berpotensi menyebabkan pelarian kontainer, akses tidak sah ke host yang mendasarinya, dan pelanggaran yang memengaruhi kontainer lain pada host yang sama. Mengikuti prinsip keamanan standar, AWS merekomendasikan agar Anda memberikan hak istimewa paling sedikit, yang berarti Anda hanya memberikan izin yang diperlukan untuk melakukan tugas.

Meninjau dan memodifikasi definisi tugas

Dalam paparan, identifikasi definisi tugas ARN. Buka definisi tugas di konsol Amazon ECS. Dalam definisi tugas, cari flag istimewa yang disetel ke true dalam definisi container. Jika mode istimewa tidak diperlukan, buat revisi definisi tugas baru tanpa bendera istimewa. Jika mode istimewa diperlukan, pertimbangkan untuk mengonfigurasi wadah untuk menggunakan sistem file hanya-baca untuk mencegah modifikasi yang tidak sah.

Layanan Amazon ECS memiliki wadah yang dapat mengambil peran IAM

Peran IAM memungkinkan tugas Amazon ECS untuk mengakses AWS layanan lain dengan aman menggunakan kredensi sementara. Peran eksekusi tugas mungkin diperlukan untuk tugas Amazon ECS di mana penampung perlu berinteraksi dengan AWS sumber daya lain. Meskipun hal ini terkadang diperlukan untuk fungsionalitas kontainer, peran yang tidak dikonfigurasi dengan benar dapat memberikan hak istimewa yang berlebihan yang dapat dieksploitasi oleh penyerang jika kontainer dikompromikan, berpotensi memungkinkan akses tidak sah ke AWS sumber daya, pencurian data, atau modifikasi infrastruktur Anda yang tidak sah. Mengikuti prinsip keamanan standar, AWS merekomendasikan penerapan akses hak istimewa paling sedikit dan meninjau peran IAM yang dilampirkan pada tugas Amazon ECS Anda.

Tinjau peran terlampir

Buka dasbor IAM, dan pilih peran yang diidentifikasi. Tinjau kebijakan izin yang dilampirkan pada peran IAM. Jika tugas memerlukan interaksi dengan AWS layanan lain, pertahankan peran eksekusi

tugas dan pertimbangkan untuk menerapkan izin hak istimewa paling sedikit. Jika tidak, buat revisi definisi tugas baru tanpa peran eksekusi.

Layanan Amazon ECS menggunakan definisi tugas yang memungkinkan kontainer mengakses sistem file root

Container Amazon ECS dengan akses ke sistem file root host berpotensi membaca, memodifikasi, atau mengeksekusi file penting pada sistem host. Konfigurasi ini meningkatkan risiko bahwa wadah yang dikompromikan dapat digunakan untuk mengakses atau memodifikasi sumber daya di luar cakupan yang dimaksudkan, berpotensi mengekspos data sensitif pada sistem file host. Mengikuti prinsip keamanan standar, AWS merekomendasikan agar Anda memberikan hak istimewa paling sedikit, yang berarti Anda hanya memberikan izin yang diperlukan untuk melakukan tugas.

Tinjau dan modifikasi kontainer dengan akses sistem file host

Dalam temuan eksposur, identifikasi definisi tugas ARN. Buka definisi tugas di konsol Amazon ECS. Cari bagian volume dalam definisi tugas yang mendefinisikan pemetaan jalur host. Tinjau definisi tugas untuk menentukan apakah akses sistem file host diperlukan untuk fungsionalitas kontainer. s Jika akses sistem file host tidak diperlukan, buat revisi definisi tugas baru dan hapus definisi volume apa pun yang menggunakan jalur host. Jika akses sistem file host diperlukan, pertimbangkan untuk mengonfigurasi wadah untuk menggunakan sistem file hanya-baca untuk mencegah modifikasi yang tidak sah.

Layanan Amazon ECS menggunakan definisi tugas yang dikonfigurasi untuk berbagi namespace proses host

Kontainer Amazon ECS yang berjalan dengan ruang nama terbuka berpotensi mengakses sumber daya sistem host dan ruang nama kontainer lainnya. Konfigurasi ini dapat memungkinkan wadah yang dikompromikan untuk melarikan diri dari batas isolasinya, yang dapat menyebabkan proses mengakses, antarmuka jaringan, atau sumber daya lain di luar ruang lingkup yang dimaksudkan. Namespace ID proses (PID) menyediakan pemisahan antar proses. Ini mencegah proses sistem agar tidak terlihat, dan memungkinkan PIDs untuk digunakan kembali, termasuk PID 1. Jika namespace PID host dibagikan dengan kontainer, itu akan memungkinkan kontainer untuk melihat semua proses pada sistem host. Ini mengurangi manfaat isolasi tingkat proses antara host dan wadah. Faktor-faktor ini dapat menyebabkan akses tidak sah ke proses pada host itu sendiri, termasuk kemampuan untuk memanipulasi dan menghentikannya. Mengikuti prinsip keamanan standar, AWS merekomendasikan untuk mempertahankan isolasi namespace yang tepat untuk kontainer.

Perbarui definisi tugas dengan ruang nama terbuka

Buka tab Resources dari eksposur, identifikasi definisi tugas dengan namespace yang terbuka. Buka definisi tugas di konsol Amazon ECS. Cari pengaturan PidMode dengan nilai host, yang akan berbagi ruang nama ID proses dengan host. Hapus pengaturan PidMode: host dari definisi tugas Anda untuk memastikan kontainer berjalan dengan isolasi namespace yang tepat.

Layanan Amazon ECS menggunakan definisi tugas yang dikonfigurasi dengan kredensial cleartext dalam variabel lingkungan

Container Amazon ECS dengan kredensial cleartext dalam variabel lingkungan mengekspos informasi otentikasi sensitif yang dapat dikompromikan jika penyerang mendapatkan akses ke definisi tugas, lingkungan kontainer, atau log kontainer. Ini menciptakan risiko keamanan yang signifikan, karena kredensial yang bocor dapat digunakan untuk mengakses AWS layanan atau sumber daya lain.

Ganti kredensial cleartext

Dalam temuan eksposur, identifikasi definisi tugas dengan kredensial cleartext. Buka definisi tugas di konsol Amazon ECS. Cari variabel lingkungan dalam definisi kontainer yang berisi nilai sensitif seperti kunci AWS akses, kata sandi database, atau token API.

Pertimbangkan alternatif berikut untuk lulus kredensial:

- Alih-alih menggunakan kunci AWS akses, gunakan peran eksekusi tugas IAM dan peran tugas untuk memberikan izin ke kontainer Anda.
- Simpan kredensial sebagai AWS rahasia di Secrets Manager dan referensikan dalam definisi tugas Anda.

Perbarui definisi tugas

Buat revisi baru definisi tugas Anda yang menangani kredensial dengan aman. Kemudian perbarui layanan Amazon ECS Anda untuk menggunakan revisi definisi tugas baru.

Layanan Amazon ECS memiliki grup keamanan terbuka

Grup keamanan bertindak sebagai firewall virtual untuk tugas Amazon ECS Anda untuk mengontrol lalu lintas masuk dan keluar. Grup keamanan terbuka, yang memungkinkan akses tidak terbatas dari alamat IP apa pun, dapat mengekspos wadah Anda ke akses tidak sah, meningkatkan risiko paparan alat pemindaian otomatis dan serangan yang ditargetkan. Mengikuti prinsip keamanan standar, AWS merekomendasikan untuk membatasi akses grup keamanan ke alamat IP dan port tertentu.

Tinjau aturan grup keamanan dan nilai konfigurasi saat ini

Buka sumber daya untuk Amazon ECS Security Group. Evaluasi port mana yang terbuka dan dapat diakses dari rentang IP yang luas, seperti (0.0.0.0/0 or ::/0).

Ubah aturan grup keamanan

Ubah aturan grup keamanan Anda untuk membatasi akses ke alamat atau rentang IP tepercaya tertentu. Saat memperbarui aturan grup keamanan Anda, pertimbangkan untuk memisahkan persyaratan akses untuk segmen jaringan yang berbeda dengan membuat aturan untuk setiap rentang IP sumber yang diperlukan atau membatasi akses ke port tertentu.

Ubah aturan grup keamanan

Pertimbangkan opsi berikut untuk metode akses alternatif:

- Session Manager menyediakan akses shell aman ke EC2 instans Amazon Anda tanpa memerlukan port masuk, mengelola kunci SSH, atau memelihara host bastion.
- NACLs memberikan lapisan keamanan tambahan di tingkat subnet. Tidak seperti kelompok keamanan, NACLs tidak memiliki kewarganegaraan dan memerlukan aturan masuk dan keluar untuk didefinisikan secara eksplisit.

Layanan Amazon ECS memiliki alamat IP publik

Layanan Amazon ECS dengan alamat IP publik yang ditetapkan untuk tugas mereka dapat diakses langsung dari internet. Meskipun ini mungkin diperlukan untuk layanan yang perlu tersedia untuk umum, ini meningkatkan permukaan serangan dan potensi akses yang tidak sah.

Identifikasi layanan dengan alamat IP publik

Dalam temuan eksposur, identifikasi layanan Amazon ECS yang memiliki alamat IP publik yang ditetapkan untuk tugasnya. Cari `assignPublicIp` pengaturan dengan nilai `ENABLED` dalam konfigurasi layanan.

Perbarui definisi tugas

Buat revisi baru definisi tugas Anda yang menonaktifkan alamat IP publik. Kemudian perbarui layanan Amazon ECS Anda untuk menggunakan revisi definisi tugas baru.

Menerapkan pola akses jaringan pribadi

Untuk contoh yang menjalankan aplikasi web, pertimbangkan untuk menggunakan Load Balancer (LB). LBs dapat dikonfigurasi untuk memungkinkan instance Anda berjalan di subnet pribadi sementara LB berjalan di subnet publik dan menangani lalu lintas internet.

Layanan Amazon ECS menggunakan definisi tugas yang dikonfigurasi dengan mode jaringan host diaktifkan

Kontainer Amazon ECS yang berjalan dengan mode jaringan host berbagi namespace jaringan dengan host, memungkinkan akses langsung ke antarmuka jaringan host, port, dan tabel perutean. Konfigurasi ini melewati isolasi jaringan yang disediakan oleh kontainer, berpotensi mengekspos layanan yang berjalan pada kontainer langsung ke jaringan eksternal dan memungkinkan kontainer untuk memodifikasi pengaturan jaringan host. Mengikuti prinsip keamanan standar, AWS merekomendasikan untuk menjaga isolasi jaringan yang tepat untuk kontainer.

Nonaktifkan mode jaringan host

Dalam temuan eksposur, identifikasi definisi tugas dengan mode jaringan host. Buka definisi tugas di konsol Amazon ECS. Cari pengaturan NetworkMode dengan nilai host dalam definisi tugas.

Pertimbangkan opsi berikut untuk menonaktifkan mode jaringan host:

- Mode `awsvpc` jaringan menyediakan tingkat isolasi jaringan terkuat dengan memberikan setiap tugas elastis network interface sendiri.
- Mode `bridge` jaringan menyediakan isolasi sambil memungkinkan pemetaan port untuk mengekspos port kontainer tertentu ke host.

Perbarui definisi tugas

Buat revisi baru definisi tugas Anda dengan konfigurasi mode jaringan yang diperbarui. Kemudian perbarui layanan Amazon ECS Anda untuk menggunakan revisi definisi tugas baru.

Peran IAM yang terkait dengan layanan Amazon ECS memiliki kebijakan akses administratif

Peran IAM dengan kebijakan akses administratif yang dilampirkan pada tugas Amazon ECS memberikan izin luas yang melebihi apa yang biasanya diperlukan untuk pengoperasian kontainer. Konfigurasi ini meningkatkan risiko bahwa wadah yang dikompromikan dapat digunakan untuk mengakses atau memodifikasi sumber daya di seluruh AWS lingkungan Anda. Mengikuti prinsip keamanan standar, AWS merekomendasikan penerapan akses hak istimewa paling sedikit dengan hanya memberikan izin yang diperlukan agar tugas berfungsi.

Meninjau dan mengidentifikasi kebijakan administratif

n ID Sumber Daya, identifikasi nama peran IAM. Buka dasbor IAM dan pilih peran yang diidentifikasi. Tinjau kebijakan izin yang dilampirkan pada peran IAM. Jika kebijakan tersebut adalah kebijakan AWS terkelola, cari `AdministratorAccess`. Jika tidak, dalam dokumen kebijakan, cari pernyataan yang memiliki pernyataan `"Effect": "Allow", "Action": "*", and "Resource": "*"` bersama.

Terapkan akses hak akses paling rendah

Ganti kebijakan administratif dengan kebijakan yang hanya memberikan izin khusus yang diperlukan agar instans berfungsi. Untuk mengidentifikasi izin yang tidak perlu, Anda dapat menggunakan IAM Access Analyzer untuk memahami cara mengubah kebijakan berdasarkan riwayat akses. Atau, Anda dapat membuat peran IAM baru untuk menghindari dampak aplikasi lain yang menggunakan peran yang ada. Dalam skenario ini, buat peran IAM baru, lalu kaitkan peran IAM baru dengan instance.

Pertimbangan konfigurasi yang aman

Jika izin administratif tingkat layanan diperlukan untuk contoh ini, pertimbangkan untuk menerapkan kontrol keamanan tambahan ini untuk mengurangi risiko:

- MFA menambahkan lapisan keamanan tambahan dengan membutuhkan bentuk otentikasi tambahan. Ini membantu mencegah akses yang tidak sah bahkan jika kredensialnya dikompromikan.
- Menyiapkan elemen kondisi memungkinkan Anda membatasi kapan dan bagaimana izin administratif dapat digunakan berdasarkan faktor-faktor seperti IP sumber atau usia MFA.

Perbarui definisi tugas

Buat revisi baru definisi tugas Anda yang mereferensikan peran IAM baru atau yang diperbarui. Kemudian perbarui layanan Amazon ECS Anda untuk menggunakan revisi definisi tugas baru.

Ciri kerentanan untuk layanan Amazon ECS

Berikut adalah ciri-ciri jangkauan untuk Amazon ECS dan langkah-langkah remediasi yang disarankan.

Layanan Amazon ECS memiliki wadah dengan kerentanan perangkat lunak yang dapat dieksploitasi jaringan dengan kemungkinan eksploitasi yang tinggi

1. Memahami eksposur

Temuan kerentanan Package mengidentifikasi paket perangkat lunak di AWS lingkungan Anda yang terkena Common Vulnerabilities and Exposures (). CVEs Penyerang dapat mengeksploitasi kerentanan yang belum ditambal ini untuk membahayakan kerahasiaan, integritas, atau ketersediaan data, atau untuk mengakses sistem lain. Gambar kontainer ECR dapat memiliki temuan kerentanan paket.

2. Memperbaiki eksposur

a. Perbarui versi paket

Tinjau temuan kerentanan paket untuk fungsi Lambda Anda. Perbarui versi paket seperti yang disarankan oleh Amazon Inspector. Untuk selengkapnya, lihat [Melihat detail untuk temuan Amazon Inspector Anda di Panduan Pengguna Amazon Inspector](#). Bagian Remediation dari rincian temuan di konsol Amazon Inspector memberi tahu Anda perintah mana yang dapat Anda jalankan untuk memperbarui paket.

b. Perbarui gambar wadah dasar

Membangun kembali dan memperbarui gambar wadah dasar secara teratur untuk menjaga kontainer Anda tetap up to date. Saat membangun kembali gambar, jangan sertakan komponen yang tidak perlu untuk mengurangi permukaan serangan. Untuk petunjuk tentang membangun kembali gambar kontainer, lihat [Membangun ulang gambar Anda](#) sesering mungkin.

Layanan Amazon ECS memiliki wadah dengan kerentanan perangkat lunak

Paket perangkat lunak yang diinstal pada container Amazon ECS dapat terkena Common Vulnerabilities and Exposures (). CVEs Kerentanan prioritas rendah mewakili kelemahan keamanan dengan tingkat keparahan atau eksploitasi yang lebih rendah dibandingkan dengan kerentanan prioritas tinggi. Sementara kerentanan ini menimbulkan risiko yang kurang langsung, penyerang masih dapat mengeksploitasi kerentanan yang belum ditambal ini untuk membahayakan kerahasiaan, integritas, atau ketersediaan data, atau untuk mengakses sistem lain.

Perbarui gambar kontainer yang terpengaruh

Tinjau bagian Referensi di tab Kerentanan dari sifat tersebut. Dokumentasi vendor dapat mencakup panduan remediasi khusus.

Terapkan remediasi yang sesuai dengan mengikuti pedoman umum ini:

- Perbarui gambar kontainer Anda untuk menggunakan versi patch dari paket yang terpengaruh.
- Perbarui dependensi yang terpengaruh dalam aplikasi Anda ke versi aman terbaru mereka.

Setelah memperbarui gambar kontainer Anda, dorong ke registri penampung Anda dan perbarui definisi tugas Amazon ECS Anda untuk menggunakan gambar baru.

Pertimbangan masa depan

Untuk lebih memperkuat postur keamanan gambar kontainer Anda, pertimbangkan untuk mengikuti praktik terbaik tugas Amazon ECS dan keamanan kontainer. Amazon Inspector dapat dikonfigurasi untuk memindai kontainer Anda CVEs secara otomatis. Amazon Inspector juga dapat diintegrasikan dengan Security Hub untuk perbaikan otomatis. Pertimbangkan untuk menerapkan jadwal patching reguler menggunakan Windows Systems Manager Maintenance untuk meminimalkan gangguan pada container Anda.

Memulihkan eksposur untuk kluster Amazon EKS

AWS Security Hub dapat menghasilkan temuan eksposur untuk cluster Amazon Elastic Kubernetes Service (Amazon EKS).

Cluster Amazon EKS yang terlibat dalam temuan eksposur dan informasi pengidentifikasinya tercantum di bagian Sumber Daya dari detail temuan. Anda dapat mengambil detail sumber daya ini di konsol Security Hub atau secara terprogram dengan [GetFindingsV2](#) pengoperasian Security Hub API.

Setelah mengidentifikasi sumber daya yang terlibat dalam temuan eksposur, Anda dapat menghapus sumber daya jika Anda tidak membutuhkannya. Menghapus sumber daya yang tidak penting dapat mengurangi profil dan AWS biaya eksposur Anda. Jika sumber daya sangat penting, ikuti langkah-langkah remediasi yang direkomendasikan ini untuk membantu mengurangi risiko. Topik remediasi dibagi berdasarkan jenis sifatnya.

Temuan eksposur tunggal berisi masalah yang diidentifikasi dalam beberapa topik remediasi. Sebaliknya, Anda dapat mengatasi temuan eksposur dan menurunkan tingkat keparahannya dengan hanya membahas satu topik remediasi. Pendekatan Anda terhadap remediasi risiko tergantung pada kebutuhan organisasi dan beban kerja Anda.

Note

Panduan remediasi yang diberikan dalam topik ini mungkin memerlukan konsultasi tambahan dalam AWS sumber daya lain.

Daftar Isi

- [Ciri salah konfigurasi untuk kluster Amazon EKS](#)
 - [Cluster Amazon EKS memungkinkan akses publik](#)
 - [Cluster Amazon EKS menggunakan versi Kubernetes yang tidak didukung](#)
 - [Cluster Amazon EKS menggunakan rahasia Kubernetes yang tidak terenkripsi](#)
- [Ciri-ciri kerentanan untuk kluster Amazon EKS](#)
 - [Cluster Amazon EKS memiliki wadah dengan kerentanan perangkat lunak yang dapat dieksploitasi jaringan dengan kemungkinan eksploitasi yang tinggi](#)
 - [Cluster Amazon EKS memiliki wadah dengan kerentanan perangkat lunak](#)

Ciri salah konfigurasi untuk kluster Amazon EKS

Berikut adalah ciri kesalahan konfigurasi untuk kluster Amazon EKS dan langkah-langkah perbaikan yang disarankan.

Cluster Amazon EKS memungkinkan akses publik

Endpoint kluster Amazon EKS adalah endpoint yang Anda gunakan untuk berkomunikasi dengan server API Kubernetes kluster Anda. Secara default, titik akhir ini bersifat publik ke internet. Titik akhir publik meningkatkan area permukaan serangan Anda dan risiko akses tidak sah ke server API Kubernetes Anda, yang berpotensi memungkinkan penyerang mengakses atau memodifikasi sumber daya kluster atau mengakses data sensitif. Mengikuti praktik terbaik keamanan, AWS merekomendasikan untuk membatasi akses ke titik akhir kluster EKS Anda hanya ke rentang IP yang diperlukan.

Ubah akses titik akhir

Dalam temuan eksposur, buka sumber daya. Ini akan membuka cluster Amazon EKS yang terpengaruh. Anda dapat mengonfigurasi kluster Anda untuk menggunakan akses pribadi, akses publik, atau keduanya. Dengan akses pribadi, permintaan Kubernetes API yang berasal dari VPC kluster Anda menggunakan titik akhir VPC pribadi. Dengan akses publik, permintaan Kubernetes API yang berasal dari luar VPC kluster Anda menggunakan titik akhir publik.

Memodifikasi atau menghapus akses publik ke cluster

Untuk mengubah akses endpoint untuk kluster yang ada, lihat [Memodifikasi akses endpoint cluster](#) di Panduan Pengguna Amazon Elastic Kubernetes Service. Menerapkan aturan yang lebih ketat berdasarkan rentang IP tertentu atau grup keamanan. Jika akses publik terbatas diperlukan, batasi akses ke rentang blok CIDR tertentu atau gunakan daftar awalan.

Cluster Amazon EKS menggunakan versi Kubernetes yang tidak didukung

Amazon EKS mendukung setiap versi Kubernetes untuk jangka waktu terbatas. Menjalankan cluster dengan versi Kubernetes yang tidak didukung dapat mengekspos lingkungan Anda ke kerentanan keamanan, karena patch CVE akan berhenti dirilis untuk versi yang sudah ketinggalan zaman. Versi yang tidak didukung mungkin mengandung kerentanan keamanan yang diketahui yang dapat dieksploitasi oleh penyerang dan tidak memiliki fitur keamanan yang mungkin tersedia dalam versi yang lebih baru. Mengikuti praktik terbaik keamanan, AWS merekomendasikan agar versi Kubernetes Anda diperbarui.

Perbarui versi Kubernetes

Dalam temuan eksposur, buka sumber daya. Ini akan membuka cluster Amazon EKS yang terpengaruh. Sebelum memperbarui kluster Anda, tinjau [versi yang tersedia pada dukungan standar](#) di Panduan Pengguna Amazon Elastic Kubernetes Service untuk daftar versi Kubernetes yang saat ini didukung.

Cluster Amazon EKS menggunakan rahasia Kubernetes yang tidak terenkripsi

Rahasia Kubernetes, secara default, disimpan tanpa terenkripsi di penyimpanan data dasar server API (etcd). Siapa pun yang memiliki akses API atau dengan akses ke etcd dapat mengambil atau memodifikasi rahasia. Untuk mencegah hal ini, Anda harus mengenkripsi rahasia Kubernetes saat istirahat. Jika Rahasia Kubernetes tidak dienkripsi, mereka rentan terhadap akses yang tidak sah jika etcd dikompromikan. Karena rahasia sering berisi informasi sensitif seperti kata sandi dan token API, eksposur mereka dapat menyebabkan akses tidak sah ke aplikasi dan data lain. Mengikuti praktik terbaik keamanan, AWS merekomendasikan untuk mengenkripsi semua informasi sensitif yang disimpan dalam rahasia Kubernetes.

Enkripsi rahasia Kubernetes

Amazon EKS mendukung enkripsi rahasia Kubernetes menggunakan kunci KMS melalui enkripsi amplop. Untuk mengaktifkan enkripsi rahasia Kubernetes untuk kluster EKS Anda, lihat [Enkripsi rahasia Kubernetes dengan KMS pada kluster yang ada di Panduan Pengguna Amazon EKS](#).

Ciri-ciri kerentanan untuk kluster Amazon EKS

Berikut adalah ciri-ciri kerentanan untuk cluster Amazon EKS.

Cluster Amazon EKS memiliki wadah dengan kerentanan perangkat lunak yang dapat dieksploitasi jaringan dengan kemungkinan eksploitasi yang tinggi

Paket perangkat lunak yang diinstal pada kluster EKS dapat terkena Common Vulnerabilities and Exposures (). CVEs Kritis CVEs menimbulkan risiko keamanan yang signifikan terhadap AWS lingkungan Anda. Pengguna yang tidak sah dapat mengeksploitasi kerentanan yang belum ditambal ini untuk membahayakan kerahasiaan, integritas, atau ketersediaan data, atau untuk mengakses sistem lain. Kerentanan kritis dengan kemungkinan eksploitasi tinggi mewakili ancaman keamanan langsung, karena kode eksploitasi mungkin sudah tersedia untuk umum dan digunakan secara aktif oleh penyerang atau alat pemindaian otomatis. Mengikuti praktik terbaik keamanan, AWS merekomendasikan untuk menambal kerentanan ini untuk melindungi instance Anda dari serangan.

Perbarui instance yang terpengaruh

Perbarui gambar kontainer Anda ke versi yang lebih baru yang menyertakan perbaikan keamanan untuk kerentanan yang diidentifikasi. Ini biasanya melibatkan membangun kembali gambar kontainer Anda dengan gambar dasar atau dependensi yang diperbarui, lalu menerapkan gambar baru ke cluster Amazon EKS Anda.

Cluster Amazon EKS memiliki wadah dengan kerentanan perangkat lunak

Paket perangkat lunak yang diinstal pada kluster Amazon EKS dapat terkena Kerentanan Umum dan Eksposur (). CVEs Nonkritis CVEs mewakili kelemahan keamanan dengan tingkat keparahan atau eksploitasi yang lebih rendah dibandingkan dengan kritis. CVEs Sementara kerentanan ini menimbulkan risiko yang kurang langsung, penyerang masih dapat mengeksploitasi kerentanan yang belum ditambal ini untuk membahayakan kerahasiaan, integritas, atau ketersediaan data, atau untuk mengakses sistem lain. Mengikuti praktik terbaik keamanan, AWS merekomendasikan untuk menambal kerentanan ini untuk melindungi instance Anda dari serangan.

Perbarui instance yang terpengaruh

Perbarui gambar kontainer Anda ke versi yang lebih baru yang menyertakan perbaikan keamanan untuk kerentanan yang diidentifikasi. Ini biasanya melibatkan membangun kembali gambar kontainer Anda dengan gambar dasar atau dependensi yang diperbarui, lalu menerapkan gambar baru ke cluster Amazon EKS Anda.

Memulihkan eksposur untuk pengguna IAM

AWS Security Hub dapat menghasilkan temuan eksposur untuk pengguna AWS Identity and Access Management (IAM).

Di konsol Security Hub, pengguna IAM yang terlibat dalam temuan eksposur dan informasi pengidentifikasinya tercantum di bagian Sumber Daya pada detail temuan. Secara terprogram, Anda dapat mengambil detail sumber daya dengan [GetFindingsV2](#) pengoperasian Security Hub API.

Setelah mengidentifikasi sumber daya yang terlibat dalam temuan eksposur, Anda dapat menghapus sumber daya jika Anda tidak membutuhkannya. Menghapus sumber daya yang tidak penting dapat mengurangi profil dan AWS biaya eksposur Anda. Jika sumber daya sangat penting, ikuti langkah-langkah remediasi yang direkomendasikan ini untuk membantu mengurangi risiko. Topik remediasi dibagi berdasarkan jenis sifatnya.

Temuan eksposur tunggal berisi masalah yang diidentifikasi dalam beberapa topik remediasi. Sebaliknya, Anda dapat mengatasi temuan eksposur dan menurunkan tingkat keparahannya dengan hanya membahas satu topik remediasi. Pendekatan Anda terhadap remediasi risiko tergantung pada kebutuhan organisasi dan beban kerja Anda.

Note

Panduan remediasi yang diberikan dalam topik ini mungkin memerlukan konsultasi tambahan dalam AWS sumber daya lain.

Praktik terbaik IAM merekomendasikan agar Anda membuat peran IAM atau menggunakan federasi dengan penyedia identitas untuk mengakses AWS menggunakan kredensial sementara alih-alih membuat pengguna IAM individu. Jika itu adalah opsi untuk organisasi dan kasus penggunaan Anda, sebaiknya beralih ke peran atau federasi daripada menggunakan pengguna IAM. Untuk informasi selengkapnya, lihat [Pengguna IAM](#) di Panduan Pengguna IAM.

Daftar Isi

- [Ciri salah konfigurasi untuk pengguna IAM](#)
 - [Pengguna IAM memiliki kebijakan dengan akses administratif](#)
 - [Pengguna IAM tidak mengaktifkan MFA](#)
 - [Pengguna IAM memiliki kebijakan dengan akses administratif ke Layanan AWS](#)
 - [AWS Akun untuk pengguna IAM memiliki kebijakan kata sandi yang lemah](#)
 - [Pengguna IAM memiliki kredensial yang tidak digunakan](#)
 - [Pengguna IAM memiliki kunci akses yang tidak diputar](#)
 - [Pengguna IAM memiliki kebijakan yang memungkinkan akses tidak terbatas ke dekripsi kunci KMS](#)

Ciri salah konfigurasi untuk pengguna IAM

Berikut adalah ciri kesalahan konfigurasi untuk pengguna IAM dan langkah-langkah perbaikan yang disarankan.

Pengguna IAM memiliki kebijakan dengan akses administratif

Kebijakan IAM memberikan serangkaian hak istimewa kepada pengguna IAM saat mengakses sumber daya. Kebijakan administratif memberi pengguna IAM izin luas untuk AWS layanan dan sumber daya. Memberikan hak administratif penuh, alih-alih set izin minimum yang dibutuhkan pengguna, dapat meningkatkan cakupan serangan jika kredensial dikompromikan. Mengikuti prinsip keamanan standar, AWS merekomendasikan agar Anda memberikan hak istimewa paling sedikit, yang berarti Anda hanya memberikan izin yang diperlukan untuk melakukan tugas.

1. Tinjau dan identifikasi kebijakan administratif — Di ID Sumber Daya, identifikasi nama peran IAM. Buka dasbor IAM dan pilih peran yang diidentifikasi. Tinjau kebijakan izin yang dilampirkan pada pengguna IAM. Jika kebijakan tersebut adalah kebijakan AWS terkelola, cari `AdministratorAccess` atau `IAMFullAccess`. Jika tidak, dalam dokumen kebijakan, cari pernyataan yang memiliki pernyataan `"Effect": "Allow"` `"Action": "*" lebih dari "Resource": "*" .`
2. Menerapkan akses hak istimewa terkecil — Ganti kebijakan administratif layanan dengan kebijakan yang hanya memberikan izin khusus yang diperlukan agar pengguna dapat berfungsi. Untuk informasi selengkapnya tentang praktik terbaik keamanan untuk kebijakan IAM, lihat [Menerapkan izin hak istimewa terkecil](#) di Panduan Pengguna.AWS Identity and Access Management Untuk mengidentifikasi izin yang tidak perlu, Anda dapat menggunakan IAM Access Analyzer untuk memahami cara mengubah kebijakan berdasarkan riwayat akses. Untuk informasi selengkapnya, lihat [Temuan untuk akses eksternal dan tidak terpakai](#) di Panduan AWS Identity and Access Management Pengguna.
3. Pertimbangan konfigurasi aman — Jika izin administratif layanan diperlukan untuk instans, pertimbangkan untuk menerapkan kontrol keamanan tambahan ini untuk mengurangi risiko:
 - Otentikasi multi-faktor (MFA) — MFA menambahkan lapisan keamanan tambahan dengan memerlukan bentuk otentikasi tambahan. Ini membantu mencegah akses yang tidak sah bahkan jika kredensialnya dikompromikan. Untuk informasi selengkapnya, lihat [Memerlukan otentikasi multi-faktor \(MFA\) di Panduan Pengguna.AWS Identity and Access Management](#)
 - Kondisi IAM - Menyiapkan elemen kondisi memungkinkan Anda membatasi kapan dan bagaimana izin administratif dapat digunakan berdasarkan faktor-faktor seperti IP sumber atau

usia MFA. Untuk informasi selengkapnya, lihat [Gunakan ketentuan dalam kebijakan IAM](#) untuk membatasi akses lebih lanjut di AWS Identity and Access Management Panduan Pengguna.

- Batas izin — Batas izin menetapkan izin maksimum yang dapat dimiliki peran, menyediakan pagar pembatas untuk peran dengan akses administratif. Untuk informasi selengkapnya, lihat [Menggunakan batas izin untuk mendelegasikan manajemen izin dalam akun di Panduan Pengguna](#).AWS Identity and Access Management

Pengguna IAM tidak mengaktifkan MFA

Otentikasi multi-faktor (MFA) menambahkan lapisan perlindungan tambahan di atas nama pengguna dan kata sandi. Ketika MFA diaktifkan dan pengguna IAM masuk ke AWS situs web, mereka diminta untuk nama pengguna, kata sandi, dan kode otentikasi dari perangkat MFA mereka. AWS Prinsipal otentikasi harus memiliki perangkat yang memancarkan kunci sensitif waktu dan harus memiliki pengetahuan tentang kredensi. Tanpa MFA, jika kata sandi pengguna dikompromikan, penyerang mendapatkan akses penuh ke izin pengguna. AWS Mengikuti prinsip keamanan standar, AWS merekomendasikan mengaktifkan MFA untuk semua akun dan pengguna yang AWS Management Console memiliki akses.

Tinjau jenis MFA

AWS mendukung jenis [MFA](#) berikut:

- Kunci sandi dan kunci keamanan
- Aplikasi otentikator virtual
- Token TOTP perangkat keras

Meskipun otentikasi dengan perangkat fisik biasanya memberikan perlindungan keamanan yang lebih ketat, menggunakan semua jenis MFA lebih aman daripada menonaktifkan MFA.

Aktifkan MFA

Untuk mengaktifkan jenis MFA yang sesuai dengan kebutuhan Anda, lihat [otentikasi AWS multi-faktor di IAM di Panduan Pengguna IAM](#). Ikuti langkah-langkah untuk jenis MFA tertentu yang ingin Anda terapkan. Untuk organisasi yang mengelola banyak pengguna, Anda mungkin ingin menegakkan penggunaan MFA dengan mewajibkan MFA untuk mengakses sumber daya sensitif.

Pengguna IAM memiliki kebijakan dengan akses administratif ke Layanan AWS

Kebijakan admin layanan memberi pengguna IAM izin untuk melakukan semua tindakan dalam layanan tertentu AWS. Kebijakan ini biasanya mencakup izin yang tidak diperlukan bagi pengguna untuk menjalankan fungsi pekerjaan mereka. Menyediakan pengguna IAM dengan hak administrator layanan, alih-alih set izin minimum yang diperlukan, meningkatkan cakupan serangan jika kredensial dikompromikan. Mengikuti prinsip keamanan standar, AWS merekomendasikan agar Anda memberikan hak istimewa paling sedikit, yang berarti Anda hanya memberikan izin yang diperlukan untuk melakukan tugas.

Meninjau dan mengidentifikasi kebijakan admin layanan

Di ID Sumber Daya, identifikasi nama peran IAM. Buka dasbor IAM dan pilih peran yang diidentifikasi. Tinjau kebijakan izin yang dilampirkan pada pengguna IAM. Jika kebijakan tersebut adalah kebijakan yang dikelola AWS, cari `AdministratorAccess` atau `IAMFullAccess`. Jika tidak, dalam dokumen kebijakan, cari pernyataan yang memiliki pernyataan `"Effect": "Allow" with "Action": "*" over "Resource": "*"`.

Terapkan akses hak akses paling rendah

Ganti kebijakan administratif layanan dengan kebijakan yang hanya memberikan izin khusus yang diperlukan agar pengguna dapat berfungsi. Untuk mengidentifikasi izin yang tidak perlu, Anda dapat menggunakan IAM Access Analyzer untuk memahami cara mengubah kebijakan berdasarkan riwayat akses.

Pertimbangan konfigurasi yang aman

Jika izin administratif layanan diperlukan untuk instans, pertimbangkan untuk menerapkan kontrol keamanan tambahan ini untuk mengurangi eksposur:

- MFA menambahkan lapisan keamanan tambahan dengan membutuhkan bentuk otentikasi tambahan. Ini membantu mencegah akses yang tidak sah bahkan jika kredensialnya dikompromikan.
- Gunakan elemen kondisi untuk membatasi kapan dan bagaimana izin administratif dapat digunakan berdasarkan faktor-faktor seperti IP sumber atau usia MFA.
- Gunakan batas izin untuk menetapkan izin maksimum yang dapat dimiliki peran, menyediakan pagar pembatas untuk peran dengan akses administratif.

AWS Akun untuk pengguna IAM memiliki kebijakan kata sandi yang lemah

Kebijakan kata sandi membantu melindungi terhadap akses yang tidak sah dengan menerapkan persyaratan kompleksitas minimum untuk kata sandi pengguna IAM. Tanpa kebijakan kata sandi yang kuat, ada peningkatan risiko bahwa akun pengguna dapat dikompromikan melalui tebakan kata sandi atau serangan brute force. Mengikuti prinsip keamanan standar, AWS merekomendasikan penerapan kebijakan kata sandi yang kuat untuk memastikan pengguna membuat kata sandi kompleks yang sulit ditebak.

Konfigurasi kebijakan kata sandi yang kuat

Buka dasbor IAM dan arahkan ke Pengaturan akun. Tinjau pengaturan kebijakan kata sandi saat ini untuk akun Anda, termasuk panjang minimum, jenis karakter yang diperlukan, dan pengaturan kedaluwarsa kata sandi.

Minimal, AWS merekomendasikan untuk mengikuti praktik terbaik ini saat menyetel kebijakan kata sandi Anda:

- Membutuhkan setidaknya satu karakter huruf besar.
- Memerlukan setidaknya satu karakter huruf kecil.
- Membutuhkan setidaknya satu simbol.
- Membutuhkan setidaknya satu nomor.
- Membutuhkan setidaknya delapan karakter.

Pertimbangan keamanan tambahan

Pertimbangkan langkah-langkah keamanan tambahan ini selain kebijakan kata sandi yang kuat:

- MFA menambahkan lapisan keamanan tambahan dengan membutuhkan bentuk otentikasi tambahan. Ini membantu mencegah akses yang tidak sah bahkan jika kredensialnya dikompromikan.
- Menyiapkan elemen kondisi untuk membatasi kapan dan bagaimana izin administratif dapat digunakan berdasarkan faktor-faktor seperti IP sumber atau usia MFA.

Pengguna IAM memiliki kredensial yang tidak digunakan

Kredensi yang tidak digunakan, termasuk kata sandi dan kunci akses yang tetap tidak aktif selama 90 hari atau lebih menimbulkan risiko keamanan bagi lingkungan Anda. AWS Kredensi yang

tidak terpakai ini menciptakan vektor serangan potensial untuk penyerang dan meningkatkan permukaan serangan organisasi Anda secara keseluruhan. Mengikuti praktik terbaik keamanan, AWS merekomendasikan untuk menonaktifkan atau menghapus kredensial yang belum digunakan dalam 90 hari atau lebih untuk mengurangi permukaan serangan Anda.

Nonaktifkan atau hapus kredensial yang tidak digunakan

Dalam temuan eksposur, buka sumber daya. Ini akan membuka jendela detail pengguna. Sebelum mengambil tindakan pada kredensial yang tidak digunakan, menilai dampak potensial terhadap lingkungan Anda. Menghapus kredensial tanpa penilaian yang tepat dapat mengganggu proses latar belakang, pekerjaan terjadwal, dan banyak lagi. Pertimbangkan periode penonaktifan singkat sebelum penghapusan permanen untuk memverifikasi dampak penghapusan kredensial yang tidak digunakan.

Ambil tindakan yang sesuai berdasarkan jenis kredensial:

- Untuk kata sandi konsol yang tidak digunakan, pertimbangkan terlebih dahulu mengubah kata sandi dan menonaktifkannya untuk sementara. Jika tidak ada masalah yang muncul, lanjutkan dengan penonaktifan atau penghapusan permanen.
- Untuk kunci akses yang tidak digunakan, pertimbangkan untuk menonaktifkan kunci terlebih dahulu. Setelah mengonfirmasi tidak ada sistem yang terpengaruh, lanjutkan dengan penonaktifan atau penghapusan permanen.
- Untuk pengguna yang tidak digunakan, pertimbangkan untuk menonaktifkan sementara pengguna dengan melampirkan kebijakan pembatasan sebelum penghapusan penuh.

Pengguna IAM memiliki kunci akses yang tidak diputar

Kunci akses terdiri dari ID kunci akses dan kunci akses rahasia yang memungkinkan akses terprogram ke AWS sumber daya. Ketika kunci akses tetap tidak berubah untuk jangka waktu yang lama, mereka meningkatkan risiko akses tidak sah jika dikompromikan. Mengikuti praktik terbaik keamanan, AWS merekomendasikan memutar kunci akses setiap 90 hari untuk meminimalkan jendela peluang bagi penyerang untuk menggunakan kredensial yang disusupi.

Putar tombol akses

Dalam temuan eksposur, buka sumber daya. Ini akan membuka jendela detail pengguna. Untuk memutar kunci akses, lihat [Mengelola kunci akses untuk pengguna IAM](#) di Panduan Pengguna IAM.

Pengguna IAM memiliki kebijakan yang memungkinkan akses tidak terbatas ke dekripsi kunci KMS

AWS KMS memungkinkan Anda untuk membuat dan mengelola kunci kriptografi yang digunakan untuk melindungi data Anda. Kebijakan IAM yang mengizinkan izin AWS KMS dekripsi tidak terbatas (misalnya, `kms:Decrypt` atau `kms:ReEncryptFrom`) pada semua kunci KMS dapat menyebabkan akses data yang tidak sah jika kredensial pengguna IAM dikompromikan. Jika penyerang mendapatkan akses ke kredensial ini, mereka berpotensi mendekripsi data terenkripsi apa pun di lingkungan Anda, yang dapat mencakup data sensitif. Mengikuti praktik terbaik keamanan, AWS merekomendasikan penerapan hak istimewa paling sedikit dengan membatasi izin AWS KMS dekripsi hanya untuk kunci tertentu yang dibutuhkan pengguna untuk fungsi pekerjaan mereka.

Menerapkan akses hak istimewa yang paling rendah

Dalam temuan eksposur, buka sumber daya. Ini akan membuka jendela Kebijakan IAM. Cari izin di KMS yang memungkinkan `kms:Decrypt` atau `kms:ReEncryptFrom` atau `KMS:*` dengan spesifikasi sumber daya. "*" Perbarui kebijakan untuk membatasi izin AWS KMS dekripsi hanya pada kunci tertentu yang diperlukan. Ubah kebijakan untuk mengganti "*" sumber daya dengan AWS KMS kunci spesifik ARNs yang diperlukan.

Pertimbangan konfigurasi yang aman

Pertimbangkan untuk menambahkan kondisi untuk membatasi lebih lanjut kapan izin ini dapat digunakan. Misalnya, Anda dapat membatasi operasi dekripsi ke titik akhir VPC tertentu atau rentang IP sumber. Anda juga dapat mengonfigurasi kebijakan kunci untuk membatasi lebih lanjut siapa yang dapat menggunakan kunci KMS tertentu.

Memperbaiki eksposur untuk fungsi Lambda

 Note

Security Hub dalam rilis pratinjau dan dapat berubah sewaktu-waktu.

AWS Security Hub dapat menghasilkan temuan eksposur untuk AWS Lambda fungsi (Lambda).

Pada konsol Security Hub, fungsi Lambda yang terlibat dalam temuan eksposur dan informasi pengidentifikasinya tercantum di bagian Sumber Daya pada detail temuan. Secara terprogram, Anda dapat mengambil detail sumber daya dengan [GetFindingsV2](#) pengoperasian Security Hub API.

Setelah mengidentifikasi sumber daya yang terlibat dalam temuan eksposur, Anda dapat menghapus sumber daya jika Anda tidak membutuhkannya. Menghapus sumber daya yang tidak penting dapat

mengurangi profil dan AWS biaya eksposur Anda. Jika sumber daya sangat penting, ikuti langkah-langkah remediasi yang direkomendasikan ini untuk membantu mengurangi risiko. Topik remediasi dibagi berdasarkan jenis sifatnya.

Temuan eksposur tunggal berisi masalah yang diidentifikasi dalam beberapa topik remediasi. Sebaliknya, Anda dapat mengatasi temuan eksposur dan menurunkan tingkat keparahannya dengan hanya membahas satu topik remediasi. Pendekatan Anda terhadap remediasi risiko tergantung pada kebutuhan organisasi dan beban kerja Anda.

Note

Panduan remediasi yang diberikan dalam topik ini mungkin memerlukan konsultasi tambahan dalam AWS sumber daya lain.

Note

Panduan remediasi yang diberikan dalam topik ini mungkin memerlukan konsultasi tambahan dalam AWS sumber daya lain.

Daftar Isi

- [Ciri salah konfigurasi untuk fungsi Lambda](#)
 - [Fungsi Lambda menjalankan runtime yang tidak didukung](#)
 - [Fungsi Lambda digunakan di luar VPC Amazon](#)
 - [Fungsi Lambda dapat mengambil peran IAM](#)
 - [Peran IAM yang terkait dengan fungsi Lambda memiliki kebijakan akses Administratif](#)
 - [Peran IAM yang terkait dengan fungsi Lambda memiliki kebijakan dengan akses administratif ke Layanan AWS](#)
- [Ciri-ciri jangkauan untuk fungsi Lambda](#)
 - [Fungsi Lambda dapat dipanggil secara publik](#)
- [Ciri-ciri kerentanan untuk fungsi Lambda](#)
 - [Fungsi Lambda memiliki kerentanan perangkat lunak yang dapat dieksploitasi jaringan](#)
 - [Fungsi Lambda memiliki kerentanan perangkat lunak](#)

Ciri salah konfigurasi untuk fungsi Lambda

Berikut adalah sifat kesalahan konfigurasi untuk fungsi Lambda dan langkah-langkah perbaikan yang disarankan.

Fungsi Lambda menjalankan runtime yang tidak didukung

Lambda memungkinkan pengembang untuk menjalankan kode tanpa menyediakan atau mengelola server melalui runtime yang mengeksekusi kode Anda di lingkungan terkelola. Lambda secara otomatis menerapkan tambalan dan pembaruan keamanan ke runtime terkelola dan gambar dasar kontainer yang sesuai. Ketika versi runtime tidak lagi didukung, ia tidak lagi menerima pembaruan keamanan, perbaikan bug, atau dukungan teknis. Fungsi yang berjalan pada runtime yang tidak digunakan lagi dapat memiliki kerentanan keamanan dan pada akhirnya dapat berhenti berfungsi karena masalah seperti kedaluwarsa sertifikat. Selain itu, runtime yang tidak didukung mungkin rentan terhadap eksploitasi keamanan yang baru ditemukan tanpa patch yang tersedia. Mengikuti praktik terbaik keamanan, sebaiknya gunakan runtime yang ditambal dan didukung untuk fungsi Lambda.

Upgrade fungsi runtime

Di tab Sumber daya eksposur, buka sumber daya dengan hyperlink. Ini akan membuka jendela fungsi Lambda. Untuk memutakhirkan fungsi Anda ke runtime yang didukung, konfigurasi manajemen runtime. Anda dapat memilih agar fungsi Anda diperbarui secara otomatis ke versi runtime terbaru, tetapi sebelum memilih opsi ini, menilai apakah peningkatan otomatis dapat memengaruhi aplikasi yang sedang berjalan. Untuk informasi selengkapnya, lihat [Memahami cara Lambda mengelola pembaruan versi runtime](#).

Fungsi Lambda digunakan di luar VPC Amazon

Fungsi Lambda secara default digunakan dengan akses ke internet publik. Konfigurasi default ini memberi fungsi Lambda kemampuan untuk mencapai titik akhir AWS layanan dan eksternal APIs, tetapi juga mengekspos mereka pada potensi risiko keamanan. Fungsi dengan akses internet dapat digunakan untuk mengekstraksi data, berkomunikasi dengan server yang tidak sah, atau menjadi titik masuk bagi aktor eksternal jika dikompromikan. Amazon VPC menyediakan isolasi jaringan dengan membatasi fungsi Lambda Anda untuk berkomunikasi hanya dengan sumber daya dalam jaringan pribadi yang Anda tentukan. Mengikuti prinsip keamanan standar, sebaiknya gunakan fungsi Lambda dalam VPC untuk meningkatkan keamanan melalui isolasi jaringan.

Lampirkan fungsi ke VPC

Dalam temuan eksposur, buka sumber daya dengan hyperlink. Ini akan membuka jendela fungsi Lambda. Untuk mengamankan fungsi Lambda Anda dengan membatasi akses jaringannya, lampirkan ke VPC yang memiliki kontrol jaringan yang sesuai. Sebelum melampirkan fungsi Anda ke VPC, rencanakan akses layanan AWS apa pun yang mungkin diperlukan, karena fungsi di subnet pribadi tanpa gateway NAT atau titik akhir VPC tidak akan dapat mencapai layanan. AWS APIs Untuk informasi tentang cara melampirkan fungsi Lambda ke VPC Amazon di akun Anda, lihat [Melampirkan fungsi Lambda ke VPC Amazon di akun Anda](#). Akun AWS Pertimbangkan untuk menggunakan titik akhir VPC untuk konektivitas layanan tanpa akses internet jika fungsi Anda memerlukan akses AWS layanan dari dalam subnet pribadi. Konfigurasi Gateway NAT jika Anda memerlukan konektivitas internet keluar dari subnet pribadi.

Fungsi Lambda dapat mengambil peran IAM

Fungsi Lambda menggunakan peran IAM untuk berinteraksi dengan layanan. AWS Peran ini memberikan izin untuk fungsi Lambda untuk AWS mengakses sumber daya selama eksekusi. Sementara peran ini kadang-kadang diperlukan untuk fungsi Lambda untuk melakukan tugasnya, peran ini harus mengikuti prinsip hak istimewa yang paling sedikit. Mengikuti prinsip keamanan standar, AWS merekomendasikan agar Anda meninjau apakah izin yang dilampirkan pada peran sesuai berdasarkan fungsionalitas fungsi yang dimaksudkan.

1. Tentukan apakah Peran IAM terlampir diperlukan

Tentukan apakah fungsi Lambda memerlukan peran eksekusi IAM untuk dikonfigurasi. Sebagian besar fungsi Lambda memerlukan izin dasar untuk beroperasi, seperti menulis log ke CloudWatch Tinjau izin yang dilampirkan pada peran eksekusi fungsi dan tentukan apakah Peran IAM diperlukan untuk fungsi tersebut. Untuk informasi tentang peran eksekusi Lambda, lihat [Mendefinisikan izin fungsi Lambda dengan peran eksekusi](#) di Panduan Pengembang.AWS Lambda

2. Menerapkan akses hak istimewa paling sedikit

Ganti kebijakan yang terlalu permisif dengan kebijakan yang hanya memberikan izin khusus yang diperlukan agar fungsi dapat beroperasi. Untuk informasi tentang praktik terbaik keamanan untuk peran IAM, lihat [Menerapkan izin hak istimewa terkecil](#) di Panduan Pengguna.AWS Identity and Access Management Untuk mengidentifikasi izin yang tidak perlu, Anda dapat menggunakan IAM Access Analyzer untuk memahami cara mengubah kebijakan berdasarkan riwayat akses. Untuk informasi selengkapnya, lihat [Temuan untuk akses eksternal dan tidak terpakai](#) di Panduan AWS Identity and Access Management Pengguna. Atau, Anda dapat membuat peran IAM baru agar tidak memengaruhi fungsi Lambda lain yang menggunakan peran yang ada. Dalam skenario

ini, buat peran IAM baru, lalu kaitkan peran IAM baru dengan instance. Untuk petunjuk cara mengganti peran IAM untuk suatu fungsi, lihat [Memperbarui peran eksekusi fungsi](#) di Panduan AWS Lambda Pengembang.

Peran IAM yang terkait dengan fungsi Lambda memiliki kebijakan akses Administratif

Kebijakan akses administratif menyediakan fungsi Lambda dengan izin luas untuk AWS layanan dan sumber daya. Kebijakan ini biasanya mencakup izin yang tidak diperlukan untuk fungsionalitas. Memberikan identitas IAM dengan kebijakan akses administratif pada fungsi Lambda, alih-alih set izin minimum yang dibutuhkan peran eksekusi, dapat meningkatkan cakupan serangan jika fungsi tersebut dikompromikan. Mengikuti prinsip keamanan standar, AWS merekomendasikan agar Anda memberikan hak istimewa paling sedikit, yang berarti Anda hanya memberikan izin yang diperlukan untuk melakukan tugas.

1. Meninjau dan mengidentifikasi kebijakan administratif

Dalam temuan eksposur, identifikasi nama peran. Buka dasbor IAM dan temukan peran dengan nama peran yang diidentifikasi sebelumnya. Tinjau kebijakan izin yang dilampirkan pada peran IAM. Jika kebijakan tersebut adalah kebijakan AWS terkelola, cari AdministratorAccess atau IAMFullAccess. Jika tidak, dalam dokumen kebijakan, cari pernyataan yang memiliki pernyataan "Effect": "Allow", "Action": "*" dan "Resource": "*" bersama-sama.

2. Menerapkan akses hak istimewa paling sedikit

Ganti kebijakan administratif dengan kebijakan yang hanya memberikan izin khusus yang diperlukan agar fungsi dapat beroperasi. Untuk informasi selengkapnya tentang praktik terbaik keamanan untuk peran IAM, lihat [Menerapkan izin hak istimewa terkecil](#) di Panduan Pengguna AWS Identity and Access Management. Untuk mengidentifikasi izin yang tidak perlu, Anda dapat menggunakan IAM Access Analyzer untuk memahami cara mengubah kebijakan berdasarkan riwayat akses. Untuk informasi selengkapnya, lihat [Temuan untuk akses eksternal dan tidak terpakai](#) di Panduan AWS Identity and Access Management Pengguna. Atau, Anda dapat membuat peran IAM baru agar tidak memengaruhi fungsi Lambda lainnya menggunakan peran yang ada. Dalam skenario ini, buat peran IAM baru. Kemudian kaitkan peran baru dengan instance. Untuk informasi tentang mengganti peran IAM untuk suatu fungsi, lihat [Memperbarui peran eksekusi fungsi](#) di Panduan AWS Lambda Pengembang.

3. Pertimbangan konfigurasi yang aman

Jika izin akses administratif diperlukan untuk contoh ini, pertimbangkan untuk menerapkan kontrol keamanan tambahan ini untuk mengurangi risiko:

- Otentikasi multi-faktor (MFA) — MFA menambahkan lapisan keamanan tambahan dengan memerlukan bentuk otentikasi tambahan. Ini membantu mencegah akses yang tidak sah bahkan jika kredensialnya dikompromikan. Untuk informasi selengkapnya, lihat [Memerlukan otentikasi multi-faktor \(MFA\) di Panduan Pengguna](#).AWS Identity and Access Management
- Kondisi IAM - Menyiapkan elemen kondisi memungkinkan Anda membatasi kapan dan bagaimana izin administratif dapat digunakan berdasarkan faktor-faktor seperti IP sumber atau usia MFA. Untuk informasi selengkapnya, lihat [Gunakan ketentuan dalam kebijakan IAM untuk membatasi akses lebih lanjut](#) di Panduan Pengguna IAM.
- Batas izin — Batas izin menetapkan izin maksimum yang dapat dimiliki peran, menyediakan pagar pembatas untuk peran dengan akses administratif. Untuk informasi selengkapnya, lihat [Menggunakan batas izin untuk mendelegasikan manajemen izin dalam akun di Panduan Pengguna](#).AWS Identity and Access Management

Peran IAM yang terkait dengan fungsi Lambda memiliki kebijakan dengan akses administratif ke Layanan AWS

Kebijakan admin layanan memungkinkan fungsi Lambda untuk melakukan semua tindakan dalam layanan tertentu AWS . Kebijakan ini biasanya memberikan izin lebih dari yang diperlukan untuk operasi fungsi. Jika fungsi Lambda dengan kebijakan admin layanan disusupi, penyerang dapat menggunakan izin tersebut untuk mengakses atau memodifikasi data atau layanan sensitif di lingkungan Anda. AWS Mengikuti prinsip keamanan standar, kami menyarankan Anda memberikan hak istimewa paling sedikit, yang berarti Anda hanya memberikan izin yang diperlukan untuk melakukan tugas.

1. Meninjau dan mengidentifikasi kebijakan administratif

Dalam temuan eksposur, identifikasi nama peran di ARN. Buka dasbor IAM, dan temukan nama peran. Tinjau kebijakan izin yang dilampirkan pada peran. Jika kebijakan tersebut adalah kebijakan AWS terkelola, cari `AdministratorAccess` atau `IAMFullAccess`. Jika tidak, dalam dokumen kebijakan, cari pernyataan yang memiliki pernyataan `"Effect": "Allow"`, `"Action": "*"` dan `"Resource": "*"`.

2. Menerapkan akses hak istimewa paling sedikit

Ganti kebijakan administratif dengan kebijakan yang hanya memberikan izin khusus yang diperlukan agar fungsi dapat beroperasi. Untuk informasi selengkapnya, lihat [Menerapkan izin hak istimewa terkecil](#) di Panduan Pengguna.AWS Identity and Access Management Untuk mengidentifikasi izin yang tidak perlu, Anda dapat menggunakan IAM Access Analyzer untuk

memahami cara mengubah kebijakan berdasarkan riwayat akses. Untuk informasi selengkapnya, lihat [Temuan untuk akses eksternal dan tidak terpakai](#) di Panduan AWS Identity and Access Management Pengguna. Atau, Anda dapat membuat peran IAM baru agar tidak memengaruhi fungsi Lambda lain yang menggunakan peran yang ada. Dalam skenario ini, buat peran IAM baru, lalu kaitkan peran IAM baru dengan instance. Untuk petunjuk cara mengganti peran IAM untuk suatu fungsi, lihat [Memperbarui peran eksekusi fungsi](#) di Panduan AWS Lambda Pengembang.

3. Pertimbangan konfigurasi yang aman

Jika izin administratif tingkat layanan diperlukan untuk instans, pertimbangkan untuk menerapkan kontrol keamanan tambahan ini untuk mengurangi risiko:

- Otentikasi multi-faktor (MFA) — MFA menambahkan lapisan keamanan tambahan dengan memerlukan bentuk otentikasi tambahan. Ini membantu mencegah akses yang tidak sah bahkan jika kredensialnya dikompromikan. Untuk informasi selengkapnya, lihat [Memerlukan otentikasi multi-faktor \(MFA\) di Panduan Pengguna](#).AWS Identity and Access Management
- Kondisi IAM - Menyiapkan elemen kondisi memungkinkan Anda membatasi kapan dan bagaimana izin administratif dapat digunakan berdasarkan faktor-faktor seperti IP sumber atau usia MFA. Untuk informasi selengkapnya, lihat [Gunakan ketentuan dalam kebijakan IAM untuk membatasi akses lebih lanjut](#) di AWS Identity and Access Management Panduan Pengguna.
- Batas izin — Batas izin menetapkan izin maksimum yang dapat dimiliki peran, menyediakan pagar pembatas untuk peran dengan akses administratif. Untuk informasi selengkapnya, lihat [Menggunakan batas izin untuk mendelegasikan manajemen izin di Panduan](#) Pengguna.AWS Identity and Access Management

Ciri-ciri jangkauan untuk fungsi Lambda

Berikut adalah ciri-ciri jangkauan untuk fungsi Lambda dan langkah-langkah remediasi yang disarankan.

Fungsi Lambda dapat dipanggil secara publik

Kebijakan berbasis sumber daya Lambda menentukan siapa yang dapat menjalankan fungsi Anda. Fungsi dengan kebijakan sumber daya yang menyertakan “*” sebagai prinsipal (atau tidak ada prinsipal sama sekali) memungkinkan AWS pengguna yang diautentikasi untuk memanggilnya. Ini menciptakan risiko yang signifikan, terutama untuk fungsi yang memproses data sensitif, memodifikasi sumber daya, atau memiliki izin tinggi. Pengguna yang tidak sah dapat memanfaatkan konfigurasi ini untuk melakukan operasi yang tidak diinginkan, berpotensi mengekspos data,

memanipulasi sumber daya, atau menyalahgunakan kemampuan fungsi. Mengikuti praktik terbaik keamanan, kami sarankan untuk membatasi akses fungsi Lambda hanya ke prinsipal resmi.

Ubah kebijakan berbasis sumber daya fungsi

Di tab Sumber daya eksposur, buka sumber daya dengan hyperlink. Ini akan membuka jendela fungsi Lambda. Batasi akses ke fungsi Lambda Anda dengan hanya menentukan IDs akun AWS resmi atau kepala IAM tertentu (pengguna, peran, atau layanan) dalam kebijakan berbasis sumber daya. Anda hanya dapat mengubah kebijakan berbasis sumber daya secara terprogram.

Ciri-ciri kerentanan untuk fungsi Lambda

Berikut adalah ciri-ciri kerentanan untuk fungsi Lambda dan langkah-langkah remediasi yang disarankan.

Fungsi Lambda memiliki kerentanan perangkat lunak yang dapat dieksploitasi jaringan

Paket perangkat lunak yang digunakan dalam kode fungsi Lambda dapat berisi Kerentanan Umum dan Eksposur (CVEs) yang memiliki peluang tinggi untuk dieksploitasi. Kritis CVEs menimbulkan risiko keamanan yang signifikan terhadap AWS lingkungan Anda. Penyerang dapat mengeksploitasi kerentanan yang belum ditambal ini untuk membahayakan kerahasiaan, integritas, atau ketersediaan data, atau untuk mengakses sistem lain. Kerentanan kritis dengan kemungkinan eksploitasi tinggi mewakili ancaman keamanan langsung, karena kode eksploitasi mungkin sudah tersedia untuk umum dan digunakan secara aktif oleh penyerang atau alat pemindaian otomatis. Mengikuti praktik terbaik keamanan, kami sarankan untuk menambal kerentanan ini untuk melindungi fungsi Anda dari serangan.

Perbarui fungsi yang terpengaruh

Tinjau bagian Referensi di tab Kerentanan untuk sifat tersebut. Dokumentasi vendor dapat mencakup panduan remediasi khusus. Perbarui pustaka rentan ke versi aman terbaru mereka mengikuti prosedur yang direkomendasikan vendor. Biasanya, alur kerja remediasi bergantung pada apakah Anda menggunakan paket Lambda dengan mengunggah file zip atau dengan membuat fungsi Lambda dengan gambar kontainer. Setelah memperbarui pustaka, perbarui kode fungsi Lambda untuk menggunakan versi tetap. Setelah itu, gunakan versi yang diperbarui.

Fungsi Lambda memiliki kerentanan perangkat lunak

Fungsi Lambda sering menggunakan pustaka dan dependensi pihak ketiga yang mungkin berisi kerentanan keamanan dengan tingkat keparahan atau eksploitasi yang lebih rendah dibandingkan

dengan kritis. CVEs Meskipun kerentanan non-kritis ini mungkin tidak segera dieksploitasi, mereka masih mewakili kelemahan keamanan yang dapat dirantai bersama dengan kerentanan lain untuk membahayakan fungsi Anda. Seiring waktu, teknik eksploitasi baru mungkin juga muncul yang meningkatkan risiko kerentanan ini. Mengikuti prinsip keamanan standar, kami merekomendasikan untuk menambal kerentanan ini untuk menjaga lingkungan yang aman.

Tinjau bagian Referensi di tab Kerentanan untuk sifat tersebut. Dokumentasi vendor dapat mencakup panduan remediasi khusus. Perbarui pustaka rentan ke versi aman terbaru mereka mengikuti prosedur yang direkomendasikan vendor. Biasanya, alur kerja remediasi bergantung pada apakah Anda menggunakan paket Lambda dengan mengunggah file zip atau dengan membuat fungsi Lambda dengan gambar kontainer. Setelah memperbarui pustaka, perbarui kode fungsi Lambda untuk menggunakan versi tetap. Setelah itu, gunakan versi yang diperbarui.

Memulihkan eksposur untuk fungsi Amazon RDS

Note

Security Hub dalam rilis pratinjau dan dapat berubah sewaktu-waktu.

AWS Security Hub dapat menghasilkan temuan eksposur untuk fungsi Amazon RDS.

Di konsol Security Hub, fungsi Amazon RDS yang terlibat dalam temuan eksposur dan informasi pengenalnya tercantum di bagian Sumber Daya pada detail temuan. Secara terprogram, Anda dapat mengambil detail sumber daya dengan [GetFindingsV2](#) pengoperasian Security Hub API.

Setelah mengidentifikasi sumber daya yang terlibat dalam temuan eksposur, Anda dapat menghapus sumber daya jika Anda tidak membutuhkannya. Menghapus sumber daya yang tidak penting dapat mengurangi profil dan AWS biaya eksposur Anda. Jika sumber daya sangat penting, ikuti langkah-langkah remediasi yang direkomendasikan ini untuk membantu mengurangi risiko. Topik remediasi dibagi berdasarkan jenis sifatnya.

Temuan eksposur tunggal berisi masalah yang diidentifikasi dalam beberapa topik remediasi. Sebaliknya, Anda dapat mengatasi temuan eksposur dan menurunkan tingkat keparahannya dengan hanya membahas satu topik remediasi. Pendekatan Anda terhadap remediasi risiko tergantung pada kebutuhan organisasi dan beban kerja Anda.

 Note

Panduan remediasi yang diberikan dalam topik ini mungkin memerlukan konsultasi tambahan dalam AWS sumber daya lain.

Daftar Isi

- [Ciri salah konfigurasi untuk fungsi Amazon RDS](#)
 - [Instans Amazon RDS DB dikonfigurasi dengan akses publik](#)
 - [Cluster Amazon RDS DB memiliki snapshost yang dibagikan secara publik](#)
 - [Instans Amazon RDS DB memiliki snapshot yang tidak dienkrpsi saat istirahat](#)
 - [Cluster Amazon RDS DB memiliki snapshot yang tidak dienkrpsi saat istirahat](#)
 - [Instans Amazon RDS DB memiliki grup keamanan terbuka](#)
 - [Instans Amazon RDS DB memiliki otentikasi database IAM dinonaktifkan](#)
 - [Instans Amazon RDS DB menggunakan nama pengguna admin default](#)
 - [Cluster Amazon RDS DB menggunakan nama pengguna admin default](#)
 - [Instans Amazon RDS DB memiliki peningkatan versi minor otomatis dinonaktifkan](#)
 - [Instans Amazon RDS DB memiliki pencadangan otomatis dinonaktifkan](#)
 - [Instans Amazon RDS DB memiliki perlindungan penghapusan dinonaktifkan](#)
 - [Cluster Amazon RDS DB memiliki perlindungan penghapusan dinonaktifkan](#)
 - [Instans Amazon RDS DB menggunakan port default untuk mesin database](#)
 - [Instans Amazon RDS DB tidak tercakup oleh paket cadangan](#)

Ciri salah konfigurasi untuk fungsi Amazon RDS

Berikut ini menjelaskan sifat kesalahan konfigurasi dan langkah-langkah remediasi untuk fungsi Amazon RDS.

Instans Amazon RDS DB dikonfigurasi dengan akses publik

Instans Amazon RDS dengan akses publik berpotensi dapat diakses melalui internet melalui titik akhir mereka. Meskipun akses publik terkadang diperlukan untuk fungsionalitas misalnya, konfigurasi ini dapat digunakan sebagai vektor serangan potensial bagi pengguna yang tidak sah untuk mencoba mengakses database Anda. Database yang dapat diakses publik dapat terkena

pemindaian port, serangan brute force, dan upaya eksploitasi. Mengikuti prinsip keamanan standar, kami menyarankan Anda membatasi eksposur publik sumber daya database Anda.

1. Ubah pengaturan akses publik

Dalam temuan eksposur, buka sumber daya dengan hyperlink. Ini akan membuka instans DB yang terpengaruh. Evaluasi apakah instans DB memerlukan aksesibilitas publik berdasarkan arsitektur aplikasi Anda. Untuk informasi selengkapnya, lihat [Menyiapkan akses publik atau pribadi di Amazon RDS](#).

Cluster Amazon RDS DB memiliki snapshot yang dibagikan secara publik

Snapshot publik dapat diakses oleh siapa pun Akun AWS, yang berpotensi mengekspos data sensitif kepada pengguna yang tidak sah. Setiap Akun AWS memiliki izin untuk menyalin snapshot publik ini dan membuat instance DB darinya, yang dapat menyebabkan pelanggaran data atau akses data yang tidak sah. Mengikuti praktik terbaik keamanan, kami sarankan untuk membatasi akses ke snapshot Amazon RDS Anda hanya untuk tepercaya Akun AWS dan organisasi.

1. Konfigurasi snapshot Amazon RDS untuk akses pribadi

Dalam temuan eksposur, buka sumber daya melalui hyperlink. Untuk selengkapnya tentang cara mengubah setelan berbagi snapshot, lihat [Berbagi snapshot di Panduan Pengguna Amazon Aurora](#). Untuk informasi tentang cara berhenti berbagi snapshot, lihat [Menghentikan berbagi snapshot di Panduan Pengguna Amazon Aurora](#).

Instans Amazon RDS DB memiliki snapshot yang tidak dienkripsi saat istirahat

Snapshot instans Amazon RDS DB yang tidak terenkripsi dapat mengekspos data sensitif jika akses tidak sah ke lapisan penyimpanan diperoleh. Tanpa enkripsi, data dalam snapshot berpotensi diekspos melalui akses yang tidak sah. Ini menciptakan risiko pelanggaran data dan pelanggaran kepatuhan. Mengikuti praktik terbaik keamanan, kami sarankan untuk mengenkripsi semua sumber daya database dan cadangannya untuk menjaga kerahasiaan data.

Dalam temuan eksposur, buka sumber daya dengan hyperlink. Ini akan membuka snapshot yang terpengaruh. Anda tidak dapat langsung mengenkripsi snapshot tidak terenkripsi yang ada. Sebagai gantinya, buat salinan terenkripsi dari snapshot yang tidak terenkripsi. Untuk petunjuk mendetail, lihat [penyalinan snapshot cluster DB dan Mengenkripsi sumber daya Amazon RDS](#) di Panduan Pengguna Amazon Aurora. ..

Cluster Amazon RDS DB memiliki snapshot yang tidak dienkripsi saat istirahat

Snapshot kluster Amazon RDS DB yang tidak terenkripsi dapat mengekspos data sensitif jika akses tidak sah ke lapisan penyimpanan diperoleh. Tanpa enkripsi, data dalam snapshot berpotensi diekspos melalui akses yang tidak sah. Ini menciptakan risiko pelanggaran data dan pelanggaran kepatuhan. Mengikuti praktik terbaik keamanan, kami sarankan untuk mengenkripsi semua sumber daya database dan cadangannya untuk menjaga kerahasiaan data.

1. Buat salinan snapshot terenkripsi

Dalam temuan eksposur, buka sumber daya dengan hyperlink. Ini akan membuka snapshot yang terpengaruh. Anda tidak dapat langsung mengenkripsi snapshot tidak terenkripsi yang ada. Sebagai gantinya, buat salinan terenkripsi dari snapshot yang tidak terenkripsi. Untuk petunjuk mendetail, lihat [penyalinan snapshot cluster DB dan Mengenkripsi sumber daya Amazon RDS](#) di Panduan Pengguna Amazon Aurora. ..

Instans Amazon RDS DB memiliki grup keamanan terbuka

Grup keamanan bertindak sebagai firewall virtual untuk instans Amazon RDS Anda untuk mengontrol lalu lintas masuk dan keluar. Grup keamanan terbuka, yang memungkinkan akses tidak terbatas dari alamat IP apa pun, dapat mengekspos instance database Anda ke akses tidak sah dan potensi serangan. Mengikuti prinsip keamanan standar, kami merekomendasikan untuk membatasi akses grup keamanan ke alamat IP dan port tertentu untuk mempertahankan prinsip hak istimewa yang paling rendah.

Tinjau aturan grup keamanan dan nilai konfigurasi saat ini

Dalam temuan eksposur, buka sumber daya untuk Grup Keamanan instans DB. Evaluasi port mana yang terbuka dan dapat diakses dari rentang IP yang luas, seperti (0.0.0.0/0 or ::/0). Untuk informasi tentang melihat detail grup keamanan, lihat [DescribeSecurityGroups](#) di Referensi Amazon Elastic Compute Cloud API.

Ubah aturan grup keamanan

Ubah aturan grup keamanan Anda untuk membatasi akses ke alamat atau rentang IP tepercaya tertentu. Saat memperbarui aturan grup keamanan Anda, pertimbangkan untuk memisahkan persyaratan akses untuk segmen jaringan yang berbeda dengan membuat aturan untuk setiap rentang IP sumber yang diperlukan atau membatasi akses ke port tertentu. Untuk mengubah aturan grup keamanan, lihat [Mengonfigurasi aturan grup keamanan](#) di Panduan EC2 Pengguna Amazon. Untuk mengubah port default instans database Amazon RDS yang ada, lihat [Memodifikasi cluster DB menggunakan konsol, CLI, dan API di](#) Panduan Pengguna Amazon Aurora.

Instans Amazon RDS DB memiliki otentikasi database IAM dinonaktifkan

Autentikasi basis data IAM memungkinkan Anda untuk mengautentikasi ke database Amazon RDS Anda menggunakan kredensi IAM alih-alih kata sandi basis data. Ini memberikan beberapa manfaat keamanan, seperti manajemen akses terpusat, kredensi sementara, dan penghapusan penyimpanan kata sandi database dalam kode aplikasi. Autentikasi basis data IAM memungkinkan otentikasi ke instance database dengan token otentikasi, bukan kata sandi. Akibatnya, lalu lintas jaringan ke dan dari instance database dienkripsi menggunakan SSL. Tanpa autentikasi IAM, database biasanya mengandalkan otentikasi berbasis kata sandi, yang dapat menyebabkan penggunaan kembali kata sandi dan kata sandi yang lemah. Mengikuti praktik terbaik keamanan, kami sarankan untuk mengaktifkan otentikasi database IAM.

Aktifkan autentikasi basis data IAM

Dalam temuan eksposur, buka sumber daya dengan hyperlink. Ini akan membuka instans DB yang terpengaruh. Anda dapat mengaktifkan otentikasi database IAM dalam opsi Database. Untuk informasi selengkapnya, lihat [Mengaktifkan dan menonaktifkan autentikasi database IAM di Panduan Pengguna](#) Amazon RDS. Setelah mengaktifkan otentikasi IAM, perbarui instans DB Anda untuk menggunakan otentikasi IAM alih-alih otentikasi berbasis kata sandi.

Instans Amazon RDS DB menggunakan nama pengguna admin default

Menggunakan nama pengguna default (misalnya, “admin”, “root”) untuk instans DB meningkatkan risiko keamanan karena ini dikenal luas dan umumnya ditargetkan dalam serangan brute force. Nama pengguna default dapat diprediksi dan memudahkan pengguna yang tidak sah untuk mencoba mendapatkan akses ke database Anda. Dengan nama pengguna default, penyerang hanya perlu mendapatkan kata sandi daripada membutuhkan keduanya untuk mendapatkan akses ke database Anda. Mengikuti praktik terbaik keamanan, sebaiknya gunakan nama pengguna administrator unik untuk instans database Anda untuk meningkatkan keamanan melalui ketidakjelasan dan mengurangi risiko upaya akses yang tidak sah.

Konfigurasikan nama pengguna administrator yang unik

Dalam temuan eksposur, buka sumber daya dengan hyperlink. Ini akan membuka instans DB yang terpengaruh. Pertimbangkan frekuensi cadangan, periode retensi, dan aturan siklus hidup yang terbaik untuk aplikasi Anda.

Cluster Amazon RDS DB menggunakan nama pengguna admin default

Menggunakan nama pengguna default (misalnya, “admin”, “root”) untuk instans DB meningkatkan risiko keamanan karena ini dikenal luas dan umumnya ditargetkan dalam serangan brute force.

Nama pengguna default dapat diprediksi dan memudahkan pengguna yang tidak sah untuk mencoba mendapatkan akses ke database Anda. Dengan nama pengguna default, penyerang hanya perlu mendapatkan kata sandi daripada membutuhkan keduanya untuk mendapatkan akses ke database Anda. Mengikuti praktik terbaik keamanan, sebaiknya gunakan nama pengguna administrator unik untuk instans database Anda untuk meningkatkan keamanan melalui ketidakjelasan dan mengurangi risiko upaya akses yang tidak sah.

Konfigurasikan nama pengguna administrator yang unik

Dalam temuan eksposur, buka sumber daya dengan hyperlink. Ini akan membuka instans DB yang terpengaruh. Anda tidak dapat mengubah nama pengguna administrator instans Amazon RDS DB yang ada. Untuk membuat nama administrator yang unik, Anda perlu membuat instans DB baru dengan nama pengguna khusus dan memigrasikan data Anda.

Instans Amazon RDS DB memiliki peningkatan versi minor otomatis dinonaktifkan

Upgrade versi minor otomatis memastikan bahwa instans Amazon RDS Anda secara otomatis menerima upgrade versi mesin minor saat tersedia. Upgrade ini sering kali mencakup patch keamanan penting dan perbaikan bug yang membantu menjaga keamanan dan stabilitas database Anda. Database Anda berisiko berjalan dengan kerentanan keamanan yang diketahui yang telah diperbaiki dalam versi minor yang lebih baru. Tanpa pembaruan otomatis, instance database dapat mengakumulasi kerentanan keamanan saat baru CVEs ditemukan. Mengikuti praktik terbaik keamanan, sebaiknya aktifkan pemutakhiran versi minor otomatis untuk semua instans Amazon RDS.

Aktifkan upgrade versi minor otomatis

Dalam temuan eksposur, buka sumber daya dengan hyperlink. Ini akan membuka instans DB yang terpengaruh. Anda dapat melihat pengaturan pemutakhiran kecil otomatis di tab Pemeliharaan & pencadangan. Untuk informasi selengkapnya, lihat [Upgrade versi minor otomatis untuk Amazon RDS](#) for MySQL. Anda juga dapat mengonfigurasi jendela pemeliharaan agar terjadi selama periode aktivitas database rendah.

Instans Amazon RDS DB memiliki pencadangan otomatis dinonaktifkan

Pencadangan otomatis menyediakan point-in-time pemulihan untuk instans Amazon RDS Anda, memungkinkan Anda memulihkan database ke titik mana pun dalam periode retensi Anda. Saat pencadangan otomatis dinonaktifkan, Anda berisiko kehilangan data jika terjadi penghapusan berbahaya, korupsi data, atau skenario kehilangan data lainnya. Jika terjadi aktivitas berbahaya

seperti serangan ransomware, penghapusan tabel database, atau korupsi, kemampuan untuk mengembalikan ke titik waktu sebelum insiden mengurangi waktu yang diperlukan untuk pulih dari suatu insiden. [Mengikuti praktik terbaik keamanan, kami merekomendasikan untuk mengaktifkan pencadangan otomatis dengan periode retensi yang sesuai untuk semua basis data produksi.](#)

Instans Amazon RDS DB memiliki perlindungan penghapusan dinonaktifkan

Perlindungan penghapusan database adalah fitur yang membantu mencegah penghapusan instance database Anda. Ketika perlindungan penghapusan dinonaktifkan, database Anda dapat dihapus oleh setiap pengguna dengan izin yang cukup, berpotensi mengakibatkan kehilangan data atau downtime aplikasi. Penyerang dapat menghapus database Anda, yang menyebabkan gangguan layanan, kehilangan data, dan peningkatan waktu pemulihan. Mengikuti praktik terbaik keamanan, sebaiknya aktifkan perlindungan penghapusan untuk instans RDS DB Anda untuk mencegah penghapusan berbahaya.

Aktifkan perlindungan hapus untuk cluster Amazon RDS DB Anda

Dalam temuan eksposur, buka sumber daya dengan hyperlink. Ini akan membuka cluster DB yang terpengaruh.

Cluster Amazon RDS DB memiliki perlindungan penghapusan dinonaktifkan

Perlindungan penghapusan database adalah fitur yang membantu mencegah penghapusan instance database Anda. Ketika perlindungan penghapusan dinonaktifkan, database Anda dapat dihapus oleh setiap pengguna dengan izin yang cukup, berpotensi mengakibatkan kehilangan data atau downtime aplikasi. Penyerang dapat menghapus database Anda, yang menyebabkan gangguan layanan, kehilangan data, dan peningkatan waktu pemulihan. Mengikuti praktik terbaik keamanan, sebaiknya aktifkan perlindungan penghapusan untuk klaster RDS DB Anda untuk mencegah penghapusan berbahaya.

Aktifkan perlindungan hapus untuk cluster Amazon RDS DB Anda

Dalam temuan eksposur, buka sumber daya dengan hyperlink. Ini akan membuka cluster DB yang terpengaruh.

Instans Amazon RDS DB menggunakan port default untuk mesin database

Instans Amazon RDS yang menggunakan port default untuk mesin database mungkin menghadapi peningkatan risiko keamanan, karena port default ini dikenal luas dan sering ditargetkan oleh alat pemindaian otomatis. Memodifikasi instans DB Anda untuk menggunakan port non-default

menambahkan lapisan keamanan tambahan melalui ketidakjelasan, sehingga lebih sulit bagi pengguna yang tidak sah untuk melakukan serangan otomatis atau ditargetkan pada database Anda. Port default biasanya dipindai oleh orang yang tidak berwenang, dan dapat menyebabkan instans DB Anda ditargetkan. Mengikuti praktik terbaik keamanan, kami sarankan untuk mengubah port default ke port khusus untuk mengurangi risiko serangan otomatis atau tertarget.

Dalam temuan eksposur, buka sumber daya dengan hyperlink. Ini akan membuka instans DB yang terpengaruh.

Perbarui string koneksi aplikasi

Setelah mengubah port, perbarui semua aplikasi dan layanan yang terhubung ke instans Amazon RDS Anda untuk menggunakan nomor port baru.

Instans Amazon RDS DB tidak tercakup oleh paket cadangan

AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya yang memusatkan dan mengotomatiskan pencadangan data di seluruh. Layanan AWS Jika instans DB Anda tidak tercakup oleh rencana cadangan, Anda berisiko kehilangan data jika terjadi penghapusan berbahaya, korupsi data, atau skenario kehilangan data lainnya. Jika terjadi aktivitas berbahaya seperti serangan ransomware, penghapusan tabel database, atau korupsi, kemampuan untuk mengembalikan ke titik waktu sebelum insiden mengurangi waktu yang diperlukan untuk pulih dari suatu insiden. Mengikuti praktik terbaik keamanan, sebaiknya sertakan instans Amazon RDS Anda dalam paket cadangan untuk memastikan perlindungan data.

Buat dan tetapkan rencana cadangan untuk instans DB Anda

Dalam temuan eksposur, buka sumber daya dengan hyperlink. Ini akan membuka instans DB yang terpengaruh. Pertimbangkan frekuensi cadangan, periode retensi, dan aturan siklus hidup yang terbaik untuk aplikasi Anda.

Memulihkan eksposur untuk ember Amazon S3

 Note

Security Hub dalam rilis pratinjau dan dapat berubah sewaktu-waktu.

AWS Security Hub dapat menghasilkan temuan eksposur untuk bucket Amazon Simple Storage Service (S3).

Di konsol Security Hub, bucket Amazon S3 yang terlibat dalam temuan eksposur dan informasi pengenalannya tercantum di bagian Sumber Daya pada detail temuan. Secara terprogram, Anda dapat mengambil detail sumber daya dengan [GetFindingsV2](#) pengoperasian Security Hub API.

Setelah mengidentifikasi sumber daya yang terlibat dalam temuan eksposur, Anda dapat menghapus sumber daya jika Anda tidak membutuhkannya. Menghapus sumber daya yang tidak penting dapat mengurangi profil dan AWS biaya eksposur Anda. Jika sumber daya sangat penting, ikuti langkah-langkah remediasi yang direkomendasikan ini untuk membantu mengurangi risiko. Topik remediasi dibagi berdasarkan jenis sifatnya.

Temuan eksposur tunggal berisi masalah yang diidentifikasi dalam beberapa topik remediasi. Sebaliknya, Anda dapat mengatasi temuan eksposur dan menurunkan tingkat keparahannya dengan hanya membahas satu topik remediasi. Pendekatan Anda terhadap remediasi risiko tergantung pada kebutuhan organisasi dan beban kerja Anda.

 Note

Panduan remediasi yang diberikan dalam topik ini mungkin memerlukan konsultasi tambahan dalam AWS sumber daya lain.

Daftar Isi

- [Ciri salah konfigurasi untuk bucket Amazon S3](#)
 - [Bucket Amazon S3 menonaktifkan versi](#)
 - [Bucket Amazon S3 menonaktifkan Object Lock](#)
 - [Bucket Amazon S3 tidak dienkripsi saat istirahat dengan kunci AWS KMS](#)
 - [Penghapusan otentikasi multi-faktor \(MFA\) dinonaktifkan pada bucket Amazon S3 berversi](#)
 - [Bucket Amazon S3 memungkinkan prinsipal dari akun lain AWS untuk mengubah izin bucket](#)
- [Ciri-ciri jangkauan untuk bucket Amazon S3](#)
 - [Bucket Amazon S3 memiliki akses publik](#)
 - [Bucket Amazon S3 memiliki akses baca publik](#)
 - [Bucket Amazon S3 memiliki akses tulis](#)
 - [Jalur akses Amazon S3 memiliki pengaturan akses publik yang diaktifkan](#)
- [Ciri data sensitif untuk bucket Amazon S3](#)
 - [Ciri data sensitif untuk bucket Amazon S3](#)

Ciri salah konfigurasi untuk bucket Amazon S3

Berikut adalah ciri kesalahan konfigurasi untuk bucket Amazon S3 dan langkah-langkah perbaikan yang disarankan.

Bucket Amazon S3 menonaktifkan versi

Amazon S3 Versioning membantu Anda menyimpan beberapa varian objek dalam bucket yang sama. Saat pembuatan versi dinonaktifkan, Amazon S3 hanya menyimpan versi terbaru dari setiap objek, yang berarti bahwa jika objek secara tidak sengaja atau jahat dihapus atau ditimpa, mereka tidak dapat dipulihkan. Bucket berkemampuan versi memberikan perlindungan terhadap penghapusan yang tidak disengaja, kegagalan aplikasi, dan insiden keamanan seperti serangan ransomware, di mana modifikasi atau penghapusan data yang tidak sah dapat terjadi. Mengikuti praktik terbaik keamanan, sebaiknya aktifkan pembuatan versi untuk bucket yang berisi data penting yang sulit atau tidak mungkin dibuat ulang jika hilang.

1. Mengaktifkan pembuatan versi — Untuk mengaktifkan Pembuatan Versi Amazon S3 pada bucket, [lihat Mengaktifkan pembuatan versi pada bucket di Panduan Pengguna Layanan Penyimpanan Sederhana](#) Amazon. Saat mengaktifkan pembuatan versi, pertimbangkan untuk menerapkan aturan siklus hidup untuk mengelola penyimpanan, karena pembuatan versi akan mempertahankan banyak salinan objek.

Bucket Amazon S3 menonaktifkan Object Lock

Amazon S3 Object Lock menyediakan model write-once-read-many (WORM) untuk objek Amazon S3, mencegahnya dihapus atau ditimpa untuk jangka waktu tertentu atau tanpa batas waktu. Ketika Object Lock dinonaktifkan, objek Anda bisa rentan terhadap penghapusan, modifikasi, atau enkripsi yang tidak disengaja atau berbahaya oleh ransomware. Object Lock sangat penting untuk memenuhi persyaratan peraturan yang menuntut penyimpanan data yang tidak dapat diubah dan untuk perlindungan terhadap ancaman canggih seperti ransomware yang mungkin mencoba mengenkripsi data Anda. Dengan mengaktifkan Object Lock, Anda dapat menerapkan kebijakan retensi sebagai lapisan perlindungan data tambahan dan membuat strategi pencadangan yang tidak dapat diubah untuk data penting Anda. Mengikuti praktik terbaik keamanan, kami sarankan Anda mengaktifkan Object Lock untuk mencegah modifikasi berbahaya pada objek Anda.

1. Perhatikan bahwa Object Lock hanya dapat diaktifkan saat membuat bucket baru, jadi Anda perlu membuat bucket baru dengan Object Lock diaktifkan. Untuk migrasi besar, pertimbangkan untuk menggunakan Operasi Batch untuk menyalin objek ke bucket baru. Sebelum Anda mengunci objek apa pun, Anda juga harus mengaktifkan Amazon S3 Versioning dan Object Lock pada

bucket. Karena Object Lock hanya dapat diaktifkan pada bucket baru, Anda harus memigrasikan data yang ada ke bucket baru dengan Object Lock diaktifkan. Mengonfigurasi Kunci Objek Amazon S3 — Untuk informasi tentang cara mengonfigurasi Kunci Objek pada bucket, lihat [Kunci ConfiguringAmazon S3Object di Panduan Pengguna](#) Layanan Penyimpanan Sederhana Amazon. Setelah mengatur Object Lock, pilih mode retensi yang sesuai dengan lingkungan Anda.

Bucket Amazon S3 tidak dienkripsi saat istirahat dengan kunci AWS KMS

Amazon S3 menerapkan enkripsi sisi server dengan kunci terkelola Amazon S3 sebagai tingkat enkripsi default untuk semua bucket baru. Meskipun kunci terkelola Amazon S3 memberikan perlindungan enkripsi yang kuat, kunci ini tidak menawarkan tingkat kontrol akses dan kemampuan audit yang sama dengan kunci. AWS Key Management Service Saat menggunakan kunci KMS, akses ke objek memerlukan izin ke bucket Amazon S3 dan kunci KMS yang mengenkripsi objek. Ini sangat penting untuk data sensitif di mana Anda memerlukan kontrol terperinci atas siapa yang dapat mengakses objek terenkripsi dan pencatatan audit komprehensif penggunaan kunci enkripsi. Mengikuti praktik terbaik keamanan, sebaiknya gunakan kunci KMS untuk mengenkripsi bucket yang berisi data sensitif atau untuk lingkungan dengan persyaratan kepatuhan yang ketat.

1. Konfigurasi kunci bucket Amazon S3

Untuk mengonfigurasi bucket agar menggunakan kunci bucket Amazon S3 untuk objek baru, lihat [Mengonfigurasi bucket untuk menggunakan Kunci Bucket Amazon S3 dengan SSE-KMS untuk objek baru di](#) Panduan Pengguna Layanan Penyimpanan Sederhana Amazon. Untuk informasi tentang cara mengenkripsi objek yang ada, lihat [Mengenkripsi objek dengan Operasi Batch Amazon S3](#) di Blog Penyimpanan. AWS

Saat menerapkan AWS KMS enkripsi, pertimbangkan hal berikut:

- Manajemen kunci — Tentukan apakah akan menggunakan kunci AWS terkelola atau kunci yang dikelola pelanggan (CMK). CMKs menawarkan pelanggan kontrol penuh atas siklus hidup dan penggunaan kunci mereka. Untuk informasi selengkapnya tentang perbedaan antara kedua jenis kunci ini, lihat [kunci AWS KMS](#) di Panduan AWS Key Management Service Pengembang.
- Rotasi kunci - Untuk langkah-langkah keamanan tambahan, aktifkan rotasi tombol otomatis untuk kunci KMS Anda. Untuk informasi selengkapnya, lihat [Mengaktifkan rotasi kunci otomatis](#) di Panduan AWS Key Management Service Pengembang.

Penghapusan otentikasi multi-faktor (MFA) dinonaktifkan pada bucket Amazon S3 berversi

Penghapusan autentikasi multi-faktor (MFA) memberikan lapisan keamanan tambahan untuk bucket Amazon S3 Anda. Ini membutuhkan otentikasi multi-faktor untuk operasi Amazon S3 yang merusak. Saat penghapusan MFA dinonaktifkan, pengguna dengan izin yang sesuai dapat menghapus versi objek secara permanen atau menanggukuhkan pembuatan versi di bucket Anda tanpa tantangan autentikasi tambahan. Mengaktifkan penghapusan MFA membantu melindungi dari penghapusan data Anda yang tidak sah atau tidak disengaja, memberikan perlindungan yang ditingkatkan terhadap serangan ransomware, ancaman orang dalam, dan kesalahan operasional. Penghapusan MFA sangat berharga untuk bucket yang berisi data kritis atau sensitif kepatuhan yang harus dilindungi dari penghapusan yang tidak sah. Mengikuti praktik terbaik keamanan, sebaiknya aktifkan MFA untuk bucket Amazon S3 Anda.

1. Tinjau jenis MFA

AWS mendukung jenis [MFA](#) berikut. Meskipun otentikasi dengan perangkat fisik biasanya memberikan perlindungan keamanan yang lebih ketat, menggunakan semua jenis MFA lebih aman daripada menonaktifkan MFA.

2. Menegakkan MFA di tingkat kebijakan sumber daya

Gunakan kunci `aws:MultiFactorAuthAge` kondisi dalam kebijakan bucket untuk meminta MFA untuk operasi sensitif. Untuk informasi selengkapnya, lihat [Memerlukan MFA](#) di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

3. Aktifkan MFA

Untuk mengaktifkan penghapusan MFA, pertama-tama, pastikan pembuatan versi diaktifkan di bucket Amazon S3 Anda. Penghapusan MFA hanya didukung pada bucket yang mengaktifkan versi. Untuk informasi tentang cara mengaktifkan versi Amazon S3, lihat [Mengaktifkan pembuatan versi pada bucket di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon](#). Penghapusan MFA tidak dapat diaktifkan melalui konsol Amazon S3. Anda harus menggunakan Amazon S3 API atau AWS CLI Untuk informasi selengkapnya, lihat [Mengonfigurasi penghapusan MFA](#) di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

Bucket Amazon S3 memungkinkan prinsipal dari akun lain AWS untuk mengubah izin bucket

Kebijakan bucket Amazon S3 mengontrol akses ke bucket dan objek. Jika kebijakan bucket mengizinkan prinsipal dari AWS akun lain untuk mengubah izin bucket, pengguna yang tidak sah dapat mengonfigurasi ulang bucket Anda. Jika kredensial utama eksternal dikompromikan, pengguna

yang tidak memiliki hak atas bucket Anda dapat memperoleh kendali atas bucket Anda, yang menyebabkan pelanggaran data atau gangguan layanan. Mengikuti prinsip keamanan standar, AWS merekomendasikan agar Anda membatasi tindakan manajemen izin hanya untuk prinsipal terpercaya.

1. Meninjau dan mengidentifikasi kebijakan bucket

Dalam eksposur, identifikasi bucket Amazon S3 di bidang ARN. Di konsol Amazon S3, pilih bucket, lalu arahkan ke tab Izin untuk meninjau kebijakan bucket. Tinjau kebijakan izin yang dilampirkan pada bucket. Cari pernyataan kebijakan yang memberikan tindakan seperti `s3:PutBucketPolicy`, `s3:PutBucketAcl`, `s3:DeleteBucketPolicy`, `s3:*` atau pernyataan kebijakan yang memungkinkan akses ke prinsipal di luar akun Anda, sebagaimana dilambangkan dalam pernyataan utama.

2. Ubah kebijakan bucket

Ubah kebijakan bucket untuk menghapus atau membatasi tindakan yang diberikan ke AWS akun lain:

- Hapus pernyataan kebijakan yang memberikan tindakan pengelolaan izin akun eksternal.
- Jika akses lintas akun diperlukan, ganti izin luas (`s3:*`) dengan tindakan spesifik yang tidak menyertakan manajemen izin bucket.

Untuk informasi tentang memodifikasi kebijakan bucket, lihat [Menambahkan kebijakan bucket menggunakan konsol Amazon S3](#) di Panduan Pengguna Amazon S3.

Ciri-ciri jangkauan untuk bucket Amazon S3

Berikut adalah ciri-ciri jangkauan untuk bucket Amazon S3 dan langkah-langkah remediasi yang disarankan.

Bucket Amazon S3 memiliki akses publik

Secara default, ember dan objek Amazon S3 bersifat pribadi, tetapi dapat dipublikasikan melalui berbagai konfigurasi. Jika Anda mengubah kebijakan bucket, kebijakan titik akses, atau izin objek untuk mengizinkan akses publik, Anda berisiko mengekspos data sensitif.

1. Nilai ember

Menilai apakah bucket Anda dapat dibuat pribadi berdasarkan kebijakan organisasi Anda, persyaratan kepatuhan, atau klasifikasi data. Jika Anda tidak berniat memberikan akses bucket ke publik atau lainnya Akun AWS, ikuti instruksi remediasi yang tersisa.

2. Konfigurasi bucket menjadi pribadi

Pilih salah satu opsi berikut untuk mengonfigurasi akses pribadi untuk bucket Amazon S3 Anda:

- Tingkat akun — Untuk memblokir akses publik untuk semua bucket di akun Anda menggunakan setelan tingkat akun, lihat [Mengonfigurasi blokir setelan akses publik untuk akun Anda di Panduan Pengguna](#) Layanan Penyimpanan Sederhana Amazon.
- Tingkat bucket — Untuk memblokir akses publik untuk bucket tertentu, lihat [Mengonfigurasi setelan blokir akses publik untuk Bucket Amazon S3 Buckets Anda](#) di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.
- Bucket ACL atau kebijakan — Untuk mengubah daftar kontrol akses bucket (ACL), kebijakan bucket, kebijakan Titik Akses Multi-Wilayah (MRAP), atau kebijakan titik akses untuk menghapus akses publik ke bucket, lihat [Meninjau dan mengubah akses bucket di](#) Panduan Pengguna Layanan Penyimpanan Sederhana Amazon. Jika Anda memblokir akses publik di tingkat akun atau tingkat bucket, blok tersebut lebih diutamakan daripada kebijakan yang mengizinkan akses publik.

Bucket Amazon S3 memiliki akses baca publik

Bucket Amazon S3 dengan akses baca publik memungkinkan siapa pun di internet untuk melihat konten bucket Anda. Meskipun ini mungkin diperlukan untuk situs web yang dapat diakses publik atau sumber daya bersama, hal ini dapat menimbulkan risiko keamanan jika bucket berisi data sensitif. Akses baca publik dapat menyebabkan tampilan dan pengunduhan yang tidak sah, yang dapat menyebabkan pelanggaran data jika data sensitif disimpan dalam ember tersebut. Mengikuti prinsip keamanan standar, AWS merekomendasikan untuk membatasi akses ke bucket Amazon S3 untuk pengguna dan sistem yang diperlukan.

1. Blokir akses publik di tingkat bucket

Amazon S3 menyediakan pengaturan Blokir Akses Publik yang dapat dikonfigurasi di tingkat bucket dan akun untuk mencegah akses publik terlepas dari kebijakan bucket atau ACLs. Untuk informasi selengkapnya, lihat [Memblokir akses publik ke penyimpanan Amazon S3 Anda](#) di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon. Setelah memblokir akses publik, tinjau konfigurasi kontrol akses bucket Anda untuk memastikannya selaras dengan persyaratan akses Anda. Kemudian tinjau kebijakan bucket Amazon S3 Anda untuk menentukan secara eksplisit siapa yang dapat mengakses bucket Anda. Untuk contoh kebijakan bucket, lihat [Contoh kebijakan bucket Amazon S3 di](#) Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

2. Metode akses alternatif

Jika akses baca publik diperlukan, pertimbangkan alternatif yang lebih aman ini:

- CloudFront— Gunakan CloudFront dengan Origin Access Identity (OAI) atau Origin Access Control (OAC) untuk mengizinkan akses baca dari bucket Amazon S3 pribadi. Alternatif ini membatasi akses langsung ke bucket Amazon S3 Anda sambil memungkinkan konten dapat diakses publik melalui CloudFront. Untuk informasi selengkapnya, lihat [Membatasi akses ke asal Amazon S3 Amazon](#) di Panduan Pengembang CloudFront Amazon.
- Presigned URLs — Gunakan presigned URLs untuk akses sementara ke objek tertentu. Untuk informasi selengkapnya, lihat [Berbagi objek dengan presigned URLs](#) di Panduan AWS Amazon S3 User.

Bucket Amazon S3 memiliki akses tulis

Bucket Amazon S3 dengan akses tulis publik memungkinkan siapa pun di internet untuk mengunggah, memodifikasi, atau menghapus objek di bucket Anda. Ini menciptakan risiko keamanan yang signifikan, termasuk potensi seseorang untuk mengunggah file berbahaya, memodifikasi file yang ada, dan menghapus data. Akses tulis publik menciptakan kerentanan keamanan yang dapat dieksploitasi oleh penyerang. Mengikuti prinsip keamanan standar, AWS merekomendasikan untuk membatasi akses tulis ke bucket Amazon S3 Anda hanya untuk pengguna dan sistem yang diperlukan.

1. Blokir akses publik di tingkat akun dan bucket

Amazon S3 menyediakan setelan blokir akses publik yang dapat dikonfigurasi di tingkat bucket dan akun untuk mencegah akses publik terlepas dari kebijakan bucket atau ACLs. Untuk informasi selengkapnya, lihat [Memblokir akses publik ke penyimpanan Amazon S3 Anda](#) di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

2. Ubah kebijakan bucket

Untuk pendekatan yang lebih terperinci untuk menghapus akses tulis publik, tinjau kebijakan bucket. Anda dapat mencari `s3:PutObject`, `s3:DeleteObject`, atau `s3:*`. Untuk informasi selengkapnya tentang mengelola kebijakan bucket, lihat [Kebijakan Bucket untuk Amazon S3](#) di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

3. Metode akses alternatif Jika akses baca publik diperlukan, pertimbangkan alternatif yang lebih aman ini:

- CloudFront— Gunakan CloudFront dengan Origin Access Identity (OAI) atau Origin Access Control (OAC) untuk mengizinkan akses baca dari bucket Amazon S3 pribadi. Alternatif ini

membatasi akses langsung ke bucket Amazon S3 Anda sambil memungkinkan konten dapat diakses publik melalui CloudFront. Untuk informasi selengkapnya, lihat [Membatasi akses ke asal Amazon S3](#) di Panduan Pengembang CloudFront Amazon.

- Presigned URLs — Gunakan presigned URLs untuk akses sementara ke objek tertentu. Untuk informasi selengkapnya, lihat [Berbagi objek dengan presigned URLs](#) di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

Jalur akses Amazon S3 memiliki pengaturan akses publik yang diaktifkan

Jalur akses Amazon S3 menyediakan akses khusus ke kumpulan data bersama di bucket Amazon S3. Ketika Anda mengaktifkan akses publik untuk titik akses, siapa pun di internet untuk mengakses data Anda. Mengikuti prinsip keamanan standar, AWS merekomendasikan untuk membatasi akses publik ke jalur akses Amazon S3.

1. Buat titik akses baru dengan mengaktifkan akses publik blok

Amazon S3 tidak mendukung perubahan pengaturan akses publik titik akses setelah titik akses dibuat. Untuk informasi tentang membuat jalur akses, lihat [Mengelola akses publik ke titik akses untuk bucket tujuan umum](#) di Panduan Pengguna Amazon S3. Untuk informasi selengkapnya tentang mengelola akses publik ke titik akses, lihat [Membuat titik akses untuk bucket tujuan umum](#) di Panduan Pengguna Amazon S3.

Ciri data sensitif untuk bucket Amazon S3

Berikut adalah ciri data sensitif untuk bucket Amazon S3 dan langkah-langkah perbaikan yang disarankan.

Ciri data sensitif untuk bucket Amazon S3

Saat Macie mengidentifikasi data sensitif di bucket Amazon S3 Anda, ini menunjukkan potensi eksposur keamanan dan kepatuhan yang memerlukan perhatian segera.

Data sensitif dapat mencakup:

- Kredensial
- Informasi pengenalan pribadi
- Informasi keuangan
- Konten rahasia yang membutuhkan perlindungan

Jika data sensitif diekspos melalui kesalahan konfigurasi atau akses yang tidak sah, hal itu dapat menyebabkan pelanggaran kepatuhan, pelanggaran data, pencurian identitas, atau kerugian finansial. Mengikuti praktik terbaik keamanan, AWS merekomendasikan klasifikasi data yang tepat dan pemantauan terus menerus terhadap data sensitif di bucket Amazon S3 Anda.

Menerapkan kontrol untuk data sensitif

Dalam temuan eksposur, pilih sumber daya Terbuka. Tinjau jenis data sensitif yang terdeteksi dan lokasinya di bucket. Untuk bantuan menafsirkan temuan Macie, lihat [Jenis temuan Macie di Panduan Pengguna](#) Amazon Macie.

Berdasarkan jenis data sensitif yang ditemukan, terapkan kontrol keamanan yang sesuai:

- Batasi akses ke bucket — Tinjau izin bucket untuk memastikan izin tersebut mengikuti prinsip hak istimewa paling sedikit. Gunakan kebijakan IAM, kebijakan bucket, dan ACLs untuk membatasi akses. Untuk informasi selengkapnya, lihat [Identity and Access Management untuk Amazon S3](#) di Panduan Pengguna Amazon Simple Storage Service.
- Aktifkan enkripsi sisi server - Aktifkan enkripsi sisi server dengan kunci KMS untuk perlindungan tambahan. Untuk informasi selengkapnya, lihat [Menggunakan enkripsi sisi server dengan kunci KMS \(AWS SSE-KMS\)](#) di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.
- Gunakan AWS Glue DataBrew — Gunakan Glue DataBrew untuk persiapan dan pembersihan data. Untuk informasi selengkapnya, lihat [Apa yang ada AWS Glue DataBrew](#) di Panduan AWS Glue DataBrew Pengembang.

Temuan urutan serangan di Security Hub

Note

Security Hub dalam rilis pratinjau dan dapat berubah sewaktu-waktu.

[Urutan serangan](#) adalah jenis ancaman keamanan. GuardDuty menghasilkan temuan untuk urutan serangan ketika peristiwa cocok dengan pola aktivitas yang mencurigakan. Jika Anda [mengaktifkan GuardDuty](#), Anda dapat mengakses jenis temuan ini di konsol Security Hub. Ini memungkinkan Anda untuk menyelidiki dan memulihkan semua ancaman keamanan Anda tanpa beralih konsol. Anda dapat meninjau temuan urutan serangan dari layar Ancaman konsol Security Hub.

Meninjau temuan urutan serangan

Note

Security Hub dalam rilis pratinjau dan dapat berubah sewaktu-waktu.

Anda dapat meninjau temuan urutan serangan dari layar Ancaman konsol Security Hub. Topik berikut menjelaskan bagaimana Anda meninjau detail untuk menemukan urutan serangan.

Meninjau detail untuk temuan urutan serangan

Note

Security Hub dalam rilis pratinjau dan dapat berubah sewaktu-waktu.

Topik ini menjelaskan cara meninjau detail tentang temuan urutan serangan di konsol Security Hub dan dengan API.

Meninjau detail untuk urutan serangan di konsol Security Hub

Berikut ini menjelaskan cara meninjau detail untuk urutan serangan di konsol Security Hub:

Untuk meninjau temuan urutan serangan di konsol

1. [Masuk menggunakan kredensial Anda, dan buka konsol Security Hub di https://console.aws.amazon.com/securityhub/v2/home?wilayah=us-timur-1](https://console.aws.amazon.com/securityhub/v2/home?wilayah=us-timur-1).
2. Dari panel navigasi, pilih Ancaman.
3. Dari daftar temuan urutan serangan, pilih temuan urutan serangan yang ingin Anda lihat detailnya.

Meninjau detail untuk temuan urutan serangan dengan API

Anda dapat meninjau temuan urutan serangan dengan [GetFindingsV2](#) API atau AWS CLI. Anda dapat memfilter hasil dengan [FindingProviderFields](#) parameter dan dengan memberikan nilai filter TTPs/AttackSequence jika Anda hanya ingin mengembalikan temuan urutan serangan. Anda dapat memfilter berdasarkan bidang lain untuk mempersempit hasil.

Perintah contoh

Berikut ini adalah AWS CLI contoh yang mengambil 10 temuan urutan serangan yang paling baru dihasilkan di akun Anda. Contoh diformat untuk Linux, macOS, dan Unix, dan karakter garis miring terbalik (\) digunakan untuk meningkatkan keterbacaan.

```
$ aws securityhub get-findings-v2 \
--filters '{"FindingProviderFieldsTypes":[{"Value": "TTPs/AttackSequence", "Comparison": "PREFIX"}]}' \
--sort-criteria '{ "Field": "LastObservedAt", "SortOrder": "desc" }' \
--max-items 10
```

Remediasi temuan urutan serangan

Note

Security Hub dalam rilis pratinjau dan dapat berubah sewaktu-waktu.

Untuk informasi tentang remediasi temuan urutan serangan, lihat [Memperbaiki temuan GuardDuty keamanan yang terdeteksi](#) di GuardDuty Panduan Pengguna Amazon.

Aturan otomatisasi di Security Hub

Note

Security Hub dalam rilis pratinjau dan dapat berubah sewaktu-waktu.

Aturan otomatisasi Security Hub adalah versi yang lebih dapat diperluas dan dikonfigurasi dari aturan otomatisasi [CSPM Security Hub](#). Security Hub berevolusi dari sistem otomatisasi khusus penemuan menjadi platform konfigurasi yang lebih luas. Sementara Security Hub CSPM mendukung ASFF, Security Hub memperkenalkan dukungan untuk OCSF dan menetapkan dasar untuk lebih banyak konfigurasi. Salah satu fitur utama aturan otomatisasi untuk Security Hub adalah integrasinya dengan konfigurasi agregator. Ini menawarkan kemampuan untuk menyempurnakan dan menerapkan konfigurasi secara terperinci ke serangkaian tautan Wilayah AWS sambil mempertahankan fleksibilitas untuk mengatur pengalaman Regional melalui unlinked satu per satu. Wilayah AWS

Sumber daya Security Hub di Anda Akun AWS dan Wilayah AWS, termasuk aturan otomatisasi, konektor, dan agregator akan berhenti bekerja dalam skenario di bawah ini.

- Standalone Akun AWS menjadi anggota AWS organisasi dengan admin yang didelegasikan
- Akun manajemen AWS organisasi menghapus administrator yang didelegasikan untuk organisasi dan menetapkan administrator yang didelegasikan baru
- Konfigurasi agregator administrator yang didelegasikan atau mandiri diubah untuk membuat wilayah yang tidak Akun AWS ditautkan menjadi wilayah tertaut

Dalam skenario ini, akun anggota masih dapat mengelola sumber daya ini melalui daftar, mendapatkan, dan menghapus operasi di AWS CLI satu-satunya. Ketika wilayah yang tidak ditautkan dibuat sebagai wilayah tertaut, admin yang didelegasikan atau AWS akun mandiri masih dapat mengelola sumber daya lama di wilayah tertaut melalui operasi daftar, dapatkan, dan hapus.

Penyempurnaan Utama

Aturan otomatisasi di Security Hub CSPM bersifat Regional dan hanya berlaku untuk temuan di Wilayah AWS tempat pembuatannya. Aturan otomatisasi di Security Hub dapat dikonfigurasi sekali di Wilayah AWS (Wilayah agregasi) dan kemudian diterapkan di semua yang dikonfigurasi Wilayah AWS (Wilayah tertaut) melalui pengaturan Agregator V2. Salah satu manfaat dari fitur ini adalah kemampuan untuk mengotomatisasi dan memulihkan temuan keamanan dalam beberapa Wilayah AWS hanya dengan menyiapkannya. Wilayah AWS Ini berarti bahwa, jika temuan dihasilkan di Wilayah tertaut, itu dapat diperbaiki secara otomatis berdasarkan konfigurasi Wilayah agregasi.

Integrasi Eksternal

Aturan otomatisasi di Security Hub mendukung jenis tindakan untuk pembuatan tiket ITSM. Hal ini memungkinkan pelanggan untuk merutekan temuan OCSF tertentu secara langsung ke satu atau lebih integrasi ITSM yang dikonfigurasi. Jika temuan OCSF cocok dengan kriteria, Anda dapat membuat tiket di Jira Cloud atau ServiceNow ITSM Untuk informasi selengkapnya, lihat [Integrasi pihak ketiga untuk Security Hub](#).

Kriteria yang didukung OCSF

Security Hub CSPM mendukung evaluasi bidang ASFF pada temuan sementara Security Hub cocok dengan bidang OCSF. Misalnya, kumpulan filter yang didukung untuk Criteria parameter yang digunakan dalam aturan otomatisasi V2 cocok dengan kumpulan filter yang didukung untuk

Criteria parameter yang digunakan [GetFindingsV2](#). Ini berarti filter yang digunakan untuk mengambil temuan V2 dapat digunakan dalam aturan otomatisasi V2 yang cocok dengan temuan.

Bidang OCSF untuk **AutomationRulesFindingFieldsUpdate**

Daftar bidang yang dapat diperbarui [AutomationRulesFindingFieldsUpdate](#) di Security Hub CSPM telah berubah di Security Hub. Untuk [AutomationRulesFindingFieldsUpdateV2](#) daftar bidang yang dapat diperbarui termasuk yang berikut ini:

- Comment
- SeverityId
- StatusId

Integrasi pihak ketiga untuk Security Hub

Note

Security Hub dalam rilis pratinjau dan dapat berubah sewaktu-waktu.

Anda dapat meningkatkan postur keamanan Anda dengan integrasi pihak ketiga untuk AWS Security Hub. Dengan fitur ini, Anda dapat mengonfigurasi integrasi untuk membuat insiden atau masalah untuk temuan Security Hub.

Buat kunci KMS untuk mengenkripsi kredensial

Prosedur integrasi di bagian ini memberi Anda opsi untuk mengenkripsi kredensial Anda dengan kunci yang AWS dimiliki atau kunci yang dikelola pelanggan. Kunci yang AWS dimiliki adalah kunci KMS yang tidak ada di Akun AWS karena AWS layanan yang mengenkripsi kredensial Anda memiliki dan mengelola kunci KMS. Jika Anda ingin kontrol total atas kunci KMS yang digunakan untuk mengenkripsi kredensial Anda, [buat kunci yang](#) dikelola pelanggan. Kunci yang dikelola pelanggan adalah kunci KMS yang Anda miliki dan kelola.

Akses operasi enkripsi Security Hub

Pernyataan kebijakan ini memungkinkan Security Hub untuk menggunakan AWS KMS kunci untuk operasi enkripsi. Ini memungkinkan Security Hub untuk melindungi rahasia klien Anda menggunakan

kunci ini. Izin dibatasi untuk operasi yang terkait dengan konektor Security Hub tertentu melalui blok kondisi yang memeriksa ARN sumber dan konteks enkripsi.

```
{
  "Sid": "Allow Security Hub access to the customer managed key",
  "Effect": "Allow",
  "Principal": {
    "Service": "connector.securityhub.amazonaws.com"
  },
  "Action": [
    "kms:GenerateDataKey",
    "kms:Decrypt",
    "kms:ReEncrypt*"
  ],
  "Resource": "*",
  "Condition": {
    "ArnLike": {
      "aws:SourceArn": "arn:aws:securityhub:${Region}:${AccountId}:connectorv2/*"
    },
    "StringLike": {
      "kms:EncryptionContext:aws:securityhub:connectorV2Arn":
"arn:aws:securityhub:${Region}:${AccountId}:connectorv2/*",
      "kms:EncryptionContext:aws:securityhub:providerName":
"${CloudProviderName}"
    }
  }
}
```

Note

Untuk *CloudProviderName*, masukkan JIRA_CLOUD atau SERVICENOW. Untuk *Region* dan *AccountId*, masukkan Wilayah AWS dan Akun AWS ID Anda.

Akses baca kunci Security Hub

Pernyataan kebijakan ini memungkinkan Security Hub membaca metadata tentang kunci KMS dengan mengizinkan pengoperasian. `DescribeKey` Izin ini diperlukan untuk Security Hub untuk memverifikasi status dan konfigurasi kunci. Akses terbatas pada konektor Security Hub tertentu melalui kondisi ARN sumber.

```
{
  "Sid": "Allow Security Hub read access to the customer managed key",
  "Effect": "Allow",
  "Principal": {
    "Service": "connector.securityhub.amazonaws.com"
  },
  "Action": [
    "kms:DescribeKey"
  ],
  "Resource": "*",
  "Condition": {
    "ArnLike": {
      "aws:SourceArn": "arn:aws:securityhub:${Region}:${AccountId}:connectorv2/*"
    }
  }
}
```

Note

Untuk *Region* dan *AccountId*, masukkan Wilayah AWS dan Akun AWS ID Anda.

Akses utama IAM untuk operasi Security Hub

Pernyataan kebijakan ini memberikan izin peran IAM yang ditentukan untuk melakukan operasi kunci (mendeskripsikan, menghasilkan, mendekripsi, mengenkripsi ulang, dan mencantumkan alias) saat berinteraksi dengan Security Hub menggunakan V2 dan V2. CreateConnector CreateTicket APIs
Kondisi ini memastikan operasi ini hanya dapat dilakukan melalui layanan Security Hub di wilayah yang ditentukan.

```
{
  "Sid": "Allow permissions to access key through Security Hub",
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::${AccountId}:role/${RoleName}"
  },
  "Action": [
    "kms:GenerateDataKey",
    "kms:Decrypt",
    "kms:ReEncrypt*"
  ],
```



```
"Resource": "*",
"Condition": {
  "StringEquals": {
    "kms:ViaService": [
      "securityhub.${Region}.amazonaws.com"
    ]
  },
  "StringLike": {
    "kms:EncryptionContext:aws:securityhub:providerName": "SERVICENOW"
  }
}
}

{
  "Sid": "Allow read permissions to access key through Security Hub",
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::${AccountId}:role/${RoleName}"
  },
  "Action": [
    "kms:DescribeKey"
  ],
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:ViaService": [
        "securityhub.${Region}.amazonaws.com"
      ]
    }
  }
}
}
```

 Note

Untuk *RoleName*, masukkan nama peran IAM yang melakukan panggilan ke Security Hub.
Untuk *Region* dan *AccountId*, masukkan Wilayah AWS dan Akun AWS ID Anda.

Integrasi untuk AWS Security Hub Jira Cloud

Note

Security Hub dalam rilis pratinjau dan dapat berubah sewaktu-waktu.

Topik ini menjelaskan cara mengakses konsol Security Hub untuk mengonfigurasi integrasi Jira Cloud. Sebelum menyelesaikan salah satu prosedur dalam topik ini, Anda harus membeli paket Jira Cloud berlangganan. Untuk informasi tentang paket berlangganan, lihat [Harga](#) di Atlassian situs web.

Prasyarat

Selesaikan prasyarat berikut sebelum mengonfigurasi integrasi untuk Jira Cloud

1. Instal Security Hub untuk Jira Cloud

Prosedur berikut menjelaskan cara menginstal plugin yang diperlukan.

1. Masuk ke Atlassian situs Anda sebagai administrator.
2. Buka Pengaturan situs, dan pilih Temukan aplikasi baru.
3. Pilih Security Hub untuk Jira Cloud, dan pilih Dapatkan aplikasi.

2. Buat proyek (jika Anda belum membuatnya)

Langkah ini diperlukan jika Anda belum membuat proyek. Untuk informasi tentang cara membuat proyek, lihat [Membuat proyek baru](#) dalam Jira Cloud Support dokumentasi.

Persyaratan untuk membuat proyek

Pastikan untuk melakukan hal berikut saat membuat proyek baru.

- Pilih Pengembangan perangkat lunak untuk template proyek.
- Pilih yang dikelola perusahaan untuk jenis proyek.
- Catat kunci proyek.

3. Tambahkan proyek pengembangan perangkat lunak Anda ke Security Hub for Jira Cloud app

Prosedur berikut menjelaskan cara menambahkan proyek pengembangan perangkat lunak Anda ke Security Hub for Jira Cloud app.

1. Masuk ke Atlassian situs Anda sebagai administrator.
2. Buka Pengaturan situs, dan pilih Temukan aplikasi baru.
3. Dari panel navigasi, di bawah Aplikasi, pilih Security Hub CSPM V2.
4. Pilih tab Pengaturan konektor.
5. Di bawah Proyek diaktifkan, pilih Tambahkan Proyek Jira.
 - a. Dari dropdown, pilih Tambahkan semua, atau pilih proyek. Ulangi bagian langkah ini jika Anda ingin menambahkan lebih dari satu proyek, tetapi tidak semua proyek.
 - b. Pilih Simpan.

Note

Anda dapat memilih tab Manajer Instalasi untuk memverifikasi semua proyek yang Anda pilih berhasil diinstal.

Untuk informasi tambahan mengenai Jira Cloud, lihat [Jira Cloud sumber daya](#) di Atlassian situs web.

Rekomendasi

Berikut ini adalah rekomendasi untuk dipertimbangkan sebelum mengonfigurasi integrasi untuk Jira Cloud.

- Buat akun sistem khusus di Jira Cloud.
- Gunakan satu akun sistem per Jira Cloud instance.

Konfigurasi integrasi untuk Jira Cloud

Security Hub secara otomatis membuat masalah dalam Integrasi Jira Cloud. ini memungkinkan Anda mengirim temuan Security Hub Jira Cloud, sehingga Anda dapat mengelolanya sebagai bagian dari alur kerja operasional Anda. Misalnya, Anda dapat menetapkan kepemilikan untuk masalah yang memerlukan penyelidikan dan remediasi. Anda harus menyelesaikan prosedur berikut untuk setiap Jira Cloud proyek yang ingin Anda kirim temuan Security Hub.

 Note

Saat Anda membuat Jira Cloud konektor, Anda dialihkan dari arus Wilayah AWS ke "https://3rdp.oauth.console.api.aws", sehingga Anda dapat menyelesaikan pendaftaran konektor. Setelah itu, Anda dikembalikan ke Wilayah AWS tempat konektor sedang dibuat.

Untuk mengkonfigurasi integrasi untuk Jira Cloud

1. [Masuk ke AWS akun Anda dengan kredensi Anda, dan buka konsol Security Hub di https://console.aws.amazon.com/securityhub/v2/home?wilayah=us-timur-1](https://console.aws.amazon.com/securityhub/v2/home?wilayah=us-timur-1).
2. Dari panel navigasi, pilih Manajemen, lalu pilih Integrasi.
3. Pilih Tambahkan Jira Cloud.
4. Untuk Detail, masukkan nama unik dan deskriptif untuk integrasi Anda, dan tentukan apakah akan memasukkan deskripsi opsional untuk integrasi Anda.
5. Untuk pengaturan Keamanan, tentukan cara mengenkripsi Jira Cloud kredensi Anda di Security Hub. Jika Anda memilih kunci milik Layanan, kunci yang AWS dimiliki digunakan untuk mengenkripsi data Anda. Jika Anda memilih kunci Disesuaikan, Anda harus memasukkan ARN untuk kunci khusus yang ada, atau membuat kunci baru dengan memilih Buat AWS KMS kunci. Untuk informasi tentang cara membuat kunci KMS, lihat [Membuat kunci KMS enkripsi simetris](#).

 Note

Anda tidak dapat mengubah pengaturan ini setelah Anda menyelesaikan konfigurasi ini. Namun, Jika Anda memilih Kunci yang disesuaikan, Anda dapat mengedit kebijakan kunci yang disesuaikan kapan saja.

6. (Opsional) Untuk Tag, buat dan tambahkan tag ke integrasi Anda. Anda dapat menambahkan hingga 50 tanda.
7. Untuk Otorisasi, pilih Buat konektor dan otorisasi. Muncul pop-up di mana Anda memilih Izinkan untuk menyelesaikan otorisasi. Setelah Anda menyelesaikan otorisasi, kotak centang muncul memberi tahu Anda bahwa otorisasi berhasil.
8. Untuk Konfigurasi, masukkan ID Jira Cloud proyek.
9. Pilih Konfigurasi lengkap. Setelah Anda menyelesaikan konfigurasi, Anda dapat melihat integrasi yang dikonfigurasi di tab Integrasi yang dikonfigurasi.

Membuat tiket untuk Jira Cloud integrasi

Note

Security Hub dalam rilis pratinjau dan dapat berubah sewaktu-waktu.

Setelah Anda membuat integrasi dengan Jira Cloud, Anda dapat membuat tiket untuk temuan.

Note

Temuan akan selalu dikaitkan dengan satu tiket melalui seluruh siklus hidupnya. Semua pembaruan berikutnya untuk temuan setelah pembuatan awal akan dikirim ke tiket yang sama. Jika konektor yang terkait dengan aturan otomatisasi diubah, konektor yang diperbarui hanya akan digunakan untuk temuan baru dan masuk yang sesuai dengan kriteria aturan.

Untuk membuat tiket untuk temuan

1. [Masuk ke AWS akun Anda dengan kredensi Anda, dan buka konsol Security Hub di https://console.aws.amazon.com/securityhub/v2/home?wilayah=us-timur-1](https://console.aws.amazon.com/securityhub/v2/home?wilayah=us-timur-1).
2. Dari panel navigasi, di bawah Inventaris, pilih Temuan.
3. Pilih temuan. Dalam temuan, pilih Buat tiket.
4. Untuk Integrasi, buka menu dropdown, dan pilih integrasi. Integrasi ini adalah integrasi yang sebelumnya Anda buat saat Anda mengonfigurasi Jira Cloud proyek. Pilih integrasi di mana Anda ingin temuan dikirim.
5. Pilih Buat.

Melihat tiket untuk Jira Cloud integrasi

Note

Security Hub dalam rilis pratinjau dan dapat berubah sewaktu-waktu.

Setelah Anda membuat tiket untuk temuan, Anda dapat membuka tiket pada Jira Cloud instans Anda.

Untuk melihat temuan pada Jira Cloud instans Anda

1. [Masuk ke AWS akun Anda dengan kredensi Anda, dan buka konsol Security Hub di https://console.aws.amazon.com/securityhub/v2/home?wilayah=us-timur-1](https://console.aws.amazon.com/securityhub/v2/home?wilayah=us-timur-1).
2. Dari panel navigasi, di bawah Inventaris, pilih Temuan.
3. Pilih temuan tempat Anda membuat tiket.
4. Dalam temuan, pilih ID tiket untuk melihat tiket pada Jira Cloud instans Anda atau Lihat JSON.

Integrasi untuk ServiceNow

Note

Security Hub dalam rilis pratinjau dan dapat berubah sewaktu-waktu.

Topik ini menjelaskan cara mengakses konsol Security Hub untuk mengonfigurasi integrasi ServiceNow ITSM. Sebelum menyelesaikan salah satu prosedur dalam topik ini, Anda harus berlangganan ServiceNow ITSM sebelum Anda dapat menambahkan integrasi ini. Untuk informasi lebih lanjut, lihat [halaman harga](#) di ServiceNow situs web.

Prasyarat

Selesaikan prasyarat berikut sebelum mengonfigurasi integrasi untuk ServiceNow ITSM

1. Instal integrasi temuan Security Hub V2 untuk IT Service Management (ITSM)

Prosedur berikut menjelaskan cara menginstal plugin Security Hub V2.

1. Masuk ke ServiceNow ITSM instance Anda, lalu buka navigator aplikasi.
2. Arahkan ke [ServiceNow Toko](#).
3. Cari integrasi temuan Security Hub V2 untuk IT Service Management (ITSM), lalu pilih Dapatkan untuk menginstal aplikasi.

 Note

Dalam pengaturan untuk aplikasi Security Hub V2, pilih tindakan yang akan diambil saat temuan Security Hub baru dikirim ke ServiceNow ITSM lingkungan Anda. Anda dapat memilih Tidak melakukan apa-apa, Buat insiden, Buat masalah, atau Buat keduanya (insiden/masalah

2. Konfigurasi jenis hibah Kredensial Klien untuk permintaan masuk OAuth

Anda harus mengonfigurasi jenis hibah ini untuk OAuth permintaan masuk. Untuk informasi selengkapnya, lihat [Jenis hibah Kredensial Klien untuk Inbound OAuth didukung](#) di halaman web SupportServiceNow.

3. Buat OAuth aplikasi

Jika Anda sudah membuat OAuth aplikasi, Anda dapat melewati prasyarat ini. Untuk informasi tentang membuat OAuth aplikasi, lihat [Menyiapkan OAuth](#).

Konfigurasi integrasi untuk ServiceNow ITSM

Security Hub dapat membuat insiden atau masalah secara otomatis masukServiceNow ITSM.

Untuk mengkonfigurasi integrasi untuk ServiceNow ITSM

1. [Masuk ke AWS akun Anda dengan kredensi Anda, dan buka konsol Security Hub di https://console.aws.amazon.com/securityhub/v2/home?wilayah=us-timur-1](https://console.aws.amazon.com/securityhub/v2/home?wilayah=us-timur-1).
2. Dari panel navigasi, pilih Manajemen, lalu pilih Integrasi.
3. Di bawah ServiceNow ITSM, pilih Tambahkan integrasi.
4. Untuk Detail, masukkan nama untuk integrasi Anda, dan tentukan apakah akan memasukkan deskripsi opsional untuk integrasi Anda.
5. Untuk pengaturan Keamanan, tentukan cara mengenkripsi Jira Cloud kredensi Anda di Security Hub. Jika Anda memilih kunci milik Layanan, kunci yang AWS dimiliki digunakan untuk mengenkripsi data Anda. Jika Anda memilih kunci Disesuaikan, Anda harus memasukkan ARN untuk kunci khusus yang ada, atau membuat kunci baru dengan memilih Buat AWS KMS kunci. Untuk informasi tentang cara membuat kunci KMS, lihat [Membuat kunci KMS enkripsi simetris](#).

 Note

Anda tidak dapat mengubah pengaturan ini setelah Anda menyelesaikan konfigurasi ini. Namun, jika Anda memilih Kunci yang disesuaikan, Anda dapat mengedit kebijakan kunci yang disesuaikan kapan saja.

6. Untuk Otorisasi, masukkan ServiceNow ITSM URL, ID Klien, dan Rahasia Klien.
7. Untuk Tag, tentukan apakah akan membuat dan menambahkan tag opsional ke integrasi Anda.
8. Pilih Konfigurasi lengkap. Setelah Anda menyelesaikan konfigurasi, Anda dapat melihat integrasi yang dikonfigurasi di tab Integrasi yang dikonfigurasi.

Membuat tiket untuk ServiceNow ITSM integrasi

 Note

Security Hub dalam rilis pratinjau dan dapat berubah sewaktu-waktu.

Setelah Anda membuat integrasi dengan ServiceNow ITSM, Anda dapat membuat tiket untuk temuan.

 Note

Temuan akan selalu dikaitkan dengan satu tiket melalui seluruh siklus hidupnya. Semua pembaruan berikutnya untuk temuan setelah pembuatan awal akan dikirim ke tiket yang sama. Jika konektor yang terkait dengan aturan otomatisasi diubah, konektor yang diperbarui hanya akan digunakan untuk temuan baru dan masuk yang sesuai dengan kriteria aturan.

Untuk membuat tiket untuk temuan

1. [Masuk ke AWS akun Anda dengan kredensi Anda, dan buka konsol Security Hub di https://console.aws.amazon.com/securityhub/v2/home?wilayah=us-timur-1](https://console.aws.amazon.com/securityhub/v2/home?wilayah=us-timur-1).
2. Dari panel navigasi, di bawah Inventaris, pilih Temuan.
3. Pilih temuan. Dalam temuan, pilih Buat tiket.
4. Untuk Integrasi, buka menu dropdown, dan pilih integrasi.

5. Pilih Buat.

Melihat tiket untuk ServiceNow ITSM integrasi

Note

Security Hub dalam rilis pratinjau dan dapat berubah sewaktu-waktu.

Setelah Anda membuat tiket untuk temuan, Anda dapat membuka tiket pada ServiceNow ITSM instans Anda.

Untuk melihat temuan pada ServiceNow ITSM instans Anda

1. [Masuk ke AWS akun Anda dengan kredensi Anda, dan buka konsol Security Hub di https://console.aws.amazon.com/securityhub/v2/home?wilayah=us-timur-1.](https://console.aws.amazon.com/securityhub/v2/home?wilayah=us-timur-1)
2. Dari panel navigasi, di bawah Inventaris, pilih Temuan.
3. Pilih temuan tempat Anda membuat tiket.
4. Dalam temuan, pilih ID tiket untuk melihat tiket pada ServiceNow ITSM instans Anda atau Lihat JSON.

Bekerja di dasbor Ringkasan di Security Hub

Note

Security Hub dalam rilis pratinjau dan dapat berubah sewaktu-waktu.

Topik ini menjelaskan dasbor Ringkasan di konsol Security Hub. Halaman ini menampilkan ikhtisar eksposur, ancaman, sumber daya terbatas, dan cakupan layanan keamanan Anda di beberapa widget keamanan. Widget ini membantu Anda memvisualisasikan eksposur dan ancaman berdasarkan tingkat keparahan dan akun berdasarkan kemampuan keamanan. Setiap kali Anda membuka halaman ini, data otomatis akan diperbarui.

Anda dapat menyesuaikan halaman ini dengan menambahkan dan menghapus widget keamanan yang berbeda dan menetapkan kriteria filter untuk mengambil data tertentu di setiap widget. Kustomisasi ke halaman ini disimpan untuk digunakan di masa mendatang. Jika akun Anda adalah

akun administrator yang didelegasikan untuk organisasi, penyesuaian disimpan secara independen dari penyesuaian akun anggota.

Note

Kami menyarankan agar Anda tidak menyertakan informasi rahasia, sensitif, atau pribadi (PII) dalam filter tersimpan, widget khusus, atau bidang teks bentuk bebas terkait lainnya.

Jika akun Anda adalah akun administrator yang didelegasikan untuk suatu organisasi, data tersebut mencakup temuan untuk akun dan akun anggota Anda. Jika akun Anda adalah akun anggota atau akun mandiri, data hanya mencakup temuan untuk akun Anda. Jika Anda mengonfigurasi agregasi lintas wilayah di Security Hub, halaman ini menampilkan temuan dari agregasi Anda.

Widget ringkasan eksposur

Widget ini menampilkan semua eksposur Anda berdasarkan tingkat keparahan. Anda dapat melihat frekuensi setiap eksposur di lingkungan Anda. Eksposur dengan tingkat keparahan yang lebih besar muncul lebih dulu. Eksposur didasarkan pada analisis temuan dan sifat dari Security Hub dan lainnya Layanan AWS, seperti Amazon Inspector. Daftar eksposur dalam widget ini terbatas pada delapan eksposur tertinggi dengan jumlah temuan kritis terbesar. Jika dua atau lebih eksposur memiliki jumlah temuan kritis yang sama, daftar tersebut secara otomatis mengelompokkan temuan tersebut di balik temuan kritis yang lebih baru.

Widget ringkasan ancaman

Widget ini menunjukkan semua ancaman Anda berdasarkan tingkat keparahan. Ancaman dengan tingkat keparahan yang lebih besar muncul lebih dulu. Ancaman terkait dengan serangkaian peristiwa dan mengidentifikasi potensi ancaman di lingkungan Anda. Mereka juga berasal. GuardDuty Daftar ancaman dalam widget ini terbatas pada delapan ancaman dengan tingkat keparahan tertinggi. Jika dua atau lebih ancaman memiliki tingkat keparahan yang sama, daftar tersebut secara otomatis mengelompokkan temuan tersebut di balik temuan yang lebih baru. Anda harus mengaktifkan GuardDuty untuk menerima data di widget ini.

Widget cakupan keamanan

Widget ini menampilkan ikhtisar cakupan keamanan Anda dan didasarkan pada temuan cakupan untuk layanan yang didukung. Ini menampilkan pemeriksaan cakupan mana yang lulus, gagal, atau

tidak tersedia. Tidak tersedia menunjukkan pemeriksaan pertanggungjawaban tidak dapat diselesaikan. Ini dapat disebabkan oleh sumber daya yang dihapus atau server yang gagal.

Persentase untuk pemeriksaan cakupan menunjukkan jumlah cek yang lulus dan gagal. Misalnya, satu pemeriksaan cakupan lolos, dan satu pemeriksaan cakupan gagal. Ini menunjukkan 50% dari cek Anda lulus, dan 50% dari cek Anda gagal. Dalam beberapa kasus, persentase dibulatkan ke bilangan bulat terdekat.

Tidak seperti layanan keamanan seperti GuardDuty, Amazon Inspector, dan Macie, Security Hub CSPM menerbitkan satu temuan cakupan per akun, yang PASS/FAIL tergantung pada standar yang diaktifkan, seperti PASS jika setidaknya 1 standar diaktifkan. Persentase cakupan untuk Security Hub CSPM adalah jumlah temuan cakupan CSPM Security Hub yang diteruskan ke jumlah total temuan cakupan CSPM Security Hub.

Note

Kami menyarankan agar Anda tidak menyertakan informasi rahasia, sensitif, atau pribadi (PII) dalam filter tersimpan, widget khusus, atau bidang teks bentuk bebas terkait lainnya.

Melihat detail tentang sumber daya di Security Hub

Note

Security Hub dalam rilis pratinjau dan dapat berubah sewaktu-waktu.

Halaman Sumber Daya melacak sumber daya umum di seluruh akun Anda. Anda dapat mengakses halaman Resources di konsol Security Hub dengan memilih Resources di panel navigasi. Saat memilih jenis sumber daya, Anda dapat meninjau semua sumber daya yang terkait dengan jenis sumber daya. Anda dapat meninjau temuan apa pun yang terkait dengan sumber daya.

Note

Administrator yang didelegasikan dapat melihat semua sumber daya yang terkait dengan akun anggota. Jika Anda mengonfigurasi rumah Wilayah AWS, Anda dapat melihat semua sumber daya di rumah Anda Wilayah AWS dari yang ditautkan Wilayah AWS.

Jika Anda memilih sumber daya, Anda dapat meninjau detail untuk sumber daya tersebut. Rincian ini termasuk nama sumber daya, ID, ARN, jenis, dan kategori. Anda dapat meninjau ID akun yang terkait dengan sumber daya, saat sumber daya dibuat (stempel waktu), dan tempat sumber daya dibuat (Wilayah AWS). Anda juga dapat meninjau detail tambahan dalam cuplikan JSON yang dapat Anda salin.

Jika Anda beralih dari tab Ikhtisar ke tab Temuan, Anda dapat meninjau temuan apa pun yang terkait dengan sumber daya. Tab Temuan menunjukkan nama setiap temuan, jenis setiap temuan, dan tingkat keparahan setiap temuan. Anda dapat mengelompokkan temuan berdasarkan bidang yang berbeda dan mencari temuan menggunakan filter. Jika Anda memilih temuan, Anda dapat meninjau ikhtisar temuan, yang mencakup informasi tentang kepatuhan dan cara memulihkan masalah yang terkait dengan temuan tersebut. Jika Anda kembali ke sumber daya, Anda dapat memilih Buka sumber daya untuk meninjau sumber daya di konsol untuk jenis sumber dayanya. Misalnya, jika sumber daya adalah sumber daya IAM, Anda dapat membuka sumber daya di konsol IAM.

Halaman sumber daya memberi Anda berbagai cara untuk mengatur dan mencari sumber daya. Anda dapat mengelompokkan sumber daya berdasarkan jenis. Misalnya, Anda dapat mengelompokkan sumber daya berdasarkan ID akun, jenis pencarian Wilayah AWS, kategori sumber daya, nama sumber daya, dan jenis sumber daya. Anda dapat mencari temuan menggunakan filter. Filter cepat membantu Anda meninjau sumber daya berdasarkan kategori, akun, dan jenis pencarian.

Manfaat dari halaman Sumber Daya adalah membantu Anda memantau postur keamanan Anda, mengatur sumber daya Anda, dan meninjau detail tentang sumber daya Anda.

Melihat eksposur di Security Hub dengan grafik jalur serangan potensial

Note

Security Hub dalam rilis pratinjau dan dapat berubah sewaktu-waktu.

Grafik jalur serangan potensial adalah visualisasi interaktif yang menunjukkan bagaimana penyerang potensial dapat mengakses dan mengendalikan sumber daya yang terkait dengan temuan eksposur. Anda dapat mengakses grafik ini hanya di konsol Security Hub dan dari layar Exposures. Saat Anda melihat detail untuk temuan eksposur, tab Ikhtisar menyertakan bagian yang disebut Jalur serangan potensial.

Di bagian tab Ikhtisar ini, Anda dapat memilih dan menyeret AWS sumber daya dalam grafik jalur serangan potensial. Anda dapat fokus pada area tertentu dari grafik jalur serangan dengan ikon

zoom-in dan zoom-out. Anda dapat memperluas grafik jalur serangan masuk dan keluar dari mode layar penuh melalui ikon layar penuh. Legenda mengkodekan sumber daya utama, sumber daya yang terlibat, dan menyumbangkan jumlah sifat berdasarkan warna dan menunjukkan kategori sifat dan jumlah sifat dalam grafik jalur serangan. Anda dapat melihat detail untuk sumber daya dengan memilih sumber daya dan memilih Lihat detail sumber daya. Anda juga dapat menyalin ID dan Akun AWS nomor yang terkait dengan sumber daya. Temuan paparan dengan sifat jangkauan menunjukkan internet publik dan jalur jaringan yang runtuh dalam grafik jalur serangan. Anda dapat melihat detail ini dengan memilih node jalur jaringan yang ditiutkan.

Menonaktifkan Security Hub

Note

Security Hub dalam rilis pratinjau dan dapat berubah sewaktu-waktu.

Jika akun Anda bukan bagian dari organisasi, Anda dapat menonaktifkan Security Hub di konsol Security Hub kapan saja. Saat Anda menonaktifkan Security Hub, berhenti menelan temuan. Anda juga kehilangan akses ke temuan dan konfigurasi yang ada. Prosedur berikut menjelaskan cara menonaktifkan Security Hub.

Untuk menonaktifkan Security Hub

1. [Masuk ke AWS akun Anda dengan kredensi Anda, dan buka konsol Security Hub di https://console.aws.amazon.com/securityhub/v2/home.](https://console.aws.amazon.com/securityhub/v2/home)
2. Dari panel navigasi, pilih Umum.
3. Di Security Hub, pilih Nonaktifkan. Di jendela pop-up, masukkan Nonaktifkan, dan pilih Nonaktifkan.

Apa itu AWS Security Hub CSPM?

AWS Security Hub Cloud Security Posture Management (CSPM) memberi Anda pandangan komprehensif tentang status keamanan Anda AWS dan membantu Anda menilai AWS lingkungan Anda berdasarkan standar industri keamanan dan praktik terbaik.

Security Hub CSPM mengumpulkan data keamanan di seluruh Akun AWS Layanan AWS, dan mendukung produk pihak ketiga serta membantu Anda menganalisis tren keamanan dan mengidentifikasi masalah keamanan prioritas tertinggi.

Untuk membantu Anda mengelola status keamanan organisasi Anda, Security Hub CSPM mendukung beberapa standar keamanan. Ini termasuk standar Praktik Terbaik Keamanan AWS Dasar (FSBP) yang dikembangkan oleh AWS, dan kerangka kerja kepatuhan eksternal seperti Pusat Keamanan Internet (CIS), Standar Keamanan Data Industri Kartu Pembayaran (PCI DSS), dan Institut Standar dan Teknologi Nasional (NIST). Setiap standar mencakup beberapa kontrol keamanan, yang masing-masing mewakili praktik terbaik keamanan. Security Hub CSPM menjalankan pemeriksaan terhadap kontrol keamanan dan menghasilkan temuan kontrol untuk membantu Anda menilai kepatuhan Anda terhadap praktik terbaik keamanan.

Selain menghasilkan temuan kontrol, Security Hub CSPM juga menerima temuan dari pihak lain Layanan AWS- seperti Amazon, Amazon GuardDuty Inspector, dan Amazon Macie - dan mendukung produk pihak ketiga. Ini memberi Anda satu panel kaca ke dalam berbagai masalah terkait keamanan. Anda juga dapat mengirim temuan CSPM Security Hub ke produk pihak ketiga lainnya Layanan AWS dan yang didukung.

Security Hub CSPM menawarkan fitur otomatisasi yang membantu Anda melakukan triase dan memulihkan masalah keamanan. Misalnya, Anda dapat menggunakan aturan otomatisasi untuk memperbarui temuan penting secara otomatis saat pemeriksaan keamanan gagal. Anda juga dapat memanfaatkan integrasi dengan Amazon EventBridge untuk memicu respons otomatis terhadap temuan tertentu.

Topik

- [Manfaat CSPM Security Hub](#)
- [Mengakses Security Hub CSPM](#)
- [Layanan terkait](#)
- [Security Hub CSPM uji coba gratis dan harga](#)

Manfaat CSPM Security Hub

Berikut adalah beberapa cara utama Security Hub CSPM membantu Anda memantau kepatuhan dan postur keamanan Anda di seluruh lingkungan Anda AWS .

Mengurangi upaya mengumpulkan dan memprioritaskan temuan

Security Hub CSPM mengurangi upaya untuk mengumpulkan dan memprioritaskan temuan keamanan di seluruh akun dari produk terintegrasi Layanan AWS dan mitra. AWS Security Hub CSPM memproses pencarian data menggunakan AWS Security Finding Format (ASFF), format pencarian standar. Ini menghilangkan kebutuhan untuk mengelola temuan dari berbagai sumber dalam berbagai format. Security Hub CSPM juga menghubungkan temuan di seluruh penyedia untuk membantu Anda memprioritaskan yang paling penting.

Pemeriksaan keamanan otomatis terhadap praktik dan standar terbaik

Security Hub CSPM secara otomatis menjalankan konfigurasi tingkat akun dan pemeriksaan keamanan yang berkelanjutan berdasarkan praktik AWS terbaik dan standar industri. Security Hub CSPM menggunakan hasil pemeriksaan ini untuk menghitung skor keamanan, dan mengidentifikasi akun dan sumber daya tertentu yang memerlukan perhatian.

Pandangan konsolidasi temuan di seluruh akun dan penyedia

Security Hub CSPM mengkonsolidasikan temuan keamanan Anda di seluruh akun dan produk penyedia dan menampilkan hasilnya di konsol CSPM Security Hub. Anda juga dapat mengambil temuan melalui Security Hub CSPM API,, AWS CLI atau. SDKs Dengan pandangan holistik tentang status keamanan Anda saat ini, Anda dapat melihat tren, mengidentifikasi potensi masalah, dan mengambil langkah-langkah perbaikan yang diperlukan.

Kemampuan untuk mengotomatiskan menemukan pembaruan dan remediasi

Anda dapat membuat aturan otomatisasi yang memodifikasi atau menekan temuan berdasarkan kriteria yang Anda tetapkan. Security Hub CSPM juga mendukung integrasi dengan Amazon. EventBridge Untuk mengotomatiskan remediasi temuan tertentu, Anda dapat menentukan tindakan khusus yang harus diambil saat temuan dihasilkan. Misalnya, Anda dapat mengonfigurasi tindakan kustom untuk mengirim temuan ke sistem tiket atau ke sistem remediasi otomatis.

Mengakses Security Hub CSPM

Security Hub CSPM tersedia di sebagian besar Wilayah AWS. Untuk daftar Wilayah di mana Security Hub CSPM saat ini tersedia, lihat [titik akhir dan kuota AWS Security Hub Cloud Security Posture Management \(CSPM\)](#) Security Hub di. Referensi Umum AWS Untuk informasi tentang mengelola Wilayah AWS akun Anda Akun AWS, lihat [Menentukan Wilayah AWS akun mana yang dapat digunakan](#) dalam Panduan AWS Account Management Referensi.

Di setiap Wilayah, Anda dapat mengakses dan menggunakan Security Hub CSPM dengan salah satu cara berikut:

Konsol CSPM Security Hub

AWS Management Console Ini adalah antarmuka berbasis browser yang dapat Anda gunakan untuk membuat dan mengelola AWS sumber daya. Sebagai bagian dari konsol tersebut, konsol CSPM Security Hub menyediakan akses ke akun, data, dan sumber daya CSPM Security Hub Anda. Anda dapat melakukan tugas CSPM Security Hub dengan menggunakan konsol CSPM Security Hub — melihat temuan, membuat aturan otomatisasi, membuat Wilayah agregasi, dan banyak lagi.

Security Hub CSPM API

Security Hub CSPM API memberi Anda akses terprogram ke akun, data, dan sumber daya CSPM Security Hub Anda. Dengan API, Anda dapat mengirim permintaan HTTPS langsung ke Security Hub CSPM. Untuk informasi tentang API, lihat Referensi API [AWS Security Hub Cloud Security Posture Management \(CSPM\)](#) Security Hub.

AWS CLI

Dengan itu AWS CLI, Anda dapat menjalankan perintah di baris perintah sistem Anda untuk melakukan tugas CSPM Security Hub. Dalam beberapa kasus, menggunakan baris perintah bisa lebih cepat dan lebih nyaman daripada menggunakan konsol. Baris perintah juga berguna jika Anda ingin membangun skrip yang melakukan tugas. Untuk informasi tentang menginstal dan menggunakan AWS CLI, lihat [Panduan AWS Command Line Interface Pengguna](#).

AWS SDKs

AWS menyediakan SDKs yang terdiri dari pustaka dan kode sampel untuk berbagai bahasa dan platform pemrograman — misalnya, Java, Go, Python, C ++, dan .NET. Ini SDKs menyediakan akses terprogram yang nyaman ke Security Hub CSPM dan lainnya Layanan AWS dalam bahasa

pilihan Anda. SDK menangani tugas seperti menandatangani permintaan secara kriptografis, mengelola kesalahan, dan mencoba kembali permintaan secara otomatis. Untuk informasi tentang menginstal dan menggunakan AWS SDKs, lihat [Alat untuk Dibangun AWS](#).

Important

Security Hub CSPM hanya mendeteksi dan mengkonsolidasikan temuan yang dihasilkan setelah Anda mengaktifkan Security Hub CSPM. Itu tidak secara retroaktif mendeteksi dan mengkonsolidasikan temuan keamanan yang dihasilkan sebelum Anda mengaktifkan Security Hub CSPM.

Security Hub CSPM hanya menerima dan memproses temuan di Wilayah tempat Anda mengaktifkan CSPM Security Hub di akun Anda.

Untuk kepatuhan penuh dengan pemeriksaan keamanan CIS AWS Foundations Benchmark, Anda harus mengaktifkan Security Hub CSPM di semua Wilayah yang didukung. AWS

Layanan terkait

Untuk lebih mengamankan AWS lingkungan Anda, pertimbangkan untuk menggunakan yang lain Layanan AWS dalam kombinasi dengan Security Hub CSPM. Beberapa Layanan AWS mengirim temuan mereka ke Security Hub CSPM, dan Security Hub CSPM menormalkan temuan ke dalam format standar. Beberapa juga Layanan AWS dapat menerima temuan dari Security Hub CSPM.

Untuk daftar orang lain Layanan AWS yang mengirim atau menerima temuan CSPM Security Hub, lihat. [Layanan AWS integrasi dengan Security Hub CSPM](#)

Security Hub CSPM menggunakan aturan terkait layanan dari AWS Config untuk menjalankan pemeriksaan keamanan untuk sebagian besar kontrol. Kontrol mengacu pada spesifik Layanan AWS dan AWS sumber daya. Untuk mengetahui daftar kontrol CSPM Security Hub, lihat. [Referensi kontrol untuk Security Hub CSPM](#) Anda harus mengaktifkan AWS Config dan merekam sumber daya di AWS Config CSPM Security Hub untuk menghasilkan sebagian besar temuan kontrol. Untuk informasi selengkapnya, lihat [Pertimbangan sebelum mengaktifkan dan mengonfigurasi AWS Config](#).

Security Hub CSPM uji coba gratis dan harga

Saat Anda mengaktifkan CSPM Security Hub Akun AWS untuk pertama kalinya, akun tersebut secara otomatis terdaftar dalam uji coba gratis CSPM Security Hub 30 hari.

Ketika Anda menggunakan Security Hub CSPM selama uji coba gratis, Anda dikenakan biaya untuk penggunaan layanan lain yang berinteraksi dengan Security Hub CSPM, seperti item. AWS Config Anda tidak dikenakan biaya untuk AWS Config aturan yang diaktifkan hanya oleh standar keamanan CSPM Security Hub.

Anda tidak dikenakan biaya untuk menggunakan Security Hub CSPM sampai uji coba gratis Anda berakhir.

Melihat detail penggunaan dan perkiraan biaya

Security Hub CSPM menyediakan informasi penggunaan, termasuk perkiraan biaya 30 hari untuk menggunakan Security Hub CSPM. Rincian penggunaan termasuk waktu yang tersisa dalam uji coba gratis. Informasi penggunaan dapat membantu Anda memahami berapa biaya CSPM Security Hub Anda setelah uji coba gratis berakhir. Informasi penggunaan juga tersedia setelah uji coba gratis berakhir.

Untuk menampilkan informasi penggunaan (konsol)

1. Buka konsol AWS Security Hub Cloud Security Posture Management (CSPM) di <https://console.aws.amazon.com/securityhub/>
2. Di panel navigasi, pilih Penggunaan di bawah Pengaturan.

Perkiraan biaya bulanan didasarkan pada penggunaan CSPM Security Hub akun Anda untuk temuan dan pemeriksaan keamanan yang diproyeksikan selama periode 30 hari.

Informasi penggunaan dan perkiraan biaya hanya untuk akun saat ini dan Wilayah saat ini. Di Wilayah agregasi, informasi penggunaan dan perkiraan biaya tidak termasuk Wilayah yang ditautkan. Untuk informasi selengkapnya tentang Wilayah tertaut, lihat [the section called “Jenis data yang dikumpulkan”](#).

Detail harga

Untuk informasi selengkapnya tentang cara CSPM Security Hub mengenakan biaya untuk temuan tertelan dan pemeriksaan keamanan, lihat harga CSPM [Security Hub](#).

Konsep dan terminologi di Security Hub CSPM

Di AWS Security Hub Cloud Security Posture Management (CSPM), kami membangun AWS konsep dan terminologi umum dan menggunakan istilah tambahan ini.

Akun

Akun Amazon Web Services (AWS) standar yang berisi AWS sumber daya Anda. Anda dapat masuk AWS dengan akun Anda dan mengaktifkan Security Hub CSPM.

Akun dapat mengundang akun lain untuk mengaktifkan CSPM Security Hub dan menjadi terkait dengan akun tersebut di Security Hub CSPM. Menerima undangan keanggotaan bersifat opsional. Jika undangan diterima, akun menjadi akun administrator, dan akun yang ditambahkan adalah akun anggota. Akun administrator dapat melihat temuan di akun anggota mereka.

Jika Anda terdaftar AWS Organizations, maka organisasi Anda menetapkan akun administrator CSPM Security Hub untuk organisasi tersebut. Akun administrator CSPM Security Hub dapat mengaktifkan akun organisasi lain sebagai akun anggota.

Akun tidak dapat berupa akun administrator dan akun anggota secara bersamaan. Akun hanya dapat memiliki satu akun administrator.

Untuk informasi selengkapnya, lihat [Mengelola akun administrator dan anggota di Security Hub CSPM](#).

Akun Administrator

Akun di Security Hub CSPM yang diberikan akses untuk melihat temuan untuk akun anggota terkait.

Akun menjadi akun administrator dengan salah satu cara berikut:

- Akun tersebut mengundang akun lain untuk dikaitkan dengannya di Security Hub CSPM. Ketika akun tersebut menerima undangan, mereka menjadi akun anggota, dan akun yang mengundang menjadi akun administrator mereka.
- Akun ini ditetapkan oleh akun manajemen organisasi sebagai akun administrator CSPM Security Hub. Akun administrator CSPM Security Hub dapat mengaktifkan akun organisasi apa pun sebagai akun anggota, dan juga dapat mengundang akun lain untuk menjadi akun anggota.

Akun hanya dapat memiliki satu akun administrator. Akun tidak dapat berupa akun administrator dan akun anggota secara bersamaan.

Wilayah Agregasi

Menyetel Wilayah agregasi memungkinkan Anda melihat temuan keamanan dari beberapa Wilayah AWS dalam satu panel kaca.

Wilayah agregasi adalah Wilayah tempat Anda melihat dan mengelola temuan. Temuan dikumpulkan ke Wilayah agregasi dari Wilayah terkait. Pembaruan temuan direplikasi di seluruh Wilayah.

Di Wilayah agregasi, halaman standar Keamanan, Wawasan, dan Temuan mencakup data dari semua Wilayah terkait.

Untuk informasi selengkapnya, lihat [Menggabungkan data CSPM di seluruh Wilayah](#).

Temuan yang diarsipkan

Temuan yang status catatannya (RecordState) adalah ARCHIVED. Mengarsipkan temuan menunjukkan bahwa penyedia temuan percaya bahwa temuan tersebut tidak lagi relevan. Status rekaman berbeda dari status alur kerja, yang melacak status investigasi menjadi temuan.

Penyedia pencarian dapat menggunakan [BatchImportFindings](#) pengoperasian API CSPM Security Hub untuk mengarsipkan temuan yang mereka buat. Security Hub CSPM secara otomatis mengarsipkan temuan kontrol yang memenuhi kriteria tertentu. Untuk informasi selengkapnya, lihat [Menghasilkan, memperbarui, dan mengarsipkan temuan kontrol](#).

Di konsol CSPM Security Hub, pengaturan filter default mengecualikan temuan yang diarsipkan dari daftar dan tabel pencarian. Anda dapat memperbarui pengaturan untuk menyertakan temuan yang diarsipkan. Jika Anda mengambil temuan dengan menggunakan [GetFindings](#) pengoperasian API CSPM Security Hub, operasi akan mengambil temuan yang diarsipkan dan aktif. Untuk mengecualikan temuan yang diarsipkan, Anda dapat memfilter hasilnya. Misalnya:

```
"RecordState": [
  {
    "Comparison": "EQUALS",
    "Value": "ARCHIVED"
  }
],
```

AWS Format Pencarian Keamanan (ASFF)

Format standar untuk isi temuan yang dikumpulkan atau dihasilkan oleh Security Hub CSPM. Format Pencarian AWS Keamanan memungkinkan Anda menggunakan CSPM Security Hub

untuk melihat dan menganalisis temuan yang dihasilkan oleh layanan AWS keamanan, solusi pihak ketiga, atau CSPM Security Hub sendiri dari menjalankan pemeriksaan keamanan. Untuk informasi selengkapnya, lihat [AWS Format Pencarian Keamanan \(ASFF\)](#).

Kontrol

Pengamanan atau penanggulangan yang ditentukan untuk sistem informasi atau organisasi yang dirancang untuk melindungi kerahasiaan, integritas, dan ketersediaan informasinya dan untuk memenuhi serangkaian persyaratan keamanan yang ditetapkan. Standar keamanan dikaitkan dengan kumpulan kontrol.

Istilah kontrol keamanan mengacu pada kontrol yang memiliki ID kontrol tunggal dan judul di seluruh standar. Istilah kontrol standar mengacu pada kontrol yang memiliki kontrol IDs dan judul khusus standar. Saat ini, Security Hub CSPM mendukung kontrol standar hanya di Wilayah Tiongkok dan. AWS GovCloud (US) Regions Kontrol keamanan didukung di semua Wilayah lainnya.

Tindakan kustom

Mekanisme CSPM Security Hub untuk mengirimkan temuan yang dipilih ke. EventBridge Tindakan kustom dibuat di Security Hub CSPM. Hal ini kemudian dikaitkan dengan EventBridge aturan. Aturan menentukan tindakan tertentu yang harus diambil saat temuan diterima yang terkait dengan ID tindakan kustom. Tindakan khusus dapat digunakan, misalnya, untuk mengirim temuan tertentu, atau serangkaian kecil temuan, ke alur kerja respons atau remediasi. Untuk informasi selengkapnya, lihat [the section called “Membuat tindakan kustom”](#).

Akun administrator yang didelegasikan (Organizations)

Di AWS Organizations, akun administrator yang didelegasikan untuk suatu layanan dapat mengelola penggunaan layanan untuk organisasi.

Di Security Hub CSPM, akun administrator CSPM Security Hub juga merupakan akun administrator yang didelegasikan untuk Security Hub CSPM. Saat akun manajemen organisasi pertama kali menetapkan akun administrator CSPM Security Hub, Security Hub CSPM memanggil Organizations untuk menjadikan akun tersebut sebagai akun administrator yang didelegasikan.

Akun manajemen organisasi kemudian harus memilih akun administrator yang didelegasikan sebagai akun administrator CSPM Security Hub di semua Wilayah.

Temuan

Catatan yang dapat diamati dari pemeriksaan keamanan atau deteksi terkait keamanan. Security Hub CSPM menghasilkan temuan setelah menyelesaikan pemeriksaan keamanan untuk kontrol.

Ini disebut temuan kontrol. Temuan juga dapat berasal dari integrasi dengan produk lain Layanan AWS dan pihak ketiga.

Untuk informasi selengkapnya, lihat [Temuan CSPM](#).

Agregasi Lintas Wilayah

Agregasi temuan, wawasan, status kepatuhan kontrol, dan skor keamanan dari Wilayah terkait ke Wilayah agregasi. Anda kemudian dapat melihat semua data Anda dari Wilayah agregasi dan memperbarui temuan dan wawasan dari Wilayah agregasi.

Untuk informasi selengkapnya, lihat [Menggabungkan data CSPM di seluruh Wilayah](#).

Menemukan konsumsi

Impor temuan ke Security Hub CSPM dari AWS layanan lain dan dari penyedia mitra pihak ketiga.

Menemukan peristiwa konsumsi mencakup temuan baru dan pembaruan untuk temuan yang ada.

Wawasan

Kumpulan temuan terkait yang ditentukan oleh pernyataan agregasi dan filter opsional. Wawasan mengidentifikasi area keamanan yang membutuhkan perhatian dan intervensi. Security Hub CSPM menawarkan beberapa wawasan terkelola (default) yang tidak dapat Anda ubah. Anda juga dapat membuat wawasan CSPM Security Hub khusus untuk melacak masalah keamanan yang unik untuk AWS lingkungan dan penggunaan Anda. Untuk informasi selengkapnya, lihat [Wawasan CSPM](#).

Wilayah Tertaut

Saat Anda mengaktifkan agregasi Lintas wilayah, Wilayah tertaut adalah wilayah yang menggabungkan temuan, wawasan, mengontrol status kepatuhan, dan skor keamanan ke Wilayah agregasi.

Di Wilayah terkait, halaman Temuan dan Wawasan hanya berisi temuan dari Wilayah tersebut.

Untuk informasi selengkapnya, lihat [Menggabungkan data CSPM di seluruh Wilayah](#).

Akun anggota

Akun yang telah memberikan izin kepada akun administrator untuk melihat dan mengambil tindakan atas temuan mereka.

Akun menjadi akun anggota dengan salah satu cara berikut:

- Akun menerima undangan dari akun lain.

- Untuk akun organisasi, akun administrator CSPM Security Hub mengaktifkan akun tersebut sebagai akun anggota.

Persyaratan terkait

Seperangkat persyaratan industri atau peraturan yang dipetakan ke kontrol.

Aturan

Seperangkat kriteria otomatis yang digunakan untuk menilai apakah suatu kontrol dipatuhi. Ketika aturan dievaluasi, itu bisa lulus atau gagal. Jika evaluasi tidak dapat menentukan apakah aturan lolos atau gagal, maka aturan tersebut dalam keadaan peringatan. Jika aturan tidak dapat dievaluasi, maka itu dalam keadaan tidak tersedia.

Pemeriksaan keamanan

point-in-timeEvaluasi spesifik aturan terhadap sumber daya tunggal yang menghasilkanPASSED,FAILED,WARNING, atau NOT_AVAILABLE negara. Menjalankan pemeriksaan keamanan menghasilkan temuan.

Akun administrator CSPM Security Hub

Akun organisasi yang mengelola keanggotaan CSPM Security Hub untuk suatu organisasi.

Akun manajemen organisasi menunjuk akun administrator CSPM Security Hub di setiap Wilayah. Akun manajemen organisasi harus memilih akun administrator CSPM Security Hub yang sama di semua Wilayah.

Akun administrator CSPM Security Hub juga merupakan akun administrator yang didelegasikan untuk Security Hub CSPM di Organizations.

Akun administrator CSPM Security Hub dapat mengaktifkan akun organisasi apa pun sebagai akun anggota. Akun administrator CSPM Security Hub juga dapat mengundang akun lain untuk menjadi akun anggota.

Standar keamanan

Pernyataan yang diterbitkan tentang topik yang menentukan karakteristik, biasanya dapat diukur dan dalam bentuk kontrol, yang harus dipenuhi atau dicapai untuk kepatuhan. Standar keamanan dapat didasarkan pada kerangka peraturan, praktik terbaik, atau kebijakan internal perusahaan. Kontrol dapat dikaitkan dengan satu atau lebih standar yang didukung di Security Hub CSPM. Untuk mempelajari lebih lanjut tentang standar keamanan di Security Hub CSPM, lihat. [Memahami standar keamanan di Security Hub CSPM](#)

Kepelikan

Tingkat keparahan yang ditetapkan ke kontrol CSPM Security Hub mengidentifikasi pentingnya kontrol. Tingkat keparahan kontrol dapat menjadi Kritis, Tinggi, Sedang, Rendah, atau Informasi. Tingkat keparahan yang ditugaskan untuk mengontrol temuan sama dengan tingkat keparahan kontrol itu sendiri. Untuk mempelajari tentang cara Security Hub CSPM menetapkan tingkat keparahan pada kontrol, lihat [Tingkat keparahan untuk temuan kontrol](#)

Status alur kerja

Status investigasi terhadap sebuah temuan. Ini dilacak menggunakan `WorkflowStatus` atribut.

Status alur kerja pada awalnya `NEW`. Jika Anda memberi tahu pemilik sumber daya untuk mengambil tindakan atas temuan tersebut, Anda dapat menyetel status alur kerja. `NOTIFIED` Jika temuan tidak menjadi masalah, dan tidak memerlukan tindakan apa pun, setel status alur kerja ke `SUPPRESSED`. Setelah Anda meninjau dan memulihkan temuan, setel status alur kerja ke `RESOLVED`

Secara default, sebagian besar daftar temuan hanya menyertakan temuan dengan status alur kerja `NEW` atau `NOTIFIED`. Menemukan daftar untuk kontrol juga mencakup `RESOLVED` temuan.

Untuk [GetFindings](#) operasi, Anda dapat menyertakan filter untuk status alur kerja.

```
"WorkflowStatus": [  
  {  
    "Comparison": "EQUALS",  
    "Value": "RESOLVED"  
  }  
],
```

Konsol CSPM Security Hub menyediakan opsi untuk mengatur status alur kerja untuk temuan. Pelanggan (atau SIEM, tiket, manajemen insiden, atau alat SOAR yang bekerja atas nama pelanggan untuk memperbarui temuan dari penyedia pencarian) juga dapat digunakan [BatchUpdateFindings](#) untuk memperbarui status alur kerja.

Mengaktifkan Security Hub CSPM

Ada dua cara untuk mengaktifkan AWS Security Hub Cloud Security Posture Management (CSPM), dengan mengintegrasikan dengan AWS Organizations atau secara manual.

Kami sangat menyarankan untuk berintegrasi dengan Organizations untuk lingkungan multi-akun dan Multi-wilayah. Jika Anda memiliki akun mandiri, Anda perlu menyiapkan Security Hub CSPM secara manual.

Memverifikasi izin yang diperlukan

Setelah mendaftar Amazon Web Services (AWS), Anda harus mengaktifkan Security Hub CSPM untuk menggunakan kemampuan dan fitur-fiturnya. Untuk mengaktifkan CSPM Security Hub, pertama-tama Anda harus menyiapkan izin yang memungkinkan Anda mengakses konsol CSPM Security Hub dan operasi API. Anda atau AWS administrator Anda dapat melakukan ini dengan menggunakan AWS Identity and Access Management (IAM) untuk melampirkan kebijakan AWS terkelola yang dipanggil `AWSSecurityHubFullAccess` ke identitas IAM Anda.

Untuk mengaktifkan dan mengelola Security Hub CSPM melalui integrasi Organizations, Anda juga harus melampirkan kebijakan AWS terkelola yang disebut `AWSSecurityHubOrganizationsAccess`

Untuk informasi selengkapnya, lihat [AWS kebijakan terkelola untuk Security Hub](#).

Mengaktifkan CSPM Security Hub dengan Integrasi Organizations

Untuk mulai menggunakan CSPM Security Hub AWS Organizations, akun AWS Organizations manajemen untuk organisasi menetapkan akun sebagai akun administrator CSPM Security Hub yang didelegasikan untuk organisasi. Security Hub CSPM secara otomatis diaktifkan di akun administrator yang didelegasikan di Wilayah saat ini.

Pilih metode pilihan Anda, dan ikuti langkah-langkah untuk menunjuk administrator yang didelegasikan.

Security Hub CSPM console

Untuk menunjuk administrator CSPM Security Hub yang didelegasikan saat melakukan orientasi

1. Buka konsol AWS Security Hub Cloud Security Posture Management (CSPM) di <https://console.aws.amazon.com/securityhub/>
2. Pilih Buka Security Hub CSPM. Anda diminta untuk masuk ke akun manajemen Organisasi.
3. Pada halaman Tentukan administrator yang didelegasikan, di bagian Akun administrator yang didelegasikan, tentukan akun administrator yang didelegasikan. Sebaiknya pilih administrator yang didelegasikan sama yang telah Anda tetapkan untuk layanan AWS keamanan dan kepatuhan lainnya.
4. Pilih Setel administrator yang didelegasikan.

Security Hub CSPM API

Memanggil [EnableOrganizationAdminAccount](#) API dari akun manajemen Organizations. Berikan Akun AWS ID akun administrator yang didelegasikan CSPM Security Hub.

AWS CLI

Jalankan [enable-organization-admin-account](#) perintah dari akun manajemen Organizations. Berikan Akun AWS ID akun administrator yang didelegasikan CSPM Security Hub.

Contoh perintah:

```
aws securityhub enable-organization-admin-account --admin-account-id 777788889999
```

Untuk informasi selengkapnya tentang integrasi dengan Organizations, lihat [Mengintegrasikan CSPM Security Hub dengan AWS Organizations](#).

Konfigurasi pusat

Saat mengintegrasikan Security Hub CSPM dan Organizations, Anda memiliki opsi untuk menggunakan fitur yang disebut [konfigurasi pusat](#) untuk menyiapkan dan mengelola CSPM Security Hub untuk organisasi Anda. Kami sangat menyarankan menggunakan konfigurasi pusat karena memungkinkan administrator menyesuaikan cakupan keamanan untuk organisasi. Jika perlu, administrator yang didelegasikan dapat mengizinkan akun anggota untuk mengonfigurasi pengaturan cakupan keamanannya sendiri.

Konfigurasi pusat memungkinkan administrator yang didelegasikan mengonfigurasi CSPM Security Hub di seluruh akun, OUs dan Wilayah AWS Administrator yang didelegasikan mengonfigurasi CSPM Security Hub dengan membuat kebijakan konfigurasi. Dalam kebijakan konfigurasi, Anda dapat menentukan pengaturan berikut:

- Apakah CSPM Security Hub diaktifkan atau dinonaktifkan
- Standar keamanan mana yang diaktifkan dan dinonaktifkan
- Kontrol keamanan mana yang diaktifkan dan dinonaktifkan
- Apakah akan menyesuaikan parameter untuk kontrol tertentu

Sebagai administrator yang didelegasikan, Anda dapat membuat kebijakan konfigurasi tunggal untuk seluruh organisasi atau kebijakan konfigurasi yang berbeda untuk berbagai akun dan OUs. Misalnya, akun pengujian dan akun produksi dapat menggunakan kebijakan konfigurasi yang berbeda.

Akun anggota dan OUs yang menggunakan kebijakan konfigurasi dikelola secara terpusat dan hanya dapat dikonfigurasi oleh administrator yang didelegasikan. Administrator yang didelegasikan dapat menunjuk akun anggota tertentu dan OUs dikelola sendiri untuk memberi anggota kemampuan untuk mengonfigurasi pengaturannya sendiri berdasarkan suatu dasar. Region-by-Region

Jika Anda tidak menggunakan konfigurasi pusat, Anda harus mengonfigurasi CSPM Security Hub secara terpisah di setiap akun dan Wilayah. Ini disebut [konfigurasi lokal](#). Di bawah konfigurasi lokal, administrator yang didelegasikan dapat secara otomatis mengaktifkan CSPM Security Hub dan serangkaian standar keamanan terbatas di akun organisasi baru di Wilayah saat ini. Konfigurasi lokal tidak berlaku untuk akun organisasi yang ada atau Wilayah selain Wilayah saat ini. Konfigurasi lokal juga tidak mendukung penggunaan kebijakan konfigurasi.

Mengaktifkan Security Hub CSPM secara manual

Anda harus mengaktifkan Security Hub CSPM secara manual jika Anda memiliki akun mandiri, atau jika Anda tidak mengintegrasikan dengan AWS Organizations. Akun mandiri tidak dapat diintegrasikan dengan AWS Organizations dan harus menggunakan pengaktifan manual.

Saat mengaktifkan CSPM Security Hub secara manual, Anda menetapkan akun administrator CSPM Security Hub dan mengundang akun lain untuk menjadi akun anggota. Hubungan administrator-anggota terbentuk ketika akun calon anggota menerima undangan.

Pilih metode pilihan Anda, dan ikuti langkah-langkah untuk mengaktifkan Security Hub CSPM. Saat mengaktifkan CSPM Security Hub dari konsol, Anda juga memiliki opsi untuk mengaktifkan standar keamanan yang didukung.

Security Hub CSPM console

1. Buka konsol AWS Security Hub Cloud Security Posture Management (CSPM) di <https://console.aws.amazon.com/securityhub/>
2. Saat Anda membuka konsol CSPM Security Hub untuk pertama kalinya, pilih Buka CSPM Security Hub.
3. Pada halaman selamat datang, bagian Standar keamanan mencantumkan standar keamanan yang didukung Security Hub CSPM.

Pilih kotak centang untuk standar untuk mengaktifkannya, dan kosongkan kotak centang untuk menonaktifkannya.

Anda dapat mengaktifkan atau menonaktifkan standar atau kontrol individualnya kapan saja. Untuk informasi tentang mengelola standar keamanan, lihat [Memahami standar keamanan di Security Hub CSPM](#).

4. Pilih Aktifkan Security Hub.

Security Hub CSPM API

Memanggil [EnableSecurityHub](#) API. Bila Anda mengaktifkan Security Hub CSPM dari API, maka secara otomatis mengaktifkan standar keamanan default berikut:

- AWS Praktik Terbaik Keamanan Dasar
- Tolok Ukur AWS Yayasan Pusat Keamanan Internet (CIS) v1.2.0

Jika Anda tidak ingin mengaktifkan standar ini, maka atur `EnableDefaultStandards` ke `false`.

Anda juga dapat menggunakan `Tags` parameter untuk menetapkan nilai tag ke sumber daya hub.

AWS CLI

Jalankan perintah [enable-security-hub](#). Untuk mengaktifkan standar default, sertakan `--enable-default-standards`. Untuk tidak mengaktifkan standar default, sertakan `--no-enable-default-standards`. Standar keamanan default adalah sebagai berikut:

- AWS Praktik Terbaik Keamanan Dasar
- Tolok Ukur AWS Yayasan Pusat Keamanan Internet (CIS) v1.2.0

```
aws securityhub enable-security-hub [--tags <tag values>] [--enable-default-standards | --no-enable-default-standards]
```

Contoh

```
aws securityhub enable-security-hub --enable-default-standards --tags  
'{"Department": "Security"}'
```

Skrip pengaktifan multi-akun

Note

Alih-alih skrip ini, sebaiknya gunakan konfigurasi pusat untuk mengaktifkan dan mengkonfigurasi CSPM Security Hub di beberapa akun dan Wilayah.

[Skrip pengaktifan multi-akun Security Hub CSPM GitHub](#) memungkinkan Anda mengaktifkan CSPM Security Hub di seluruh akun dan Wilayah. Skrip ini juga mengotomatiskan proses pengiriman undangan ke akun anggota dan mengaktifkan. AWS Config

Skrip secara otomatis memungkinkan perekaman AWS Config sumber daya untuk semua sumber daya, termasuk sumber daya global, di semua Wilayah. Ini tidak membatasi pencatatan sumber daya global ke satu Wilayah. Untuk menghemat biaya, kami sarankan untuk mencatat sumber daya global hanya dalam satu Wilayah. Jika Anda menggunakan konfigurasi pusat atau agregasi lintas wilayah, ini harus menjadi Wilayah asal Anda. Untuk informasi selengkapnya, lihat [Merekam sumber daya di AWS Config](#).

Ada skrip yang sesuai untuk menonaktifkan CSPM Security Hub di seluruh akun dan Wilayah.

Langkah selanjutnya: Manajemen dan integrasi postur

Setelah mengaktifkan Security Hub CSPM, sebaiknya aktifkan standar keamanan dan kontrol untuk memantau postur keamanan Anda. Setelah Anda mengaktifkan kontrol, Security Hub CSPM mulai

menjalankan pemeriksaan keamanan dan menghasilkan temuan kontrol yang membantu Anda mendeteksi kesalahan konfigurasi di lingkungan Anda. AWS Untuk menerima temuan kontrol, Anda harus mengaktifkan dan mengonfigurasi AWS Config untuk Security Hub CSPM. Untuk informasi selengkapnya, lihat [Mengaktifkan dan mengonfigurasi AWS Config untuk Security Hub CSPM](#).

Setelah mengaktifkan Security Hub CSPM, Anda juga dapat memanfaatkan integrasi antara Security Hub CSPM dan solusi pihak ketiga lainnya Layanan AWS untuk melihat temuan mereka di Security Hub CSPM. Security Hub CSPM mengumpulkan temuan dari berbagai sumber dan mencernanya dalam format yang konsisten. Lihat informasi yang lebih lengkap di [Memahami integrasi dalam Security Hub CSPM](#).

Mengaktifkan dan mengonfigurasi AWS Config untuk Security Hub CSPM

AWS Security Hub Cloud Security Posture Management (CSPM) menggunakan AWS Config aturan untuk menjalankan pemeriksaan keamanan dan menghasilkan temuan untuk sebagian besar kontrol. AWS Config memberikan tampilan rinci tentang konfigurasi AWS sumber daya di Akun AWS. Ini menggunakan aturan untuk membuat konfigurasi dasar untuk sumber daya Anda dan perekam konfigurasi untuk mendeteksi apakah sumber daya tertentu melanggar ketentuan aturan. Beberapa aturan, yang disebut aturan AWS Config terkelola, telah ditentukan dan dikembangkan oleh AWS Config. Aturan lainnya adalah aturan AWS Config khusus yang dikembangkan Security Hub CSPM.

AWS Config aturan yang digunakan CSPM Security Hub untuk kontrol disebut sebagai aturan terkait layanan. Aturan terkait layanan memungkinkan Layanan AWS seperti Security Hub CSPM untuk membuat AWS Config aturan di akun Anda.

Untuk menerima temuan kontrol di Security Hub CSPM, Anda harus mengaktifkan AWS Config di akun Anda dan mengaktifkan rekaman untuk sumber daya yang dievaluasi oleh kontrol yang diaktifkan. Halaman ini menjelaskan cara mengaktifkan AWS Config CSPM Security Hub dan mengaktifkan perekaman sumber daya.

Pertimbangan sebelum mengaktifkan dan mengonfigurasi AWS Config

Untuk menerima temuan kontrol di Security Hub CSPM, akun Anda harus AWS Config diaktifkan di setiap Wilayah AWS tempat CSPM Security Hub diaktifkan. Jika Anda menggunakan Security Hub CSPM untuk lingkungan multi-akun, AWS Config harus diaktifkan di setiap Wilayah untuk akun administrator dan semua akun anggota.

Kami sangat menyarankan agar Anda mengaktifkan perekaman sumber daya AWS Config sebelum Anda mengaktifkan standar dan kontrol CSPM Security Hub. Ini membantu Anda memastikan bahwa temuan kontrol Anda akurat.

Untuk mengaktifkan perekaman sumber daya AWS Config, Anda harus memiliki izin yang cukup untuk merekam sumber daya dalam peran AWS Identity and Access Management (IAM) yang dilampirkan ke perekam konfigurasi. Selain itu, pastikan tidak ada kebijakan atau kebijakan IAM yang dikelola AWS Organizations yang AWS Config mencegah izin untuk merekam sumber daya Anda. Pemeriksaan kontrol CSPM Security Hub mengevaluasi konfigurasi sumber daya secara langsung dan tidak memperhitungkan AWS Organizations kebijakan. Untuk informasi selengkapnya tentang AWS Config perekaman, lihat [Bekerja dengan perekam konfigurasi](#) di Panduan AWS Config Pengembang.

Jika Anda mengaktifkan standar di Security Hub CSPM tetapi belum diaktifkan AWS Config, Security Hub CSPM mencoba membuat AWS Config aturan sesuai dengan jadwal berikut:

- Pada hari Anda mengaktifkan standar.
- Sehari setelah Anda mengaktifkan standar.
- 3 hari setelah Anda mengaktifkan standar.
- 7 hari setelah Anda mengaktifkan standar, dan terus menerus setiap 7 hari setelahnya.

Jika Anda menggunakan konfigurasi pusat, Security Hub CSPM juga mencoba membuat AWS Config aturan terkait layanan setiap kali Anda mengaitkan kebijakan konfigurasi yang memungkinkan satu atau beberapa standar dengan akun, unit organisasi (OUs), atau root.

Merekam sumber daya di AWS Config

Saat Anda mengaktifkan AWS Config, Anda harus menentukan AWS sumber daya mana yang ingin direkam oleh perekam AWS Config konfigurasi. Melalui aturan terkait layanan, perekam konfigurasi memungkinkan CSPM Security Hub mendeteksi perubahan pada konfigurasi sumber daya Anda.

Agar CSPM Security Hub menghasilkan temuan kontrol yang akurat, Anda harus mengaktifkan perekaman AWS Config untuk sumber daya yang sesuai dengan kontrol yang diaktifkan. Ini terutama mengaktifkan kontrol dengan jenis jadwal yang dipicu perubahan yang memerlukan perekaman sumber daya. Beberapa kontrol dengan jenis jadwal periodik juga memerlukan perekaman sumber daya. Untuk daftar kontrol ini dan sumber daya yang sesuai, lihat [AWS Config Sumber daya yang diperlukan untuk temuan kontrol](#).

Warning

Jika Anda tidak mengonfigurasi AWS Config perekaman dengan benar untuk kontrol CSPM Security Hub, ini dapat menghasilkan temuan kontrol yang tidak akurat, terutama dalam kasus berikut:

- Anda tidak pernah merekam sumber daya untuk kontrol tertentu, atau Anda menonaktifkan perekaman sumber daya sebelum membuat jenis sumber daya tersebut. Dalam kasus ini, Anda menerima WARNING temuan untuk kontrol yang dipermasalahkan, meskipun Anda mungkin telah membuat sumber daya dalam lingkup kontrol setelah Anda menonaktifkan perekaman. WARNING Temuan ini adalah temuan default yang tidak benar-benar mengevaluasi status konfigurasi sumber daya.
- Anda menonaktifkan perekaman untuk sumber daya yang dievaluasi oleh kontrol tertentu. Dalam hal ini, Security Hub CSPM mempertahankan temuan kontrol yang dihasilkan sebelum Anda menonaktifkan perekaman, meskipun kontrol tidak mengevaluasi sumber daya baru atau yang diperbarui. Security Hub CSPM juga mengubah status kepatuhan temuan menjadi. WARNING Temuan yang dipertahankan ini mungkin tidak secara akurat mencerminkan status konfigurasi sumber daya saat ini.

Secara default, AWS Config mencatat semua sumber daya Regional yang didukung yang ditemukan Wilayah AWS di mana ia berjalan. Untuk menerima semua temuan kontrol CSPM Security Hub, Anda juga harus mengonfigurasi AWS Config untuk merekam sumber daya global. Untuk menghemat biaya, kami sarankan untuk mencatat sumber daya global hanya dalam satu Wilayah. Jika Anda menggunakan konfigurasi pusat atau agregasi lintas wilayah, Wilayah ini harus menjadi Wilayah asal Anda.

Di AWS Config, Anda dapat memilih antara perekaman berkelanjutan dan perekaman harian perubahan status sumber daya. Jika Anda memilih perekaman harian, AWS Config mengirimkan data konfigurasi sumber daya pada akhir setiap periode 24 jam jika ada perubahan status sumber daya. Jika tidak ada perubahan, tidak ada data yang dikirimkan. Hal ini dapat menunda pembuatan temuan CSPM Security Hub untuk kontrol yang dipicu perubahan hingga periode 24 jam selesai.

Untuk informasi selengkapnya tentang AWS Config perekaman, lihat [Merekam AWS sumber daya](#) di Panduan AWS Config Pengembang.

Cara untuk mengaktifkan dan mengkonfigurasi AWS Config

Anda dapat mengaktifkan AWS Config dan mengaktifkan perekaman sumber daya dengan salah satu cara berikut:

- **AWS Config konsol** — Anda dapat mengaktifkan AWS Config akun dengan menggunakan AWS Config konsol. Untuk petunjuk, lihat [Menyiapkan AWS Config dengan konsol](#) di Panduan AWS Config Pengembang.
- **AWS CLI atau SDKs** — Anda dapat mengaktifkan AWS Config akun dengan menggunakan AWS Command Line Interface (AWS CLI). Untuk petunjuk, lihat [Menyiapkan AWS Config dengan AWS CLI](#) di Panduan AWS Config Pengembang. AWS kit pengembangan perangkat lunak (SDKs) juga tersedia untuk banyak bahasa pemrograman.
- **CloudFormation template** — AWS Config Untuk mengaktifkan banyak akun, kami sarankan menggunakan AWS CloudFormation template bernama Enable AWS Config. Untuk mengakses template ini, lihat [AWS CloudFormation StackSet contoh template](#) di Panduan AWS CloudFormation Pengguna.

Secara default, template ini tidak termasuk rekaman untuk sumber daya global IAM. Pastikan Anda mengaktifkan perekaman untuk sumber daya global IAM hanya dalam satu Wilayah AWS untuk menghemat biaya perekaman. Jika Anda mengaktifkan agregasi lintas wilayah, ini harus menjadi Wilayah asal [CSPM Security Hub](#) Anda. Jika tidak, dapat berupa Wilayah mana pun yang tersedia CSPM Security Hub yang mendukung perekaman sumber daya global IAM. Kami merekomendasikan menjalankan satu StackSet untuk merekam semua sumber daya, termasuk sumber daya global IAM, di Wilayah asal atau Wilayah terpilih lainnya. Kemudian, jalankan satu detik StackSet untuk merekam semua sumber daya kecuali sumber daya global IAM di Wilayah lain.

- **GitHub script** — Security Hub CSPM menawarkan [GitHubskrip](#) yang memungkinkan Security Hub CSPM dan AWS Config untuk beberapa akun di seluruh Wilayah. Skrip ini berguna jika Anda belum terintegrasi AWS Organizations, atau Anda memiliki beberapa akun anggota yang bukan bagian dari organisasi.

Untuk informasi lebih lanjut, lihat posting blog berikut di blog AWS Keamanan: [Optimalkan AWS Config untuk AWS Security Hub Cloud Security Posture Management \(CSPM\) untuk mengelola postur keamanan cloud Anda secara efektif](#).

Kontrol Config.1

Di CSPM Security Hub, kontrol [Config.1](#) menghasilkan FAILED temuan di akun Anda jika dinonaktifkan. AWS Config Ini juga menghasilkan FAILED temuan di akun Anda jika AWS Config diaktifkan tetapi perekaman sumber daya tidak diaktifkan.

Jika AWS Config diaktifkan dan perekaman sumber daya diaktifkan, tetapi perekaman sumber daya tidak diaktifkan untuk jenis sumber daya yang diperiksa oleh kontrol yang diaktifkan, CSPM Security Hub akan menghasilkan FAILED temuan untuk kontrol Config.1. Selain FAILED temuan ini, Security Hub CSPM menghasilkan WARNING temuan untuk kontrol yang diaktifkan dan jenis sumber daya yang diperiksa kontrol. Misalnya, jika Anda mengaktifkan kontrol [KMS.5](#) dan perekaman sumber daya tidak diaktifkan, Security AWS KMS keys Hub CSPM akan menghasilkan FAILED temuan untuk kontrol Config.1. Security Hub CSPM juga menghasilkan WARNING temuan untuk kontrol KMS.5 dan kunci KMS Anda.

Untuk menerima PASSED temuan untuk kontrol Config.1, aktifkan perekaman sumber daya untuk semua jenis sumber daya yang sesuai dengan kontrol yang diaktifkan. Juga nonaktifkan kontrol yang tidak diperlukan untuk organisasi Anda. Ini membantu memastikan bahwa Anda tidak memiliki celah konfigurasi dalam pemeriksaan kontrol keamanan Anda. Ini juga membantu memastikan bahwa Anda menerima temuan akurat tentang sumber daya yang salah konfigurasi.

Jika Anda adalah administrator CSPM Security Hub yang didelegasikan untuk organisasi, AWS Config rekaman harus dikonfigurasi dengan benar untuk akun dan akun anggota Anda. Jika Anda menggunakan agregasi lintas wilayah, AWS Config perekaman harus dikonfigurasi dengan benar di Wilayah beranda dan semua Wilayah yang ditautkan. Sumber daya global tidak perlu dicatat di Wilayah terkait.

Menghasilkan aturan terkait layanan

Untuk setiap kontrol yang menggunakan AWS Config aturan terkait layanan, Security Hub CSPM membuat instance aturan yang diperlukan di lingkungan Anda. AWS

Aturan terkait layanan ini khusus untuk Security Hub CSPM. Security Hub CSPM membuat aturan terkait layanan ini meskipun contoh lain dari aturan yang sama sudah ada. Aturan terkait layanan ditambahkan securityhub sebelum nama aturan asli dan pengidentifikasi unik setelah nama aturan. Misalnya, untuk aturan AWS Config terkelolavpc-flow-logs-enabled, nama aturan terkait layanan mungkin securityhub-vpc-flow-logs-enabled-12345

Ada kuota untuk jumlah aturan AWS Config terkelola yang dapat digunakan untuk mengevaluasi kontrol. AWS Config aturan yang dibuat oleh Security Hub CSPM tidak diperhitungkan dalam kuota tersebut. Anda dapat mengaktifkan standar keamanan meskipun Anda telah mencapai AWS Config kuota untuk aturan terkelola di akun Anda. Untuk mempelajari kuota AWS Config aturan selengkapnya, lihat [Batas layanan AWS Config](#) di Panduan AWS Config Pengembang.

Pertimbangan biaya

Security Hub CSPM dapat memengaruhi biaya perekam AWS Config konfigurasi Anda dengan memperbarui item `AWS::Config::ResourceCompliance` konfigurasi. Pembaruan dapat terjadi setiap kali kontrol CSPM Security Hub yang terkait dengan AWS Config aturan mengubah status kepatuhan, diaktifkan atau dinonaktifkan, atau memiliki pembaruan parameter. Jika Anda menggunakan perekam AWS Config konfigurasi hanya untuk Security Hub CSPM, dan tidak menggunakan item konfigurasi ini untuk tujuan lain, kami sarankan untuk mematikan perekaman untuk itu. AWS Config ini dapat mengurangi AWS Config biaya Anda. Anda tidak perlu merekam pemeriksaan keamanan `AWS::Config::ResourceCompliance` agar berfungsi di Security Hub CSPM.

[Untuk informasi tentang biaya yang terkait dengan perekaman sumber daya, lihat harga dan harga AWS Security Hub Cloud Security Posture Management \(CSPM\) Security Hub.AWS Config](#)

Memahami konfigurasi lokal di Security Hub CSPM

Konfigurasi lokal adalah cara default AWS organisasi dikonfigurasi di Security Hub CSPM. Jika Anda tidak ikut serta dan mengaktifkan konfigurasi pusat, organisasi Anda menggunakan konfigurasi lokal secara default.

Di bawah konfigurasi lokal, akun administrator CSPM Security Hub yang didelegasikan memiliki kontrol terbatas atas pengaturan konfigurasi. Satu-satunya pengaturan yang dapat diterapkan oleh administrator yang didelegasikan secara otomatis mengaktifkan CSPM Security Hub dan standar keamanan default di akun organisasi baru. Pengaturan ini hanya berlaku di Wilayah tempat Anda menetapkan akun administrator yang didelegasikan. Standar keamanan default adalah AWS Foundational Security Best Practices (FSBP) dan Center for Internet Security (CIS) AWS Foundations Benchmark v1.2.0. Setelan konfigurasi lokal tidak berlaku untuk akun organisasi yang ada atau ke Wilayah selain yang ditunjuk untuk akun administrator yang didelegasikan.

Selain mengaktifkan CSPM Security Hub dan standar default di akun organisasi baru di satu Wilayah, Anda harus mengonfigurasi setelan CSPM Security Hub lainnya, termasuk standar dan kontrol,

secara terpisah di setiap Wilayah dan akun. Karena ini bisa menjadi proses duplikatif, sebaiknya gunakan konfigurasi pusat untuk lingkungan multi-akun jika satu atau beberapa hal berikut berlaku untuk Anda:

- Anda menginginkan pengaturan konfigurasi yang berbeda untuk berbagai bagian organisasi Anda (misalnya, standar atau kontrol yang diaktifkan berbeda untuk tim yang berbeda).
- Anda beroperasi di beberapa Wilayah dan ingin mengurangi waktu dan kompleksitas mengonfigurasi layanan di seluruh Wilayah ini.
- Anda ingin akun baru menggunakan pengaturan konfigurasi tertentu saat mereka bergabung dengan organisasi.
- Anda ingin akun organisasi mewarisi pengaturan konfigurasi tertentu dari akun induk atau root.

Untuk informasi tentang konfigurasi pusat, lihat [Memahami konfigurasi pusat di Security Hub CSPM](#).

Memahami konfigurasi pusat di Security Hub CSPM

Konfigurasi pusat adalah fitur AWS Security Hub Cloud Security Posture Management (CSPM) yang membantu Anda mengatur dan mengelola Security Hub CSPM di beberapa dan. Akun AWS Wilayah AWS Untuk menggunakan konfigurasi pusat, Anda harus terlebih dahulu mengintegrasikan Security Hub CSPM dan. AWS Organizations Anda dapat mengintegrasikan layanan dengan membuat organisasi dan menunjuk akun administrator CSPM Security Hub yang didelegasikan untuk organisasi.

Dari akun administrator CSPM Security Hub yang didelegasikan, Anda dapat mengaktifkan CSPM Security Hub untuk akun organisasi dan unit organisasi () di seluruh Wilayah. OUs Anda juga dapat mengaktifkan, mengonfigurasi, dan menonaktifkan standar keamanan individual dan kontrol keamanan untuk akun dan OUs di seluruh Wilayah. Anda dapat mengonfigurasi pengaturan ini hanya dalam beberapa langkah dari satu Wilayah utama, yang disebut sebagai Wilayah asal.

Bila Anda menggunakan konfigurasi pusat, administrator yang didelegasikan dapat memilih akun mana dan OUs untuk mengkonfigurasi. Jika administrator yang didelegasikan menetapkan akun anggota atau OU sebagai dikelola sendiri, anggota dapat mengonfigurasi pengaturannya sendiri secara terpisah di setiap Wilayah. Jika administrator yang didelegasikan menetapkan akun anggota atau OU sebagai dikelola secara terpusat, hanya administrator yang didelegasikan yang dapat mengonfigurasi akun anggota atau OU di seluruh Wilayah. Anda dapat menetapkan semua akun dan OUs di organisasi Anda sebagai dikelola secara terpusat, semua dikelola sendiri, atau kombinasi keduanya.

Untuk mengonfigurasi akun yang dikelola secara terpusat, administrator yang didelegasikan menggunakan kebijakan konfigurasi CSPM Security Hub. Kebijakan konfigurasi memungkinkan administrator yang didelegasikan menentukan apakah CSPM Security Hub diaktifkan atau dinonaktifkan, dan standar serta kontrol mana yang diaktifkan atau dinonaktifkan. Mereka juga dapat digunakan untuk menyesuaikan parameter untuk kontrol tertentu.

Kebijakan konfigurasi berlaku di Wilayah asal dan semua Wilayah yang ditautkan. Administrator yang didelegasikan menentukan Wilayah asal organisasi dan Wilayah yang ditautkan sebelum mulai menggunakan konfigurasi pusat. Menentukan Wilayah terkait adalah opsional. Administrator yang didelegasikan dapat membuat kebijakan konfigurasi tunggal untuk seluruh organisasi, atau membuat beberapa kebijakan konfigurasi untuk mengonfigurasi setelan variabel untuk akun yang berbeda dan OUs.

Tip

Jika Anda tidak menggunakan konfigurasi pusat, Anda harus mengonfigurasi CSPM Security Hub secara terpisah di setiap akun dan Wilayah. Ini disebut konfigurasi lokal. Di bawah konfigurasi lokal, administrator yang didelegasikan dapat secara otomatis mengaktifkan CSPM Security Hub dan serangkaian standar keamanan terbatas di akun organisasi baru di Wilayah saat ini. Konfigurasi lokal tidak berlaku untuk akun organisasi yang ada atau Wilayah selain Wilayah saat ini. Konfigurasi lokal juga tidak mendukung penggunaan kebijakan konfigurasi.

Bagian ini memberikan gambaran umum tentang konfigurasi pusat.

Manfaat menggunakan konfigurasi pusat

Manfaat konfigurasi pusat meliputi:

Menyederhanakan konfigurasi layanan dan kemampuan CSPM Security Hub

Bila Anda menggunakan konfigurasi pusat, Security Hub CSPM memandu Anda melalui proses mengonfigurasi praktik terbaik keamanan untuk organisasi Anda. Ini juga menyebarkan kebijakan konfigurasi yang dihasilkan ke akun tertentu dan OUs secara otomatis. Jika Anda memiliki setelan CSPM Security Hub yang ada, seperti mengaktifkan kontrol keamanan baru secara otomatis, Anda dapat menggunakannya sebagai titik awal untuk kebijakan konfigurasi Anda. Selain itu, halaman Konfigurasi di konsol CSPM Security Hub menampilkan ringkasan real-time dari kebijakan konfigurasi Anda dan akun mana dan OUs menggunakan setiap kebijakan.

Konfigurasi di seluruh akun dan Wilayah

Anda dapat menggunakan konfigurasi pusat untuk mengonfigurasi CSPM Security Hub di beberapa akun dan Wilayah. Ini membantu memastikan bahwa setiap bagian dari organisasi Anda mempertahankan konfigurasi yang konsisten dan cakupan keamanan yang memadai.

Mengakomodasi konfigurasi yang berbeda di akun yang berbeda dan OUs

Dengan konfigurasi pusat, Anda dapat memilih untuk mengonfigurasi akun organisasi Anda dan dengan OUs cara yang berbeda. Misalnya, akun pengujian dan akun produksi Anda mungkin memerlukan konfigurasi yang berbeda. Anda juga dapat membuat kebijakan konfigurasi yang mencakup akun baru saat mereka bergabung dengan organisasi.

Mencegah penyimpangan konfigurasi

Penyimpangan konfigurasi terjadi ketika pengguna membuat perubahan pada layanan atau fitur yang bertentangan dengan pilihan administrator yang didelegasikan. Konfigurasi pusat mencegah penyimpangan ini. Saat Anda menetapkan akun atau OU sebagai dikelola secara terpusat, akun tersebut hanya dapat dikonfigurasi oleh administrator yang didelegasikan untuk organisasi. Jika Anda lebih suka akun tertentu atau OU untuk mengonfigurasi pengaturannya sendiri, Anda dapat menentukannya sebagai dikelola sendiri.

Kapan menggunakan konfigurasi pusat?

Konfigurasi pusat paling bermanfaat untuk AWS lingkungan yang mencakup beberapa akun CSPM Security Hub. Ini dirancang untuk membantu Anda mengelola CSPM Security Hub secara terpusat untuk beberapa akun.

Anda dapat menggunakan konfigurasi pusat untuk mengonfigurasi layanan CSPM Security Hub, standar keamanan, dan kontrol keamanan. Anda juga dapat menggunakannya untuk menyesuaikan parameter kontrol tertentu. Untuk informasi selengkapnya tentang standar keamanan, lihat [Memahami standar keamanan di Security Hub CSPM](#). Untuk informasi selengkapnya tentang kontrol keamanan, lihat [Memahami kontrol keamanan di Security Hub CSPM](#).

Istilah dan konsep konfigurasi pusat

Memahami istilah dan konsep utama berikut dapat membantu Anda menggunakan konfigurasi pusat CSPM Security Hub.

Konfigurasi pusat

Fitur CSPM Security Hub yang membantu akun administrator CSPM Security Hub yang didelegasikan untuk organisasi mengonfigurasi layanan CSPM Security Hub, standar keamanan, dan kontrol keamanan di beberapa akun dan Wilayah. Untuk mengonfigurasi setelan ini, administrator yang didelegasikan membuat dan mengelola kebijakan konfigurasi CSPM Security Hub untuk akun yang dikelola secara terpusat di organisasinya. Akun yang dikelola sendiri dapat mengonfigurasi pengaturannya sendiri secara terpisah di setiap Wilayah. Untuk menggunakan konfigurasi pusat, Anda harus mengintegrasikan Security Hub CSPM dan AWS Organizations

Beranda Wilayah

Wilayah AWS Dari mana administrator yang didelegasikan secara terpusat mengonfigurasi CSPM Security Hub, dengan membuat dan mengelola kebijakan konfigurasi. Kebijakan konfigurasi berlaku di Wilayah asal dan semua Wilayah yang ditautkan.

Wilayah asal juga berfungsi sebagai Wilayah agregasi CSPM Security Hub, menerima temuan, wawasan, dan data lainnya dari Wilayah terkait.

Wilayah yang AWS diperkenalkan pada atau setelah 20 Maret 2019 dikenal sebagai Wilayah keikutsertaan. Wilayah keikutsertaan tidak bisa menjadi Wilayah asal, tetapi bisa menjadi Wilayah terkait. Untuk daftar Wilayah keikutsertaan, lihat [Pertimbangan sebelum mengaktifkan dan menonaktifkan Wilayah](#) di Panduan Referensi Manajemen Akun.AWS

Wilayah Tertaut

An Wilayah AWS yang dapat dikonfigurasi dari Wilayah asal. Kebijakan konfigurasi dibuat oleh administrator yang didelegasikan di Wilayah beranda. Kebijakan berlaku di Wilayah asal dan semua Wilayah terkait. Menentukan Wilayah terkait adalah opsional.

Wilayah terkait juga mengirimkan temuan, wawasan, dan data lainnya ke Wilayah asal.

Wilayah yang AWS diperkenalkan pada atau setelah 20 Maret 2019 dikenal sebagai Wilayah keikutsertaan. Anda harus mengaktifkan Wilayah tersebut untuk akun sebelum kebijakan konfigurasi dapat diterapkan padanya. Akun manajemen Organisasi dapat mengaktifkan Wilayah keikutsertaan untuk akun anggota. Untuk informasi selengkapnya, lihat [Menentukan Wilayah AWS akun mana yang dapat digunakan](#) dalam Panduan Referensi Manajemen AWS Akun.

Target

Sebuah Akun AWS, unit organisasi (OU), atau akar organisasi.

Kebijakan konfigurasi CSPM Security Hub

Kumpulan setelan CSPM Security Hub yang dapat dikonfigurasi oleh administrator yang didelegasikan untuk target yang dikelola secara terpusat. Hal ini mencakup:

- Apakah akan mengaktifkan atau menonaktifkan Security Hub CSPM.
- Apakah akan mengaktifkan satu atau lebih [standar keamanan](#).
- [Kontrol keamanan](#) mana yang diaktifkan di seluruh standar yang diaktifkan. Administrator yang didelegasikan dapat melakukan ini dengan menyediakan daftar kontrol khusus yang harus diaktifkan, dan Security Hub CSPM menonaktifkan semua kontrol lainnya (termasuk kontrol baru saat dirilis). Atau, administrator yang didelegasikan dapat memberikan daftar kontrol khusus yang harus dinonaktifkan, dan Security Hub CSPM mengaktifkan semua kontrol lainnya (termasuk kontrol baru saat dirilis).
- Secara opsional, [sesuaikan parameter](#) untuk memilih kontrol yang diaktifkan di seluruh standar yang diaktifkan.

Kebijakan konfigurasi berlaku di Wilayah asal dan semua Wilayah tertaut setelah dikaitkan dengan setidaknya satu akun, unit organisasi (OU), atau root.

Pada konsol CSPM Security Hub, administrator yang didelegasikan dapat memilih kebijakan konfigurasi yang direkomendasikan CSPM Security Hub atau membuat kebijakan konfigurasi khusus. Dengan Security Hub CSPM API dan AWS CLI, administrator yang didelegasikan hanya dapat membuat kebijakan konfigurasi kustom. Administrator yang didelegasikan dapat membuat maksimal 20 kebijakan konfigurasi kustom.

Dalam kebijakan konfigurasi yang direkomendasikan, Security Hub CSPM, standar Praktik Terbaik Keamanan AWS Dasar (FSBP), dan semua kontrol FSBP yang ada dan yang baru diaktifkan. Kontrol yang menerima parameter menggunakan nilai default. Kebijakan konfigurasi yang disarankan berlaku untuk seluruh organisasi.

Untuk menerapkan pengaturan berbeda ke organisasi, atau menerapkan kebijakan konfigurasi yang berbeda ke akun yang berbeda dan OUs, buat kebijakan konfigurasi kustom.

Konfigurasi lokal

Jenis konfigurasi default untuk organisasi, setelah mengintegrasikan Security Hub CSPM dan AWS Organizations Dengan konfigurasi lokal, administrator yang didelegasikan dapat memilih untuk mengaktifkan CSPM Security Hub secara otomatis dan [standar keamanan default](#) di akun organisasi baru di Wilayah saat ini. Jika administrator yang didelegasikan secara otomatis

mengaktifkan standar default, semua kontrol yang merupakan bagian dari standar ini juga diaktifkan secara otomatis dengan parameter default untuk akun organisasi baru. Pengaturan ini tidak berlaku untuk akun yang ada, jadi penyimpangan konfigurasi dimungkinkan setelah akun bergabung dengan organisasi. Menonaktifkan kontrol spesifik yang merupakan bagian dari standar default, dan mengonfigurasi standar dan kontrol tambahan, harus dilakukan secara terpisah di setiap akun dan Wilayah.

Konfigurasi lokal tidak mendukung penggunaan kebijakan konfigurasi. Untuk menggunakan kebijakan konfigurasi, Anda harus beralih ke konfigurasi pusat.

Manajemen akun manual

Jika Anda tidak mengintegrasikan CSPM Security Hub dengan AWS Organizations atau memiliki akun mandiri, Anda harus menentukan pengaturan untuk setiap akun secara terpisah di setiap Wilayah. Manajemen akun manual tidak mendukung penggunaan kebijakan konfigurasi.

Konfigurasi pusat APIs

Operasi CSPM Security Hub yang hanya administrator CSPM Security Hub yang didelegasikan CSPM Security Hub yang dapat digunakan di Wilayah asal untuk mengelola kebijakan konfigurasi untuk akun yang dikelola secara terpusat. Operasi meliputi:

- `CreateConfigurationPolicy`
- `DeleteConfigurationPolicy`
- `GetConfigurationPolicy`
- `ListConfigurationPolicies`
- `UpdateConfigurationPolicy`
- `StartConfigurationPolicyAssociation`
- `StartConfigurationPolicyDisassociation`
- `GetConfigurationPolicyAssociation`
- `BatchGetConfigurationPolicyAssociations`
- `ListConfigurationPolicyAssociations`

Khusus akun APIs

Operasi CSPM Security Hub yang dapat digunakan untuk mengaktifkan atau menonaktifkan Security Hub CSPM, standar, dan kontrol atas dasar. `account-by-account` Operasi ini digunakan di masing-masing Wilayah.

Akun yang dikelola sendiri dapat menggunakan operasi khusus akun untuk mengonfigurasi pengaturan mereka sendiri. Akun yang dikelola secara terpusat tidak dapat menggunakan operasi khusus akun berikut di Wilayah asal dan Wilayah yang ditautkan. Di Wilayah tersebut, hanya administrator yang didelegasikan yang dapat mengonfigurasi akun yang dikelola secara terpusat melalui operasi konfigurasi pusat dan kebijakan konfigurasi.

- `BatchDisableStandards`
- `BatchEnableStandards`
- `BatchUpdateStandardsControlAssociations`
- `DisableSecurityHub`
- `EnableSecurityHub`
- `UpdateStandardsControl`

Untuk memeriksa status akun, pemilik akun yang dikelola secara terpusat dapat menggunakan salah satu `Get` atau `Describe` operasi Security Hub CSPM API.

Jika Anda menggunakan konfigurasi lokal atau manajemen akun manual, alih-alih konfigurasi pusat, operasi khusus akun ini dapat digunakan.

Akun yang dikelola sendiri juga dapat digunakan `*Invitations` dan `*Members` dioperasikan. Namun, kami menyarankan agar akun yang dikelola sendiri tidak menggunakan operasi ini. Asosiasi kebijakan dapat gagal jika akun anggota memiliki anggotanya sendiri yang merupakan bagian dari organisasi yang berbeda dari administrator yang didelegasikan.

Unit organisasi (OU)

Di AWS Organizations dan Security Hub CSPM, wadah untuk sekelompok. Akun AWS Unit organisasi (OU) juga dapat berisi yang lain OUs, memungkinkan Anda untuk membuat hierarki yang menyerupai pohon terbalik, dengan OU induk di bagian atas dan cabang-cabang OUs yang menjangkau ke bawah, berakhir dengan akun yang merupakan daun pohon. OU dapat memiliki tepat satu orang tua, dan setiap akun organisasi dapat menjadi anggota dari satu OU.

Anda dapat mengelola OUs di AWS Organizations atau AWS Control Tower. Untuk informasi selengkapnya, lihat [Mengelola unit organisasi](#) dalam Panduan AWS Organizations Pengguna atau [Mengatur organisasi dan akun AWS Control Tower](#) di Panduan AWS Control Tower Pengguna.

Administrator yang didelegasikan dapat mengaitkan kebijakan konfigurasi dengan akun tertentu atau OUs, atau dengan root untuk mencakup semua akun dan OUs dalam organisasi.

Dikelola secara terpusat

Target yang hanya dapat dikonfigurasi oleh administrator yang didelegasikan di seluruh Wilayah dengan menggunakan kebijakan konfigurasi.

Akun administrator yang didelegasikan menentukan apakah target dikelola secara terpusat. Administrator yang didelegasikan juga dapat mengubah status target dari yang dikelola secara terpusat menjadi dikelola sendiri, atau sebaliknya.

Dikelola sendiri

Target yang mengelola pengaturan CSPM Security Hub sendiri. Target yang dikelola sendiri menggunakan operasi khusus akun untuk mengonfigurasi CSPM Security Hub untuk dirinya sendiri secara terpisah di setiap Wilayah. Ini berbeda dengan target yang dikelola secara terpusat, yang hanya dapat dikonfigurasi oleh administrator yang didelegasikan di seluruh Wilayah melalui kebijakan konfigurasi.

Akun administrator yang didelegasikan menentukan apakah target dikelola sendiri. Administrator yang didelegasikan dapat menerapkan perilaku yang dikelola sendiri ke target. Atau, akun atau OU dapat mewarisi perilaku yang dikelola sendiri dari orang tua.

Akun administrator yang didelegasikan itu sendiri dapat menjadi akun yang dikelola sendiri. Akun administrator yang didelegasikan dapat mengubah status target dari dikelola sendiri menjadi dikelola secara terpusat, atau sebaliknya.

Asosiasi kebijakan konfigurasi

Tautan antara kebijakan konfigurasi dan akun, unit organisasi (OU), atau root. Ketika asosiasi kebijakan ada, akun, OU, atau root menggunakan pengaturan yang ditentukan oleh kebijakan konfigurasi. Asosiasi ada dalam salah satu dari kasus ini:

- Ketika administrator yang didelegasikan secara langsung menerapkan kebijakan konfigurasi ke akun, OU, atau root
- Ketika akun atau OU mewarisi kebijakan konfigurasi dari OU induk atau root

Asosiasi ada sampai konfigurasi yang berbeda diterapkan atau diwariskan.

Kebijakan konfigurasi yang diterapkan

Jenis asosiasi kebijakan konfigurasi di mana administrator yang didelegasikan secara langsung menerapkan kebijakan konfigurasi ke akun target OUs, atau root. Target dikonfigurasi dengan cara yang ditentukan oleh kebijakan konfigurasi, dan hanya administrator yang didelegasikan yang dapat mengubah konfigurasinya. Jika diterapkan ke root, kebijakan konfigurasi

memengaruhi semua akun dan OUs di organisasi yang tidak menggunakan konfigurasi berbeda melalui aplikasi atau warisan dari induk terdekat.

Administrator yang didelegasikan juga dapat menerapkan konfigurasi yang dikelola sendiri ke akun tertentu, OUs, atau root.

Kebijakan konfigurasi yang diwariskan

Jenis asosiasi kebijakan konfigurasi di mana akun atau OU mengadopsi konfigurasi OU induk terdekat atau root. Jika kebijakan konfigurasi tidak langsung diterapkan ke akun atau OU, kebijakan tersebut mewarisi konfigurasi induk terdekat. Semua elemen kebijakan diwariskan. Dengan kata lain, akun atau OU tidak dapat memilih untuk secara selektif mewarisi hanya bagian dari kebijakan. Jika orang tua terdekat dikelola sendiri, akun anak atau OU mewarisi perilaku yang dikelola sendiri dari orang tua.

Warisan tidak dapat mengganti konfigurasi yang diterapkan. Artinya, jika kebijakan konfigurasi atau konfigurasi yang dikelola sendiri langsung diterapkan ke akun atau OU, ia menggunakan konfigurasi itu dan tidak mewarisi konfigurasi induk.

Akar

Dalam AWS Organizations dan Security Hub CSPM, node induk tingkat atas dalam suatu organisasi. Jika administrator yang didelegasikan menerapkan kebijakan konfigurasi ke root, kebijakan tersebut dikaitkan dengan semua akun dan OUs di organisasi kecuali mereka menggunakan kebijakan yang berbeda, melalui aplikasi atau warisan, atau ditetapkan sebagai dikelola sendiri. Jika administrator menetapkan root sebagai dikelola sendiri, semua akun dan OUs dalam organisasi dikelola sendiri kecuali mereka menggunakan kebijakan konfigurasi melalui aplikasi atau warisan. Jika root dikelola sendiri dan tidak ada kebijakan konfigurasi saat ini, semua akun baru di organisasi akan mempertahankan pengaturannya saat ini.

Akun baru yang bergabung dengan organisasi berada di bawah root sampai mereka ditugaskan ke OU tertentu. Jika akun baru tidak ditetapkan ke OU, akun tersebut mewarisi konfigurasi root kecuali administrator yang didelegasikan menentukannya sebagai akun yang dikelola sendiri.

Mengaktifkan konfigurasi pusat di Security Hub CSPM

Akun administrator AWS Security Hub Cloud Security Posture Management (CSPM) yang didelegasikan dapat menggunakan konfigurasi pusat untuk mengonfigurasi CSPM Security Hub, standar, dan kontrol untuk beberapa akun dan unit organisasi () secara keseluruhan. OUs Wilayah AWS

Untuk informasi latar belakang tentang manfaat konfigurasi pusat dan cara kerjanya, lihat [Memahami konfigurasi pusat di Security Hub CSPM](#).

Bagian ini menjelaskan prasyarat untuk konfigurasi pusat dan cara mulai menggunakannya.

Prasyarat untuk konfigurasi pusat

Sebelum Anda dapat mulai menggunakan konfigurasi pusat, Anda harus mengintegrasikan Security Hub CSPM dengan AWS Organizations dan menunjuk Wilayah rumah. Jika Anda menggunakan konsol CSPM Security Hub, prasyarat ini disertakan dalam alur kerja opt-in untuk konfigurasi pusat.

Integrasi dengan Organizations

Anda harus mengintegrasikan Security Hub CSPM dan Organizations untuk menggunakan konfigurasi pusat.

Untuk mengintegrasikan layanan ini, Anda mulai dengan membuat organisasi di Organizations. Dari akun manajemen Organizations, Anda kemudian menunjuk akun administrator yang didelegasikan CSPM Security Hub. Untuk petunjuk, lihat [Mengintegrasikan CSPM Security Hub dengan AWS Organizations](#).

Pastikan bahwa Anda menunjuk administrator yang didelegasikan di Wilayah rumah yang dituju. Saat Anda mulai menggunakan konfigurasi pusat, administrator yang didelegasikan yang sama secara otomatis diatur di semua Wilayah yang ditautkan juga. Akun manajemen Organisasi tidak dapat ditetapkan sebagai akun administrator yang didelegasikan.

Important

Bila Anda menggunakan konfigurasi pusat, Anda tidak dapat menggunakan konsol CSPM Security Hub atau Security Hub CSPM APIs untuk mengubah atau menghapus akun administrator yang didelegasikan. Jika akun manajemen Organizations digunakan AWS Organizations APIs untuk mengubah atau menghapus administrator delegasi Security Hub CSPM, Security Hub CSPM secara otomatis menghentikan konfigurasi pusat. Kebijakan konfigurasi Anda juga dipisahkan dan dihapus. Akun anggota mempertahankan konfigurasi yang mereka miliki sebelum administrator yang didelegasikan diubah atau dihapus.

Tentukan Wilayah rumah

Anda harus menunjuk Wilayah rumah untuk menggunakan konfigurasi pusat. Wilayah asal adalah Wilayah tempat administrator yang didelegasikan mengkonfigurasi organisasi.

 Note

Wilayah asal tidak dapat menjadi Wilayah yang AWS telah ditetapkan sebagai Wilayah keikutsertaan. Wilayah keikutsertaan dinonaktifkan secara default. Untuk daftar Wilayah keikutsertaan, lihat [Pertimbangan sebelum mengaktifkan dan menonaktifkan Wilayah](#) di Panduan Referensi Manajemen Akun.AWS

Secara opsional, Anda dapat menentukan satu atau beberapa Wilayah tertaut yang dapat dikonfigurasi dari Wilayah beranda.

Administrator yang didelegasikan dapat membuat dan mengelola kebijakan konfigurasi hanya dari Wilayah beranda. Kebijakan konfigurasi berlaku di Wilayah asal dan semua Wilayah yang ditautkan. Anda tidak dapat membuat kebijakan konfigurasi yang hanya berlaku untuk subset Wilayah ini, dan bukan yang lain. Pengecualian untuk ini adalah kontrol yang melibatkan sumber daya global. Jika Anda menggunakan konfigurasi pusat, Security Hub CSPM secara otomatis menonaktifkan kontrol yang melibatkan sumber daya global di semua Wilayah kecuali Wilayah asal. Untuk informasi selengkapnya, lihat [Kontrol yang menggunakan sumber daya global](#).

Wilayah asal juga merupakan Wilayah agregasi CSPM Security Hub Anda yang menerima temuan, wawasan, dan data lainnya dari Wilayah tertaut.

Jika Anda telah menetapkan Region agregasi untuk agregasi Cross-region, maka itu adalah Region home default Anda untuk konfigurasi pusat. Anda dapat mengubah Wilayah rumah sebelum mulai menggunakan konfigurasi pusat dengan menghapus agregator temuan Anda saat ini dan membuat yang baru di Wilayah rumah yang Anda inginkan. Agregator temuan adalah sumber daya CSPM Security Hub yang menentukan Wilayah asal dan Wilayah terkait.

Untuk menunjuk Wilayah asal, lihat [langkah-langkah untuk menyetel Wilayah agregasi](#). Jika Anda sudah memiliki Wilayah beranda, Anda dapat memanggil [GetFindingAggregator](#) API untuk melihat detailnya, termasuk Wilayah mana yang saat ini ditautkan dengannya.

Petunjuk untuk mengaktifkan konfigurasi pusat

Pilih metode pilihan Anda, dan ikuti langkah-langkah untuk mengaktifkan konfigurasi pusat untuk organisasi Anda.

Security Hub CSPM console

Untuk mengaktifkan konfigurasi pusat (konsol)

1. Buka konsol AWS Security Hub Cloud Security Posture Management (CSPM) di <https://console.aws.amazon.com/securityhub/>
2. Pada panel navigasi, pilih Pengaturan dan Konfigurasi. Kemudian, pilih Mulai konfigurasi pusat.

Jika Anda melakukan onboarding ke Security Hub CSPM, pilih Buka CSPM Security Hub.

3. Pada halaman Administrator yang didelegasikan, pilih akun administrator yang didelegasikan atau masukkan ID akunnya. Jika berlaku, sebaiknya pilih administrator yang didelegasikan sama yang telah Anda tetapkan untuk layanan AWS keamanan dan kepatuhan lainnya. Pilih Setel administrator yang didelegasikan.
4. Pada halaman Sentralisasi organisasi, di bagian Wilayah, pilih Wilayah rumah Anda. Anda harus masuk ke Wilayah asal untuk melanjutkan. Jika Anda telah menetapkan Region agregasi untuk agregasi Lintas wilayah, itu akan ditampilkan sebagai Wilayah beranda. Untuk mengubah wilayah beranda, pilih Edit pengaturan Wilayah. Anda kemudian dapat memilih Wilayah rumah pilihan Anda dan kembali ke alur kerja ini.
5. Pilih setidaknya satu Wilayah untuk ditautkan ke Wilayah asal. Secara opsional, pilih apakah Anda ingin secara otomatis menautkan Wilayah yang didukung future ke Wilayah asal. Wilayah yang Anda pilih di sini akan dapat dikonfigurasi dari Wilayah asal oleh administrator yang didelegasikan. Kebijakan konfigurasi berlaku di Wilayah asal Anda dan semua Wilayah yang ditautkan.
6. Pilih Konfirmasi dan lanjutkan.
7. Anda sekarang dapat menggunakan konfigurasi pusat. Lanjutkan mengikuti petunjuk konsol untuk membuat kebijakan konfigurasi pertama Anda. Jika Anda belum siap untuk membuat kebijakan konfigurasi, pilih Saya belum siap untuk mengonfigurasi. Anda dapat membuat kebijakan nanti dengan memilih Pengaturan dan Konfigurasi di panel navigasi. Untuk petunjuk cara membuat kebijakan konfigurasi, lihat [Membuat dan mengaitkan kebijakan konfigurasi](#).

Security Hub CSPM API

Untuk mengaktifkan konfigurasi pusat (API)

1. Menggunakan kredensial akun administrator yang didelegasikan, panggil [UpdateOrganizationConfiguration](#) API dari Wilayah beranda.
2. Atur `AutoEnable` bidang ke `false`.
3. Atur `ConfigurationType` bidang di `OrganizationConfiguration` objek ke `CENTRAL`. Tindakan ini memiliki dampak sebagai berikut:
 - Menetapkan akun panggilan sebagai administrator yang didelegasikan CSPM Security Hub di semua Wilayah yang ditautkan.
 - Mengaktifkan CSPM Security Hub di akun administrator yang didelegasikan di semua Wilayah yang ditautkan.
 - Menetapkan akun panggilan sebagai administrator yang didelegasikan CSPM Security Hub untuk akun baru dan yang sudah ada yang menggunakan Security Hub CSPM dan milik organisasi. Ini terjadi di Wilayah asal dan semua Wilayah yang terkait. Akun panggilan ditetapkan sebagai administrator yang didelegasikan untuk akun organisasi baru hanya jika akun tersebut dikaitkan dengan kebijakan konfigurasi yang mengaktifkan CSPM Security Hub. Akun panggilan ditetapkan sebagai administrator yang didelegasikan untuk akun organisasi yang ada hanya jika akun tersebut sudah mengaktifkan CSPM Security Hub.
 - Setel [AutoEnable](#) ke `false` semua Wilayah tertaut, dan disetel [AutoEnableStandards](#) ke `NONE` Wilayah asal dan semua Wilayah yang ditautkan. Parameter ini tidak relevan di wilayah beranda dan terkait saat Anda menggunakan konfigurasi pusat, tetapi Anda dapat secara otomatis mengaktifkan CSPM Security Hub dan standar keamanan default di akun organisasi melalui penggunaan kebijakan konfigurasi.
4. Anda sekarang dapat menggunakan konfigurasi pusat. Administrator yang didelegasikan dapat membuat kebijakan konfigurasi untuk mengonfigurasi CSPM Security Hub di organisasi Anda. Untuk petunjuk cara membuat kebijakan konfigurasi, lihat [Membuat dan mengaitkan kebijakan konfigurasi](#).

Contoh permintaan API:

```
{
  "AutoEnable": false,
  "OrganizationConfiguration": {
    "ConfigurationType": "CENTRAL"
  }
}
```



```
}  
}
```

AWS CLI

Untuk mengaktifkan konfigurasi pusat (AWS CLI)

1. Menggunakan kredensi akun administrator yang didelegasikan, jalankan [update-organization-configuration](#) perintah dari wilayah rumah.
2. Sertakan `no-auto-enable` parameternya.
3. Atur `ConfigurationType` bidang di `organization-configuration` objek keCENTRAL. Tindakan ini memiliki dampak sebagai berikut:
 - Menetapkan akun panggilan sebagai administrator yang didelegasikan CSPM Security Hub di semua Wilayah yang ditautkan.
 - Mengaktifkan CSPM Security Hub di akun administrator yang didelegasikan di semua Wilayah yang ditautkan.
 - Menetapkan akun panggilan sebagai administrator yang didelegasikan CSPM Security Hub untuk akun baru dan yang sudah ada yang menggunakan Security Hub CSPM dan milik organisasi. Ini terjadi di Wilayah asal dan semua Wilayah yang terkait. Akun panggilan ditetapkan sebagai administrator yang didelegasikan untuk akun organisasi baru hanya jika akun tersebut dikaitkan dengan kebijakan konfigurasi yang mengaktifkan Security Hub. Akun panggilan ditetapkan sebagai administrator yang didelegasikan untuk akun organisasi yang ada hanya jika akun tersebut sudah mengaktifkan CSPM Security Hub.
 - Menetapkan opsi pengaktifan otomatis ke [no-auto-enable](#) semua Wilayah yang ditautkan, dan disetel [auto-enable-standards](#) ke Wilayah NONE beranda dan semua Wilayah yang ditautkan. Parameter ini tidak relevan di wilayah beranda dan terkait saat Anda menggunakan konfigurasi pusat, tetapi Anda dapat secara otomatis mengaktifkan CSPM Security Hub dan standar keamanan default di akun organisasi melalui penggunaan kebijakan konfigurasi.
4. Anda sekarang dapat menggunakan konfigurasi pusat. Administrator yang didelegasikan dapat membuat kebijakan konfigurasi untuk mengonfigurasi CSPM Security Hub di organisasi Anda. Untuk petunjuk cara membuat kebijakan konfigurasi, lihat [Membuat dan mengaitkan kebijakan konfigurasi](#).

Contoh perintah:

```
aws securityhub --region us-east-1 update-organization-configuration \
--no-auto-enable \
--organization-configuration '{"ConfigurationType": "CENTRAL"}
```

Target yang dikelola secara terpusat versus yang dikelola sendiri

Saat Anda mengaktifkan konfigurasi pusat, administrator AWS Security Hub Cloud Security Posture Management (CSPM) yang didelegasikan dapat menetapkan setiap akun organisasi, unit organisasi (OU), dan root sebagai dikelola secara terpusat atau dikelola sendiri. Jenis manajemen target menentukan bagaimana Anda dapat menentukan pengaturan CSPM Security Hub.

Untuk informasi latar belakang tentang manfaat konfigurasi pusat dan cara kerjanya, lihat [Memahami konfigurasi pusat di Security Hub CSPM](#).

Bagian ini menjelaskan perbedaan antara penunjukan yang dikelola secara terpusat dan dikelola sendiri dan bagaimana memilih jenis manajemen akun, OU, atau root.

Dikelola sendiri

Pemilik akun yang dikelola sendiri, OU, atau root harus mengonfigurasi pengaturannya secara terpisah di masing-masing Wilayah AWS akun. Administrator yang didelegasikan tidak dapat membuat kebijakan konfigurasi untuk target yang dikelola sendiri.

Dikelola secara terpusat

Hanya administrator CSPM Security Hub yang didelegasikan yang dapat mengonfigurasi pengaturan untuk akun yang dikelola secara terpusat OUs, atau root di seluruh Wilayah beranda dan Wilayah yang ditautkan. Kebijakan konfigurasi dapat dikaitkan dengan akun yang dikelola secara terpusat dan OUs.

Administrator yang didelegasikan dapat mengubah status target antara dikelola sendiri dan dikelola secara terpusat. Secara default, semua akun dan OU dikelola sendiri saat Anda memulai konfigurasi pusat melalui Security Hub CSPM API. Di konsol, jenis manajemen bergantung pada kebijakan konfigurasi pertama Anda. Akun dan OUs yang Anda kaitkan dengan kebijakan pertama Anda dikelola secara terpusat. Akun lain dan OUs dikelola sendiri secara default.

Jika Anda mengaitkan kebijakan konfigurasi dengan akun yang dikelola sendiri sebelumnya, setelah kebijakan akan mengganti penunjukan yang dikelola sendiri. Akun menjadi dikelola secara terpusat dan mengadopsi pengaturan yang tercermin dalam kebijakan konfigurasi.

Jika Anda mengubah akun yang dikelola secara terpusat menjadi akun yang dikelola sendiri, pengaturan yang sebelumnya diterapkan ke akun melalui kebijakan konfigurasi tetap berlaku. Misalnya, akun yang dikelola secara terpusat pada awalnya dapat dikaitkan dengan kebijakan yang mengaktifkan CSPM Security Hub, mengaktifkan Praktik Terbaik Keamanan AWS Dasar, dan dinonaktifkan .1. CloudTrail Jika Anda kemudian menetapkan akun sebagai dikelola sendiri, semua pengaturan tetap tidak berubah. Namun, pemilik akun dapat secara mandiri mengubah pengaturan untuk akun ke depan.

Akun anak dan OUs dapat mewarisi perilaku yang dikelola sendiri dari induk yang dikelola sendiri, dengan cara yang sama seperti akun anak dan OUs dapat mewarisi kebijakan konfigurasi dari induk yang dikelola secara terpusat. Untuk informasi selengkapnya, lihat [Asosiasi kebijakan melalui aplikasi dan warisan](#).

Akun yang dikelola sendiri atau OU tidak dapat mewarisi kebijakan konfigurasi dari node induk atau dari root. Misalnya, jika Anda ingin semua akun dan OUs organisasi Anda mewarisi kebijakan konfigurasi dari root, Anda harus mengubah jenis manajemen node yang dikelola sendiri menjadi dikelola secara terpusat.

Opsi untuk mengonfigurasi pengaturan di akun yang dikelola sendiri

Akun yang dikelola sendiri harus mengonfigurasi pengaturannya sendiri secara terpisah di setiap Wilayah.

Pemilik akun yang dikelola sendiri dapat menjalankan operasi API CSPM Security Hub berikut di setiap Wilayah untuk mengonfigurasi setelahnya:

- `EnableSecurityHub` dan `DisableSecurityHub` untuk mengaktifkan atau menonaktifkan layanan CSPM Security Hub (jika akun yang dikelola sendiri memiliki administrator CSPM Security Hub yang didelegasikan, administrator [harus memisahkan](#) akun sebelum pemilik akun dapat menonaktifkan CSPM Security Hub).
- `BatchEnableStandards` dan `BatchDisableStandards` untuk mengaktifkan atau menonaktifkan standar
- `BatchUpdateStandardsControlAssociations` atau `UpdateStandardsControl` untuk mengaktifkan atau menonaktifkan kontrol

Akun yang dikelola sendiri juga dapat digunakan *Invitations dan *Members dioperasikan. Namun, kami menyarankan agar akun yang dikelola sendiri tidak menggunakan operasi ini. Asosiasi kebijakan dapat gagal jika akun anggota memiliki anggotanya sendiri yang merupakan bagian dari organisasi yang berbeda dari administrator yang didelegasikan.

Untuk deskripsi tindakan API CSPM Security Hub, lihat Referensi API [AWS Security Hub Cloud Security Posture Management \(CSPM\) Security Hub](#).

Akun yang dikelola sendiri juga dapat menggunakan konsol CSPM Security Hub atau AWS CLI untuk mengonfigurasi pengaturannya di setiap Wilayah.

Akun yang dikelola sendiri tidak dapat memanggil kebijakan konfigurasi dan APIs asosiasi kebijakan CSPM Security Hub. Hanya administrator yang didelegasikan yang dapat memanggil konfigurasi pusat APIs dan menggunakan kebijakan konfigurasi untuk mengonfigurasi akun yang dikelola secara terpusat.

Memilih jenis manajemen target

Pilih metode pilihan Anda, dan ikuti langkah-langkah untuk menetapkan akun atau OU sebagai dikelola secara terpusat atau dikelola sendiri di AWS Security Hub Cloud Security Posture Management (CSPM).

Security Hub CSPM console

Untuk memilih jenis manajemen akun atau OU

1. Buka konsol AWS Security Hub Cloud Security Posture Management (CSPM) di <https://console.aws.amazon.com/securityhub/>

Masuk menggunakan kredensial akun administrator CSPM Security Hub yang didelegasikan di Wilayah asal.

2. Pilih Konfigurasi.
3. Pada tab Organisasi, pilih akun target atau OU. Pilih Edit.
4. Pada halaman Tentukan konfigurasi, untuk tipe Manajemen, pilih Dikelola secara terpusat jika Anda ingin administrator yang didelegasikan mengonfigurasi akun target atau OU. Kemudian, pilih Terapkan kebijakan tertentu jika Anda ingin mengaitkan kebijakan konfigurasi yang ada dengan target. Pilih Mewarisi dari organisasi saya jika Anda ingin target mewarisi konfigurasi induk terdekatnya. Pilih Self-managed jika Anda ingin akun atau OU untuk mengkonfigurasi pengaturan sendiri.

5. Pilih Berikutnya. Tinjau perubahan Anda, dan pilih Simpan.

Security Hub CSPM API

Untuk memilih jenis manajemen akun atau OU

1. Memanggil [StartConfigurationPolicyAssociation](#) API dari akun administrator yang didelegasikan CSPM Security Hub di Wilayah asal.
2. Untuk `ConfigurationPolicyIdentifier` bidang ini, berikan `SELF_MANAGED_SECURITY_HUB` jika Anda ingin akun atau OU mengontrol pengaturannya sendiri. Berikan Nama Sumber Daya Amazon (ARN) atau ID kebijakan konfigurasi yang relevan jika Anda ingin administrator yang didelegasikan mengontrol pengaturan untuk akun atau OU.
3. Untuk `Target` bidang, berikan Akun AWS ID, ID OU, atau ID root target yang tipe manajemennya ingin Anda ubah. Ini mengaitkan perilaku yang dikelola sendiri atau kebijakan konfigurasi tertentu dengan target. Akun anak dari target dapat mewarisi kebijakan perilaku atau konfigurasi yang dikelola sendiri.

Contoh permintaan API untuk menunjuk akun yang dikelola sendiri:

```
{
  "ConfigurationPolicyIdentifier": "SELF_MANAGED_SECURITY_HUB",
  "Target": {"AccountId": "123456789012"}
}
```

AWS CLI

Untuk memilih jenis manajemen akun atau OU

1. Jalankan [start-configuration-policy-association](#) perintah dari akun administrator yang didelegasikan CSPM Security Hub di wilayah rumah.
2. Untuk `configuration-policy-identifier` bidang, berikan `SELF_MANAGED_SECURITY_HUB` jika Anda ingin akun atau OU mengontrol pengaturannya sendiri. Berikan Nama Sumber Daya Amazon (ARN) atau ID kebijakan konfigurasi yang relevan jika Anda ingin administrator yang didelegasikan untuk mengontrol pengaturan untuk akun atau OU..

3. Untuk target bidang, berikan Akun AWS ID, ID OU, atau ID root target yang tipe manajemennya ingin Anda ubah. Ini mengaitkan perilaku yang dikelola sendiri atau kebijakan konfigurasi tertentu dengan target. Akun anak dari target dapat mewarisi kebijakan perilaku atau konfigurasi yang dikelola sendiri.

Contoh perintah untuk menunjuk akun yang dikelola sendiri:

```
aws securityhub --region us-east-1 start-configuration-policy-association \
--configuration-policy-identifier "SELF_MANAGED_SECURITY_HUB" \
--target '{"AccountId": "123456789012"}'
```

Cara kerja kebijakan konfigurasi di Security Hub CSPM

Administrator AWS Security Hub Cloud Security Posture Management (CSPM) yang didelegasikan dapat membuat kebijakan konfigurasi untuk mengonfigurasi CSPM Security Hub, standar keamanan, dan kontrol keamanan untuk organisasi. Setelah membuat kebijakan konfigurasi, administrator yang didelegasikan dapat mengaitkannya dengan akun tertentu, unit organisasi (OUs), atau root. Kebijakan tersebut kemudian berlaku di akun yang ditentukan, OUs, atau root.

Untuk informasi latar belakang tentang manfaat konfigurasi pusat dan cara kerjanya, lihat [Memahami konfigurasi pusat di Security Hub CSPM](#).

Bagian ini memberikan gambaran rinci tentang kebijakan konfigurasi.

Pertimbangan kebijakan

Sebelum Anda membuat kebijakan konfigurasi di Security Hub CSPM, pertimbangkan detail berikut.

- Kebijakan konfigurasi harus dikaitkan agar berlaku — Setelah membuat kebijakan konfigurasi, Anda dapat mengaitkannya dengan satu atau beberapa akun, unit organisasi (OUs), atau root. Kebijakan konfigurasi dapat dikaitkan dengan akun atau OUs melalui aplikasi langsung, atau melalui warisan dari OU induk.
- Akun atau OU hanya dapat dikaitkan dengan satu kebijakan konfigurasi — Untuk mencegah pengaturan yang bertentangan, akun atau OU hanya dapat dikaitkan dengan satu kebijakan konfigurasi pada waktu tertentu. Atau, akun atau OU dapat dikelola sendiri.
- Kebijakan konfigurasi selesai — Kebijakan konfigurasi menyediakan spesifikasi pengaturan yang lengkap. Misalnya, akun anak tidak dapat menerima pengaturan untuk beberapa kontrol dari satu

kebijakan dan pengaturan untuk kontrol lain dari kebijakan lain. Saat Anda mengaitkan kebijakan dengan akun anak, pastikan kebijakan tersebut menentukan semua setelan yang ingin digunakan oleh akun anak tersebut.

- Kebijakan konfigurasi tidak dapat dikembalikan — Tidak ada opsi untuk mengembalikan kebijakan konfigurasi setelah Anda mengaitkannya dengan akun atau OUs. Misalnya, jika Anda mengaitkan kebijakan konfigurasi yang menonaktifkan CloudWatch kontrol dengan akun tertentu, lalu memisahkan kebijakan tersebut, CloudWatch kontrol akan terus dinonaktifkan di akun tersebut. Untuk mengaktifkan CloudWatch kontrol lagi, Anda dapat mengaitkan akun dengan kebijakan baru yang memungkinkan kontrol. Atau, Anda dapat mengubah akun menjadi dikelola sendiri dan mengaktifkan setiap CloudWatch kontrol di akun.
- Kebijakan konfigurasi berlaku di Wilayah asal Anda dan semua Wilayah tertaut — Kebijakan konfigurasi memengaruhi semua akun terkait di Wilayah asal dan semua Wilayah yang ditautkan. Anda tidak dapat membuat kebijakan konfigurasi yang berlaku hanya di beberapa Wilayah ini dan bukan yang lain. Pengecualian untuk ini adalah [kontrol yang menggunakan sumber daya global](#). Security Hub CSPM secara otomatis menonaktifkan kontrol yang melibatkan sumber daya global di semua Wilayah kecuali Wilayah asal.

Wilayah yang AWS diperkenalkan pada atau setelah 20 Maret 2019 dikenal sebagai Wilayah keikutsertaan. Anda harus mengaktifkan Wilayah tersebut untuk akun sebelum kebijakan konfigurasi berlaku di sana. Akun manajemen Organisasi dapat mengaktifkan Wilayah keikutsertaan untuk akun anggota. Untuk petunjuk tentang mengaktifkan Wilayah keikutsertaan, lihat [Menentukan Wilayah AWS akun mana yang dapat digunakan dalam Panduan](#) Referensi Manajemen AWS Akun.

Jika kebijakan Anda mengonfigurasi kontrol yang tidak tersedia di Wilayah beranda atau satu atau beberapa Wilayah tertaut, CSPM Security Hub akan melewati konfigurasi kontrol di Wilayah yang tidak tersedia tetapi menerapkan konfigurasi di Wilayah tempat kontrol tersedia. Anda tidak memiliki cakupan untuk kontrol yang tidak tersedia di Wilayah asal atau Wilayah yang ditautkan.

- Kebijakan konfigurasi adalah sumber daya — Sebagai sumber daya, kebijakan konfigurasi memiliki Nama Sumber Daya Amazon (ARN) dan pengenalan unik universal (UUID). ARN menggunakan format berikut: `arn:partition:securityhub:region:delegated administrator account ID:configuration-policy/configuration policy UUID` Konfigurasi yang dikelola sendiri tidak memiliki ARN atau UUID. Pengidentifikasi untuk konfigurasi yang dikelola sendiri adalah SELF_MANAGED_SECURITY_HUB

Jenis kebijakan konfigurasi

Setiap kebijakan konfigurasi menentukan setelan berikut:

- Mengaktifkan atau menonaktifkan Security Hub CSPM.
- Aktifkan satu atau lebih [standar keamanan](#).
- Tunjukkan [kontrol keamanan](#) mana yang diaktifkan di seluruh standar yang diaktifkan. Anda dapat melakukannya dengan menyediakan daftar kontrol khusus yang harus diaktifkan, dan Security Hub CSPM menonaktifkan semua kontrol lainnya, termasuk kontrol baru saat dirilis. Atau, Anda dapat memberikan daftar kontrol khusus yang harus dinonaktifkan, dan Security Hub CSPM mengaktifkan semua kontrol lainnya, termasuk kontrol baru saat dirilis.
- Secara opsional, [sesuaikan parameter](#) untuk memilih kontrol yang diaktifkan di seluruh standar yang diaktifkan.

Kebijakan konfigurasi pusat tidak menyertakan pengaturan AWS Config perekam. Anda harus mengaktifkan AWS Config dan mengaktifkan perekaman secara terpisah untuk sumber daya yang diperlukan agar CSPM Security Hub menghasilkan temuan kontrol. Untuk informasi selengkapnya, lihat [Pertimbangan sebelum mengaktifkan dan mengonfigurasi AWS Config](#).

Jika Anda menggunakan konfigurasi pusat, Security Hub CSPM secara otomatis menonaktifkan kontrol yang melibatkan sumber daya global di semua Wilayah kecuali Wilayah asal. Kontrol lain yang Anda pilih untuk diaktifkan meskipun kebijakan konfigurasi diaktifkan di semua Wilayah yang tersedia. Untuk membatasi temuan untuk kontrol ini hanya pada satu Wilayah, Anda dapat memperbarui pengaturan AWS Config perekam dan menonaktifkan perekaman sumber daya global di semua Wilayah kecuali Wilayah asal.

Jika kontrol yang diaktifkan yang melibatkan sumber daya global tidak didukung di Wilayah asal, CSPM Security Hub mencoba mengaktifkan kontrol di satu Wilayah tertaut di mana kontrol didukung. Dengan konfigurasi pusat, Anda tidak memiliki cakupan untuk kontrol yang tidak tersedia di Wilayah asal atau Wilayah yang ditautkan.

Untuk daftar kontrol yang melibatkan sumber daya global, lihat [Kontrol yang menggunakan sumber daya global](#).

Kebijakan konfigurasi yang disarankan

Saat membuat kebijakan konfigurasi untuk pertama kalinya di konsol CSPM Security Hub, Anda memiliki opsi untuk memilih kebijakan yang direkomendasikan CSPM Security Hub.

Kebijakan yang direkomendasikan memungkinkan Security Hub CSPM, standar Praktik Terbaik Keamanan AWS Dasar (FSBP), dan semua kontrol FSBP yang ada dan yang baru. Kontrol yang menerima parameter menggunakan nilai default. Kebijakan yang disarankan berlaku untuk root (semua akun dan OUs, baik yang baru maupun yang sudah ada). Setelah membuat kebijakan yang disarankan untuk organisasi, Anda dapat memodifikasinya dari akun administrator yang didelegasikan. Misalnya, Anda dapat mengaktifkan standar atau kontrol tambahan atau menonaktifkan kontrol FSBP tertentu. Untuk petunjuk tentang memodifikasi kebijakan konfigurasi, lihat [Memperbarui kebijakan konfigurasi](#).

Kebijakan konfigurasi kustom

Alih-alih kebijakan yang disarankan, administrator yang didelegasikan dapat membuat hingga 20 kebijakan konfigurasi kustom. Anda dapat mengaitkan satu kebijakan kustom dengan seluruh organisasi Anda atau kebijakan kustom yang berbeda dengan akun yang berbeda dan OUs. Untuk kebijakan konfigurasi kustom, Anda menentukan pengaturan yang Anda inginkan. Misalnya, Anda dapat membuat kebijakan khusus yang memungkinkan FSBP, Tolok Ukur AWS Yayasan Center for Internet Security (CIS) v1.4.0, dan semua kontrol dalam standar tersebut kecuali kontrol Amazon Redshift. Tingkat perincian yang Anda gunakan dalam kebijakan konfigurasi khusus bergantung pada cakupan cakupan keamanan yang dimaksudkan di seluruh organisasi Anda.

Note

Anda tidak dapat mengaitkan kebijakan konfigurasi yang menonaktifkan CSPM Security Hub dengan akun administrator yang didelegasikan. Kebijakan semacam itu dapat dikaitkan dengan akun lain tetapi melewati asosiasi dengan administrator yang didelegasikan. Akun administrator yang didelegasikan mempertahankan konfigurasi saat ini.

Setelah membuat kebijakan konfigurasi kustom, Anda dapat beralih ke kebijakan konfigurasi yang disarankan dengan memperbarui kebijakan konfigurasi untuk mencerminkan konfigurasi yang disarankan. Namun, Anda tidak melihat pilihan untuk membuat kebijakan konfigurasi yang disarankan di konsol CSPM Security Hub setelah kebijakan pertama Anda dibuat.

Asosiasi kebijakan melalui aplikasi dan warisan

Saat Anda pertama kali ikut serta dalam konfigurasi pusat, organisasi Anda tidak memiliki asosiasi dan berperilaku dengan cara yang sama seperti sebelum ikut serta. Administrator yang didelegasikan kemudian dapat membuat asosiasi antara kebijakan konfigurasi atau perilaku dan akun yang dikelola sendiri OUs, atau root. Asosiasi dapat dibentuk melalui aplikasi atau warisan.

Dari akun administrator yang didelegasikan, Anda dapat langsung menerapkan kebijakan konfigurasi ke akun, OU, atau root. Atau, administrator yang didelegasikan dapat langsung menerapkan penunjukan yang dikelola sendiri ke akun, OU, atau root.

Dengan tidak adanya aplikasi langsung, akun atau OU mewarisi pengaturan induk terdekat yang memiliki kebijakan konfigurasi atau perilaku yang dikelola sendiri. Jika induk terdekat dikaitkan dengan kebijakan konfigurasi, anak mewarisi kebijakan tersebut dan hanya dapat dikonfigurasi oleh administrator yang didelegasikan dari Wilayah beranda. Jika orang tua terdekat dikelola sendiri, anak mewarisi perilaku yang dikelola sendiri dan memiliki kemampuan untuk menentukan pengaturannya sendiri di masing-masing Wilayah AWS.

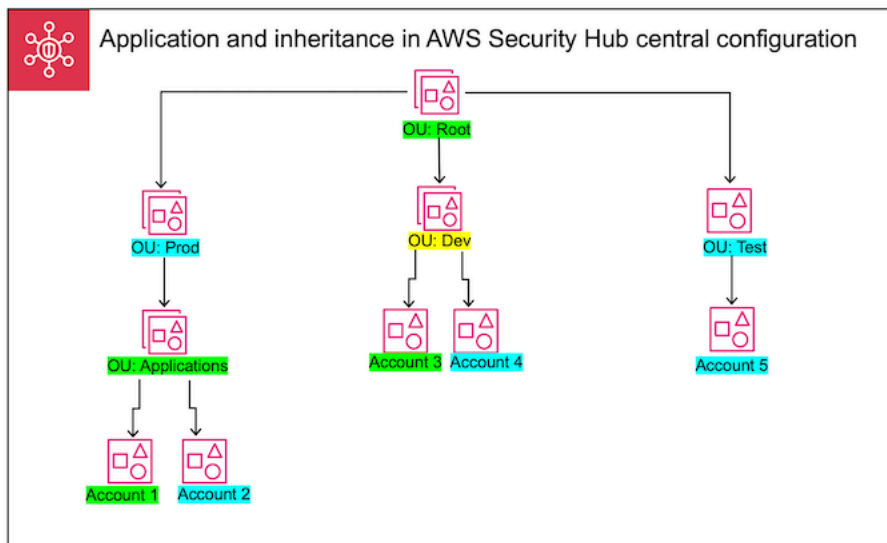
Aplikasi lebih diutamakan daripada warisan. Dengan kata lain, pewarisan tidak mengesampingkan kebijakan konfigurasi atau penunjukan yang dikelola sendiri yang telah diterapkan langsung oleh administrator yang didelegasikan ke akun atau OU.

Jika Anda langsung menerapkan kebijakan konfigurasi ke akun yang dikelola sendiri, kebijakan akan mengganti penunjukan yang dikelola sendiri. Akun menjadi dikelola secara terpusat dan mengadopsi pengaturan yang tercermin dalam kebijakan konfigurasi.

Kami merekomendasikan langsung menerapkan kebijakan konfigurasi ke root. Jika Anda menerapkan kebijakan ke root, maka akun baru yang bergabung dengan organisasi Anda akan secara otomatis mewarisi kebijakan root kecuali Anda mengaitkannya dengan kebijakan yang berbeda atau menunjuknya sebagai dikelola sendiri.

Hanya satu kebijakan konfigurasi yang dapat dikaitkan dengan akun atau OU pada waktu tertentu, baik melalui aplikasi atau warisan. Ini dirancang untuk mencegah pengaturan yang bertentangan.

Diagram berikut menggambarkan bagaimana aplikasi kebijakan dan pewarisan bekerja dalam konfigurasi pusat.



Dalam contoh ini, node yang disorot dengan warna hijau memiliki kebijakan konfigurasi yang telah diterapkan padanya. Node yang disorot dengan warna biru tidak memiliki kebijakan konfigurasi yang telah diterapkan padanya. Sebuah simpul yang disorot dengan warna kuning telah ditetapkan sebagai dikelola sendiri. Setiap akun dan OU menggunakan konfigurasi berikut:

- OU:root (Green) - OU ini menggunakan kebijakan konfigurasi yang telah diterapkan padanya.
- OU:prod (Blue) - OU ini mewarisi kebijakan konfigurasi dari ou:Root.
- OU: Applications (Green) - OU ini menggunakan kebijakan konfigurasi yang telah diterapkan untuk itu.
- Akun 1 (Hijau) — Akun ini menggunakan kebijakan konfigurasi yang telah diterapkan padanya.
- Akun 2 (Biru) — Akun ini mewarisi kebijakan konfigurasi dari OU: Aplikasi.
- OU: dev (Kuning) - OU ini dikelola sendiri.
- Akun 3 (Hijau) — Akun ini menggunakan kebijakan konfigurasi yang telah diterapkan padanya.
- Akun 4 (Biru) — Akun ini mewarisi perilaku yang dikelola sendiri dari OU: dev.
- OU:test (Biru) - Akun ini mewarisi kebijakan konfigurasi dari OU:root.
- Akun 5 (Biru) — Akun ini mewarisi kebijakan konfigurasi dari OU:root karena induk langsungnya, ou:Test, tidak terkait dengan kebijakan konfigurasi.

Menguji kebijakan konfigurasi

Untuk memastikan Anda memahami cara kerja kebijakan konfigurasi, sebaiknya buat satu kebijakan dan kaitkan dengan akun pengujian atau OU.

Untuk menguji kebijakan konfigurasi

1. Buat kebijakan konfigurasi khusus, dan verifikasi bahwa pengaturan yang ditentukan untuk pengaktifan, standar, dan kontrol CSPM Security Hub sudah benar. Untuk petunjuk, lihat [Membuat dan mengaitkan kebijakan konfigurasi](#).
2. Menerapkan kebijakan konfigurasi ke akun pengujian atau OU yang tidak memiliki akun turunan atau OUs.
3. Verifikasi bahwa akun pengujian atau OU menggunakan kebijakan konfigurasi dengan cara yang diharapkan di Wilayah asal Anda dan semua Wilayah yang ditautkan. Anda juga dapat memverifikasi bahwa semua akun lain dan OUs di organisasi Anda tetap dikelola sendiri dan dapat mengubah pengaturan mereka sendiri di setiap Wilayah.

Setelah menguji kebijakan konfigurasi dalam satu akun atau OU, Anda dapat mengaitkannya dengan akun lain dan OUs.

Membuat dan mengaitkan kebijakan konfigurasi

Akun administrator AWS Security Hub Cloud Security Posture Management (CSPM) yang didelegasikan dapat membuat kebijakan konfigurasi yang menentukan cara CSPM, standar, dan kontrol Security Hub dikonfigurasi dalam akun dan unit organisasi tertentu (). OUs Kebijakan konfigurasi berlaku hanya setelah administrator yang didelegasikan mengaitkannya dengan setidaknya satu akun atau unit organisasi (OUs), atau root. Administrator yang didelegasikan juga dapat mengaitkan konfigurasi yang dikelola sendiri dengan akun, OUs, atau root.

Jika ini adalah pertama kalinya Anda membuat kebijakan konfigurasi, sebaiknya [Cara kerja kebijakan konfigurasi di Security Hub CSPM](#) tinjau terlebih dahulu.

Pilih metode akses pilihan Anda, dan ikuti langkah-langkah untuk membuat dan mengaitkan kebijakan konfigurasi atau konfigurasi yang dikelola sendiri. Saat menggunakan konsol CSPM Security Hub, Anda dapat mengaitkan konfigurasi dengan beberapa akun atau OUs pada saat yang bersamaan. Saat menggunakan Security Hub CSPM API atau AWS CLI, Anda dapat mengaitkan konfigurasi dengan hanya satu akun atau OU di setiap permintaan.

Note

Jika Anda menggunakan konfigurasi pusat, Security Hub CSPM secara otomatis menonaktifkan kontrol yang melibatkan sumber daya global di semua Wilayah kecuali Wilayah asal. Kontrol lain yang Anda pilih untuk diaktifkan meskipun kebijakan konfigurasi

diaktifkan di semua Wilayah yang tersedia. Untuk membatasi temuan untuk kontrol ini hanya pada satu Wilayah, Anda dapat memperbarui pengaturan AWS Config perekam dan menonaktifkan perekaman sumber daya global di semua Wilayah kecuali Wilayah asal. Jika kontrol yang diaktifkan yang melibatkan sumber daya global tidak didukung di Wilayah asal, CSPM Security Hub mencoba mengaktifkan kontrol di satu Wilayah tertaut di mana kontrol didukung. Dengan konfigurasi pusat, Anda tidak memiliki cakupan untuk kontrol yang tidak tersedia di Wilayah asal atau Wilayah yang ditautkan. Untuk daftar kontrol yang melibatkan sumber daya global, lihat [Kontrol yang menggunakan sumber daya global](#).

Security Hub CSPM console

Untuk membuat dan mengaitkan kebijakan konfigurasi

1. Buka konsol AWS Security Hub Cloud Security Posture Management (CSPM) di <https://console.aws.amazon.com/securityhub/>

Masuk menggunakan kredensi akun administrator CSPM Security Hub yang didelegasikan di Wilayah asal.

2. Di panel navigasi, pilih Konfigurasi dan tab Kebijakan. Kemudian, pilih Buat kebijakan.
3. Pada halaman Konfigurasi organisasi, jika ini adalah pertama kalinya Anda membuat kebijakan konfigurasi, Anda akan melihat tiga opsi di bawah Jenis konfigurasi. Jika Anda telah membuat setidaknya satu kebijakan konfigurasi, Anda hanya melihat opsi Kebijakan kustom.
 - Pilih Gunakan konfigurasi CSPM Security Hub yang AWS direkomendasikan di seluruh organisasi saya untuk menggunakan kebijakan yang kami rekomendasikan. Kebijakan yang direkomendasikan memungkinkan CSPM Security Hub di semua akun organisasi, mengaktifkan standar Praktik Terbaik Keamanan AWS Dasar (FSBP), dan memungkinkan semua kontrol FSBP baru dan yang sudah ada. Kontrol menggunakan nilai parameter default.
 - Pilih Saya belum siap untuk mengonfigurasi untuk membuat kebijakan konfigurasi nanti.
 - Pilih Kebijakan khusus untuk membuat kebijakan konfigurasi kustom. Tentukan apakah akan mengaktifkan atau menonaktifkan CSPM Security Hub, standar mana yang akan diaktifkan, dan kontrol mana yang akan diaktifkan di seluruh standar tersebut. Secara

opsional, tentukan [nilai parameter khusus](#) untuk satu atau beberapa kontrol yang diaktifkan yang mendukung parameter kustom.

4. Di bagian Akun, pilih akun target mana OUs, atau root yang Anda inginkan untuk diterapkan oleh kebijakan konfigurasi Anda.
 - Pilih Semua akun jika Anda ingin menerapkan kebijakan konfigurasi ke root. Ini termasuk semua akun dan OUs di organisasi yang tidak memiliki kebijakan lain yang diterapkan atau diwariskan.
 - Pilih Akun khusus jika Anda ingin menerapkan kebijakan konfigurasi ke akun tertentu atau OUs. Masukkan akun IDs, atau pilih akun dan OUs dari struktur organisasi. Anda dapat menerapkan kebijakan ke maksimal 15 target (akun OUs, atau root) saat Anda membuatnya. Untuk menentukan angka yang lebih besar, edit kebijakan Anda setelah dibuat, dan terapkan ke target tambahan.
 - Pilih Administrator yang didelegasikan hanya untuk menerapkan kebijakan konfigurasi ke akun administrator yang didelegasikan saat ini.
5. Pilih Berikutnya.
6. Pada halaman Tinjau dan terapkan, tinjau detail kebijakan konfigurasi Anda. Kemudian, pilih Buat kebijakan dan terapkan. Di Wilayah beranda dan Wilayah tertaut, tindakan ini mengesampingkan setelan konfigurasi akun yang ada yang terkait dengan kebijakan konfigurasi ini. Akun dapat dikaitkan dengan kebijakan konfigurasi melalui aplikasi, atau warisan dari node induk. Akun turunan dan target OUs yang diterapkan akan secara otomatis mewarisi kebijakan konfigurasi ini kecuali secara khusus dikecualikan, dikelola sendiri, atau menggunakan kebijakan konfigurasi yang berbeda.

Security Hub CSPM API

Untuk membuat dan mengaitkan kebijakan konfigurasi

1. Memanggil [CreateConfigurationPolicy](#) API dari akun administrator yang didelegasikan CSPM Security Hub di Wilayah asal.
2. Untuk `Name`, berikan nama unik untuk kebijakan konfigurasi. Secara opsional, untuk `Description`, berikan deskripsi untuk kebijakan konfigurasi.
3. Untuk `ServiceEnabled` bidang, tentukan apakah Anda ingin CSPM Security Hub diaktifkan atau dinonaktifkan dalam kebijakan konfigurasi ini.
4. Untuk `EnabledStandardIdentifiers` bidang, tentukan standar CSPM Security Hub mana yang ingin Anda aktifkan dalam kebijakan konfigurasi ini.

5. Untuk `SecurityControlsConfiguration` objek, tentukan kontrol mana yang ingin Anda aktifkan atau nonaktifkan dalam kebijakan konfigurasi ini. Memilih `EnabledSecurityControlIdentifiers` berarti bahwa kontrol yang ditentukan diaktifkan. Kontrol lain yang merupakan bagian dari standar Anda yang diaktifkan (termasuk kontrol yang baru dirilis) dinonaktifkan. Memilih `DisabledSecurityControlIdentifiers` berarti bahwa kontrol yang ditentukan dinonaktifkan. Kontrol lain yang merupakan bagian dari standar Anda yang diaktifkan (termasuk kontrol yang baru dirilis) diaktifkan.
6. Secara opsional, untuk `SecurityControlCustomParameters` bidang, tentukan kontrol yang diaktifkan yang ingin Anda sesuaikan parameternya. Berikan `CUSTOM ValueType` bidang dan nilai parameter khusus untuk `Value` bidang tersebut. Nilai harus tipe data yang benar dan dalam rentang valid yang ditentukan oleh Security Hub CSPM. Hanya kontrol pilih yang mendukung nilai parameter khusus. Untuk informasi selengkapnya, lihat [Memahami parameter kontrol di Security Hub CSPM](#).
7. Untuk menerapkan kebijakan konfigurasi Anda ke akun atau OUs, panggil [StartConfigurationPolicyAssociation](#) API dari akun administrator yang didelegasikan CSPM Security Hub di Wilayah beranda.
8. Untuk `ConfigurationPolicyIdentifier` bidang ini, berikan Nama Sumber Daya Amazon (ARN) atau pengenal unik universal (UUID) kebijakan. ARN dan UUID dikembalikan oleh API. `CreateConfigurationPolicy` Untuk konfigurasi yang dikelola sendiri, `ConfigurationPolicyIdentifier` bidangnya sama dengan `SELF_MANAGED_SECURITY_HUB`.
9. Untuk `Target` bidang, berikan OU, akun, atau ID root yang Anda inginkan untuk menerapkan kebijakan konfigurasi ini. Anda hanya dapat memberikan satu target di setiap permintaan API. Akun turunan dan target OUs yang dipilih akan secara otomatis mewarisi kebijakan konfigurasi ini kecuali akun tersebut dikelola sendiri atau menggunakan kebijakan konfigurasi yang berbeda.

Contoh permintaan API untuk membuat kebijakan konfigurasi:

```
{
  "Name": "SampleConfigurationPolicy",
  "Description": "Configuration policy for production accounts",
  "ConfigurationPolicy": {
    "SecurityHub": {
      "ServiceEnabled": true,
      "EnabledStandardIdentifiers": [
```

```

        "arn:aws:securityhub:us-east-1::standards/aws-foundational-
security-best-practices/v/1.0.0",
        "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0"
    ],
    "SecurityControlsConfiguration": {
        "DisabledSecurityControlIdentifiers": [
            "CloudTrail.2"
        ],
        "SecurityControlCustomParameters": [
            {
                "SecurityControlId": "ACM.1",
                "Parameters": {
                    "daysToExpiration": {
                        "ValueType": "CUSTOM",
                        "Value": {
                            "Integer": 15
                        }
                    }
                }
            }
        ]
    }
}

```

Contoh permintaan API untuk mengaitkan kebijakan konfigurasi:

```

{
    "ConfigurationPolicyIdentifier": "arn:aws:securityhub:us-
east-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "Target": {"OrganizationalUnitId": "ou-examplerootid111-exampleouid111"}
}

```

AWS CLI

Untuk membuat dan mengaitkan kebijakan konfigurasi

1. Jalankan [create-configuration-policy](#) perintah dari akun administrator yang didelegasikan CSPM Security Hub di wilayah rumah.

2. Untuk `name`, berikan nama unik untuk kebijakan konfigurasi. Secara opsional, untuk `description`, berikan deskripsi untuk kebijakan konfigurasi.
3. Untuk `ServiceEnabled` bidang, tentukan apakah Anda ingin CSPM Security Hub diaktifkan atau dinonaktifkan dalam kebijakan konfigurasi ini.
4. Untuk `EnabledStandardIdentifiers` bidang, tentukan standar CSPM Security Hub mana yang ingin Anda aktifkan dalam kebijakan konfigurasi ini.
5. Untuk `SecurityControlsConfiguration` bidang, tentukan kontrol mana yang ingin Anda aktifkan atau nonaktifkan dalam kebijakan konfigurasi ini. Memilih `EnabledSecurityControlIdentifiers` berarti bahwa kontrol yang ditentukan diaktifkan. Kontrol lain yang merupakan bagian dari standar Anda yang diaktifkan (termasuk kontrol yang baru dirilis) dinonaktifkan. Memilih `DisabledSecurityControlIdentifiers` berarti bahwa kontrol yang ditentukan dinonaktifkan. Kontrol lain yang berlaku untuk standar Anda yang diaktifkan (termasuk kontrol yang baru dirilis) diaktifkan.
6. Secara opsional, untuk `SecurityControlCustomParameters` bidang, tentukan kontrol yang diaktifkan yang ingin Anda sesuaikan parameternya. Berikan `CUSTOM ValueType` bidang dan nilai parameter khusus untuk `Value` bidang tersebut. Nilai harus tipe data yang benar dan dalam rentang valid yang ditentukan oleh Security Hub CSPM. Hanya kontrol pilih yang mendukung nilai parameter khusus. Untuk informasi selengkapnya, lihat [Memahami parameter kontrol di Security Hub CSPM](#).
7. Untuk menerapkan kebijakan konfigurasi Anda ke akun atau OUs, jalankan [start-configuration-policy-association](#) perintah dari akun administrator yang didelegasikan CSPM Security Hub di Wilayah beranda.
8. Untuk `configuration-policy-identifier` bidang, berikan Nama Sumber Daya Amazon (ARN) atau ID kebijakan konfigurasi. ARN dan ID ini dikembalikan oleh perintah `create-configuration-policy`.
9. Untuk `target` bidang, berikan OU, akun, atau ID root yang Anda inginkan untuk menerapkan kebijakan konfigurasi ini. Anda hanya dapat memberikan satu target setiap kali Anda menjalankan perintah. Anak-anak dari target yang dipilih akan secara otomatis mewarisi kebijakan konfigurasi ini kecuali mereka dikelola sendiri atau menggunakan kebijakan konfigurasi yang berbeda.

Contoh perintah untuk membuat kebijakan konfigurasi:

```
aws securityhub --region us-east-1 create-configuration-policy \
--name "SampleConfigurationPolicy" \
```

```
--description "Configuration policy for production accounts" \
--configuration-policy '{"SecurityHub": {"ServiceEnabled": true,
  "EnabledStandardIdentifiers": ["arn:aws:securityhub:us-east-1::standards/aws-
foundational-security-best-practices/v/1.0.0", "arn:aws:securityhub:::ruleset/
cis-aws-foundations-benchmark/v/1.2.0"], "SecurityControlsConfiguration":
{"DisabledSecurityControlIdentifiers": ["CloudTrail.2"],
  "SecurityControlCustomParameters": [{"SecurityControlId": "ACM.1", "Parameters":
{"daysToExpiration": {"ValueType": "CUSTOM", "Value": {"Integer": 15}}}]}}}'
```

Contoh perintah untuk mengaitkan kebijakan konfigurasi:

```
aws securityhub --region us-east-1 start-configuration-policy-association \
--configuration-policy-identifier "arn:aws:securityhub:us-
east-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111" \
--target '{"OrganizationalUnitId": "ou-examplerootid111-exampleouid111"}'
```

StartConfigurationPolicyAssociationAPI mengembalikan bidang yang disebut AssociationStatus. Bidang ini memberi tahu Anda apakah asosiasi kebijakan sedang tertunda atau dalam keadaan berhasil atau gagal. Diperlukan waktu hingga 24 jam agar status berubah dari PENDING ke SUCCESS atau FAILURE. Untuk informasi selengkapnya tentang status asosiasi, lihat [Meninjau status asosiasi kebijakan konfigurasi](#).

Meninjau status dan detail kebijakan konfigurasi

Administrator AWS Security Hub Cloud Security Posture Management (CSPM) yang didelegasikan dapat melihat kebijakan konfigurasi untuk organisasi dan detailnya. Ini termasuk akun dan unit organisasi (OUs) mana yang terkait dengan kebijakan.

Untuk informasi latar belakang tentang manfaat konfigurasi pusat dan cara kerjanya, lihat [Memahami konfigurasi pusat di Security Hub CSPM](#).

Pilih metode pilihan Anda, dan ikuti langkah-langkah untuk melihat kebijakan konfigurasi Anda.

Security Hub CSPM console

Untuk melihat kebijakan konfigurasi (konsol)

1. Buka konsol AWS Security Hub Cloud Security Posture Management (CSPM) di. <https://console.aws.amazon.com/securityhub/>

Masuk menggunakan kredensial akun administrator CSPM Security Hub yang didelegasikan di Wilayah asal.

2. Di panel navigasi, pilih Pengaturan dan Konfigurasi.
3. Pilih tab Kebijakan untuk ikhtisar kebijakan konfigurasi Anda.
4. Pilih kebijakan konfigurasi, dan pilih Lihat detail untuk melihat detail tambahan tentangnya, termasuk akun mana dan OUs yang terkait dengannya.

Security Hub CSPM API

Untuk melihat daftar ringkasan semua kebijakan konfigurasi Anda, gunakan [ListConfigurationPolicies](#) pengoperasian API CSPM Security Hub. Jika Anda menggunakan AWS CLI, jalankan [list-configuration-policies](#) perintah. Akun administrator CSPM Security Hub yang didelegasikan harus menjalankan operasi di Wilayah asal.

```
$ aws securityhub list-configuration-policies \
--max-items 5 \
--starting-token U2FsdGVkX19nUI2zoh+Pou9YyutLYJHWpn9xnG4hqS0hvw3o2JqjI23QDxdf
```

Untuk melihat detail tentang kebijakan konfigurasi tertentu, gunakan [GetConfigurationPolicy](#) operasi. Jika Anda menggunakan AWS CLI, jalankan [get-configuration-policy](#). Akun administrator yang didelegasikan harus menjalankan operasi di Wilayah asal. Berikan Nama Sumber Daya Amazon (ARN) atau ID kebijakan konfigurasi yang detailnya ingin Anda lihat.

```
$ aws securityhub get-configuration-policy \
--identifier "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE1111"
```

Untuk melihat daftar ringkasan semua kebijakan konfigurasi Anda dan asosiasi akun mereka, gunakan [ListConfigurationPolicyAssociations](#) operasi. Jika Anda menggunakan AWS CLI, jalankan [list-configuration-policy-associations](#) perintah. Akun administrator yang didelegasikan harus menjalankan operasi di Wilayah asal. Secara opsional, Anda dapat memberikan parameter pagination atau memfilter hasil berdasarkan ID kebijakan tertentu, jenis asosiasi, atau status asosiasi.

```
$ aws securityhub list-configuration-policy-associations \
--filters '{"AssociationType": "APPLIED"}'
```

Untuk melihat asosiasi untuk akun tertentu, gunakan [GetConfigurationPolicyAssociation](#) operasi. Jika Anda menggunakan AWS CLI, jalankan [get-configuration-policy-association](#) perintah. Akun administrator yang didelegasikan harus menjalankan operasi di Wilayah asal. Untuk `target`, berikan nomor akun, ID OU, atau ID root.

```
$ aws securityhub get-configuration-policy-association \
--target '{"AccountId": "123456789012"}'
```

Meninjau status asosiasi kebijakan konfigurasi

Operasi API konfigurasi pusat berikut mengembalikan bidang yang disebut `AssociationStatus`:

- `BatchGetConfigurationPolicyAssociations`
- `GetConfigurationPolicyAssociation`
- `ListConfigurationPolicyAssociations`
- `StartConfigurationPolicyAssociation`

Bidang ini dikembalikan baik ketika konfigurasi yang mendasarinya adalah kebijakan konfigurasi dan ketika itu adalah perilaku yang dikelola sendiri.

Nilai `AssociationStatus` memberi tahu Anda apakah asosiasi kebijakan tertunda atau dalam keadaan berhasil atau gagal untuk akun tertentu. Diperlukan waktu hingga 24 jam agar status berubah dari `PENDING` ke `SUCCESS` atau `FAILED`. Status `SUCCESS` berarti bahwa semua pengaturan yang ditentukan dalam kebijakan konfigurasi dikaitkan dengan akun. Status `FAILED` berarti bahwa satu atau beberapa pengaturan yang ditentukan dalam kebijakan konfigurasi gagal dikaitkan dengan akun. Meskipun `FAILED` status, akun dapat dikonfigurasi sebagian sesuai dengan kebijakan. Misalnya, Anda dapat mencoba mengaitkan akun dengan kebijakan konfigurasi yang mengaktifkan CSPM Security Hub, mengaktifkan Praktik Terbaik Keamanan AWS Dasar, dan menonaktifkan.1. CloudTrail Dua pengaturan awal bisa berhasil, tetapi pengaturan CloudTrail .1 bisa gagal. Dalam contoh ini, status asosiasi `FAILED` meskipun beberapa pengaturan telah dikonfigurasi dengan benar.

Status asosiasi OU orang tua atau root tergantung pada status anak-anaknya. Jika status asosiasi semua anak adalah `SUCCESS`, status asosiasi orang tua adalah `SUCCESS`. Jika status asosiasi satu atau lebih anak adalah `FAILED`, status asosiasi orang tua adalah `FAILED`.

Nilai `AssociationStatus` tergantung pada status asosiasi kebijakan di semua Wilayah terkait. Jika asosiasi berhasil di Wilayah asal dan semua Daerah terkait, nilainya `AssociationStatus`

adalah `SUCCESS`. Jika asosiasi gagal di satu atau lebih Wilayah ini, nilainya `AssociationStatus` adalah `FAILED`.

Perilaku berikut juga berdampak pada nilai `AssociationStatus`:

- Jika targetnya adalah OU orang tua atau root, ia memiliki `AssociationStatus` dari `SUCCESS` atau `FAILED` hanya ketika semua anak memiliki `FAILED` status `SUCCESS` atau. Jika status asosiasi akun turunan atau OU berubah (misalnya, saat Wilayah tertaut ditambahkan atau dihapus) setelah Anda pertama kali mengaitkan induk dengan konfigurasi, perubahan tersebut tidak akan memperbarui status asosiasi induk kecuali Anda menjalankan `StartConfigurationPolicyAssociation` API lagi.
- Jika targetnya adalah akun, ia memiliki `AssociationStatus` dari `SUCCESS` atau `FAILED` hanya jika asosiasi memiliki hasil dari `SUCCESS` atau `FAILED` di Wilayah asal dan semua Wilayah yang ditautkan. Jika status asosiasi akun target berubah (misalnya, saat Wilayah tertaut ditambahkan atau dihapus) setelah Anda pertama kali mengaitkannya dengan konfigurasi, status asosiasinya akan diperbarui. Namun, perubahan tidak memperbarui status asosiasi induk kecuali Anda memanggil `StartConfigurationPolicyAssociation` API lagi.

Jika Anda menambahkan Wilayah tertaut baru, Security Hub CSPM mereplikasi asosiasi Anda yang ada di `PENDING`, `SUCCESS`, atau `FAILED` negara bagian di Wilayah baru.

Bahkan ketika status asosiasi adalah `SUCCESS`, status pemberdayaan standar yang merupakan bagian dari kebijakan dapat beralih ke keadaan yang tidak lengkap. Dalam hal ini, Security Hub CSPM tidak dapat menghasilkan temuan untuk kontrol standar. Untuk informasi selengkapnya, lihat [Memeriksa status standar](#).

Mengatasi masalah kegagalan asosiasi

Di AWS Security Hub Cloud Security Posture Management (CSPM), asosiasi kebijakan konfigurasi mungkin gagal karena alasan umum berikut.

- Akun manajemen Organisasi bukan anggota - Jika Anda ingin mengaitkan kebijakan konfigurasi dengan akun manajemen Organizations, akun tersebut harus sudah mengaktifkan AWS Security Hub Cloud Security Posture Management (CSPM). Ini membuat akun manajemen menjadi akun anggota dalam organisasi.
- AWS Config tidak diaktifkan atau dikonfigurasi dengan benar — Untuk mengaktifkan standar dalam kebijakan konfigurasi, AWS Config harus diaktifkan dan dikonfigurasi untuk merekam sumber daya yang relevan.

- Harus dikaitkan dari akun administrator yang didelegasikan — Anda hanya dapat mengaitkan kebijakan dengan akun target dan OUs saat Anda masuk ke akun administrator CSPM Security Hub yang didelegasikan.
- Harus dikaitkan dari wilayah asal — Anda hanya dapat mengaitkan kebijakan dengan akun target dan OUs saat Anda masuk ke Wilayah asal Anda.
- Keikutsertaan Wilayah tidak diaktifkan — Asosiasi kebijakan gagal untuk akun anggota atau OU di Wilayah tertaut jika itu adalah Wilayah keikutsertaan yang belum diaktifkan oleh administrator yang didelegasikan. Anda dapat mencoba lagi setelah mengaktifkan Region dari akun administrator yang didelegasikan.
- Akun anggota ditangguhkan — Asosiasi kebijakan gagal jika Anda mencoba mengaitkan kebijakan dengan akun anggota yang ditangguhkan.

Memperbarui kebijakan konfigurasi

Setelah membuat kebijakan konfigurasi, akun administrator AWS Security Hub Cloud Security Posture Management (CSPM) yang didelegasikan dapat memperbarui detail kebijakan dan asosiasi kebijakan. Saat detail kebijakan diperbarui, akun yang terkait dengan kebijakan konfigurasi secara otomatis mulai menggunakan kebijakan yang diperbarui.

Untuk informasi latar belakang tentang manfaat konfigurasi pusat dan cara kerjanya, lihat [Memahami konfigurasi pusat di Security Hub CSPM](#).

Administrator yang didelegasikan dapat memperbarui setelan kebijakan berikut:

- Mengaktifkan atau menonaktifkan Security Hub CSPM.
- Aktifkan satu atau lebih [standar keamanan](#).
- Tunjukkan [kontrol keamanan](#) mana yang diaktifkan di seluruh standar yang diaktifkan. Anda dapat melakukannya dengan menyediakan daftar kontrol khusus yang harus diaktifkan, dan Security Hub CSPM menonaktifkan semua kontrol lainnya, termasuk kontrol baru saat dirilis. Atau, Anda dapat memberikan daftar kontrol khusus yang harus dinonaktifkan, dan Security Hub CSPM mengaktifkan semua kontrol lainnya, termasuk kontrol baru saat dirilis.
- Secara opsional, [sesuaikan parameter](#) untuk memilih kontrol yang diaktifkan di seluruh standar yang diaktifkan.

Pilih metode pilihan Anda, dan ikuti langkah-langkah untuk memperbarui kebijakan konfigurasi.

 Note

Jika Anda menggunakan konfigurasi pusat, Security Hub CSPM secara otomatis menonaktifkan kontrol yang melibatkan sumber daya global di semua Wilayah kecuali Wilayah asal. Kontrol lain yang Anda pilih untuk diaktifkan meskipun kebijakan konfigurasi diaktifkan di semua Wilayah yang tersedia. Untuk membatasi temuan untuk kontrol ini hanya pada satu Wilayah, Anda dapat memperbarui pengaturan AWS Config perekam dan menonaktifkan perekaman sumber daya global di semua Wilayah kecuali Wilayah asal. Jika kontrol yang diaktifkan yang melibatkan sumber daya global tidak didukung di Wilayah asal, CSPM Security Hub mencoba mengaktifkan kontrol di satu Wilayah tertaut di mana kontrol didukung. Dengan konfigurasi pusat, Anda tidak memiliki cakupan untuk kontrol yang tidak tersedia di Wilayah asal atau Wilayah yang ditautkan. Untuk daftar kontrol yang melibatkan sumber daya global, lihat [Kontrol yang menggunakan sumber daya global](#).

Console

Untuk memperbarui kebijakan konfigurasi

1. Buka konsol AWS Security Hub Cloud Security Posture Management (CSPM) di <https://console.aws.amazon.com/securityhub/>

Masuk menggunakan kredensial akun administrator CSPM Security Hub yang didelegasikan di Wilayah asal.

2. Di panel navigasi, pilih Pengaturan dan Konfigurasi.
3. Pilih tab Kebijakan.
4. Pilih kebijakan konfigurasi yang ingin Anda edit, lalu pilih Edit. Jika diinginkan, edit pengaturan kebijakan. Biarkan bagian ini seolah-olah Anda ingin menjaga pengaturan kebijakan tidak berubah.
5. Pilih Berikutnya. Jika diinginkan, edit asosiasi kebijakan. Biarkan bagian ini seolah-olah Anda ingin menjaga agar asosiasi kebijakan tidak berubah. Anda dapat mengaitkan atau memisahkan kebijakan dengan maksimal 15 target (akun OUs, atau root) saat Anda memperbaruinya.
6. Pilih Berikutnya.

7. Tinjau perubahan Anda, lalu pilih Simpan dan terapkan. Di Wilayah beranda dan Wilayah tertaut, tindakan ini mengesampingkan setelan konfigurasi akun yang ada yang terkait dengan kebijakan konfigurasi ini. Akun dapat dikaitkan dengan kebijakan konfigurasi melalui aplikasi, atau warisan dari node induk.

API

Untuk memperbarui kebijakan konfigurasi

1. Untuk memperbarui setelan dalam kebijakan konfigurasi, panggil [UpdateConfigurationPolicy](#) API dari akun administrator yang didelegasikan CSPM Security Hub di Wilayah beranda.
2. Berikan Nama Sumber Daya Amazon (ARN) atau ID kebijakan konfigurasi yang ingin Anda perbarui.
3. Berikan nilai yang diperbarui untuk bidang `ConfigurationPolicy`. Secara opsional, Anda juga dapat memberikan alasan untuk pembaruan.
4. Untuk menambahkan asosiasi baru untuk kebijakan konfigurasi ini, panggil [StartConfigurationPolicyAssociation](#) API dari akun administrator yang didelegasikan CSPM Security Hub di Wilayah beranda. Untuk menghapus satu atau beberapa asosiasi saat ini, panggil [StartConfigurationPolicyDisassociation](#) API dari akun administrator yang didelegasikan CSPM Security Hub di Wilayah beranda.
5. Untuk `ConfigurationPolicyIdentifier` bidang, berikan ARN atau ID kebijakan konfigurasi yang asosiasinya ingin Anda perbarui.
6. Untuk `Target` bidang, berikan akun OUs, atau ID root yang ingin Anda kaitkan atau lepaskan. Tindakan ini mengesampingkan asosiasi kebijakan sebelumnya untuk yang ditentukan OUs atau akun.

Note

Saat Anda menjalankan `UpdateConfigurationPolicy` API, Security Hub CSPM melakukan penggantian daftar lengkap untuk `EnabledStandardIdentifiers`, `EnabledSecurityControlIdentifiers`, `DisabledSecurityControlIdentifiers`, dan bidang `SecurityControlCustomParameters`. Setiap kali Anda menjalankan API ini, berikan daftar lengkap standar yang ingin Anda aktifkan dan daftar lengkap kontrol yang ingin Anda aktifkan atau nonaktifkan dan sesuaikan parameternya.

Contoh permintaan API untuk memperbarui kebijakan konfigurasi:

```
{
  "Identifier": "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "Description": "Updated configuration policy",
  "UpdatedReason": "Disabling CloudWatch.1",
  "ConfigurationPolicy": {
    "SecurityHub": {
      "ServiceEnabled": true,
      "EnabledStandardIdentifiers": [
        "arn:aws:securityhub:us-east-1::standards/aws-foundational-
security-best-practices/v/1.0.0",
        "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0"
      ],
      "SecurityControlsConfiguration": {
        "DisabledSecurityControlIdentifiers": [
          "CloudTrail.2",
          "CloudWatch.1"
        ],
        "SecurityControlCustomParameters": [
          {
            "SecurityControlId": "ACM.1",
            "Parameters": {
              "daysToExpiration": {
                "ValueType": "CUSTOM",
                "Value": {
                  "Integer": 15
                }
              }
            }
          }
        ]
      }
    }
  }
}
```

AWS CLI

Untuk memperbarui kebijakan konfigurasi

1. Untuk memperbarui pengaturan dalam kebijakan konfigurasi, jalankan [update-configuration-policy](#) perintah dari akun administrator yang didelegasikan CSPM Security Hub di Wilayah beranda.
2. Berikan Nama Sumber Daya Amazon (ARN) atau ID kebijakan konfigurasi yang ingin Anda perbarui.
3. Berikan nilai yang diperbarui untuk bidang di bawah `configuration-policy`. Secara opsional, Anda juga dapat memberikan alasan untuk pembaruan.
4. Untuk menambahkan asosiasi baru untuk kebijakan konfigurasi ini, jalankan [start-configuration-policy-association](#) perintah dari akun administrator yang didelegasikan CSPM Security Hub di Wilayah beranda. Untuk menghapus satu atau beberapa asosiasi saat ini, jalankan [start-configuration-policy-disassociation](#) perintah dari akun administrator yang didelegasikan CSPM Security Hub di Wilayah rumah.
5. Untuk `configuration-policy-identifier` bidang, berikan ARN atau ID kebijakan konfigurasi yang asosiasinya ingin Anda perbarui.
6. Untuk target bidang, berikan akun OUs, atau ID root yang ingin Anda kaitkan atau lepaskan. Tindakan ini mengesampingkan asosiasi kebijakan sebelumnya untuk yang ditentukan OUs atau akun.

Note

Saat Anda menjalankan `update-configuration-policy` perintah, Security Hub CSPM melakukan penggantian daftar lengkap untuk `EnabledStandardIdentifiers`, `EnabledSecurityControlIdentifiers`, `DisabledSecurityControlIdentifiers`, dan `SecurityControlCustomParameters` bidang. Setiap kali Anda menjalankan perintah ini, berikan daftar lengkap standar yang ingin Anda aktifkan dan daftar lengkap kontrol yang ingin Anda aktifkan atau nonaktifkan dan sesuaikan parameternya.

Contoh perintah untuk memperbarui kebijakan konfigurasi:

```
aws securityhub update-configuration-policy \  
--region us-east-1 \  

```

```
--identifier "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE1111" \
--description "Updated configuration policy" \
--updated-reason "Disabling CloudWatch.1" \
--configuration-policy '{"SecurityHub": {"ServiceEnabled": true,
"EnabledStandardIdentifiers": ["arn:aws:securityhub:us-east-1::standards/aws-
foundational-security-best-practices/v/1.0.0", "arn:aws:securityhub::ruleset/
cis-aws-foundations-benchmark/v/1.2.0"], "SecurityControlsConfiguration":
{"DisabledSecurityControlIdentifiers": ["CloudTrail.2", "CloudWatch.1"],
"SecurityControlCustomParameters": [{"SecurityControlId": "ACM.1", "Parameters":
{"daysToExpiration": {"ValueType": "CUSTOM", "Value": {"Integer": 15}}}]}}}'
```

StartConfigurationPolicyAssociationAPI mengembalikan bidang yang disebut AssociationStatus. Bidang ini memberi tahu Anda apakah asosiasi kebijakan sedang tertunda atau dalam keadaan berhasil atau gagal. Diperlukan waktu hingga 24 jam agar status berubah dari PENDING ke SUCCESS atau FAILURE. Untuk informasi selengkapnya tentang status asosiasi, lihat [Meninjau status asosiasi kebijakan konfigurasi](#).

Menghapus kebijakan konfigurasi

Setelah membuat kebijakan konfigurasi, administrator AWS Security Hub Cloud Security Posture Management (CSPM) yang didelegasikan dapat menghapusnya. Atau, administrator yang didelegasikan dapat mempertahankan kebijakan, tetapi memisahkannya dari akun tertentu atau unit organisasi (OUs), atau dari root. Untuk petunjuk tentang pemutusan kebijakan, lihat [Memutuskan konfigurasi dari targetnya](#).

Untuk informasi latar belakang tentang manfaat konfigurasi pusat dan cara kerjanya, lihat [Memahami konfigurasi pusat di Security Hub CSPM](#).

Bagian ini menjelaskan cara menghapus kebijakan konfigurasi.

Saat Anda menghapus kebijakan konfigurasi, kebijakan tersebut tidak ada lagi untuk organisasi Anda. Akun target, OUs, dan root organisasi tidak dapat lagi menggunakan kebijakan konfigurasi. Target yang dikaitkan dengan kebijakan konfigurasi yang dihapus mewarisi kebijakan konfigurasi induk terdekat, atau dikelola sendiri jika induk terdekat dikelola sendiri. Jika Anda ingin target menggunakan konfigurasi yang berbeda, Anda dapat mengaitkan target dengan kebijakan konfigurasi baru. Untuk informasi selengkapnya, lihat [Membuat dan mengaitkan kebijakan konfigurasi](#).

Sebaiknya buat dan kaitkan setidaknya satu kebijakan konfigurasi dengan organisasi Anda untuk memberikan cakupan keamanan yang memadai.

Sebelum Anda dapat menghapus kebijakan konfigurasi, Anda harus memisahkan kebijakan dari akun apa pun OUs, atau root yang berlaku saat ini.

Pilih metode pilihan Anda, dan ikuti langkah-langkah untuk menghapus kebijakan konfigurasi.

Console

Untuk menghapus kebijakan konfigurasi

1. Buka konsol AWS Security Hub Cloud Security Posture Management (CSPM) di <https://console.aws.amazon.com/securityhub/>

Masuk menggunakan kredensial akun administrator CSPM Security Hub yang didelegasikan di Wilayah asal.

2. Di panel navigasi, pilih Pengaturan dan Konfigurasi.
3. Pilih tab Kebijakan. Pilih kebijakan konfigurasi yang ingin Anda hapus, lalu pilih Hapus. Jika kebijakan konfigurasi masih terkait dengan akun apa pun atau OUs, Anda diminta untuk terlebih dahulu memisahkan kebijakan dari target tersebut sebelum dapat menghapusnya.
4. Tinjau pesan konfirmasi. Masukkan **confirm**, dan pilih Hapus.

API

Untuk menghapus kebijakan konfigurasi

Memanggil [DeleteConfigurationPolicy](#) API dari akun administrator yang didelegasikan CSPM Security Hub di Wilayah asal.

Berikan Nama Sumber Daya Amazon (ARN) atau ID kebijakan konfigurasi yang ingin Anda hapus. Jika Anda menerima `ConflictException` kesalahan, kebijakan konfigurasi masih berlaku untuk akun atau OUs di organisasi Anda. Untuk mengatasi kesalahan, putuskan kebijakan konfigurasi dari akun ini atau OUs sebelum mencoba menghapusnya.

Contoh permintaan API untuk menghapus kebijakan konfigurasi:

```
{
  "Identifier": "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

```
}
```

AWS CLI

Untuk menghapus kebijakan konfigurasi

Jalankan [delete-configuration-policy](#) perintah dari akun administrator yang didelegasikan CSPM Security Hub di wilayah rumah.

Berikan Nama Sumber Daya Amazon (ARN) atau ID kebijakan konfigurasi yang ingin Anda hapus. Jika Anda menerima `ConflictException` kesalahan, kebijakan konfigurasi masih berlaku untuk akun atau OUs di organisasi Anda. Untuk mengatasi kesalahan, putuskan kebijakan konfigurasi dari akun ini atau OUs sebelum mencoba menghapusnya.

```
aws securityhub --region us-east-1 delete-configuration-policy \
--identifier "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

Memutuskan konfigurasi dari targetnya

Dari akun administrator AWS Security Hub Cloud Security Posture Management (CSPM) yang didelegasikan, Anda dapat memisahkan kebijakan konfigurasi atau konfigurasi yang dikelola sendiri dari akun, OU, atau root. Disassociation mempertahankan kebijakan untuk penggunaan di masa mendatang, tetapi menghapus asosiasi yang ada dari akun tertentu OUs, atau root. Anda hanya dapat memisahkan konfigurasi yang diterapkan secara langsung, bukan konfigurasi yang diwariskan. Untuk mengubah konfigurasi yang diwariskan, Anda dapat menerapkan kebijakan konfigurasi atau perilaku yang dikelola sendiri ke akun atau OU yang terpengaruh. Anda juga dapat menerapkan kebijakan konfigurasi baru, yang mencakup modifikasi yang Anda inginkan, ke induk terdekat.

Disassociation tidak menghapus kebijakan konfigurasi. Kebijakan ini disimpan di akun Anda, sehingga Anda dapat mengaitkannya dengan target lain di organisasi Anda. Untuk petunjuk tentang menghapus kebijakan konfigurasi, lihat [Menghapus kebijakan konfigurasi](#). Ketika disosiasi selesai, target yang terpengaruh mewarisi kebijakan konfigurasi atau perilaku yang dikelola sendiri dari induk terdekat. Jika tidak ada konfigurasi yang dapat diwariskan, target mempertahankan pengaturan yang dimilikinya sebelum disosiasi tetapi menjadi dikelola sendiri.

Pilih metode pilihan Anda, dan ikuti langkah-langkah untuk memisahkan akun, OU, atau root dari konfigurasi saat ini.

Console

Untuk memisahkan akun atau OU dari konfigurasi saat ini

1. Buka konsol AWS Security Hub Cloud Security Posture Management (CSPM) di <https://console.aws.amazon.com/securityhub/>

Masuk menggunakan kredensial akun administrator CSPM Security Hub yang didelegasikan di Wilayah asal.
2. Di panel navigasi, pilih Pengaturan dan Konfigurasi.
3. Pada tab Organizations, pilih akun, OU, atau root yang ingin Anda lepaskan dari konfigurasi saat ini. Pilih Edit.
4. Pada halaman Tentukan konfigurasi, untuk Manajemen, pilih Kebijakan diterapkan jika Anda ingin administrator yang didelegasikan dapat menerapkan kebijakan secara langsung ke target. Pilih Inherited jika Anda ingin target mewarisi konfigurasi induk terdekatnya. Dalam salah satu kasus ini, administrator yang didelegasikan mengontrol pengaturan untuk target. Pilih Self-managed jika Anda ingin akun atau OU mengontrol pengaturannya sendiri.
5. Setelah meninjau perubahan Anda, pilih Berikutnya dan Terapkan. Tindakan ini mengesampingkan konfigurasi akun yang ada atau OUs yang berada dalam cakupan, jika konfigurasi tersebut bertentangan dengan pilihan Anda saat ini.

API

Untuk memisahkan akun atau OU dari konfigurasi saat ini

1. Memanggil [StartConfigurationPolicyDisassociation](#) API dari akun administrator yang didelegasikan CSPM Security Hub di Wilayah asal.
2. Untuk `ConfigurationPolicyIdentifier`, berikan Nama Sumber Daya Amazon (ARN) atau ID kebijakan konfigurasi yang ingin Anda putuskan. Sediakan bidang ini `SELF_MANAGED_SECURITY_HUB` untuk memisahkan perilaku yang dikelola sendiri.
3. Untuk `Target`, berikan akun, OUs, atau root yang ingin Anda memisahkan dari kebijakan konfigurasi ini.

Contoh permintaan API untuk memisahkan kebijakan konfigurasi:

```
{
  "ConfigurationPolicyIdentifier": "arn:aws:securityhub:us-
east-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "Target": {"RootId": "r-f6g7h8i9j0example"}
}
```

AWS CLI

Untuk memisahkan akun atau OU dari konfigurasi saat ini

1. Jalankan [start-configuration-policy-disassociation](#) perintah dari akun administrator yang didelegasikan CSPM Security Hub di wilayah rumah.
2. Untuk `configuration-policy-identifiler`, berikan Nama Sumber Daya Amazon (ARN) atau ID kebijakan konfigurasi yang ingin Anda putuskan. Sediakan bidang ini `SELF_MANAGED_SECURITY_HUB` untuk memisahkan perilaku yang dikelola sendiri.
3. Untuk `target`, berikan akun, OUs, atau root yang ingin Anda memisahkan dari kebijakan konfigurasi ini.

Contoh perintah untuk memisahkan kebijakan konfigurasi:

```
aws securityhub --region us-east-1 start-configuration-policy-disassociation \
--configuration-policy-identifiler "arn:aws:securityhub:us-
east-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111" \
--target '{"RootId": "r-f6g7h8i9j0example"}'
```

Mengkonfigurasi standar atau kontrol dalam konteks

Bila Anda menggunakan [konfigurasi pusat](#) di AWS Security Hub Cloud Security Posture Management (CSPM), administrator CSPM Security Hub yang didelegasikan dapat membuat kebijakan konfigurasi yang menentukan cara CSPM Security Hub, standar keamanan, dan kontrol keamanan dikonfigurasi untuk organisasi. Administrator yang didelegasikan dapat mengaitkan kebijakan dengan akun tertentu dan unit organisasi (OU). Kebijakan berlaku di Wilayah asal Anda dan semua Wilayah yang ditautkan. Administrator yang didelegasikan dapat memperbarui kebijakan konfigurasi seperlunya.

Di konsol CSPM Security Hub, administrator yang didelegasikan dapat memperbarui kebijakan konfigurasi dengan dua cara—dari halaman Konfigurasi, atau dalam konteks alur kerja yang

ada. Yang terakhir ini dapat bermanfaat karena, saat Anda melihat temuan keamanan, Anda dapat menemukan standar dan kontrol mana yang paling relevan dengan lingkungan Anda dan mengonfigurasinya pada saat yang bersamaan.

Konfigurasi dalam konteks hanya tersedia di konsol CSPM Security Hub. Secara terprogram, administrator yang didelegasikan harus memanggil [UpdateConfigurationPolicy](#) pengoperasian Security Hub CSPM API untuk mengubah cara standar atau kontrol tertentu dikonfigurasi dalam organisasi.

Ikuti langkah-langkah ini untuk mengonfigurasi standar atau kontrol CSPM Security Hub dalam konteks.

Untuk mengonfigurasi standar atau kontrol dalam konteks (konsol)

1. Buka konsol AWS Security Hub Cloud Security Posture Management (CSPM) di <https://console.aws.amazon.com/securityhub/>

Masuk menggunakan kredensial akun administrator CSPM Security Hub yang didelegasikan di Wilayah asal.

2. Di panel navigasi, pilih salah satu opsi berikut:
 - Untuk mengonfigurasi standar, pilih Standar keamanan, dan pilih standar tertentu.
 - Untuk mengonfigurasi kontrol, pilih Kontrol, dan pilih kontrol tertentu.
3. Konsol mencantumkan kebijakan konfigurasi CSPM Security Hub yang ada dan status standar atau kontrol yang dipilih di masing-masing. Pilih opsi untuk mengaktifkan atau menonaktifkan standar atau kontrol di setiap kebijakan konfigurasi yang ada. Untuk kontrol, Anda juga dapat memilih untuk menyesuaikan [parameter kontrol](#). Anda tidak dapat membuat kebijakan baru selama konfigurasi dalam konteks. Untuk membuat kebijakan baru, Anda harus pergi ke halaman Konfigurasi, pilih tab Kebijakan, lalu pilih Buat kebijakan.
4. Setelah melakukan perubahan, pilih Berikutnya.
5. Tinjau perubahan Anda, dan pilih Terapkan. Pembaruan memengaruhi semua akun dan OUs yang terkait dengan kebijakan konfigurasi yang diubah. Pembaruan juga berlaku di Wilayah asal dan semua Wilayah yang ditautkan.

Menonaktifkan konfigurasi pusat di Security Hub CSPM

Saat Anda menonaktifkan konfigurasi pusat di AWS Security Hub Cloud Security Posture Management (CSPM), administrator yang didelegasikan kehilangan kemampuan untuk

mengonfigurasi CSPM Security Hub, standar keamanan, dan kontrol keamanan di beberapa unit organisasi () Akun AWS, dan. OUs Wilayah AWS Sebagai gantinya, Anda harus mengonfigurasi sebagian besar pengaturan secara terpisah untuk setiap akun di setiap Wilayah.

 Important

Sebelum Anda dapat menonaktifkan konfigurasi pusat, Anda harus terlebih dahulu [memisahkan akun Anda dan OUs](#) dari konfigurasi mereka saat ini, apakah itu kebijakan konfigurasi atau perilaku yang dikelola sendiri.

Sebelum Anda dapat menonaktifkan konfigurasi pusat, Anda juga harus [menghapus kebijakan konfigurasi yang ada](#).

Ketika Anda menonaktifkan konfigurasi pusat, perubahan berikut terjadi:

- Administrator yang didelegasikan tidak dapat lagi membuat kebijakan konfigurasi untuk organisasi.
- Akun yang memiliki kebijakan konfigurasi yang diterapkan atau diwariskan mempertahankan pengaturan mereka saat ini, tetapi menjadi dikelola sendiri.
- Organisasi Anda beralih ke konfigurasi lokal. Di bawah konfigurasi lokal, sebagian besar pengaturan CSPM Security Hub harus dikonfigurasi secara terpisah di setiap akun organisasi dan Wilayah. Administrator yang didelegasikan dapat memilih untuk mengaktifkan CSPM Security Hub secara otomatis, [standar keamanan default](#), dan semua kontrol yang merupakan bagian dari standar default di akun organisasi baru. Standar default adalah AWS Foundational Security Best Practices (FSBP) dan Center for Internet Security (CIS) AWS Foundations Benchmark v1.2.0. Pengaturan ini hanya berlaku di Wilayah saat ini dan hanya memengaruhi akun organisasi baru. Administrator yang didelegasikan tidak dapat mengubah standar mana yang default. Konfigurasi lokal tidak mendukung penggunaan kebijakan konfigurasi atau konfigurasi di tingkat OU.

Identitas akun administrator yang didelegasikan tetap sama ketika Anda berhenti menggunakan konfigurasi pusat. Wilayah asal Anda dan Wilayah terkait juga tetap sama (Wilayah asal Anda sekarang disebut Wilayah agregasi, dan dapat digunakan untuk menemukan agregasi).

Pilih metode pilihan Anda, dan ikuti langkah-langkah untuk berhenti menggunakan konfigurasi pusat dan beralih ke konfigurasi lokal.

Security Hub CSPM console

Untuk menonaktifkan konfigurasi pusat (konsol)

1. Buka konsol AWS Security Hub Cloud Security Posture Management (CSPM) di <https://console.aws.amazon.com/securityhub/>

Masuk menggunakan kredensial akun administrator CSPM Security Hub yang didelegasikan di Wilayah asal.

2. Pada panel navigasi, pilih Pengaturan dan Konfigurasi.
3. Di bagian Ikhtisar, pilih Edit.
4. Di kotak Edit konfigurasi organisasi, pilih Konfigurasi lokal. Jika belum melakukannya, Anda diminta untuk memisahkan dan menghapus kebijakan konfigurasi Anda saat ini sebelum Anda dapat menghentikan konfigurasi pusat. Akun atau OUs yang ditetapkan sebagai dikelola sendiri harus dipisahkan dari konfigurasi yang dikelola sendiri. Anda dapat melakukan ini di konsol dengan [mengubah jenis manajemen setiap akun yang](#) dikelola sendiri atau OU menjadi dikelola secara terpusat dan Mewarisi dari organisasi saya.
5. Secara opsional, pilih pengaturan default konfigurasi lokal untuk akun organisasi baru.
6. Pilih Konfirmasi.

Security Hub CSPM API

Untuk menonaktifkan konfigurasi pusat (API)

1. Memanggil [UpdateOrganizationConfiguration](#) API.
2. Atur ConfigurationType bidang di OrganizationConfiguration objek keLOCAL. API menampilkan kesalahan jika Anda memiliki kebijakan konfigurasi atau asosiasi kebijakan yang ada. Untuk memisahkan kebijakan konfigurasi, panggil API. StartConfigurationPolicyDisassociation Untuk menghapus kebijakan konfigurasi, panggil DeleteConfigurationPolicy API.
3. Jika Anda ingin mengaktifkan CSPM Security Hub secara otomatis di akun organisasi baru, setel AutoEnable kolom ke. true Secara default, nilai bidang ini adalahfalse, dan CSPM Security Hub tidak diaktifkan secara otomatis di akun organisasi baru. Secara opsional, jika Anda ingin mengaktifkan standar keamanan default secara otomatis di akun organisasi baru, setel AutoEnableStandards bidang keDEFAULT. Ini nilai default. Jika Anda tidak

ingin mengaktifkan standar keamanan default secara otomatis di akun organisasi baru, setelah `AutoEnableStandards` bidang tersebut `NONE`.

Contoh permintaan API:

```
{
  "AutoEnable": true,
  "OrganizationConfiguration": {
    "ConfigurationType" : "LOCAL"
  }
}
```

AWS CLI

Untuk menonaktifkan konfigurasi pusat (AWS CLI)

1. Jalankan perintah [update-organization-configuration](#).
2. Atur `ConfigurationType` bidang di `organization-configuration` objek ke `LOCAL`. Perintah mengembalikan kesalahan jika Anda memiliki kebijakan konfigurasi atau asosiasi kebijakan yang ada. Untuk memisahkan kebijakan konfigurasi, jalankan `start-configuration-policy-disassociation` perintah. Untuk menghapus kebijakan konfigurasi, jalankan `delete-configuration-policy` perintah.
3. Jika Anda ingin mengaktifkan CSPM Security Hub secara otomatis di akun organisasi baru, sertakan parameternya `auto-enable`. Secara default, nilai parameter ini adalah `no-auto-enable`, dan CSPM Security Hub tidak diaktifkan secara otomatis di akun organisasi baru. Secara opsional, jika Anda ingin mengaktifkan standar keamanan default secara otomatis di akun organisasi baru, setelah `auto-enable-standards` bidang ke `DEFAULT`. Ini nilai default. Jika Anda tidak ingin mengaktifkan standar keamanan default secara otomatis di akun organisasi baru, setelah `auto-enable-standards` bidang tersebut `NONE`.

```
aws securityhub --region us-east-1 update-organization-configuration \
--auto-enable \
--organization-configuration '{"ConfigurationType": "LOCAL"}'
```

Mengelola akun administrator dan anggota di Security Hub CSPM

Jika AWS lingkungan Anda memiliki beberapa akun, Anda dapat memperlakukan akun yang menggunakan AWS Security Hub Cloud Security Posture Management (CSPM) sebagai akun anggota dan mengaitkannya dengan satu akun administrator. Administrator dapat memantau postur keamanan Anda secara keseluruhan dan mengambil [tindakan yang diizinkan](#) pada akun anggota. Administrator juga dapat melakukan berbagai tugas manajemen akun dan administrasi dalam skala besar, seperti memantau perkiraan biaya penggunaan dan menilai kuota akun.

Anda dapat mengaitkan akun anggota dengan administrator dalam dua cara, dengan mengintegrasikan Security Hub CSPM dengan AWS Organizations atau dengan mengirim dan menerima undangan keanggotaan secara manual di Security Hub CSPM.

Mengelola akun dengan AWS Organizations

AWS Organizations adalah layanan manajemen akun global yang memungkinkan AWS administrator untuk mengkonsolidasikan dan mengelola beberapa. Akun AWS Ini menyediakan manajemen akun dan fitur penagihan terkonsolidasi yang dirancang untuk mendukung kebutuhan anggaran, keamanan, dan kepatuhan. Ini ditawarkan tanpa biaya tambahan, dan terintegrasi dengan beberapa Layanan AWS, termasuk AWS Security Hub Cloud Security Posture Management (CSPM), Amazon Macie, dan Amazon GuardDuty. Untuk informasi selengkapnya, silakan lihat [Panduan Pengguna AWS Organizations](#).

Saat Anda mengintegrasikan CSPM Security Hub dan AWS Organizations, akun manajemen Organizations menunjuk administrator yang didelegasikan CSPM Security Hub. Security Hub CSPM secara otomatis diaktifkan di akun administrator yang didelegasikan Wilayah AWS di mana ia ditunjuk.

[Setelah menunjuk administrator yang didelegasikan, kami sarankan mengelola akun di Security Hub CSPM dengan konfigurasi pusat.](#) Ini adalah cara paling efisien untuk menyesuaikan Security Hub CSPM dan memastikan cakupan keamanan yang memadai untuk organisasi Anda.

Konfigurasi pusat memungkinkan administrator yang didelegasikan menyesuaikan CSPM Security Hub di beberapa akun organisasi dan Wilayah daripada mengonfigurasi Region-by-Region Anda dapat membuat kebijakan konfigurasi untuk seluruh organisasi, atau membuat kebijakan konfigurasi

yang berbeda untuk akun yang berbeda dan OUs. Kebijakan menentukan apakah CSPM Security Hub diaktifkan atau dinonaktifkan di akun terkait dan standar dan kontrol keamanan mana yang diaktifkan.

Administrator yang didelegasikan dapat menetapkan akun sebagai dikelola secara terpusat atau dikelola sendiri. Akun yang dikelola secara terpusat hanya dapat dikonfigurasi oleh administrator yang didelegasikan. Akun yang dikelola sendiri dapat menentukan pengaturan mereka sendiri.

Jika Anda tidak ikut serta dalam konfigurasi pusat, administrator yang didelegasikan memiliki kemampuan yang lebih terbatas untuk mengonfigurasi CSPM Security Hub, yang disebut konfigurasi lokal. Di bawah konfigurasi lokal, administrator yang didelegasikan dapat secara otomatis mengaktifkan CSPM Security Hub dan [standar keamanan default](#) di akun organisasi baru di Wilayah saat ini. Namun, akun yang ada tidak menggunakan pengaturan ini, sehingga penyimpangan konfigurasi dapat terjadi setelah akun bergabung dengan organisasi.

Selain pengaturan akun baru ini, konfigurasi lokal bersifat spesifik akun dan spesifik Wilayah. Setiap akun organisasi harus mengonfigurasi layanan, standar, dan kontrol CSPM Security Hub secara terpisah di setiap Wilayah. Konfigurasi lokal juga tidak mendukung penggunaan kebijakan konfigurasi.

Mengelola akun secara manual dengan undangan

Anda harus mengelola akun anggota secara manual berdasarkan undangan di Security Hub CSPM jika Anda memiliki akun mandiri atau jika Anda tidak berintegrasi dengan Organizations. Akun mandiri tidak dapat diintegrasikan dengan Organizations, jadi Anda perlu mengelolanya secara manual. Kami merekomendasikan untuk mengintegrasikan dengan AWS Organizations dan menggunakan konfigurasi pusat jika Anda menambahkan akun tambahan di masa mendatang.

Saat Anda menggunakan manajemen akun manual, Anda menetapkan akun untuk menjadi administrator CSPM Security Hub. Akun administrator dapat melihat data di akun anggota dan mengambil tindakan tertentu pada temuan akun anggota. Administrator CSPM Security Hub mengundang akun lain untuk menjadi akun anggota, dan hubungan administrator-anggota terbentuk ketika akun calon anggota menerima undangan.

Manajemen akun manual tidak mendukung penggunaan kebijakan konfigurasi. Tanpa kebijakan konfigurasi, administrator tidak dapat menyesuaikan CSPM Security Hub secara terpusat dengan mengonfigurasi setelan variabel untuk akun yang berbeda. Sebagai gantinya, setiap akun organisasi harus mengaktifkan dan mengonfigurasi CSPM Security Hub untuk dirinya sendiri secara terpisah

di setiap Wilayah. Ini dapat membuatnya lebih sulit dan memakan waktu untuk memastikan cakupan keamanan yang memadai di semua akun dan Wilayah tempat Anda menggunakan Security Hub CSPM. Ini juga dapat menyebabkan penyimpangan konfigurasi karena akun anggota dapat menentukan pengaturan mereka sendiri tanpa masukan dari administrator.

Untuk mengelola akun berdasarkan undangan, lihat [Mengelola akun dengan undangan di Security Hub CSPM](#).

Rekomendasi untuk mengelola beberapa akun di Security Hub CSPM

Bagian berikut merangkum beberapa batasan dan rekomendasi yang perlu diingat saat mengelola akun anggota di AWS Security Hub Cloud Security Posture Management (CSPM).

Jumlah maksimum akun anggota

Jika Anda menggunakan integrasi dengan AWS Organizations, Security Hub CSPM mendukung hingga 10.000 akun anggota per akun administrator yang didelegasikan di masing-masing akun. Wilayah AWS Jika Anda mengaktifkan dan mengelola Security Hub CSPM secara manual, Security Hub CSPM mendukung hingga 1.000 undangan akun anggota per akun administrator di setiap Wilayah.

Membuat hubungan administrator-anggota

Note

Jika Anda menggunakan integrasi CSPM Security Hub dengan AWS Organizations, dan belum mengundang akun anggota secara manual, bagian ini tidak berlaku untuk Anda.

Akun tidak dapat berupa akun administrator dan akun anggota secara bersamaan.

Akun anggota hanya dapat dikaitkan dengan satu akun administrator. Jika akun organisasi diaktifkan oleh akun administrator CSPM Security Hub, akun tidak dapat menerima undangan dari akun lain. Jika akun telah menerima undangan, akun tidak dapat diaktifkan oleh akun administrator CSPM Security Hub untuk organisasi. Itu juga tidak dapat menerima undangan dari akun lain.

Untuk proses undangan manual, menerima undangan keanggotaan adalah opsional.

Keanggotaan melalui AWS Organizations

Jika Anda mengintegrasikan CSPM Security Hub AWS Organizations, akun manajemen Organizations dapat menunjuk akun administrator yang didelegasikan (DA) untuk Security Hub CSPM. Akun manajemen organisasi tidak dapat ditetapkan sebagai DA di Organizations. Meskipun ini diizinkan di Security Hub CSPM, kami menyarankan agar akun manajemen Organizations tidak boleh menjadi DA.

Kami menyarankan Anda memilih akun DA yang sama di semua Wilayah. Jika Anda menggunakan [konfigurasi pusat](#), maka Security Hub CSPM menetapkan akun DA yang sama di semua Wilayah tempat Anda mengonfigurasi CSPM Security Hub untuk organisasi Anda.

Kami juga menyarankan Anda memilih akun DA yang sama di seluruh layanan AWS keamanan dan kepatuhan untuk membantu Anda mengelola masalah terkait keamanan dalam satu panel kaca.

Keanggotaan berdasarkan undangan

Untuk akun anggota yang dibuat berdasarkan undangan, asosiasi akun administrator-anggota dibuat hanya di Wilayah tempat undangan dikirim. Akun administrator harus mengaktifkan CSPM Security Hub di setiap Wilayah tempat Anda ingin menggunakannya. Akun administrator kemudian mengundang setiap akun untuk menjadi akun anggota di Wilayah tersebut.

Note

Sebaiknya gunakan AWS Organizations bukan undangan CSPM Security Hub untuk mengelola akun anggota Anda.

Mengkoordinasikan akun administrator di seluruh layanan

Security Hub CSPM mengumpulkan temuan dari berbagai AWS layanan, seperti Amazon, Amazon GuardDuty Inspector, dan Amazon Macie. Security Hub CSPM juga memungkinkan pengguna untuk beralih dari GuardDuty temuan untuk memulai penyelidikan di Amazon Detective.

Namun, hubungan administrator-anggota yang Anda atur di layanan lain ini tidak secara otomatis berlaku untuk CSPM Security Hub. Security Hub CSPM merekomendasikan agar Anda menggunakan akun yang sama dengan akun administrator untuk semua layanan ini. Akun administrator ini harus menjadi akun yang bertanggung jawab atas alat keamanan. Akun yang sama juga harus menjadi akun agregator untuk AWS Config.

Misalnya, pengguna dari akun GuardDuty administrator A dapat melihat temuan untuk akun GuardDuty anggota B dan C di GuardDuty konsol. Jika akun A kemudian mengaktifkan Security Hub CSPM, pengguna dari akun A tidak secara otomatis melihat GuardDuty temuan untuk akun B dan C di Security Hub CSPM. Hubungan administrator-anggota CSPM Security Hub juga diperlukan untuk akun ini.

Untuk melakukan ini, buat akun A sebagai akun administrator CSPM Security Hub dan aktifkan akun B dan C untuk menjadi akun anggota CSPM Security Hub.

Mengelola Security Hub CSPM untuk beberapa akun dengan AWS Organizations

Anda dapat mengintegrasikan AWS Security Hub Cloud Security Posture Management (CSPM) dengan AWS Organizations, dan kemudian mengelola Security Hub CSPM untuk akun di organisasi Anda.

Untuk mengintegrasikan CSPM Security Hub dengan AWS Organizations, Anda membuat organisasi di AWS Organizations. Akun manajemen Organizations menetapkan satu akun sebagai administrator yang didelegasikan CSPM Security Hub untuk organisasi. Administrator yang didelegasikan kemudian dapat mengaktifkan CSPM Security Hub untuk akun lain di organisasi, menambahkan akun tersebut sebagai akun anggota CSPM Security Hub, dan mengambil tindakan yang diizinkan pada akun anggota. Administrator yang didelegasikan CSPM Security Hub dapat mengaktifkan dan mengelola Security Hub CSPM hingga 10.000 akun anggota.

Tingkat kemampuan konfigurasi administrator yang didelegasikan bergantung pada apakah Anda menggunakan [konfigurasi pusat](#). Dengan konfigurasi pusat diaktifkan, Anda tidak perlu mengonfigurasi CSPM Security Hub secara terpisah di setiap akun anggota dan Wilayah AWS. Administrator yang didelegasikan dapat menerapkan pengaturan CSPM Security Hub tertentu di akun anggota tertentu dan unit organisasi (OU) di seluruh Wilayah.

Akun administrator yang didelegasikan CSPM Security Hub dapat melakukan tindakan berikut pada akun anggota:

- Jika menggunakan konfigurasi pusat, konfigurasikan CSPM Security Hub secara terpusat untuk akun anggota dan OUs dengan membuat kebijakan konfigurasi CSPM Security Hub. Kebijakan konfigurasi dapat digunakan untuk mengaktifkan dan menonaktifkan Security Hub CSPM, mengaktifkan dan menonaktifkan standar, serta mengaktifkan dan menonaktifkan kontrol.

- Secara otomatis memperlakukan akun baru sebagai akun anggota CSPM Security Hub ketika mereka bergabung dengan organisasi. Jika Anda menggunakan konfigurasi pusat, kebijakan konfigurasi yang terkait dengan OU mencakup akun yang ada dan baru yang merupakan bagian dari OU.
- Perlakukan akun organisasi yang ada sebagai akun anggota CSPM Security Hub. Ini terjadi secara otomatis jika Anda menggunakan konfigurasi pusat.
- Putuskan akun anggota yang termasuk dalam organisasi. Jika Anda menggunakan konfigurasi pusat, Anda dapat memisahkan akun anggota hanya setelah menetakannya sebagai dikelola sendiri. Atau, Anda dapat mengaitkan kebijakan konfigurasi yang menonaktifkan CSPM Security Hub dengan akun anggota tertentu yang dikelola secara terpusat.

Jika Anda tidak ikut serta dalam konfigurasi pusat, organisasi Anda menggunakan jenis konfigurasi default yang disebut konfigurasi lokal. Di bawah konfigurasi lokal, administrator yang didelegasikan memiliki kemampuan yang lebih terbatas untuk menerapkan pengaturan di akun anggota. Untuk informasi selengkapnya, lihat [Memahami konfigurasi lokal di Security Hub CSPM](#).

Untuk daftar lengkap tindakan yang dapat dilakukan administrator yang didelegasikan pada akun anggota, lihat [Tindakan yang diizinkan oleh administrator dan akun anggota di Security Hub CSPM](#).

Topik di bagian ini menjelaskan cara mengintegrasikan CSPM Security Hub dengan AWS Organizations dan cara mengelola CSPM Security Hub untuk akun dalam suatu organisasi. Jika relevan, setiap bagian mengidentifikasi manfaat dan perbedaan manajemen untuk pengguna konfigurasi pusat.

Topik

- [Mengintegrasikan CSPM Security Hub dengan AWS Organizations](#)
- [Mengaktifkan CSPM Security Hub secara otomatis di akun organisasi baru](#)
- [Mengaktifkan CSPM Security Hub secara manual di akun organisasi baru](#)
- [Memutuskan akun anggota CSPM Security Hub dari organisasi Anda](#)

Mengintegrasikan CSPM Security Hub dengan AWS Organizations

Untuk mengintegrasikan AWS Security Hub Cloud Security Posture Management (CSPM) dan AWS Organizations, Anda membuat organisasi di Organizations dan menggunakan akun manajemen organisasi untuk menunjuk akun administrator CSPM Security Hub yang didelegasikan. Hal ini memungkinkan Security Hub CSPM sebagai layanan terpercaya di Organizations. [Ini](#)

[juga memungkinkan Security Hub CSPM saat ini Wilayah AWS untuk akun administrator yang didelegasikan, dan memungkinkan administrator yang didelegasikan untuk mengaktifkan CSPM Security Hub untuk akun anggota, melihat data di akun anggota, dan melakukan tindakan lain yang diizinkan pada akun anggota.](#)

Jika Anda menggunakan [konfigurasi pusat](#), administrator yang didelegasikan juga dapat membuat kebijakan konfigurasi CSPM Security Hub yang menentukan bagaimana layanan, standar, dan kontrol CSPM Security Hub harus dikonfigurasi di akun organisasi.

Membuat organisasi

Organisasi adalah entitas yang Anda buat untuk mengkonsolidasikan Anda Akun AWS sehingga Anda dapat mengelolanya sebagai satu kesatuan.

Anda dapat membuat organisasi dengan menggunakan AWS Organizations konsol atau dengan menggunakan perintah dari AWS CLI atau salah satu SDK APIs. Untuk petunjuk mendetail, lihat [Membuat organisasi](#) di Panduan AWS Organizations Pengguna.

Anda dapat menggunakan AWS Organizations untuk melihat dan mengelola semua akun dalam organisasi secara terpusat. Sebuah organisasi memiliki satu akun manajemen bersama dengan nol atau lebih akun anggota. Anda dapat mengatur akun dalam struktur hierarkis seperti pohon dengan root di bagian atas dan unit organisasi (OUs) bersarang di bawah root. Setiap akun dapat langsung di bawah root, atau ditempatkan di salah satu OUs dalam hierarki. OU adalah wadah untuk akun tertentu. Misalnya, Anda dapat membuat OU keuangan yang mencakup semua akun yang terkait dengan operasi keuangan.

Rekomendasi untuk memilih administrator CSPM Security Hub yang didelegasikan

Jika Anda memiliki akun administrator dari proses undangan manual dan sedang beralih ke manajemen akun AWS Organizations, sebaiknya tentukan akun tersebut sebagai administrator CSPM Security Hub yang didelegasikan.

Meskipun CSPM APIs dan konsol Security Hub memungkinkan akun manajemen organisasi menjadi administrator CSPM Security Hub yang didelegasikan, sebaiknya pilih dua akun yang berbeda. Ini karena pengguna yang memiliki akses ke akun manajemen organisasi untuk mengelola penagihan cenderung berbeda dari pengguna yang membutuhkan akses ke Security Hub CSPM untuk manajemen keamanan.

Sebaiknya gunakan administrator yang didelegasikan sama di seluruh Wilayah. Jika Anda ikut serta dalam konfigurasi pusat, Security Hub CSPM secara otomatis menunjuk administrator yang didelegasikan yang sama di Wilayah asal Anda dan Wilayah yang ditautkan.

Verifikasi izin untuk mengonfigurasi administrator yang didelegasikan

Untuk menetapkan dan menghapus akun administrator CSPM Security Hub yang didelegasikan, akun manajemen organisasi harus memiliki izin dan tindakan `EnableOrganizationAdminAccount` di CSPM `DisableOrganizationAdminAccount` Security Hub. Akun manajemen Organizations juga harus memiliki izin administratif untuk Organizations.

Untuk memberikan semua izin yang diperlukan, lampirkan kebijakan terkelola CSPM Security Hub berikut ke kepala IAM untuk akun manajemen organisasi:

- [AWSSecurityHubFullAccess](#)
- [AWSSecurityHubOrganizationsAccess](#)

Menunjuk administrator yang didelegasikan

Untuk menetapkan akun administrator CSPM Security Hub yang didelegasikan, Anda dapat menggunakan konsol CSPM Security Hub, Security Hub CSPM API, atau AWS CLI Security Hub CSPM menetapkan administrator yang didelegasikan Wilayah AWS hanya di saat ini, dan Anda harus mengulangi tindakan di Wilayah lain. Jika Anda mulai menggunakan konfigurasi pusat, maka Security Hub CSPM secara otomatis menetapkan administrator yang didelegasikan yang sama di Wilayah beranda dan Wilayah yang ditautkan.

Akun manajemen organisasi tidak harus mengaktifkan CSPM Security Hub untuk menetapkan akun administrator CSPM Security Hub yang didelegasikan.

Kami menyarankan agar akun manajemen organisasi bukan akun administrator CSPM Security Hub yang didelegasikan. Namun, jika Anda memilih akun manajemen organisasi sebagai administrator yang didelegasikan CSPM Security Hub, akun manajemen harus mengaktifkan CSPM Security Hub. Jika akun manajemen tidak mengaktifkan Security Hub CSPM, Anda harus mengaktifkan Security Hub CSPM untuk itu secara manual. CSPM Security Hub tidak dapat diaktifkan secara otomatis untuk akun manajemen organisasi.

Anda harus menunjuk administrator CSPM Security Hub yang didelegasikan menggunakan salah satu metode berikut. Menunjuk administrator CSPM Security Hub yang didelegasikan dengan Organizations APIs tidak tercermin dalam Security Hub CSPM.

Pilih metode yang Anda inginkan, dan ikuti langkah-langkah untuk menetapkan akun administrator CSPM Security Hub yang didelegasikan.

Security Hub CSPM console

Untuk menunjuk administrator yang didelegasikan saat melakukan orientasi

1. Buka konsol AWS Security Hub Cloud Security Posture Management (CSPM) di <https://console.aws.amazon.com/securityhub/>
2. Pilih Buka Security Hub CSPM. Anda diminta untuk masuk ke akun manajemen organisasi.
3. Pada halaman Tentukan administrator yang didelegasikan, di bagian Akun administrator yang didelegasikan, tentukan akun administrator yang didelegasikan. Sebaiknya pilih administrator yang didelegasikan sama yang telah Anda tetapkan untuk layanan AWS keamanan dan kepatuhan lainnya.
4. Pilih Setel administrator yang didelegasikan. Anda diminta untuk masuk ke akun administrator yang didelegasikan (jika belum) untuk melanjutkan orientasi dengan konfigurasi pusat. Jika Anda tidak ingin memulai konfigurasi pusat, pilih Batal. Administrator yang didelegasikan Anda disetel, tetapi Anda belum menggunakan konfigurasi pusat.

Untuk menunjuk administrator yang didelegasikan dari halaman Pengaturan

1. Buka konsol AWS Security Hub Cloud Security Posture Management (CSPM) di <https://console.aws.amazon.com/securityhub/>
2. Di panel navigasi CSPM Security Hub, pilih Pengaturan. Kemudian pilih Umum.
3. Jika akun administrator CSPM Security Hub saat ini ditetapkan, maka sebelum Anda dapat menunjuk akun baru, Anda harus menghapus akun saat ini.

Di bawah Administrator Delegasi, untuk menghapus akun saat ini, pilih Hapus.

4. Masukkan ID akun yang ingin Anda tetapkan sebagai akun administrator CSPM Security Hub.

Anda harus menetapkan akun administrator CSPM Security Hub yang sama di semua Wilayah. Jika Anda menetapkan akun yang berbeda dari akun yang ditunjuk di Wilayah lain, konsol akan mengembalikan kesalahan.

5. Pilih Delegasikan.

Security Hub CSPM API, AWS CLI

Dari akun manajemen organisasi, gunakan [EnableOrganizationAdminAccount](#) pengoperasian Security Hub CSPM API. Jika Anda menggunakan AWS CLI, jalankan [enable-organization-admin-account](#) perintah. Berikan Akun AWS ID administrator CSPM Security Hub yang didelegasikan.

Contoh berikut menunjuk administrator CSPM Security Hub yang didelegasikan. Contoh ini diformat untuk Linux, macOS, atau Unix, dan menggunakan karakter garis miring terbalik (\) untuk meningkatkan keterbacaan.

```
$ aws securityhub enable-organization-admin-account --admin-account-id 123456789012
```

Menghapus atau mengubah administrator yang didelegasikan

Hanya akun manajemen organisasi yang dapat menghapus akun administrator CSPM Security Hub yang didelegasikan.

Untuk mengubah administrator CSPM Security Hub yang didelegasikan, Anda harus terlebih dahulu menghapus akun administrator yang didelegasikan saat ini dan kemudian menunjuk yang baru.

Warning

Bila Anda menggunakan [konfigurasi pusat](#), Anda tidak dapat menggunakan konsol CSPM Security Hub atau Security Hub CSPM APIs untuk mengubah atau menghapus akun administrator yang didelegasikan. Jika akun manajemen organisasi menggunakan AWS Organizations konsol atau mengubah atau AWS Organizations APIs menghapus administrator CSPM Security Hub yang didelegasikan, CSPM Security Hub secara otomatis menghentikan konfigurasi pusat, dan menghapus kebijakan konfigurasi dan asosiasi kebijakan Anda. Akun anggota mempertahankan konfigurasi yang mereka miliki sebelum administrator yang didelegasikan diubah atau dihapus.

Jika Anda menggunakan konsol CSPM Security Hub untuk menghapus administrator yang didelegasikan di satu Wilayah, maka secara otomatis dihapus di semua Wilayah.

Security Hub CSPM API hanya menghapus akun administrator CSPM Security Hub yang didelegasikan dari Wilayah tempat panggilan API atau perintah dikeluarkan. Anda harus mengulangi tindakan di Wilayah lain.

Jika Anda menggunakan Organizations API untuk menghapus akun administrator CSPM Security Hub yang didelegasikan, akun tersebut akan dihapus secara otomatis di semua Wilayah.

Menghapus administrator yang didelegasikan (Organizations API, AWS CLI)

Anda dapat menggunakan Organizations untuk menghapus administrator CSPM Security Hub yang didelegasikan di semua Wilayah.

Jika Anda menggunakan konfigurasi pusat untuk mengelola akun, menghapus akun administrator yang didelegasikan akan mengakibatkan penghapusan kebijakan konfigurasi dan asosiasi kebijakan Anda. Akun anggota mempertahankan konfigurasi yang mereka miliki sebelum administrator yang didelegasikan diubah atau dihapus. Namun, akun ini tidak dapat dikelola lagi oleh akun administrator yang didelegasikan yang dihapus. Mereka menjadi akun yang dikelola sendiri yang harus dikonfigurasi secara terpisah di setiap Wilayah.

Pilih metode yang Anda inginkan, dan ikuti petunjuk untuk menghapus akun administrator CSPM Security Hub yang didelegasikan. AWS Organizations

Organizations API, AWS CLI

Untuk menghapus administrator CSPM Security Hub yang didelegasikan

Dari akun manajemen organisasi, gunakan [DeregisterDelegatedAdministrator](#) pengoperasian API Organizations. Jika Anda menggunakan AWS CLI, jalankan [deregister-delegated-administrator](#) perintah. Berikan ID akun administrator yang didelegasikan, dan kepala layanan untuk Security Hub CSPM, yaitu. `securityhub.amazonaws.com`

Contoh berikut menghapus administrator CSPM Security Hub yang didelegasikan. Contoh ini diformat untuk Linux, macOS, atau Unix, dan menggunakan karakter garis miring terbalik (\) untuk meningkatkan keterbacaan.

```
$ aws organizations deregister-delegated-administrator --account-id 123456789012 --service-principal securityhub.amazonaws.com
```

Menghapus administrator yang didelegasikan (konsol CSPM Security Hub)

Anda dapat menggunakan konsol CSPM Security Hub untuk menghapus administrator CSPM Security Hub yang didelegasikan di semua Wilayah.

Ketika akun administrator CSPM Security Hub yang didelegasikan dihapus, akun anggota akan dipisahkan dari akun administrator CSPM Security Hub yang didelegasikan yang dihapus.

Security Hub CSPM masih diaktifkan di akun anggota. Mereka menjadi akun mandiri sampai administrator CSPM Security Hub baru memungkinkan mereka sebagai akun anggota.

Jika akun manajemen organisasi bukan akun yang diaktifkan di CSPM Security Hub, gunakan opsi di halaman CSPM Selamat Datang di Security Hub.

Untuk menghapus akun administrator CSPM Security Hub yang didelegasikan dari halaman CSPM Selamat Datang di Security Hub

1. Buka konsol AWS Security Hub Cloud Security Posture Management (CSPM) di <https://console.aws.amazon.com/securityhub/>
2. Pilih Buka Security Hub.
3. Di bawah Administrator Delegasi, pilih Hapus.

Jika akun manajemen organisasi adalah akun yang diaktifkan di Security Hub, maka gunakan opsi pada tab Umum pada halaman Pengaturan.

Untuk menghapus akun administrator CSPM Security Hub yang didelegasikan dari halaman Pengaturan

1. Buka konsol AWS Security Hub Cloud Security Posture Management (CSPM) di <https://console.aws.amazon.com/securityhub/>
2. Di panel navigasi CSPM Security Hub, pilih Pengaturan. Kemudian pilih Umum.
3. Di bawah Administrator Delegasi, pilih Hapus.

Menghapus administrator yang didelegasikan (Security Hub CSPM API,) AWS CLI

Anda dapat menggunakan Security Hub CSPM API atau operasi CSPM Security Hub AWS CLI untuk menghapus administrator CSPM Security Hub yang didelegasikan. Saat Anda menghapus administrator yang didelegasikan dengan salah satu metode ini, administrator hanya akan dihapus di Wilayah tempat panggilan atau perintah API dikeluarkan. Security Hub CSPM tidak memperbarui Wilayah lain, dan tidak menghapus akun administrator yang didelegasikan. AWS Organizations

Pilih metode yang Anda inginkan, dan ikuti langkah-langkah berikut untuk menghapus akun administrator CSPM Security Hub yang didelegasikan dengan Security Hub CSPM.

Security Hub CSPM API, AWS CLI

Untuk menghapus administrator CSPM Security Hub yang didelegasikan

Dari akun manajemen organisasi, gunakan [DisableOrganizationAdminAccount](#) pengoperasian Security Hub CSPM API. Jika Anda menggunakan AWS CLI, jalankan [disable-organization-admin-account](#) perintah. Berikan ID akun administrator CSPM Security Hub yang didelegasikan.

Contoh berikut menghapus administrator CSPM Security Hub yang didelegasikan. Contoh ini diformat untuk Linux, macOS, atau Unix, dan menggunakan karakter garis miring terbalik (\) untuk meningkatkan keterbacaan.

```
$ aws securityhub disable-organization-admin-account --admin-account-id 123456789012
```

Menonaktifkan integrasi CSPM Security Hub dengan AWS Organizations

Setelah AWS Organizations organisasi terintegrasi dengan AWS Security Hub Cloud Security Posture Management (CSPM), akun manajemen Organizations selanjutnya dapat menonaktifkan integrasi. Sebagai pengguna akun manajemen Organizations, Anda dapat melakukannya dengan menonaktifkan akses tepercaya untuk Security Hub CSPM di AWS Organizations

Ketika Anda menonaktifkan akses tepercaya untuk Security Hub CSPM, hal berikut akan terjadi:

- Security Hub CSPM kehilangan statusnya sebagai layanan tepercaya di AWS Organizations
- Akun administrator yang didelegasikan CSPM Security Hub kehilangan akses ke pengaturan, data, dan sumber daya CSPM Security Hub untuk semua akun anggota CSPM Security Hub secara keseluruhan. Wilayah AWS
- Jika Anda menggunakan [konfigurasi pusat](#), Security Hub CSPM secara otomatis berhenti menggunakannya untuk organisasi Anda. Kebijakan konfigurasi dan asosiasi kebijakan Anda dihapus. Akun mempertahankan konfigurasi yang mereka miliki sebelum Anda menonaktifkan akses tepercaya.
- Semua akun anggota CSPM Security Hub menjadi akun mandiri dan mempertahankan pengaturan mereka saat ini. Jika Security Hub CSPM diaktifkan untuk akun anggota di satu atau beberapa Wilayah, CSPM Security Hub tetap diaktifkan untuk akun di Wilayah tersebut. Standar dan kontrol yang diaktifkan juga tidak berubah. Anda dapat mengubah pengaturan ini secara terpisah di setiap akun dan Wilayah. Namun, akun tidak lagi dikaitkan dengan administrator yang didelegasikan di Wilayah mana pun.

Untuk informasi tambahan tentang hasil menonaktifkan akses layanan tepercaya, lihat [Menggunakan AWS Organizations dengan yang lain Layanan AWS](#) di AWS Organizations Panduan Pengguna.

Untuk menonaktifkan akses tepercaya, Anda dapat menggunakan AWS Organizations konsol, Organizations API, atau file AWS CLI. Hanya pengguna akun manajemen Organizations yang dapat menonaktifkan akses layanan tepercaya untuk Security Hub CSPM. Untuk detail tentang izin yang Anda perlukan, lihat [Izin yang diperlukan untuk menonaktifkan akses tepercaya](#) di AWS Organizations Panduan Pengguna.

Sebelum Anda menonaktifkan akses tepercaya, kami sarankan bekerja sama dengan administrator yang didelegasikan untuk organisasi Anda untuk menonaktifkan CSPM Security Hub di akun anggota dan membersihkan sumber daya CSPM Security Hub di akun tersebut.

Pilih metode pilihan Anda, dan ikuti langkah-langkah untuk menonaktifkan akses tepercaya untuk Security Hub CSPM.

Organizations console

Untuk menonaktifkan akses tepercaya untuk Security Hub CSPM

1. Masuk ke AWS Management Console menggunakan kredensi akun AWS Organizations manajemen.
2. Buka konsol Organizations di <https://console.aws.amazon.com/organizations/>.
3. Pada panel navigasi, silakan pilih Layanan.
4. Di bawah Layanan terintegrasi, pilih AWS Security Hub Cloud Security Posture Management (CSPM).
5. Pilih Menonaktifkan akses tepercaya.
6. Konfirmasikan bahwa Anda ingin menonaktifkan akses tepercaya.

Organizations API

Untuk menonaktifkan akses tepercaya untuk Security Hub CSPM

Memanggil operasi [Disable AWSService Access](#) dari AWS Organizations API. Untuk `ServicePrincipal` parameternya, tentukan prinsip layanan CSPM Security Hub (`securityhub.amazonaws.com`).

AWS CLI

Untuk menonaktifkan akses tepercaya untuk Security Hub CSPM

Jalankan [disable-aws-service-access](#) perintah AWS Organizations API. Untuk `service-principal` parameternya, tentukan prinsip layanan CSPM Security Hub (`securityhub.amazonaws.com`).

Contoh:

```
aws organizations disable-aws-service-access --service-principal
securityhub.amazonaws.com
```

Mengaktifkan CSPM Security Hub secara otomatis di akun organisasi baru

Saat akun baru bergabung dengan organisasi Anda, akun tersebut ditambahkan ke daftar di halaman Akun konsol AWS Security Hub Cloud Security Posture Management (CSPM) Security Hub. Untuk akun organisasi, Type is By Organization. Secara default, akun baru tidak menjadi anggota CSPM Security Hub saat mereka bergabung dengan organisasi. Status mereka bukan anggota. Akun administrator yang didelegasikan dapat secara otomatis menambahkan akun baru sebagai anggota dan mengaktifkan CSPM Security Hub di akun ini saat mereka bergabung dengan organisasi.

Note

Meskipun banyak Wilayah AWS yang aktif secara default untuk Anda Akun AWS, Anda harus mengaktifkan Wilayah tertentu secara manual. Wilayah ini disebut Wilayah keikutsertaan dalam dokumen ini. Untuk mengaktifkan CSPM Security Hub secara otomatis di akun baru di Region opt-in, akun tersebut harus mengaktifkan Region tersebut terlebih dahulu. Hanya pemilik akun yang dapat mengaktifkan Wilayah keikutsertaan. Untuk informasi selengkapnya tentang opt-in Regions, lihat [Menentukan yang dapat digunakan akun Wilayah AWS Anda](#).

Proses ini berbeda berdasarkan apakah Anda menggunakan konfigurasi pusat (disarankan) atau konfigurasi lokal.

Mengaktifkan akun organisasi baru secara otomatis (konfigurasi pusat)

Jika Anda menggunakan [konfigurasi pusat](#), Anda dapat mengaktifkan CSPM Security Hub secara otomatis di akun organisasi baru dan yang sudah ada dengan membuat kebijakan konfigurasi tempat CSPM Security Hub diaktifkan. Anda kemudian dapat mengaitkan kebijakan dengan root organisasi atau unit organisasi tertentu (OUs).

Jika Anda mengaitkan kebijakan konfigurasi di mana Security Hub CSPM diaktifkan dengan OU tertentu, Security Hub CSPM secara otomatis diaktifkan di semua akun (yang ada dan baru) milik OU tersebut. Akun baru yang bukan milik OU dikelola sendiri dan tidak secara otomatis mengaktifkan Security Hub CSPM. Jika Anda mengaitkan kebijakan konfigurasi di mana Security Hub CSPM diaktifkan dengan root, Security Hub CSPM secara otomatis diaktifkan di semua akun (yang ada dan baru) yang bergabung dengan organisasi. Pengecualian adalah jika akun menggunakan kebijakan yang berbeda melalui aplikasi atau warisan, atau dikelola sendiri.

Dalam kebijakan konfigurasi, Anda juga dapat menentukan standar dan kontrol keamanan mana yang harus diaktifkan di OU. Untuk menghasilkan temuan kontrol untuk standar yang diaktifkan, akun di OU harus AWS Config diaktifkan dan dikonfigurasi untuk mencatat sumber daya yang diperlukan. Untuk informasi selengkapnya tentang AWS Config perekaman, lihat [Mengaktifkan dan mengonfigurasi AWS Config](#).

Untuk petunjuk cara membuat kebijakan konfigurasi, lihat [Membuat dan mengaitkan kebijakan konfigurasi](#).

Mengaktifkan akun organisasi baru secara otomatis (konfigurasi lokal)

Saat Anda menggunakan konfigurasi lokal dan mengaktifkan pengaktifan otomatis standar default, Security Hub CSPM menambahkan akun organisasi baru sebagai anggota dan mengaktifkan CSPM Security Hub di dalamnya di Wilayah saat ini. Wilayah lain tidak terpengaruh. Selain itu, mengaktifkan pengaktifan otomatis tidak mengaktifkan CSPM Security Hub di akun organisasi yang ada kecuali akun tersebut sudah ditambahkan sebagai akun anggota.

Setelah mengaktifkan pengaktifan otomatis, standar keamanan default diaktifkan untuk akun anggota baru di Wilayah saat ini ketika mereka bergabung dengan organisasi. Standar default adalah AWS Foundational Security Best Practices (FSBP) dan Center for Internet Security (CIS) AWS Foundations Benchmark v1.2.0. Anda tidak dapat mengubah standar default. Jika Anda ingin mengaktifkan standar lain di seluruh organisasi Anda, atau mengaktifkan standar untuk akun tertentu dan OUs, sebaiknya gunakan konfigurasi pusat.

Untuk menghasilkan temuan kontrol untuk standar default (dan standar lain yang diaktifkan), akun di organisasi Anda harus telah AWS Config diaktifkan dan dikonfigurasi untuk merekam sumber daya yang diperlukan. Untuk informasi selengkapnya tentang AWS Config perekaman, lihat [Mengaktifkan dan mengonfigurasi AWS Config](#).

Pilih metode pilihan Anda, dan ikuti langkah-langkah untuk mengaktifkan CSPM Security Hub secara otomatis di akun organisasi baru. Petunjuk ini hanya berlaku jika Anda menggunakan konfigurasi lokal.

Security Hub CSPM console

Untuk mengaktifkan akun organisasi baru secara otomatis sebagai anggota CSPM Security Hub

1. Buka konsol AWS Security Hub Cloud Security Posture Management (CSPM) di <https://console.aws.amazon.com/securityhub/>

Tanda menggunakan kredensi akun administrator yang didelegasikan.

2. Di panel navigasi CSPM Security Hub, di bawah Pengaturan, pilih Konfigurasi.
3. Di bagian Akun, nyalakan Akun Aktifkan otomatis.

Security Hub CSPM API

Untuk mengaktifkan akun organisasi baru secara otomatis sebagai anggota CSPM Security Hub

Memanggil [UpdateOrganizationConfiguration](#) API dari akun administrator yang didelegasikan. Setel `AutoEnable` bidang `true` untuk mengaktifkan CSPM Security Hub secara otomatis di akun organisasi baru.

AWS CLI

Untuk mengaktifkan akun organisasi baru secara otomatis sebagai anggota CSPM Security Hub

Jalankan [update-organization-configuration](#) perintah dari akun administrator yang didelegasikan. Sertakan `auto-enable` parameter untuk mengaktifkan CSPM Security Hub secara otomatis di akun organisasi baru.

```
aws securityhub update-organization-configuration --auto-enable
```

Mengaktifkan CSPM Security Hub secara manual di akun organisasi baru

Jika Anda tidak mengaktifkan CSPM Security Hub secara otomatis di akun organisasi baru saat mereka bergabung dengan organisasi, Anda dapat menambahkan akun tersebut sebagai anggota dan mengaktifkan CSPM Security Hub di dalamnya secara manual setelah mereka bergabung dengan organisasi. Anda juga harus mengaktifkan CSPM Security Hub secara manual Akun AWS karena sebelumnya Anda terputus dari organisasi.

 Note

Bagian ini tidak berlaku untuk Anda jika Anda menggunakan [konfigurasi pusat](#). Jika Anda menggunakan konfigurasi pusat, Anda dapat membuat kebijakan konfigurasi yang mengaktifkan CSPM Security Hub di akun anggota tertentu dan unit organisasi (OU). Anda juga dapat mengaktifkan standar dan kontrol tertentu di akun tersebut dan OUs.

Anda tidak dapat mengaktifkan CSPM Security Hub di akun jika sudah menjadi akun anggota dalam organisasi yang berbeda.

Anda juga tidak dapat mengaktifkan CSPM Security Hub di akun yang saat ini ditangguhkan. Jika Anda mencoba mengaktifkan layanan di akun yang ditangguhkan, status akun berubah menjadi Akun Ditangguhkan.

- Jika akun tidak mengaktifkan CSPM Security Hub, CSPM Security Hub diaktifkan di akun tersebut. Standar AWS Foundational Security Best Practices (FSBP) dan CIS AWS Foundations Benchmark v1.2.0 juga diaktifkan di akun kecuali Anda mematikan standar keamanan default.

Pengecualian untuk ini adalah akun manajemen Organizations. Security Hub CSPM tidak dapat diaktifkan secara otomatis di akun manajemen Organisasi. Anda harus mengaktifkan CSPM Security Hub secara manual di akun manajemen Organisasi sebelum dapat menambahkannya sebagai akun anggota.

- Jika akun sudah mengaktifkan Security Hub CSPM, Security Hub CSPM tidak membuat perubahan lain pada akun tersebut. Ini hanya memungkinkan keanggotaan.

Agar Security Hub CSPM dapat menghasilkan temuan kontrol, akun anggota harus telah AWS Config diaktifkan dan dikonfigurasi untuk merekam sumber daya yang diperlukan. Untuk informasi selengkapnya, lihat [Mengaktifkan dan mengonfigurasi AWS Config](#).

Pilih metode pilihan Anda, dan ikuti langkah-langkah untuk mengaktifkan akun organisasi sebagai akun anggota CSPM Security Hub.

Security Hub CSPM console

Mengaktifkan akun organisasi secara manual sebagai anggota CSPM Security Hub

1. Buka konsol AWS Security Hub Cloud Security Posture Management (CSPM) di <https://console.aws.amazon.com/securityhub/>

Masuk menggunakan kredensi akun administrator yang didelegasikan.

2. Di panel navigasi CSPM Security Hub, di bawah Pengaturan, pilih Konfigurasi.
3. Dalam daftar Akun, pilih setiap akun organisasi yang ingin Anda aktifkan.
4. Pilih Tindakan, lalu pilih Tambah anggota.

Security Hub CSPM API

Mengaktifkan akun organisasi secara manual sebagai anggota CSPM Security Hub

Memanggil [CreateMembers](#) API dari akun administrator yang didelegasikan. Agar setiap akun dapat diaktifkan, berikan ID akun.

Tidak seperti proses undangan manual, ketika Anda memanggil `CreateMembers` untuk mengaktifkan akun organisasi, Anda tidak perlu mengirim undangan.

AWS CLI

Mengaktifkan akun organisasi secara manual sebagai anggota CSPM Security Hub

Jalankan [create-members](#) perintah dari akun administrator yang didelegasikan. Agar setiap akun dapat diaktifkan, berikan ID akun.

Berbeda dengan proses undangan manual, ketika Anda menjalankan `create-members` untuk mengaktifkan akun organisasi, Anda tidak perlu mengirim undangan.

```
aws securityhub create-members --account-details '[{"AccountId": "<accountId>"}]'
```

Contoh

```
aws securityhub create-members --account-details '[{"AccountId": "123456789111"}, {"AccountId": "123456789222"}]'
```

Memutuskan akun anggota CSPM Security Hub dari organisasi Anda

Untuk berhenti menerima dan melihat temuan dari akun anggota AWS Security Hub Cloud Security Posture Management (CSPM) Security Hub, Anda dapat memisahkan akun anggota dari organisasi Anda.

 Note

Jika Anda menggunakan [konfigurasi pusat](#), disasosiasi bekerja secara berbeda. Anda dapat membuat kebijakan konfigurasi yang menonaktifkan CSPM Security Hub di satu atau beberapa akun anggota yang dikelola secara terpusat. Setelah itu, akun-akun ini masih menjadi bagian dari organisasi, tetapi tidak akan menghasilkan temuan CSPM Security Hub. Jika Anda menggunakan konfigurasi pusat tetapi juga memiliki akun anggota yang diundang secara manual, Anda dapat memisahkan satu atau beberapa akun yang diundang secara manual.

Akun anggota yang dikelola menggunakan tidak AWS Organizations dapat memisahkan akun mereka dari akun administrator. Hanya akun administrator yang dapat memisahkan akun anggota.

Memutuskan hubungan akun anggota tidak menutup akun. Sebaliknya, itu menghapus akun anggota dari organisasi. Akun anggota yang terputus menjadi mandiri Akun AWS yang tidak lagi dikelola oleh integrasi CSPM Security Hub dengan. AWS Organizations

Pilih metode pilihan Anda, dan ikuti langkah-langkah untuk memisahkan akun anggota dari organisasi.

Security Hub CSPM console

Untuk memisahkan akun anggota dari organisasi

1. Buka konsol AWS Security Hub Cloud Security Posture Management (CSPM) di <https://console.aws.amazon.com/securityhub/>

Masuk menggunakan kredensi akun administrator yang didelegasikan.

2. Di panel navigasi, di bawah Pengaturan, pilih Konfigurasi.
3. Di bagian Akun, pilih akun yang ingin Anda pisahkan. Jika Anda menggunakan konfigurasi pusat, Anda dapat memilih akun yang diundang secara manual untuk dipisahkan dari tab. `Invitation accounts` Tab ini hanya terlihat jika Anda menggunakan konfigurasi pusat.
4. Pilih Tindakan, lalu pilih Putuskan akun.

Security Hub CSPM API

Untuk memisahkan akun anggota dari organisasi

Memanggil [DisassociateMembers](#) API dari akun administrator yang didelegasikan. Anda harus menyediakan akun anggota untuk dipisahkan. Akun AWS IDs Untuk melihat daftar akun anggota, panggil [ListMembers](#) API.

AWS CLI

Untuk memisahkan akun anggota dari organisasi

Jalankan [disassociate-membersperintah>](#) dari akun administrator yang didelegasikan. Anda harus menyediakan akun anggota untuk dipisahkan. Akun AWS IDs Untuk melihat daftar akun anggota, jalankan [list-membersperintah>](#).

```
aws securityhub disassociate-members --account-ids "<accountIds>"
```

Contoh

```
aws securityhub disassociate-members --account-ids "123456789111" "123456789222"
```

Anda juga dapat menggunakan AWS Organizations konsol, AWS CLI, atau AWS SDKs untuk memisahkan akun anggota dari organisasi Anda. Untuk informasi selengkapnya, lihat [Menghapus akun anggota dari organisasi Anda](#) di Panduan AWS Organizations Pengguna.

Mengelola akun dengan undangan di Security Hub CSPM

Anda dapat mengelola beberapa akun AWS Security Hub Cloud Security Posture Management (CSPM) secara terpusat dengan dua cara, dengan mengintegrasikan Security Hub CSPM AWS Organizations dengan atau dengan mengirim dan menerima undangan keanggotaan secara manual. Anda harus menggunakan proses manual jika Anda memiliki akun mandiri atau Anda tidak berintegrasi dengannya AWS Organizations. Dalam manajemen akun manual, administrator CSPM Security Hub mengundang akun untuk menjadi anggota. Hubungan administrator-anggota terjalin ketika calon anggota menerima undangan. Akun administrator CSPM Security Hub dapat mengelola CSPM Security Hub hingga 1.000 akun anggota berbasis undangan.

Note

[Jika Anda membuat organisasi berbasis undangan di Security Hub CSPM, Anda selanjutnya dapat beralih menggunakan. AWS Organizations](#) Jika Anda memiliki lebih dari satu akun

anggota, sebaiknya AWS Organizations gunakan undangan CSPM Security Hub untuk mengelola akun anggota Anda. Untuk informasi, lihat [Mengelola Security Hub CSPM untuk beberapa akun dengan AWS Organizations](#).

Agregasi temuan Lintas Wilayah dan data lainnya tersedia untuk akun yang Anda undang melalui proses undangan manual. Namun, administrator harus mengundang akun anggota dari Wilayah agregasi dan semua Wilayah yang ditautkan agar agregasi lintas wilayah berfungsi. Selain itu, akun anggota harus mengaktifkan CSPM Security Hub di Wilayah agregasi dan semua Wilayah yang ditautkan untuk memberikan administrator kemampuan untuk melihat temuan dari akun anggota.

Kebijakan konfigurasi tidak didukung untuk akun anggota yang diundang secara manual. Sebagai gantinya, Anda harus mengonfigurasi pengaturan CSPM Security Hub secara terpisah di setiap akun anggota dan Wilayah AWS saat Anda menggunakan proses undangan manual.

Anda juga harus menggunakan proses berbasis undangan manual untuk akun yang bukan milik organisasi Anda. Misalnya, Anda mungkin tidak menyertakan akun pengujian di organisasi Anda. Atau, Anda mungkin ingin menggabungkan akun dari beberapa organisasi di bawah satu akun administrator CSPM Security Hub. Akun administrator CSPM Security Hub harus mengirim undangan ke akun milik organisasi lain.

Pada halaman Konfigurasi konsol CSPM Security Hub, akun yang ditambahkan melalui undangan tercantum di tab Akun undangan. Jika Anda menggunakan [konfigurasi pusat](#), tetapi juga mengundang akun di luar organisasi, Anda dapat melihat temuan dari akun berbasis undangan di tab ini. Namun, administrator CSPM Security Hub tidak dapat mengonfigurasi akun berbasis undangan di seluruh Wilayah melalui penggunaan kebijakan konfigurasi.

Topik di bagian ini menjelaskan cara mengelola akun anggota melalui undangan.

Topik

- [Menambahkan dan mengundang akun anggota di Security Hub CSPM](#)
- [Menanggapi undangan untuk menjadi akun anggota CSPM Security Hub](#)
- [Memutuskan akun anggota di Security Hub CSPM](#)
- [Menghapus akun anggota di Security Hub CSPM](#)
- [Memutuskan hubungan dari akun administrator CSPM Security Hub](#)
- [Transisi ke Organizations untuk mengelola akun di Security Hub CSPM](#)

Menambahkan dan mengundang akun anggota di Security Hub CSPM

Note

Sebaiknya gunakan AWS Organizations bukan undangan CSPM Security Hub untuk mengelola akun anggota Anda. Untuk informasi, lihat [Mengelola Security Hub CSPM untuk beberapa akun dengan AWS Organizations](#).

Akun Anda menjadi administrator AWS Security Hub Cloud Security Posture Management (CSPM) untuk akun yang menerima undangan Anda untuk menjadi akun anggota CSPM Security Hub.

Ketika Anda menerima undangan dari akun lain, akun Anda menjadi akun anggota, dan akun itu menjadi administrator Anda.

Jika akun Anda adalah akun administrator, Anda tidak dapat menerima undangan untuk menjadi akun anggota.

Menambahkan akun anggota terdiri dari langkah-langkah berikut:

1. Akun administrator menambahkan akun anggota ke daftar akun anggota mereka.
2. Akun administrator mengirimkan undangan ke akun anggota.
3. Akun anggota menerima undangan.

Menambahkan akun anggota

Dari konsol CSPM Security Hub, Anda dapat menambahkan akun ke daftar akun anggota Anda. Di konsol CSPM Security Hub, Anda dapat memilih akun satu per satu, atau mengunggah .csv file yang berisi informasi akun.

Untuk setiap akun, Anda harus memberikan ID akun dan alamat email. Alamat email harus berupa alamat email untuk dihubungi tentang masalah keamanan di akun. Ini tidak digunakan untuk memverifikasi akun.

Pilih metode pilihan Anda, dan ikuti langkah-langkah untuk menambahkan akun anggota.

Security Hub CSPM console

Untuk menambahkan akun ke daftar akun anggota Anda

1. Buka konsol AWS Security Hub Cloud Security Posture Management (CSPM) di <https://console.aws.amazon.com/securityhub/>

Masuk menggunakan kredensi akun administrator.

2. Di panel kiri, pilih Pengaturan.
3. Pada halaman Pengaturan, pilih Akun, lalu pilih Tambah akun. Anda kemudian dapat menambahkan akun satu per satu atau mengunggah .csv file yang berisi daftar akun.
4. Untuk memilih akun, lakukan salah satu hal berikut:

- Untuk menambahkan akun satu per satu, di bawah Masukkan akun, masukkan ID akun dan alamat email akun yang akan ditambahkan, lalu pilih Tambah.

Ulangi proses ini untuk setiap akun.

- Untuk menggunakan file nilai yang dipisahkan koma (.csv) untuk menambahkan beberapa akun, buat file terlebih dahulu. File harus berisi ID akun dan alamat email untuk ditambahkan setiap akun.

Dalam .csv daftar Anda, akun harus muncul satu per baris. Baris pertama .csv file harus berisi header. Di header, kolom pertama adalah **Account ID** dan kolom kedua adalah **Email**.

Setiap baris berikutnya harus berisi ID akun dan alamat email yang valid untuk ditambahkan akun.

Berikut adalah contoh .csv file ketika dilihat di editor teks.

```
Account ID,Email
111111111111,user@example.com
```

Dalam program spreadsheet, bidang muncul di kolom terpisah. Format yang mendasarinya masih dipisahkan koma. Anda harus memformat akun IDs sebagai angka non-desimal. Misalnya, ID akun 444455556666 tidak dapat diformat sebagai 444455556666.0. Pastikan juga bahwa pemformatan angka tidak menghapus nol di depan dari ID akun.

Untuk memilih file, di konsol, pilih Unggah daftar (.csv). Kemudian pilih Browse.

Setelah Anda memilih file, pilih Tambah akun.

5. Setelah Anda selesai menambahkan akun, di bawah Akun yang akan ditambahkan, pilih Berikutnya.

Security Hub CSPM API

Untuk menambahkan akun ke daftar akun anggota Anda

Memanggil [CreateMembers](#) API dari akun administrator. Untuk setiap akun anggota untuk ditambahkan, Anda harus memberikan Akun AWS ID.

AWS CLI

Untuk menambahkan akun ke daftar akun anggota Anda

Jalankan [create-members](#) perintah dari akun administrator. Untuk setiap akun anggota untuk ditambahkan, Anda harus memberikan Akun AWS ID.

```
aws securityhub create-members --account-details '[{"AccountId": "<accountID1>"}]'
```

Contoh

```
aws securityhub create-members --account-details '[{"AccountId": "123456789111"}, {"AccountId": "123456789222"}]'
```

Mengundang akun anggota

Setelah Anda menambahkan akun anggota, Anda mengirim undangan ke akun anggota. Anda juga dapat mengirim ulang undangan ke akun yang Anda lepaskan dari administrator.

Security Hub CSPM console

Mengundang akun calon member

1. Buka konsol AWS Security Hub Cloud Security Posture Management (CSPM) di <https://console.aws.amazon.com/securityhub/>

Masuk menggunakan kredensi akun administrator.

2. Di panel navigasi, pilih Pengaturan, lalu pilih Akun.
3. Untuk akun yang akan diundang, pilih Undang di kolom Status.
4. Saat diminta untuk mengonfirmasi, pilih Undang.

 Note

Untuk mengirim ulang undangan ke akun yang tidak terkait, pilih setiap akun yang tidak terkait di halaman Akun. Untuk Tindakan, pilih Kirim ulang undangan.

Security Hub CSPM API

Mengundang akun calon member

Memanggil [InviteMembers](#) API dari akun administrator. Untuk setiap akun yang akan diundang, Anda harus memberikan Akun AWS ID.

AWS CLI

Mengundang akun calon member

Jalankan [invite-members](#) perintah dari akun administrator. Untuk setiap akun yang akan diundang, Anda harus memberikan Akun AWS ID.

```
aws securityhub invite-members --account-ids <accountIDs>
```

Contoh

```
aws securityhub invite-members --account-ids "123456789111" "123456789222"
```

Menanggapi undangan untuk menjadi akun anggota CSPM Security Hub

 Note

Sebaiknya gunakan AWS Organizations bukan undangan CSPM Security Hub untuk mengelola akun anggota Anda. Untuk informasi, lihat [Mengelola Security Hub CSPM untuk beberapa akun dengan AWS Organizations](#).

Anda dapat menerima atau menolak undangan untuk menjadi akun anggota AWS Security Hub Cloud Security Posture Management (CSPM).

Jika Anda menerima undangan, akun Anda menjadi akun anggota CSPM Security Hub. Akun yang mengirim undangan menjadi akun administrator CSPM Security Hub Anda. Pengguna akun administrator dapat melihat temuan untuk akun anggota Anda di Security Hub CSPM.

Jika Anda menolak undangan, maka akun Anda ditandai sebagai Mengundurkan diri pada daftar akun anggota akun administrator.

Anda hanya dapat menerima satu undangan untuk menjadi akun anggota.

Sebelum Anda dapat menerima atau menolak undangan, Anda harus mengaktifkan Security Hub CSPM.

Ingat bahwa semua akun CSPM Security Hub harus telah AWS Config diaktifkan dan dikonfigurasi untuk merekam semua sumber daya. Untuk detail tentang persyaratan AWS Config, lihat [Mengaktifkan dan mengonfigurasi AWS Config](#).

Menerima undangan

Anda dapat mengirim undangan untuk menjadi akun anggota CSPM Security Hub dari akun administrator. Anda kemudian dapat menerima undangan setelah masuk ke akun anggota.

Pilih metode pilihan Anda, dan ikuti langkah-langkah untuk menerima undangan untuk menjadi akun anggota.

Security Hub CSPM console

Untuk menerima undangan keanggotaan

1. Buka konsol AWS Security Hub Cloud Security Posture Management (CSPM) di <https://console.aws.amazon.com/securityhub/>
2. Di panel navigasi, pilih Pengaturan, lalu pilih Akun.
3. Di bagian Akun Administrator, aktifkan Terima, lalu pilih Terima undangan.

Security Hub CSPM API

Untuk menerima undangan keanggotaan

Memanggil [AcceptAdministratorInvitation](#) API. Anda harus memberikan pengenalan undangan dan Akun AWS ID akun administrator. Untuk mengambil detail tentang undangan, gunakan [ListInvitations](#) operasi.

AWS CLI

Untuk menerima undangan keanggotaan

Jalankan perintah [accept-administrator-invitation](#). Anda harus memberikan pengenalan undangan dan Akun AWS ID akun administrator. Untuk mengambil detail tentang undangan, jalankan [list-invitations](#) perintah.

```
aws securityhub accept-administrator-invitation --administrator-id <administratorAccountID> --invitation-id <invitationID>
```

Contoh

```
aws securityhub accept-administrator-invitation --administrator-id 123456789012 --invitation-id 7ab938c5d52d7904ad09f9e7c20cc4eb
```

Note

Konsol CSPM Security Hub terus digunakan. AcceptInvitation Pada akhirnya akan berubah untuk digunakan AcceptAdministratorInvitation. Setiap kebijakan IAM yang secara khusus mengontrol akses ke fungsi ini harus terus digunakan AcceptInvitation. Anda juga harus menambahkan kebijakan Anda AcceptAdministratorInvitation untuk memastikan bahwa izin yang benar diberlakukan setelah konsol mulai digunakan AcceptAdministratorInvitation.

Menolak undangan

Anda dapat menolak undangan untuk menjadi akun anggota CSPM Security Hub. Saat Anda menolak undangan di konsol CSPM Security Hub, akun Anda ditandai sebagai Mengundurkan diri pada daftar akun anggota akun administrator. Status mengundurkan diri hanya muncul saat Anda masuk ke konsol CSPM Security Hub menggunakan akun administrator. Namun, undangan tetap tidak berubah di konsol untuk akun anggota sampai Anda masuk ke akun administrator dan menghapus undangan.

Untuk menolak undangan, Anda harus masuk ke akun anggota yang menerima undangan.

Pilih metode pilihan Anda, dan ikuti langkah-langkah untuk menolak undangan menjadi akun anggota.

Security Hub CSPM console

Untuk menolak undangan keanggotaan

1. Buka konsol AWS Security Hub Cloud Security Posture Management (CSPM) di <https://console.aws.amazon.com/securityhub/>
2. Di panel navigasi, pilih Pengaturan, lalu pilih Akun.
3. Di bagian Akun Administrator, pilih Tolak undangan.

Security Hub CSPM API

Untuk menolak undangan keanggotaan

Memanggil [DeclineInvitations](#) API. Anda harus memberikan Akun AWS ID akun administrator yang mengeluarkan undangan. Untuk melihat informasi tentang undangan Anda, gunakan operasi [ListInvitations](#)

AWS CLI

Untuk menolak undangan keanggotaan

Jalankan perintah [decline-invitations](#). Anda harus memberikan Akun AWS ID akun administrator yang mengeluarkan undangan. Untuk melihat informasi tentang undangan Anda, jalankan perintah [list-invitations](#)

```
aws securityhub decline-invitations --account-ids "<administratorAccountId>"
```

Contoh

```
aws securityhub decline-invitations --account-ids "123456789012"
```


Memutuskan akun anggota di Security Hub CSPM

Note

Sebaiknya gunakan AWS Organizations bukan undangan CSPM Security Hub untuk mengelola akun anggota Anda. Untuk informasi, lihat [Mengelola Security Hub CSPM untuk beberapa akun dengan AWS Organizations](#).

Akun administrator AWS Security Hub Cloud Security Posture Management (CSPM) dapat memisahkan akun anggota untuk berhenti menerima dan melihat temuan dari akun tersebut. Anda harus memisahkan akun anggota sebelum Anda dapat menghapusnya.

Saat Anda memisahkan akun anggota, akun tersebut tetap ada dalam daftar akun anggota Anda dengan status Dihapus (Terputus). Akun Anda dihapus dari informasi akun administrator untuk akun anggota.

Untuk melanjutkan menerima temuan untuk akun, Anda dapat mengirim ulang undangan. Untuk menghapus akun anggota sepenuhnya, Anda dapat menghapus akun anggota.

Pilih metode pilihan Anda, dan ikuti langkah-langkah untuk memisahkan akun anggota yang diundang secara manual dari akun administrator.

Security Hub CSPM console

Untuk memisahkan akun anggota yang diundang secara manual

1. Buka konsol AWS Security Hub Cloud Security Posture Management (CSPM) di <https://console.aws.amazon.com/securityhub/>

Masuk menggunakan kredensi akun administrator.

2. Di panel navigasi, di bawah Pengaturan, pilih Konfigurasi.
3. Di bagian Akun, pilih akun yang ingin Anda pisahkan.
4. Pilih Tindakan, lalu pilih Disassociate account.

Security Hub CSPM API

Untuk memisahkan akun anggota yang diundang secara manual

Memanggil [DisassociateMembers](#) API dari akun administrator. Anda harus memberikan akun anggota yang ingin Anda pisahkan. Akun AWS IDs Untuk melihat daftar akun anggota, gunakan [ListMembers](#) operasi.

AWS CLI

Untuk memisahkan akun anggota yang diundang secara manual

Jalankan [disassociate-members](#) perintah dari akun administrator. Anda harus memberikan akun anggota yang ingin Anda pisahkan. Akun AWS IDs Untuk melihat daftar akun anggota, jalankan [list-members](#) perintah.

```
aws securityhub disassociate-members --account-ids <accountIds>
```

Contoh

```
aws securityhub disassociate-members --account-ids "123456789111" "123456789222"
```

Menghapus akun anggota di Security Hub CSPM

Note

Sebaiknya gunakan AWS Organizations bukan undangan CSPM Security Hub untuk mengelola akun anggota Anda. Untuk informasi, lihat [Mengelola Security Hub CSPM untuk beberapa akun dengan AWS Organizations](#).

Sebagai akun administrator AWS Security Hub Cloud Security Posture Management (CSPM), Anda dapat menghapus akun anggota yang ditambahkan melalui undangan. Sebelum Anda dapat menghapus akun yang diaktifkan, Anda harus memisahnya.

Ketika Anda menghapus akun anggota, itu sepenuhnya dihapus dari daftar. Untuk memulihkan keanggotaan akun, Anda harus menambahkan dan mengundangnya lagi seolah-olah itu adalah akun anggota yang sama sekali baru.

Anda tidak dapat menghapus akun milik organisasi dan yang dikelola menggunakan integrasi dengan AWS Organizations.

Pilih metode pilihan Anda, dan ikuti langkah-langkah untuk menghapus akun anggota yang diundang secara manual.

Security Hub CSPM console

Untuk menghapus akun anggota yang diundang secara manual

1. Buka konsol AWS Security Hub Cloud Security Posture Management (CSPM) di <https://console.aws.amazon.com/securityhub/>

Masuk menggunakan akun administrator.

2. Di panel navigasi, pilih Pengaturan, lalu pilih Konfigurasi.
3. Pilih tab Akun undangan. Kemudian, pilih akun yang akan dihapus.
4. Pilih Tindakan, lalu pilih Hapus. Opsi ini hanya tersedia jika Anda telah memisahkan akun. Anda harus memisahkan akun anggota sebelum dapat dihapus.

Security Hub CSPM API

Untuk menghapus akun anggota yang diundang secara manual

Memanggil [DeleteMembers](#) API dari akun administrator. Anda harus memberikan akun anggota yang ingin Anda hapus. Akun AWS IDs Untuk mengambil daftar akun anggota, panggil API [ListMembers](#)

AWS CLI

Untuk menghapus akun anggota yang diundang secara manual

Jalankan [delete-members](#) perintah dari akun administrator. Anda harus memberikan akun anggota yang ingin Anda hapus. Akun AWS IDs Untuk mengambil daftar akun anggota, jalankan [list-members](#) perintah.

```
aws securityhub delete-members --account-ids <memberAccountIDs>
```

Contoh

```
aws securityhub delete-members --account-ids "123456789111" "123456789222"
```

Memutuskan hubungan dari akun administrator CSPM Security Hub

Note

Sebaiknya gunakan AWS Organizations bukan undangan CSPM Security Hub untuk mengelola akun anggota Anda. Untuk informasi, lihat [Mengelola Security Hub CSPM untuk beberapa akun dengan AWS Organizations](#).

Jika akun Anda ditambahkan sebagai akun anggota AWS Security Hub Cloud Security Posture Management (CSPM) melalui undangan, Anda dapat memisahkan akun anggota dari akun administrator. Setelah Anda memisahkan akun anggota, Security Hub CSPM tidak mengirimkan temuan dari akun ke akun administrator.

Akun anggota yang dikelola menggunakan integrasi dengan tidak AWS Organizations dapat memisahkan akun mereka dari akun administrator. Hanya administrator yang didelegasikan CSPM Security Hub yang dapat memisahkan akun anggota yang dikelola dengan Organizations.

Ketika Anda memisahkan diri dari akun administrator Anda, akun Anda tetap berada dalam daftar anggota akun administrator dengan status Mengundurkan diri. Namun, akun administrator tidak menerima temuan apa pun untuk akun Anda.

Setelah Anda memisahkan diri dari akun administrator, undangan untuk menjadi anggota masih tetap ada. Anda dapat menerima undangan lagi di masa depan.

Security Hub CSPM console

Untuk memisahkan diri dari akun administrator Anda

1. Buka konsol AWS Security Hub Cloud Security Posture Management (CSPM) di <https://console.aws.amazon.com/securityhub/>
2. Di panel navigasi, pilih Pengaturan, lalu pilih Akun.
3. Di bagian Akun Administrator, matikan Terima, lalu pilih Perbarui.

Security Hub CSPM API

Untuk memisahkan diri dari akun administrator Anda

Memanggil [DisassociateFromAdministratorAccount](#) API.

AWS CLI

Untuk memisahkan diri dari akun administrator Anda

Jalankan perintah [disassociate-from-administrator-account](#).

```
aws securityhub disassociate-from-administrator-account
```

Note

Konsol CSPM Security Hub terus digunakan. `DisassociateFromMasterAccount` Pada akhirnya akan berubah untuk digunakan `DisassociateFromAdministratorAccount`. Setiap kebijakan IAM yang secara khusus mengontrol akses ke fungsi ini harus terus digunakan `DisassociateFromMasterAccount`. Anda juga harus menambahkan kebijakan Anda `DisassociateFromAdministratorAccount` untuk memastikan bahwa izin yang benar diberlakukan setelah konsol mulai digunakan `DisassociateFromAdministratorAccount`.

Transisi ke Organizations untuk mengelola akun di Security Hub CSPM

Ketika Anda mengelola akun secara manual di AWS Security Hub Cloud Security Posture Management (CSPM), Anda harus mengundang akun calon anggota dan mengonfigurasi setiap akun anggota secara terpisah di masing-masing akun. Wilayah AWS

Dengan mengintegrasikan Security Hub CSPM dan AWS Organizations, Anda dapat menghilangkan kebutuhan untuk mengirim undangan dan mendapatkan kontrol lebih besar atas bagaimana Security Hub CSPM dikonfigurasi dan disesuaikan di organisasi Anda. Untuk alasan ini, sebaiknya gunakan AWS Organizations bukan undangan CSPM Security Hub untuk mengelola akun anggota Anda. Untuk informasi, lihat [Mengelola Security Hub CSPM untuk beberapa akun dengan AWS Organizations](#).

Anda dapat menggunakan pendekatan gabungan di mana Anda menggunakan AWS Organizations integrasi, tetapi juga mengundang akun secara manual di luar organisasi Anda. Namun, kami merekomendasikan secara eksklusif menggunakan integrasi Organizations. [Konfigurasi pusat](#), fitur yang membantu Anda mengelola CSPM Security Hub di beberapa akun dan Wilayah, hanya tersedia saat Anda berintegrasi dengan Organizations.

Bagian ini mencakup bagaimana Anda dapat beralih dari manajemen akun berbasis undangan manual ke mengelola akun dengan AWS Organizations

Mengintegrasikan CSPM Security Hub dengan AWS Organizations

Pertama, Anda harus mengintegrasikan Security Hub CSPM dan AWS Organizations

Anda dapat mengintegrasikan layanan ini dengan menyelesaikan langkah-langkah berikut:

- Buat organisasi di AWS Organizations. Untuk petunjuk, lihat [Membuat organisasi](#) di Panduan AWS Organizations Pengguna.
- Dari akun manajemen Organizations, tentukan akun administrator yang didelegasikan CSPM Security Hub.

Note

Akun manajemen organisasi tidak dapat ditetapkan sebagai akun DA.

Untuk petunjuk mendetail, lihat [Mengintegrasikan CSPM Security Hub dengan AWS Organizations](#).

Dengan menyelesaikan langkah-langkah sebelumnya, Anda memberikan [akses tepercaya](#) untuk Security Hub CSPM di AWS Organizations. Ini juga memungkinkan Security Hub CSPM saat ini Wilayah AWS untuk akun administrator yang didelegasikan.

Administrator yang didelegasikan dapat mengelola organisasi di Security Hub CSPM, terutama dengan menambahkan akun organisasi sebagai akun anggota CSPM Security Hub. Administrator juga dapat mengakses pengaturan, data, dan sumber daya CSPM Security Hub tertentu untuk akun tersebut.

Saat Anda beralih ke manajemen akun menggunakan Organizations, akun berbasis undangan tidak secara otomatis menjadi anggota CSPM Security Hub. Hanya akun yang Anda tambahkan ke organisasi baru yang dapat menjadi anggota CSPM Security Hub.

Setelah mengaktifkan integrasi, Anda dapat mengelola akun dengan Organizations. Untuk informasi, lihat [Mengelola Security Hub CSPM untuk beberapa akun dengan AWS Organizations](#). Manajemen akun bervariasi berdasarkan jenis konfigurasi organisasi Anda.

Tindakan yang diizinkan oleh administrator dan akun anggota di Security Hub CSPM

Akun administrator dan anggota memiliki akses ke tindakan AWS Security Hub Cloud Security Posture Management (CSPM) yang tercantum dalam tabel berikut. Dalam tabel, nilai-nilai memiliki arti sebagai berikut:

- Apa saja — Akun dapat melakukan tindakan untuk akun anggota mana pun di bawah administrator yang sama.
- Saat ini — Akun dapat melakukan tindakan hanya untuk dirinya sendiri (akun yang saat ini Anda masuki).
- Dash — Menunjukkan bahwa akun tidak dapat melakukan tindakan.

Sebagaimana dicatat dalam tabel, tindakan yang diizinkan berbeda berdasarkan apakah Anda berintegrasi dengan AWS Organizations dan jenis konfigurasi yang digunakan organisasi Anda. Untuk informasi tentang perbedaan antara konfigurasi pusat dan lokal, lihat [Mengelola akun dengan AWS Organizations](#).

Security Hub CSPM tidak menyalin temuan akun anggota ke akun administrator. Di Security Hub CSPM, semua temuan dicerna ke Wilayah tertentu untuk akun tertentu. Di setiap Wilayah, akun administrator dapat melihat dan mengelola temuan untuk akun anggota mereka di Wilayah tersebut.

Jika Anda menetapkan Wilayah agregasi, akun administrator dapat melihat dan mengelola temuan akun anggota dari Wilayah tertaut yang direplikasi ke Wilayah agregasi. Untuk informasi selengkapnya tentang agregasi lintas wilayah, lihat agregasi [Lintas](#) Wilayah.

Tabel berikut menentukan izin default untuk akun administrator dan anggota. Anda dapat menggunakan kebijakan IAM khusus untuk membatasi akses lebih lanjut ke fitur dan fungsi CSPM Security Hub. Untuk panduan dan contoh, lihat posting blog [Menyelaraskan kebijakan IAM dengan persona pengguna untuk AWS Security Hub Cloud Security Posture Management \(CSPM\)](#).

Tindakan yang diizinkan jika Anda berintegrasi dengan Organizations dan menggunakan konfigurasi pusat

Akun administrator dan anggota dapat mengakses tindakan CSPM Security Hub sebagai berikut jika Anda berintegrasi dengan Organizations dan menggunakan konfigurasi pusat.

Tindakan	Security Hub CSPM mendelegasikan akun administrator	Akun anggota yang dikelola secara terpusat	Akun anggota yang dikelola sendiri
Membuat dan mengelola kebijakan konfigurasi CSPM Security Hub	Untuk akun yang dikelola sendiri dan terpusat	–	–
Lihat akun organisasi	Setiap	–	–
Putuskan akun anggota	Setiap	–	–
Hapus akun anggota	Akun non-organisasi apa pun	–	–
Nonaktifkan CSPM Security Hub	Untuk akun saat ini dan akun yang dikelola secara terpusat	–	Saat ini (harus dipisahkan dari akun administrator)
Lihat temuan dan temukan sejarah	Setiap	Saat ini	Saat ini
Perbarui temuan	Setiap	Saat ini	Saat ini
Lihat hasil wawasan	Setiap	Saat ini	Saat ini
Lihat detail kontrol	Setiap	Saat ini	Saat ini
Mengaktifkan atau menonaktifkan temuan kontrol konsolidasi	Setiap	–	–
Aktifkan dan nonaktifkan standar	Untuk akun saat ini dan akun yang	–	Saat ini

Tindakan	Security Hub CSPM mendelegasikan akun administrator	Akun anggota yang dikelola secara terpusat	Akun anggota yang dikelola sendiri
	dikelola secara terpusat		
Aktifkan dan nonaktifkan kontrol	Untuk akun saat ini dan akun yang dikelola secara terpusat	–	Saat ini
Mengaktifkan dan menonaktifkan integrasi	Saat ini	Saat ini	Saat ini
Konfigurasi agregasi lintas wilayah	Setiap	–	–
Pilih beranda Wilayah dan terkait Wilayah	Apa saja (harus berhenti dan memulai ulang konfigurasi pusat untuk mengubah Wilayah rumah)	–	–
Konfigurasi tindakan khusus	Saat ini	Saat ini	Saat ini
Konfigurasi aturan otomatisasi	Setiap	–	–
Konfigurasi wawasan khusus	Saat ini	Saat ini	Saat ini

Tindakan yang diizinkan jika Anda berintegrasi dengan Organizations dan menggunakan konfigurasi lokal

Akun administrator dan anggota dapat mengakses tindakan CSPM Security Hub sebagai berikut jika Anda berintegrasi dengan Organizations dan menggunakan konfigurasi lokal.

Tindakan	Security Hub CSPM mendelegasikan akun administrator	Akun anggota
Membuat dan mengelola kebijakan konfigurasi CSPM Security Hub	–	–
Lihat akun organisasi	Setiap	–
Putuskan akun anggota	Setiap	–
Hapus akun anggota	–	–
Nonaktifkan CSPM Security Hub	–	Saat ini (jika akun dipisahkan dari administrator yang didelegasikan)
Lihat temuan dan temukan sejarah	Setiap	Saat ini
Perbarui temuan	Setiap	Saat ini
Lihat hasil wawasan	Setiap	Saat ini
Lihat detail kontrol	Setiap	Saat ini
Mengaktifkan atau menonaktifkan temuan kontrol konsolidasi	Setiap	–
Aktifkan dan nonaktifkan standar	Saat ini	Saat ini

Tindakan	Security Hub CSPM mendelegasikan akun administrator	Akun anggota
Secara otomatis mengaktifkan CSPM Security Hub dan standar default di akun organisasi baru	Untuk akun saat ini dan akun organisasi baru	–
Aktifkan dan nonaktifkan kontrol	Saat ini	Saat ini
Mengaktifkan dan menonaktifkan integrasi	Saat ini	Saat ini
Konfigurasi agregasi lintas wilayah	Setiap	–
Konfigurasi tindakan khusus	Saat ini	Saat ini
Konfigurasi aturan otomatisasi	Setiap	–
Konfigurasi wawasan khusus	Saat ini	Saat ini

Tindakan yang diizinkan untuk akun berbasis undangan

Akun administrator dan anggota dapat mengakses tindakan CSPM Security Hub sebagai berikut jika Anda menggunakan metode berbasis undangan untuk mengelola akun secara manual alih-alih mengintegrasikan dengan AWS Organizations.

Tindakan	Akun administrator CSPM Security Hub	Akun anggota
Membuat dan mengelola kebijakan konfigurasi CSPM Security Hub	–	–
Lihat akun organisasi	Setiap	–
Putuskan akun anggota	Setiap	Saat ini
Hapus akun anggota	Setiap	–
Nonaktifkan CSPM Security Hub	Saat ini (jika tidak ada akun anggota yang diaktifkan)	Saat ini (jika akun dipisahkan dari akun administrator)
Lihat temuan dan temukan sejarah	Setiap	Saat ini
Perbarui temuan	Setiap	Saat ini
Lihat hasil wawasan	Setiap	Saat ini
Lihat detail kontrol	Setiap	Saat ini
Mengaktifkan atau menonaktifkan temuan kontrol konsolidasi	Setiap	–
Aktifkan dan nonaktifkan standar	Saat ini	Saat ini
Secara otomatis mengaktifkan CSPM Security Hub dan standar default di akun organisasi baru	–	–
Aktifkan dan nonaktifkan kontrol	Saat ini	Saat ini

Tindakan	Akun administrator CSPM Security Hub	Akun anggota
Mengaktifkan dan menonaktifkan integrasi	Saat ini	Saat ini
Konfigurasi agregasi lintas wilayah	Setiap	–
Konfigurasi tindakan khusus	Saat ini	Saat ini
Konfigurasi aturan otomatisasi	Setiap	–
Konfigurasi wawasan khusus	Saat ini	Saat ini

Pengaruh tindakan akun pada data CSPM Security Hub

Tindakan akun ini memiliki efek berikut pada data AWS Security Hub Cloud Security Posture Management (CSPM).

Security Hub CSPM dinonaktifkan

Jika Anda menggunakan [konfigurasi pusat](#), administrator yang didelegasikan (DA) dapat membuat kebijakan konfigurasi CSPM Security Hub yang menonaktifkan AWS Security Hub Cloud Security Posture Management (CSPM) di akun dan unit organisasi tertentu (). OUs Dalam hal ini, CSPM Security Hub dinonaktifkan di akun yang ditentukan dan OUs di Wilayah asal Anda dan Wilayah yang ditautkan. Jika Anda tidak menggunakan konfigurasi pusat, Anda harus menonaktifkan Security Hub CSPM secara terpisah di setiap akun dan Wilayah tempat Anda mengaktifkannya. Anda tidak dapat menggunakan konfigurasi pusat jika Security Hub CSPM dinonaktifkan di akun DA.

Tidak ada temuan yang dihasilkan untuk akun administrator jika CSPM Security Hub dinonaktifkan di akun administrator. Temuan arsip yang ada dihapus setelah 30 hari. Temuan aktif yang ada dihapus setelah 90 hari.

Integrasi dengan Layanan AWS yang lain dihapus.

Standar dan kontrol keamanan yang diaktifkan dinonaktifkan.

Data dan pengaturan CSPM Security Hub lainnya, termasuk tindakan kustom, wawasan, dan langganan produk pihak ketiga disimpan selama 90 hari.

Akun anggota dipisahkan dari akun administrator

Ketika akun anggota dipisahkan dari akun administrator, akun administrator kehilangan izin untuk melihat temuan di akun anggota. Namun, Security Hub CSPM masih diaktifkan di kedua akun.

Jika Anda menggunakan konfigurasi pusat, DA tidak dapat mengonfigurasi CSPM Security Hub untuk akun anggota yang dipisahkan dari akun DA.

Pengaturan atau integrasi khusus yang ditentukan untuk akun administrator tidak diterapkan pada temuan dari akun anggota sebelumnya. Misalnya, setelah akun dipisahkan, Anda mungkin memiliki tindakan kustom di akun administrator yang digunakan sebagai pola peristiwa dalam EventBridge aturan Amazon. Namun, tindakan kustom ini tidak dapat digunakan di akun anggota.

Dalam daftar Akun untuk akun administrator CSPM Security Hub, akun yang dihapus memiliki status Terputus.

Akun anggota dihapus dari organisasi

Ketika akun anggota dihapus dari organisasi, akun administrator CSPM Security Hub kehilangan izin untuk melihat temuan di akun anggota. Namun, Security Hub CSPM masih diaktifkan di kedua akun dengan pengaturan yang sama sebelum dihapus.

Jika Anda menggunakan konfigurasi pusat, Anda tidak dapat mengonfigurasi CSPM Security Hub untuk akun anggota setelah dihapus dari organisasi tempat administrator yang didelegasikan berada. Namun, akun mempertahankan pengaturan yang dimilikinya sebelum dihapus kecuali Anda mengubahnya secara manual.

Dalam daftar Akun untuk akun administrator CSPM Security Hub, akun yang dihapus memiliki status Dihapus.

Akun ditangguhkan

Ketika Akun AWS ditangguhkan, akun kehilangan izin untuk melihat temuan mereka di Security Hub CSPM. Tidak ada temuan yang dihasilkan untuk akun itu. Akun administrator untuk akun yang ditangguhkan dapat melihat temuan yang ada untuk akun tersebut.

Untuk akun organisasi, status akun anggota juga dapat berubah menjadi Akun Ditangguhkan. Ini terjadi jika akun ditangguhkan pada saat yang sama ketika akun administrator mencoba mengaktifkan akun. Akun administrator untuk akun yang Ditangguhkan Akun tidak dapat melihat temuan untuk akun tersebut. Jika tidak, status yang ditangguhkan tidak akan memengaruhi status akun anggota.

Jika Anda menggunakan konfigurasi pusat, asosiasi kebijakan gagal jika administrator yang didelegasikan mencoba mengaitkan kebijakan konfigurasi dengan akun yang ditangguhkan.

Setelah 90 hari, akun dihentikan atau diaktifkan kembali. Ketika akun diaktifkan kembali, izin CSPM Security Hub akan dipulihkan. Jika status akun anggota adalah Akun Ditangguhkan, akun administrator harus mengaktifkan akun secara manual.

Akun ditutup

Ketika Akun AWS ditutup, Security Hub CSPM merespons penutupan sebagai berikut.

Jika akun tersebut adalah akun administrator CSPM Security Hub, akun tersebut dihapus sebagai akun administrator dan semua akun anggota dihapus. Jika akun tersebut adalah akun anggota, akun tersebut dipisahkan dan dihapus sebagai anggota dari akun administrator CSPM Security Hub.

Security Hub CSPM menyimpan temuan arsip yang ada di akun selama 30 hari. Untuk temuan kontrol, perhitungan 30 hari didasarkan pada nilai untuk UpdatedAt bidang temuan. Untuk jenis temuan lain, perhitungan didasarkan pada nilai untuk UpdatedAt atau ProcessedAt bidang temuan, tanggal mana pun yang terbaru. Pada akhir periode 30 hari ini, Security Hub CSPM secara permanen menghapus temuan dari akun.

Security Hub CSPM mempertahankan temuan aktif yang ada di akun selama 90 hari. Untuk temuan kontrol, perhitungan 90 hari didasarkan pada nilai untuk UpdatedAt bidang temuan. Untuk jenis temuan lain, perhitungan didasarkan pada nilai untuk UpdatedAt atau ProcessedAt bidang temuan, tanggal mana pun yang terbaru. Pada akhir periode 90 hari ini, Security Hub CSPM secara permanen menghapus temuan dari akun.

Untuk retensi jangka panjang dari temuan yang ada, Anda dapat mengekspor temuan ke ember S3. Anda dapat melakukan ini dengan menggunakan tindakan kustom dengan EventBridge aturan Amazon. Untuk informasi selengkapnya, lihat [Menggunakan EventBridge untuk respon otomatis dan remediasi](#).

 Important

Untuk pelanggan yang masuk AWS GovCloud (US) Regions, buat cadangan, lalu hapus data kebijakan dan sumber daya akun lainnya sebelum menutup akun. Anda tidak akan memiliki akses ke sumber daya dan data setelah menutup akun.

Untuk informasi selengkapnya, lihat [Menutup Akun AWS](#) di Panduan AWS Account Management Referensi.

Memahami agregasi lintas wilayah di Security Hub CSPM

Note

Wilayah agregasi sekarang disebut Wilayah asal. Beberapa operasi Security Hub CSPM API masih menggunakan istilah agregasi Region yang lebih lama.

Dengan menggunakan agregasi lintas wilayah di AWS Security Hub Cloud Security Posture Management (CSPM), Anda dapat mengumpulkan temuan, menemukan pembaruan, wawasan, mengontrol status kepatuhan, dan skor keamanan dari beberapa ke satu wilayah asal. Wilayah AWS Anda kemudian dapat mengelola semua data ini dari Wilayah asal.

Misalkan Anda menetapkan US East (Virginia N.) sebagai Wilayah asal, dan AS Barat (Oregon) dan AS Barat (California N.) sebagai Wilayah terkait. Ketika Anda melihat halaman Temuan di AS Timur (Virginia N.), Anda melihat temuan dari ketiga Wilayah. Pembaruan temuan tersebut juga tercermin di ketiga Wilayah.

Note

Di AWS GovCloud (US), agregasi lintas wilayah hanya didukung untuk temuan, menemukan pembaruan, dan wawasan di seluruh wilayah. AWS GovCloud (US) Secara khusus, Anda hanya dapat mengumpulkan temuan, menemukan pembaruan, dan wawasan antara AWS GovCloud (AS-Timur) dan AWS GovCloud (AS-Barat). Di Wilayah Tiongkok, agregasi lintas wilayah hanya didukung untuk temuan, menemukan pembaruan, dan wawasan di seluruh Wilayah Tiongkok. Secara khusus, Anda hanya dapat mengumpulkan temuan, menemukan pembaruan, dan wawasan antara Tiongkok (Beijing) dan Tiongkok (Ningxia).

Jika kontrol diaktifkan di Wilayah tertaut tetapi dinonaktifkan di Wilayah asal, Anda dapat melihat status kepatuhan kontrol dari Wilayah asal, tetapi Anda tidak dapat mengaktifkan atau menonaktifkan kontrol tersebut dari Wilayah asal. Pengecualiannya adalah jika Anda menggunakan [konfigurasi pusat](#). Jika Anda menggunakan konfigurasi pusat, administrator CSPM Security Hub yang didelegasikan dapat mengonfigurasi kontrol di Wilayah beranda dan Wilayah tertaut dari Wilayah beranda.

Jika Anda telah menetapkan Wilayah asal, [skor keamanan](#) memperhitungkan status kontrol di semua Wilayah terkait. Untuk melihat skor keamanan lintas wilayah dan status kepatuhan, tambahkan izin berikut ke peran IAM Anda yang menggunakan CSPM Security Hub:

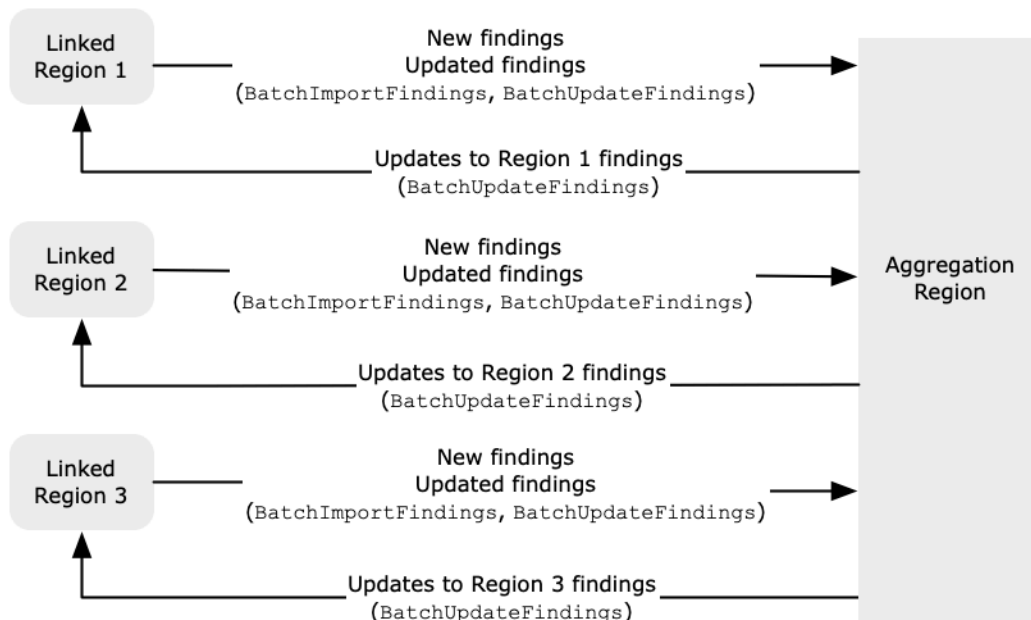
- [ListSecurityControlDefinitions](#)
- [BatchGetStandardsControlAssociations](#)
- [BatchUpdateStandardsControlAssociations](#)

Jenis data yang dikumpulkan

Bila agregasi lintas wilayah diaktifkan dengan satu atau beberapa Wilayah tertaut, Security Hub CSPM mereplikasi data berikut dari Wilayah tertaut ke Wilayah asal. Ini terjadi di setiap akun yang mengaktifkan agregasi lintas wilayah.

- Temuan
- Wawasan
- Kontrol status kepatuhan
- Skor keamanan

Selain data baru dalam daftar sebelumnya, Security Hub CSPM juga mereplikasi pembaruan data ini antara Wilayah tertaut dan Wilayah asal. Pembaruan yang terjadi di Wilayah terkait direplikasi ke Wilayah asal. Pembaruan yang terjadi di Wilayah asal direplikasi kembali ke Wilayah yang ditautkan. Jika ada pembaruan yang bertentangan di Wilayah asal dan Wilayah yang ditautkan, maka pembaruan terbaru digunakan.



Agregasi Lintas Wilayah tidak menambah biaya CSPM Security Hub. Anda tidak dikenakan biaya saat Security Hub CSPM mereplikasi data atau pembaruan baru.

Di Wilayah beranda, halaman Ringkasan memberikan tampilan temuan aktif Anda di seluruh Wilayah yang ditautkan. Untuk informasi, lihat [Melihat ringkasan temuan lintas wilayah berdasarkan tingkat keparahan](#). Panel halaman Ringkasan lainnya yang menganalisis temuan juga menampilkan informasi dari seluruh Wilayah yang ditautkan.

Skor keamanan Anda di Wilayah asal dihitung dengan membandingkan jumlah kontrol yang diteruskan dengan jumlah kontrol yang diaktifkan di semua Wilayah yang ditautkan. Selain itu, jika kontrol diaktifkan di setidaknya satu Wilayah yang ditautkan, kontrol akan terlihat di halaman detail standar Keamanan di Wilayah asal. Status kepatuhan kontrol pada halaman detail standar mencerminkan temuan di seluruh Wilayah terkait. Jika pemeriksaan keamanan yang terkait dengan kontrol gagal di satu atau beberapa Wilayah yang ditautkan, status kepatuhan kontrol tersebut ditampilkan sebagai Gagal pada halaman detail standar Wilayah asal. Jumlah pemeriksaan keamanan mencakup temuan dari semua Wilayah terkait.

Security Hub CSPM hanya mengumpulkan data dari Wilayah di mana akun memiliki CSPM Security Hub diaktifkan. Security Hub CSPM tidak diaktifkan secara otomatis untuk akun berdasarkan konfigurasi agregasi lintas wilayah.

Agregasi lintas wilayah dapat diaktifkan tanpa Wilayah yang ditautkan dipilih. Dalam hal ini, tidak ada replikasi data yang terjadi.

Agregasi untuk akun administrator dan anggota

Akun mandiri, akun anggota, dan akun administrator dapat mengonfigurasi agregasi lintas wilayah. Jika dikonfigurasi oleh administrator, keberadaan akun administrator sangat penting agar agregasi lintas wilayah berfungsi di akun yang dikelola. Jika akun administrator dihapus atau dipisahkan dari akun anggota, agregasi lintas wilayah untuk akun anggota akan berhenti. Hal ini berlaku bahkan jika akun telah mengaktifkan agregasi lintas wilayah sebelum hubungan administrator-anggota dimulai.

Saat akun administrator mengaktifkan agregasi Lintas wilayah, CSPM Security Hub mereplikasi data yang dihasilkan akun administrator di semua Wilayah tertaut ke Wilayah beranda. Selain itu, Security Hub CSPM mengidentifikasi akun anggota yang terkait dengan administrator tersebut, dan setiap akun anggota mewarisi pengaturan agregasi lintas wilayah administrator. Security Hub CSPM mereplikasi data yang dihasilkan akun anggota di semua Wilayah tertaut ke Wilayah asal.

Administrator dapat mengakses dan mengelola temuan keamanan dari semua akun anggota dalam wilayah yang dikelola. Namun, sebagai administrator CSPM Security Hub, Anda harus masuk ke Wilayah beranda untuk melihat data gabungan dari semua akun anggota dan Wilayah yang ditautkan.

Sebagai akun anggota CSPM Security Hub, Anda harus masuk ke Wilayah beranda untuk melihat data agregat dari akun Anda dari semua Wilayah yang ditautkan. Akun anggota tidak memiliki izin untuk melihat data dari akun anggota lainnya.

Akun administrator dapat mengundang akun anggota secara manual atau berfungsi sebagai administrator yang didelegasikan dari organisasi yang terintegrasi dengannya AWS Organizations. Untuk [akun anggota yang diundang secara manual](#), administrator harus mengundang akun dari Wilayah asal dan semua Wilayah yang ditautkan agar agregasi lintas wilayah berfungsi. Selain itu, akun anggota harus mengaktifkan CSPM Security Hub di Wilayah asal dan semua Wilayah yang ditautkan untuk memberikan administrator kemampuan untuk melihat temuan dari akun anggota. Jika Anda tidak menggunakan Wilayah asal untuk tujuan lain, Anda dapat menonaktifkan standar dan integrasi CSPM Security Hub di Wilayah tersebut untuk mencegah biaya.

Jika Anda berencana untuk menggunakan agregasi lintas wilayah, dan memiliki beberapa akun administrator, sebaiknya ikuti praktik terbaik berikut ini:

- Setiap akun administrator memiliki akun anggota yang berbeda.
- Setiap akun administrator memiliki akun anggota yang sama di seluruh Wilayah.
- Setiap akun administrator menggunakan Wilayah rumah yang berbeda.

 Note

Untuk memahami bagaimana agregasi lintas wilayah memengaruhi konfigurasi pusat, lihat. [Dampak konfigurasi pusat pada agregasi lintas wilayah](#)

Dampak konfigurasi pusat pada agregasi lintas wilayah

Konfigurasi pusat adalah fitur opt-in di AWS Security Hub Cloud Security Posture Management (CSPM) yang dapat Anda gunakan jika Anda berintegrasi dengannya. AWS Organizations Jika Anda menggunakan konfigurasi pusat, akun administrator yang didelegasikan dapat mengonfigurasi layanan, standar, dan kontrol CSPM Security Hub untuk akun dan unit organisasi (OU) dalam organisasi. Untuk mengonfigurasi akun dan OUs, administrator yang didelegasikan membuat kebijakan konfigurasi CSPM Security Hub. Kebijakan konfigurasi dapat digunakan untuk menentukan apakah CSPM Security Hub diaktifkan atau dinonaktifkan, dan standar dan kontrol mana yang diaktifkan. Administrator yang didelegasikan mengaitkan kebijakan konfigurasi dengan akun tertentu OUs, atau root (seluruh organisasi).

Administrator yang didelegasikan dapat membuat dan mengelola kebijakan konfigurasi untuk organisasi hanya dari Wilayah asal. Selain itu, kebijakan konfigurasi berlaku di Wilayah asal dan semua Wilayah yang ditautkan. Anda tidak dapat membuat kebijakan konfigurasi yang hanya berlaku di beberapa Wilayah tertaut dan bukan yang lain. Untuk informasi tentang agregasi lintas wilayah, lihat Agregasi [Lintas](#) Wilayah.

Untuk menggunakan konfigurasi pusat, Anda harus menunjuk Wilayah rumah. Secara opsional, Anda dapat memilih satu atau beberapa Wilayah sebagai Wilayah yang ditautkan. Anda juga dapat memilih untuk menunjuk Wilayah asal tanpa Wilayah terkait.

Mengubah setelan agregasi lintas wilayah dapat memengaruhi kebijakan konfigurasi Anda. Saat Anda menambahkan Wilayah tertaut, kebijakan konfigurasi Anda akan berlaku di Wilayah tersebut. Jika Region adalah [Region opt-in](#), Region harus diaktifkan agar kebijakan konfigurasi Anda berlaku di sana. Sebaliknya, saat Anda menghapus Wilayah tertaut, kebijakan konfigurasi tidak lagi berlaku di Wilayah tersebut. Di Wilayah itu, akun mempertahankan pengaturan yang mereka miliki saat Wilayah yang ditautkan dihapus. Anda dapat mengubah pengaturan tersebut, tetapi harus melakukannya secara terpisah di setiap akun dan Wilayah.

Jika Anda menghapus atau mengubah Wilayah beranda, kebijakan konfigurasi dan asosiasi kebijakan Anda akan dihapus. Anda tidak dapat lagi menggunakan konfigurasi pusat atau membuat

kebijakan konfigurasi di Wilayah mana pun. Akun mempertahankan pengaturan yang mereka miliki sebelum Wilayah asal diubah atau dihapus. Anda dapat mengubah pengaturan tersebut kapan saja, tetapi karena Anda tidak lagi menggunakan konfigurasi pusat, pengaturan harus dimodifikasi secara terpisah di setiap akun dan Wilayah. Anda dapat menggunakan konfigurasi pusat dan membuat kebijakan konfigurasi lagi jika Anda menunjuk Wilayah rumah baru.

Untuk informasi selengkapnya tentang konfigurasi pusat, lihat [Memahami konfigurasi pusat di Security Hub CSPM](#).

Mengaktifkan agregasi lintas wilayah

Note

Wilayah agregasi sekarang disebut Wilayah asal. Beberapa operasi Security Hub CSPM API masih menggunakan istilah agregasi Region yang lebih lama.

Anda harus mengaktifkan agregasi lintas wilayah dari Wilayah AWS yang ingin Anda tetapkan sebagai Wilayah asal.

Untuk mengaktifkan agregasi lintas wilayah, Anda membuat sumber daya CSPM Security Hub yang disebut agregator pencarian. Sumber daya agregator temuan menentukan Wilayah asal Anda dan Wilayah yang ditautkan (jika ada).

Anda tidak dapat menggunakan Wilayah AWS yang dinonaktifkan secara default sebagai Wilayah rumah Anda. Untuk daftar Wilayah yang dinonaktifkan secara default, lihat [Mengaktifkan Wilayah](#) di Referensi Umum AWS

Bila Anda mengaktifkan agregasi lintas wilayah, Anda memilih untuk menentukan satu atau beberapa Wilayah tertaut jika diinginkan. Anda juga dapat memilih apakah akan secara otomatis menautkan Wilayah baru saat Security Hub CSPM mulai mendukungnya dan Anda telah memilihnya.

Security Hub CSPM console

Untuk mengaktifkan agregasi lintas wilayah

1. Buka konsol AWS Security Hub Cloud Security Posture Management (CSPM) di <https://console.aws.amazon.com/securityhub/>

2. Menggunakan Wilayah AWS pilihan, masuk ke Wilayah yang ingin Anda gunakan sebagai Wilayah agregasi.
3. Di menu navigasi CSPM Security Hub, pilih Settings dan kemudian Regions.
4. Untuk Menemukan agregasi, pilih Konfigurasi agregasi pencarian.

Secara default, Region home diatur ke No agregasi Region.

5. Di bawah Wilayah Agregasi, pilih opsi untuk menetapkan Wilayah saat ini sebagai Wilayah asal.
6. Secara opsional, untuk Wilayah Tertaut, pilih Wilayah untuk mengumpulkan data.
7. Untuk secara otomatis menggabungkan data dari Wilayah baru di partisi sebagai Security Hub CSPM mendukungnya dan Anda memilihnya, pilih Tautkan Wilayah masa depan.
8. Pilih Simpan.

Security Hub CSPM API

Dari Region yang ingin Anda gunakan sebagai Wilayah asal, gunakan [CreateFindingAggregator](#) pengoperasian Security Hub CSPM API. Jika Anda menggunakan AWS CLI, jalankan [create-finding-aggregator](#) perintah.

Untuk `RegionLinkingMode`, pilih salah satu opsi berikut:

- `ALL_REGIONS`— Security Hub CSPM mengumpulkan data dari semua Wilayah. Security Hub CSPM juga mengumpulkan data dari Wilayah baru karena didukung dan Anda memilihnya.
- `ALL_REGIONS_EXCEPT_SPECIFIED`— Security Hub CSPM mengumpulkan data dari semua Wilayah kecuali untuk Wilayah yang ingin Anda kecualikan. Security Hub CSPM juga mengumpulkan data dari Wilayah baru karena didukung dan Anda memilihnya. Gunakan `Regions` untuk menyediakan daftar Wilayah untuk dikecualikan dari agregasi.
- `SPECIFIED_REGIONS`— Security Hub CSPM mengumpulkan data dari daftar Wilayah yang dipilih. Security Hub CSPM tidak mengumpulkan data secara otomatis dari Wilayah baru. Gunakan `Regions` untuk menyediakan daftar Wilayah untuk dikumpulkan dari.
- `NO_REGIONS`— Security Hub CSPM tidak mengumpulkan data karena Anda tidak memilih Wilayah yang ditautkan.

Contoh berikut mengkonfigurasi agregasi lintas wilayah. Wilayah asalnya adalah US East (Virginia N.). Wilayah yang terhubung adalah US West (California N.) dan US West (Oregon). Contoh ini

diformat untuk Linux, macOS, atau Unix, dan menggunakan karakter garis miring terbalik (\) untuk meningkatkan keterbacaan.

```
$ aws securityhub create-finding-aggregator --region us-east-1 --region-linking-mode SPECIFIED_REGIONS --regions us-west-1 us-west-2
```

Meninjau pengaturan agregasi lintas wilayah

Note

Wilayah agregasi sekarang disebut Wilayah asal. Beberapa operasi Security Hub CSPM API masih menggunakan istilah agregasi Region yang lebih lama.

Anda dapat melihat konfigurasi agregasi Lintas wilayah saat ini di AWS Security Hub Cloud Security Posture Management (CSPM) dari manapun. Wilayah AWS Konfigurasi mencakup Wilayah asal, Wilayah yang ditautkan (jika ada), dan apakah akan secara otomatis menautkan Wilayah baru sebagai Security Hub CSPM mendukungnya.

Akun anggota dapat melihat setelan agregasi lintas wilayah yang dikonfigurasi oleh akun administrator.

Pilih metode pilihan Anda, dan ikuti langkah-langkah untuk melihat pengaturan agregasi lintas wilayah Anda saat ini.

Security Hub CSPM console

Untuk melihat setelan agregasi lintas wilayah (konsol)

1. Buka konsol AWS Security Hub Cloud Security Posture Management (CSPM) di <https://console.aws.amazon.com/securityhub/>
2. Pada panel navigasi, pilih Pengaturan dan kemudian tab Wilayah.

Jika agregasi lintas wilayah tidak diaktifkan, maka tab Wilayah menampilkan opsi untuk mengaktifkan agregasi lintas wilayah. Hanya akun administrator dan akun mandiri yang dapat mengaktifkan agregasi lintas wilayah.

Jika agregasi lintas wilayah diaktifkan, maka tab Wilayah menampilkan informasi berikut:

- Wilayah asal
- Apakah akan secara otomatis menggabungkan temuan, wawasan, status kontrol, dan skor keamanan dari Wilayah baru yang didukung CSPM Security Hub dan yang Anda pilih
- Daftar Wilayah tertaut (jika ada yang dipilih)

Security Hub CSPM API

Untuk meninjau setelan agregasi lintas wilayah (Security Hub CSPM API)

Gunakan [GetFindingAggregator](#) pengoperasian Security Hub CSPM API. Jika Anda menggunakan AWS CLI, jalankan [get-finding-aggregator](#) perintah.

Saat Anda membuat permintaan, berikan ARN agregator temuan. Untuk mendapatkan ARN agregator temuan, gunakan operasi [list-finding-aggregators](#) atau [ListFindingAggregators](#) perintah.

Contoh berikut menunjukkan pengaturan agregasi lintas wilayah untuk ARN agregator temuan yang ditentukan. Contoh ini diformat untuk Linux, macOS, atau Unix, dan menggunakan karakter garis miring terbalik (\) untuk meningkatkan keterbacaan

```
$aws securityhub get-finding-aggregator --finding-aggregator-  
arn arn:aws:securityhub:us-east-1:222222222222:finding-aggregator/123e4567-  
e89b-12d3-a456-426652340000
```

Memperbarui pengaturan agregasi lintas wilayah

Note

Wilayah agregasi sekarang disebut Wilayah asal. Beberapa operasi Security Hub CSPM API masih menggunakan istilah agregasi Region yang lebih lama.

Anda dapat memperbarui setelan agregasi Lintas wilayah saat ini di AWS Security Hub Cloud Security Posture Management (CSPM) dengan mengubah Wilayah tertaut atau Wilayah beranda saat ini. Anda juga dapat mengubah apakah akan secara otomatis mengumpulkan data dari Wilayah AWS yang baru yang didukung CSPM Security Hub.

Perubahan pada agregasi Lintas wilayah tidak diterapkan untuk Wilayah keikutsertaan hingga Anda mengaktifkan Wilayah di wilayah Anda. Akun AWS Wilayah yang AWS diperkenalkan pada atau setelah hingga 20 Maret 2019 adalah Wilayah yang ikut serta.

Saat Anda berhenti menggabungkan data dari Wilayah tertaut, AWS Security Hub Cloud Security Posture Management (CSPM) tidak menghapus data agregat yang ada dari Wilayah tersebut yang dapat diakses di Wilayah asal.

Anda tidak dapat menggunakan prosedur pembaruan di bagian ini untuk mengubah Wilayah beranda. Untuk mengubah wilayah rumah, Anda harus melakukan hal berikut:

1. Hentikan agregasi lintas wilayah. Untuk petunjuk, lihat [the section called “Menghentikan agregasi”](#).
2. Ubah ke Wilayah yang Anda inginkan menjadi Wilayah asal baru.
3. Aktifkan agregasi lintas wilayah. Untuk petunjuk, lihat [the section called “Mengaktifkan agregasi”](#).

Anda harus memperbarui konfigurasi agregasi lintas wilayah dari Wilayah rumah saat ini.

Security Hub CSPM console

Untuk mengubah Wilayah yang ditautkan

1. Buka konsol AWS Security Hub Cloud Security Posture Management (CSPM) di <https://console.aws.amazon.com/securityhub/>

Masuk ke Wilayah agregasi saat ini.

2. Di menu navigasi CSPM Security Hub, pilih Pengaturan, lalu pilih Wilayah.
3. Untuk Menemukan agregasi, pilih Edit.
4. Untuk Wilayah Tertaut, perbarui Wilayah tertaut yang dipilih.
5. Jika perlu, ubah apakah Link future Regions dipilih. Pengaturan ini menentukan apakah Security Hub CSPM secara otomatis menautkan Wilayah baru karena menambahkan dukungan untuk mereka dan Anda memilihnya.
6. Pilih Simpan.

Security Hub CSPM API

Gunakan [UpdateFindingAggregator](#) operasi. Jika Anda menggunakan AWS CLI, jalankan [update-finding-aggregator](#) perintah. Untuk mengidentifikasi aggregator temuan, Anda harus

memberikan agregator temuan ARN. Untuk mendapatkan ARN agregator temuan, gunakan operasi atau [ListFindingAggregators](#) perintah.. [list-finding-aggregators](#)

Jika mode penautan adalah ALL_REGIONS_EXCEPT_SPECIFIED atau SPECIFIED_REGIONS, Anda dapat mengubah daftar Wilayah yang dikecualikan atau disertakan. Jika Anda ingin mengubah mode penautan Wilayah ke NO_REGIONS, Anda tidak boleh memberikan daftar Wilayah.

Ketika Anda mengubah daftar Wilayah yang dikecualikan atau disertakan, Anda harus memberikan daftar lengkap dengan pembaruan. Misalnya, Anda saat ini mengumpulkan temuan dari US East (Ohio), dan ingin juga mengumpulkan temuan dari US West (Oregon). Anda harus memberikan Regions daftar yang berisi US East (Ohio) dan US West (Oregon).

Contoh berikut memperbarui agregasi lintas wilayah ke Wilayah yang dipilih. Perintah dijalankan dari Wilayah asal saat ini, yaitu US East (Virginia N.). Wilayah yang terhubung adalah US West (California N.) dan US West (Oregon). Contoh ini diformat untuk Linux, macOS, atau Unix, dan menggunakan karakter garis miring terbalik (\) untuk meningkatkan keterbacaan.

```
aws securityhub update-finding-aggregator --region us-east-1 --finding-  
aggregator-arn arn:aws:securityhub:us-east-1:222222222222:finding-  
aggregator/123e4567-e89b-12d3-a456-426652340000 --region-linking-mode  
SPECIFIED_REGIONS --regions us-west-1 us-west-2
```

Menghentikan agregasi lintas wilayah

Note

Wilayah agregasi sekarang disebut Wilayah asal. Beberapa operasi Security Hub CSPM API masih menggunakan istilah agregasi Region yang lebih lama.

Jika Anda tidak ingin AWS Security Hub Cloud Security Posture Management (CSPM) mengumpulkan data, Anda dapat menghapus agregator temuan Anda. Atau, Anda dapat menyimpan agregator temuan Anda tetapi tidak menautkan apa pun Wilayah AWS ke Wilayah rumah dengan memperbarui agregator yang ada ke mode NO_REGIONS penautan.

Untuk mengubah Wilayah rumah Anda, Anda harus menghapus agregator temuan Anda saat ini dan membuat yang baru.

Ketika Anda menghapus agregator temuan Anda, Security Hub CSPM berhenti menggabungkan data. Itu tidak menghapus data agregat yang ada dari Wilayah asal.

Menghapus agregator temuan (konsol)

Anda dapat menghapus agregator temuan Anda dari Wilayah beranda saat ini saja.

Di Wilayah selain Wilayah rumah, panel agregasi Menemukan di konsol CSPM Security Hub menampilkan pesan bahwa Anda harus mengedit konfigurasi di Wilayah beranda. Pilih pesan ini untuk menampilkan tautan untuk beralih ke Wilayah beranda.

Security Hub CSPM console

Untuk menghentikan agregasi lintas wilayah (konsol)

1. Buka konsol AWS Security Hub Cloud Security Posture Management (CSPM) di <https://console.aws.amazon.com/securityhub/>
2. Pastikan Anda masuk ke Wilayah asal Anda saat ini.
3. Di menu navigasi CSPM Security Hub, pilih Pengaturan, lalu pilih Wilayah.
4. Di bawah Menemukan agregasi, pilih Edit.
5. Di bawah Wilayah Agregasi, pilih Tidak ada Wilayah agregasi.
6. Pilih Simpan.
7. Pada dialog konfirmasi, di bidang konfirmasi, ketik **Confirm**.
8. Pilih Konfirmasi.

Security Hub CSPM API

Gunakan [DeleteFindingAggregator](#) pengoperasian Security Hub CSPM API. Jika Anda menggunakan AWS CLI, jalankan [delete-finding-aggregator](#) perintah.

Untuk mengidentifikasi agregator temuan yang akan dihapus, berikan ARN agregator temuan. Untuk mendapatkan ARN agregator temuan, gunakan operasi [list-finding-aggregators](#) atau [ListFindingAggregators](#) perintah.

Contoh berikut menghapus agregator temuan. Perintah dijalankan dari Wilayah asal saat ini, yaitu US East (Virginia N.). Contoh ini diformat untuk Linux, macOS, atau Unix, dan menggunakan karakter garis miring terbalik (\) untuk meningkatkan keterbacaan.

```
$aws securityhub delete-finding-aggregator arn:aws:securityhub:us-east-1:222222222222:finding-aggregator/123e4567-e89b-12d3-a456-426652340000 --  
region us-east-1
```

Memahami standar keamanan di Security Hub CSPM

Dalam AWS Security Hub Cloud Security Posture Management (CSPM), standar keamanan adalah seperangkat persyaratan yang didasarkan pada kerangka kerja peraturan, praktik terbaik industri, atau kebijakan perusahaan. Untuk detail tentang standar yang didukung Security Hub CSPM saat ini, termasuk kontrol keamanan yang berlaku untuk masing-masing standar, lihat [Referensi standar untuk Security Hub CSPM](#)

Ketika Anda mengaktifkan standar, Security Hub CSPM secara otomatis mengaktifkan semua kontrol yang berlaku untuk standar. Security Hub CSPM kemudian menjalankan pemeriksaan keamanan pada kontrol, yang menghasilkan temuan CSPM Security Hub. Anda dapat menonaktifkan dan kemudian mengaktifkan kembali kontrol individual seperlunya. Anda juga dapat menonaktifkan standar sepenuhnya. Jika Anda menonaktifkan standar, Security Hub CSPM berhenti menjalankan pemeriksaan keamanan pada kontrol yang berlaku untuk standar. Temuan tidak lagi dihasilkan untuk kontrol.

Selain temuan, Security Hub CSPM menghasilkan skor keamanan untuk setiap standar yang Anda aktifkan. Skor didasarkan pada status kontrol yang berlaku untuk standar. Jika Anda menetapkan Wilayah agregasi, skor keamanan untuk standar mencerminkan status kontrol di semua Wilayah tertaut. Jika Anda administrator CSPM Security Hub untuk suatu organisasi, skor tersebut mencerminkan status kontrol untuk semua akun di organisasi Anda. Untuk informasi selengkapnya, lihat [Menghitung skor keamanan](#).

Untuk meninjau dan mengelola standar, Anda dapat menggunakan konsol CSPM Security Hub atau Security Hub CSPM API. Di konsol, halaman standar Keamanan menunjukkan semua standar keamanan yang didukung CSPM Security Hub saat ini. Ini termasuk deskripsi masing-masing standar dan status standar saat ini. Jika Anda mengaktifkan standar, Anda juga dapat menggunakan halaman ini untuk mengakses detail tambahan untuk standar. Misalnya, Anda dapat meninjau:

- Skor keamanan saat ini untuk standar.
- Statistik agregat untuk kontrol yang berlaku untuk standar.
- Daftar kontrol yang berlaku untuk standar dan saat ini diaktifkan, termasuk status kepatuhan masing-masing.
- Daftar kontrol yang berlaku untuk standar tetapi saat ini dinonaktifkan.

Untuk analisis yang lebih dalam, Anda dapat memfilter dan mengurutkan data, dan menelusuri untuk meninjau detail kontrol individual yang berlaku untuk standar.

Anda dapat mengaktifkan standar secara individual untuk satu akun dan Wilayah AWS. Namun, untuk menghemat waktu dan mengurangi penyimpangan konfigurasi di lingkungan multi-akun dan Multi-wilayah, sebaiknya gunakan [konfigurasi pusat](#) untuk mengaktifkan dan mengelola standar. Dengan konfigurasi pusat, administrator CSPM Security Hub yang didelegasikan dapat membuat kebijakan yang menentukan cara mengonfigurasi standar di beberapa akun dan Wilayah.

Topik

- [Referensi standar untuk Security Hub CSPM](#)
- [Mengaktifkan standar keamanan](#)
- [Meninjau detail standar keamanan](#)
- [Mematikan standar keamanan yang diaktifkan secara otomatis](#)
- [Menonaktifkan standar keamanan](#)

Referensi standar untuk Security Hub CSPM

Dalam AWS Security Hub Cloud Security Posture Management (CSPM), standar keamanan adalah seperangkat persyaratan yang didasarkan pada kerangka kerja peraturan, praktik terbaik industri, atau kebijakan perusahaan. Security Hub CSPM memetakan persyaratan ini ke kontrol, dan menjalankan pemeriksaan keamanan pada kontrol untuk menilai apakah persyaratan standar terpenuhi. Setiap standar mencakup beberapa kontrol.

Security Hub CSPM saat ini mendukung standar berikut:

- **AWS Praktik Terbaik Keamanan Dasar** - Dikembangkan oleh AWS dan profesional industri, standar ini adalah kompilasi praktik terbaik keamanan untuk organisasi, terlepas dari sektor atau ukurannya. Ini menyediakan serangkaian kontrol yang mendeteksi kapan Anda Akun AWS dan sumber daya menyimpang dari praktik terbaik keamanan. Ini juga memberikan panduan preskriptif tentang cara meningkatkan dan mempertahankan postur keamanan Anda.
- **AWS Resource Tagging** — Dikembangkan oleh Security Hub CSPM, standar ini dapat membantu Anda menentukan apakah AWS sumber daya Anda memiliki tag. Tag adalah pasangan kunci-nilai yang bertindak sebagai metadata untuk sumber daya. AWS Tag dapat membantu Anda mengidentifikasi, mengkategorikan, mengelola, dan mencari AWS sumber daya. Misalnya, Anda dapat menggunakan tag untuk mengkategorikan sumber daya berdasarkan tujuan, pemilik, atau lingkungan.
- **CIS AWS Foundations Benchmark** — Dikembangkan oleh Center for Internet Security (CIS), standar ini menyediakan pedoman konfigurasi yang aman untuk AWS. Ini menentukan

seperangkat pedoman konfigurasi keamanan dan praktik terbaik untuk subset Layanan AWS dan sumber daya, dengan penekanan pada pengaturan agnostik dasar, dapat diuji, dan arsitektur. Pedoman tersebut mencakup prosedur yang jelas, step-by-step implementasi dan penilaian.

- NIST SP 800-53 Revisi 5 — Standar ini sejalan dengan persyaratan National Institute of Standards and Technology (NIST) untuk melindungi kerahasiaan, integritas, dan ketersediaan sistem informasi dan sumber daya penting. Kerangka kerja terkait umumnya berlaku untuk lembaga atau organisasi federal AS yang bekerja dengan lembaga federal AS atau sistem informasi. Namun, organisasi swasta juga dapat menggunakan persyaratan sebagai kerangka panduan.
- NIST SP 800-171 Revisi 2 — Standar ini sejalan dengan rekomendasi keamanan NIST dan persyaratan untuk melindungi kerahasiaan Controlled Unclassified Information (CUI) dalam sistem dan organisasi yang bukan bagian dari pemerintah federal AS. CUI adalah informasi yang tidak memenuhi kriteria pemerintah untuk klasifikasi, tetapi dianggap sensitif dan dibuat atau dimiliki oleh pemerintah federal AS atau entitas lain atas nama pemerintah federal AS.
- PCI DSS — Standar ini sejalan dengan kerangka kepatuhan Standar Keamanan Data Industri Kartu Pembayaran (PCI DSS) yang ditentukan oleh Dewan Standar Keamanan PCI (SSC). Kerangka kerja ini menyediakan seperangkat aturan dan pedoman untuk menangani informasi kartu kredit dan debit dengan aman. Kerangka kerja ini umumnya berlaku untuk organisasi yang menyimpan, memproses, atau mengirimkan data pemegang kartu.
- Standar yang dikelola layanan, AWS Control Tower— Standar ini membantu Anda mengonfigurasi kontrol proaktif yang disediakan AWS Control Tower bersama dengan kontrol detektif yang disediakan oleh Security Hub CSPM. AWS Control Tower menawarkan cara mudah untuk mengatur dan mengatur lingkungan AWS multi-akun, mengikuti praktik terbaik preskriptif. Dengan mengaktifkan kontrol proaktif dan detektif untuk AWS lingkungan Anda, Anda dapat meningkatkan postur keamanan Anda pada tahap pengembangan yang berbeda.

Standar dan kontrol CSPM Security Hub tidak menjamin kepatuhan terhadap kerangka kerja peraturan atau audit apa pun. Sebaliknya, mereka menyediakan cara untuk mengevaluasi dan memantau keadaan Anda Akun AWS dan sumber daya. Sebaiknya aktifkan setiap standar yang relevan dengan kebutuhan bisnis, industri, atau kasus penggunaan Anda.

Kontrol individu dapat berlaku untuk lebih dari satu standar. Jika Anda mengaktifkan beberapa standar, kami sarankan Anda juga mengaktifkan temuan kontrol terkonsolidasi. Jika Anda melakukan ini, Security Hub CSPM menghasilkan satu temuan untuk setiap kontrol, bahkan jika kontrol berlaku untuk lebih dari satu standar. Jika Anda tidak mengaktifkan temuan kontrol konsolidasi, Security Hub CSPM menghasilkan temuan terpisah untuk setiap standar yang diaktifkan yang diterapkan oleh kontrol. Misalnya, jika Anda mengaktifkan dua standar dan kontrol berlaku untuk keduanya, Anda

menerima dua temuan terpisah untuk kontrol, satu untuk setiap standar. Jika Anda mengaktifkan temuan kontrol terkonsolidasi, Anda hanya menerima satu temuan untuk kontrol. Untuk informasi selengkapnya, lihat [Temuan kontrol terkonsolidasi](#).

Referensi terperinci dengan standar

- [AWS Standar Praktik Terbaik Keamanan Dasar di Security Hub CSPM](#)
- [AWS Standar Penandaan Sumber Daya di Security Hub CSPM](#)
- [Tolok Ukur AWS Yayasan CIS di Security Hub CSPM](#)
- [NIST SP 800-53 Revisi 5 di Security Hub CSPM](#)
- [NIST SP 800-171 Revisi 2 di Security Hub CSPM](#)
- [PCI DSS di Security Hub CSPM](#)
- [Standar yang dikelola layanan di Security Hub CSPM](#)

AWS Standar Praktik Terbaik Keamanan Dasar di Security Hub CSPM

Dikembangkan oleh AWS dan profesional industri, standar AWS Foundational Security Best Practices (FSBP) adalah kompilasi praktik terbaik keamanan untuk organisasi, terlepas dari sektor atau ukuran organisasi. Ini menyediakan seperangkat kontrol yang mendeteksi kapan Akun AWS dan sumber daya menyimpang dari praktik terbaik keamanan. Ini juga memberikan panduan preskriptif tentang bagaimana meningkatkan dan mempertahankan postur keamanan organisasi Anda.

Dalam AWS Security Hub Cloud Security Posture Management (CSPM), standar Praktik Terbaik Keamanan AWS Dasar mencakup kontrol yang terus mengevaluasi beban kerja Akun AWS dan Anda, dan membantu Anda mengidentifikasi area yang menyimpang dari praktik terbaik keamanan. Kontrol mencakup praktik terbaik keamanan untuk sumber daya dari beberapa sumber daya Layanan AWS. Setiap kontrol diberi kategori yang mencerminkan fungsi keamanan yang diterapkan kontrol. Untuk daftar kategori dan detail tambahan, lihat [Kategori kontrol](#).

Kontrol yang berlaku untuk standar

Daftar berikut menentukan kontrol AWS Security Hub Cloud Security Posture Management (CSPM) mana yang berlaku untuk standar Praktik Terbaik Keamanan AWS Dasar (v1.0.0). Untuk meninjau detail kontrol, pilih kontrol.

[\[Akun.1\] Informasi kontak keamanan harus disediakan untuk Akun AWS](#)

[\[ACM.1\] Sertifikat yang diimpor dan diterbitkan ACM harus diperbarui setelah jangka waktu tertentu](#)

[\[ACM.2\] Sertifikat RSA yang dikelola oleh ACM harus menggunakan panjang kunci minimal 2.048 bit](#)

[\[APIGateway.1\] API Gateway REST dan pencatatan eksekusi WebSocket API harus diaktifkan](#)

[\[APIGateway.2\] Tahapan API Gateway REST API harus dikonfigurasi untuk menggunakan sertifikat SSL untuk otentikasi backend](#)

[\[APIGateway.3\] Tahapan API Gateway REST API harus mengaktifkan AWS X-Ray penelusuran](#)

[\[APIGateway.4\] API Gateway harus dikaitkan dengan ACL Web WAF](#)

[\[APIGateway.5\] Data cache API Gateway REST API harus dienkrpsi saat istirahat](#)

[\[APIGateway.8\] Rute API Gateway harus menentukan jenis otorisasi](#)

[\[APIGateway.9\] Pencatatan akses harus dikonfigurasi untuk Tahap API Gateway V2](#)

[\[AppSync.1\] Cache AWS AppSync API harus dienkrpsi saat istirahat](#)

[\[AppSync.2\] AWS AppSync harus mengaktifkan logging tingkat lapangan](#)

[\[AppSync.5\] AWS AppSync APIs GraphQL tidak boleh diautentikasi dengan kunci API](#)

[\[AppSync.6\] Cache AWS AppSync API harus dienkrpsi saat transit](#)

[\[Athena.4\] Kelompok kerja Athena seharusnya mengaktifkan logging](#)

[\[AutoScaling.1\] Grup Auto Scaling yang terkait dengan penyeimbang beban harus menggunakan pemeriksaan kesehatan ELB](#)

[\[AutoScaling.2\] Grup EC2 Auto Scaling Amazon harus mencakup beberapa Availability Zone](#)

[\[AutoScaling.3\] Konfigurasi peluncuran grup Auto Scaling harus EC2 mengonfigurasi instance agar memerlukan Layanan Metadata Instance Versi 2 \(\) IMDSv2](#)

[\[Autoscaling.5\] Instans EC2 Amazon yang diluncurkan menggunakan konfigurasi peluncuran grup Auto Scaling seharusnya tidak memiliki alamat IP Publik](#)

[\[AutoScaling.6\] Grup Auto Scaling harus menggunakan beberapa jenis instance di beberapa Availability Zone](#)

[\[AutoScaling.9\] Grup EC2 Auto Scaling Amazon harus menggunakan templat peluncuran Amazon EC2](#)

[\[Backup.1\] titik AWS Backup pemulihan harus dienkrpsi saat istirahat](#)

[\[CloudFront.1\] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi](#)

[\[CloudFront.3\] CloudFront distribusi harus memerlukan enkripsi dalam perjalanan](#)

[\[CloudFront.4\] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi](#)

[\[CloudFront.5\] CloudFront distribusi seharusnya mengaktifkan logging](#)

[\[CloudFront.6\] CloudFront distribusi harus mengaktifkan WAF](#)

[\[CloudFront.7\] CloudFront distribusi harus menggunakan sertifikat SSL/TLS khusus](#)

[\[CloudFront.8\] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS](#)

[\[CloudFront.9\] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus](#)

[\[CloudFront.10\] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal kustom](#)

[\[CloudFront.12\] CloudFront distribusi seharusnya tidak menunjukkan asal S3 yang tidak ada](#)

[\[CloudFront.13\] CloudFront distribusi harus menggunakan kontrol akses asal](#)

[\[CloudTrail.1\] CloudTrail harus diaktifkan dan dikonfigurasi dengan setidaknya satu jejak Multi-wilayah yang mencakup acara manajemen baca dan tulis](#)

[\[CloudTrail.2\] CloudTrail harus mengaktifkan enkripsi saat istirahat](#)

[\[CloudTrail.4\] validasi file CloudTrail log harus diaktifkan](#)

[\[CloudTrail.5\] CloudTrail jalur harus diintegrasikan dengan Amazon Logs CloudWatch](#)

[\[CodeBuild.1\] Repositori sumber CodeBuild Bitbucket tidak URLs boleh berisi kredensial sensitif](#)

[\[CodeBuild.2\] variabel lingkungan CodeBuild proyek tidak boleh berisi kredensial teks yang jelas](#)

[\[CodeBuild.3\] Log CodeBuild S3 harus dienkrpsi](#)

[\[CodeBuild.4\] lingkungan CodeBuild proyek harus memiliki urasi logging AWS Config](#)

[\[CodeBuild.7\] ekspor kelompok CodeBuild laporan harus dienkrpsi saat istirahat](#)

[\[Config.1\] AWS Config harus diaktifkan dan menggunakan peran terkait layanan untuk perekaman sumber daya](#)

[\[Connect.2\] Instans Amazon Connect seharusnya mengaktifkan logging CloudWatch](#)

[\[DataFirehose.1\] Aliran pengiriman Firehose harus dienkripsi saat istirahat](#)

[\[DataSync.1\] DataSync tugas harus mengaktifkan logging](#)

[\[DMS.1\] Instans replikasi Layanan Migrasi Database tidak boleh bersifat publik](#)

[\[DMS.6\] Instans replikasi DMS harus mengaktifkan peningkatan versi minor otomatis](#)

[\[DMS.7\] Tugas replikasi DMS untuk database target seharusnya mengaktifkan logging](#)

[\[DMS.8\] Tugas replikasi DMS untuk database sumber seharusnya mengaktifkan logging](#)

[\[DMS.9\] Titik akhir DMS harus menggunakan SSL](#)

[\[DMS.10\] Titik akhir DMS untuk database Neptune harus mengaktifkan otorisasi IAM](#)

[\[DMS.11\] Titik akhir DMS untuk MongoDB harus mengaktifkan mekanisme otentikasi](#)

[\[DMS.12\] Titik akhir DMS untuk Redis OSS seharusnya mengaktifkan TLS](#)

[\[DocumentDB.1\] Cluster Amazon DocumentDB harus dienkripsi saat istirahat](#)

[\[DocumentDB.2\] Cluster Amazon DocumentDB harus memiliki periode retensi cadangan yang memadai](#)

[\[DocumentDB.3\] Cuplikan cluster manual Amazon DocumentDB seharusnya tidak bersifat publik](#)

[\[DocumentDB.4\] Cluster Amazon DocumentDB harus mempublikasikan log audit ke Log CloudWatch](#)

[\[DocumentDB.5\] Cluster Amazon DocumentDB harus mengaktifkan perlindungan penghapusan](#)

[\[DocumentDB.6\] Cluster Amazon DocumentDB harus dienkripsi saat transit](#)

[\[DynamoDB.1\] Tabel DynamoDB harus secara otomatis menskalakan kapasitas sesuai permintaan](#)

[\[DynamoDB.2\] Tabel DynamoDB harus mengaktifkan pemulihan point-in-time](#)

[\[DynamoDB.3\] Cluster DynamoDB Accelerator \(DAX\) harus dienkripsi saat istirahat](#)

[\[DynamoDB.6\] Tabel DynamoDB harus mengaktifkan perlindungan penghapusan](#)

[\[DynamoDB.7\] Cluster DynamoDB Accelerator harus dienkripsi saat transit](#)

[\[EC2.1\] Cuplikan Amazon EBS tidak boleh dipulihkan secara publik](#)

[\[EC2.2\] Grup keamanan default VPC tidak boleh mengizinkan lalu lintas masuk atau keluar](#)

[\[EC2.3\] Volume Amazon EBS yang terlampir harus dienkripsi saat istirahat](#)

[\[EC2.4\] EC2 Instans yang dihentikan harus dihapus setelah periode waktu tertentu](#)

[\[EC2.6\] Pencatatan aliran VPC harus diaktifkan di semua VPCs](#)

[\[EC2.7\] Enkripsi default EBS harus diaktifkan](#)

[\[EC2.8\] EC2 instans harus menggunakan Instance Metadata Service Versi 2 \(\) IMDSv2](#)

[\[EC2.9\] EC2 Instans Amazon seharusnya tidak memiliki alamat publik IPv4](#)

[\[EC2.10\] Amazon EC2 harus dikonfigurasi untuk menggunakan titik akhir VPC yang dibuat untuk layanan Amazon EC2](#)

[\[EC2.15\] EC2 Subnet Amazon seharusnya tidak secara otomatis menetapkan alamat IP publik](#)

[\[EC2.16\] Daftar Kontrol Akses Jaringan yang Tidak Digunakan harus dihapus](#)

[\[EC2.17\] EC2 Instans Amazon seharusnya tidak menggunakan banyak ENIs](#)

[\[EC2.18\] Grup keamanan seharusnya hanya mengizinkan lalu lintas masuk yang tidak terbatas untuk port resmi](#)

[\[EC2.19\] Kelompok keamanan tidak boleh mengizinkan akses tidak terbatas ke port dengan risiko tinggi](#)

[\[EC2.20\] Kedua terowongan VPN untuk koneksi AWS Site-to-Site VPN harus siap](#)

[\[EC2.21\] Jaringan ACLs seharusnya tidak mengizinkan masuknya dari 0.0.0.0/0 ke port 22 atau port 3389.](#)

[\[EC2.23\] Amazon EC2 Transit Gateways seharusnya tidak secara otomatis menerima permintaan lampiran VPC](#)

[\[EC2.24\] Jenis instance EC2 paravirtual Amazon tidak boleh digunakan](#)

[\[EC2.25\] Templat EC2 peluncuran Amazon tidak boleh menetapkan publik IPs ke antarmuka jaringan](#)

[\[EC2.51\] Titik akhir EC2 Client VPN harus mengaktifkan pencatatan koneksi klien](#)

[\[EC2.55\] VPCs harus dikonfigurasi dengan titik akhir antarmuka untuk ECR API](#)

[\[EC2.56\] VPCs harus dikonfigurasi dengan titik akhir antarmuka untuk Docker Registry](#)

[\[EC2.57\] VPCs harus dikonfigurasi dengan titik akhir antarmuka untuk Systems Manager](#)

[\[EC2.58\] VPCs harus dikonfigurasi dengan titik akhir antarmuka untuk Kontak Manajer Insiden Systems Manager](#)

[\[EC2.60\] VPCs harus dikonfigurasi dengan titik akhir antarmuka untuk Systems Manager Incident Manager](#)

[\[EC2.170\] templat EC2 peluncuran harus menggunakan Layanan Metadata Instance Versi 2 \(IMDSv2\)](#)

[\[EC2.171\] Koneksi EC2 VPN seharusnya mengaktifkan logging](#)

[\[EC2.172\] Pengaturan Akses Publik Blok EC2 VPC harus memblokir lalu lintas gateway internet](#)

[\[EC2.173\] Permintaan Armada EC2 Spot harus mengaktifkan enkripsi untuk volume EBS terlampir](#)

[\[ECR.1\] Repositori pribadi ECR harus memiliki pemindaian gambar yang dikonfigurasi](#)

[\[ECR.2\] Repositori pribadi ECR harus memiliki kekekalan tag yang dikonfigurasi](#)

[\[ECR.3\] Repositori ECR harus memiliki setidaknya satu kebijakan siklus hidup yang dikonfigurasi](#)

[\[ECS.1\] Definisi tugas Amazon ECS harus memiliki mode jaringan yang aman dan definisi pengguna](#)

[\[ECS.2\] Layanan ECS seharusnya tidak memiliki alamat IP publik yang ditetapkan kepadanya secara otomatis](#)

[\[ECS.3\] Definisi tugas ECS tidak boleh membagikan namespace proses host](#)

[\[ECS.4\] Kontainer ECS harus berjalan sebagai non-hak istimewa](#)

[\[ECS.5\] Wadah ECS harus dibatasi pada akses hanya-baca ke sistem file root](#)

[\[ECS.8\] Rahasia tidak boleh diteruskan sebagai variabel lingkungan kontainer](#)

[\[ECS.9\] Definisi tugas ECS harus memiliki konfigurasi logging](#)

[\[ECS.10\] Layanan ECS Fargate harus berjalan pada versi platform Fargate terbaru](#)

[\[ECS.12\] Cluster ECS harus menggunakan Wawasan Kontainer](#)

[\[ECS.16\] Set tugas ECS seharusnya tidak secara otomatis menetapkan alamat IP publik](#)

[\[EFS.1\] Sistem File Elastis harus dikonfigurasi untuk mengenkripsi data file saat istirahat menggunakan AWS KMS](#)

[\[EFS.2\] Volume Amazon EFS harus dalam rencana cadangan](#)

[\[EFS.3\] Titik akses EFS harus menegakkan direktori root](#)

[\[EFS.4\] Titik akses EFS harus menegakkan identitas pengguna](#)

[\[EFS.6\] Target pemasangan EFS tidak boleh dikaitkan dengan subnet publik](#)

[\[EFS.7\] Sistem file EFS harus mengaktifkan pencadangan otomatis](#)

[\[EFS.8\] Sistem file EFS harus dienkrpsi saat istirahat](#)

[\[EKS.1\] Titik akhir klaster EKS seharusnya tidak dapat diakses publik](#)

[\[EKS.2\] Kluster EKS harus berjalan pada versi Kubernetes yang didukung](#)

[\[EKS.3\] Kluster EKS harus menggunakan rahasia Kubernetes terenkrpsi](#)

[\[EKS.8\] Kluster EKS harus mengaktifkan pencatatan audit](#)

[\[ElastiCache.1\] Cluster ElastiCache \(Redis OSS\) harus mengaktifkan pencadangan otomatis](#)

[\[ElastiCache.2\] ElastiCache cluster harus mengaktifkan peningkatan versi minor otomatis](#)

[\[ElastiCache.3\] grup ElastiCache replikasi harus mengaktifkan failover otomatis](#)

[\[ElastiCache.4\] grup ElastiCache replikasi harus dienkrpsi saat istirahat](#)

[\[ElastiCache.5\] grup ElastiCache replikasi harus dienkrpsi saat transit](#)

[\[ElastiCache.6\] ElastiCache \(Redis OSS\) grup replikasi dari versi sebelumnya harus mengaktifkan Redis OSS AUTH](#)

[\[ElastiCache.7\] ElastiCache cluster tidak boleh menggunakan grup subnet default](#)

[\[ElasticBeanstalk.1\] Lingkungan Elastic Beanstalk seharusnya mengaktifkan pelaporan kesehatan yang ditingkatkan](#)

[\[ElasticBeanstalk.2\] Pembaruan platform yang dikelola Elastic Beanstalk harus diaktifkan](#)

[\[ElasticBeanstalk.3\] Elastic Beanstalk harus mengalirkan log ke CloudWatch](#)

[\[ELB.1\] Application Load Balancer harus dikonfigurasi untuk mengalihkan semua permintaan HTTP ke HTTPS](#)

[\[ELB.2\] Classic Load Balancer dengan pendengar SSL/HTTPS harus menggunakan sertifikat yang disediakan oleh AWS Certificate Manager](#)

[\[ELB.3\] Pendengar Classic Load Balancer harus dikonfigurasi dengan penghentian HTTPS atau TLS](#)

[\[ELB.4\] Application Load Balancer harus dikonfigurasi untuk menjatuhkan header http yang tidak valid](#)

[\[ELB.5\] Pencatatan aplikasi dan Classic Load Balancer harus diaktifkan](#)

[\[ELB.6\] Aplikasi, Gateway, dan Network Load Balancer harus mengaktifkan perlindungan penghapusan](#)

[\[ELB.7\] Classic Load Balancers harus mengaktifkan pengurusan koneksi](#)

[\[ELB.8\] Classic Load Balancer dengan pendengar SSL harus menggunakan kebijakan keamanan yang telah ditentukan sebelumnya yang memiliki urasi yang kuat AWS Config](#)

[\[ELB.9\] Classic Load Balancer harus mengaktifkan penyeimbangan beban lintas zona](#)

[\[ELB.10\] Classic Load Balancer harus menjangkau beberapa Availability Zone](#)

[\[ELB.12\] Application Load Balancer harus dikonfigurasi dengan mode mitigasi desync defensif atau paling ketat](#)

[\[ELB.13\] Penyeimbang Beban Aplikasi, Jaringan, dan Gateway harus mencakup beberapa Availability Zone](#)

[\[ELB.14\] Classic Load Balancer harus dikonfigurasi dengan mode mitigasi desync defensif atau paling ketat](#)

[\[ELB.17\] Aplikasi dan Penyeimbang Beban Jaringan dengan pendengar harus menggunakan kebijakan keamanan yang direkomendasikan](#)

[\[EMR.1\] Node primer klaster EMR Amazon seharusnya tidak memiliki alamat IP publik](#)

[\[EMR.2\] Pengaturan akses publik blok EMR Amazon harus diaktifkan](#)

[\[EMR.3\] Konfigurasi keamanan Amazon EMR harus dienkripsi saat istirahat](#)

[\[EMR.4\] Konfigurasi keamanan Amazon EMR harus dienkripsi saat transit](#)

[\[ES.1\] Domain Elasticsearch harus mengaktifkan enkripsi saat istirahat](#)

[\[ES.2\] Domain Elasticsearch tidak boleh diakses publik](#)

[\[ES.3\] Domain Elasticsearch harus mengenkripsi data yang dikirim antar node](#)

[\[ES.4\] Kesalahan domain Elasticsearch yang masuk ke CloudWatch Log harus diaktifkan](#)

[\[ES.5\] Domain Elasticsearch harus mengaktifkan pencatatan audit](#)

[\[ES.6\] Domain Elasticsearch harus memiliki setidaknya tiga node data](#)

[\[ES.7\] Domain Elasticsearch harus dikonfigurasi dengan setidaknya tiga node master khusus](#)

[\[ES.8\] Koneksi ke domain Elasticsearch harus dienkripsi menggunakan kebijakan keamanan TLS terbaru](#)

[\[EventBridge.3\] bus acara EventBridge khusus harus memiliki kebijakan berbasis sumber daya terlampir](#)

[\[FSx.1\] FSx untuk sistem file OpenZFS harus dikonfigurasi untuk menyalin tag ke cadangan dan volume](#)

[\[FSx.2\] FSx untuk sistem file Lustre harus dikonfigurasi untuk menyalin tag ke cadangan](#)

[\[FSx.3\] FSx untuk sistem file OpenZFS harus dikonfigurasi untuk penyebaran Multi-AZ](#)

[\[FSx.4\] FSx untuk sistem file NetApp ONTAP harus dikonfigurasi untuk penyebaran Multi-AZ](#)

[\[FSx.5\] FSx untuk sistem file Windows File Server harus dikonfigurasi untuk penyebaran Multi-AZ](#)

[\[Glue.3\] transformasi pembelajaran AWS Glue mesin harus dienkripsi saat istirahat](#)

[\[Glue.4\] Pekerjaan AWS Glue percikan harus berjalan pada versi yang didukung AWS Glue](#)

[\[GuardDuty.1\] GuardDuty harus diaktifkan](#)

[\[GuardDuty.5\] Pemantauan Log Audit GuardDuty EKS harus diaktifkan](#)

[\[GuardDuty.6\] Perlindungan GuardDuty Lambda harus diaktifkan](#)

[\[GuardDuty.7\] GuardDuty EKS Runtime Monitoring harus diaktifkan](#)

[\[GuardDuty.8\] Perlindungan GuardDuty Malware untuk EC2 harus diaktifkan](#)

[\[GuardDuty.9\] Perlindungan GuardDuty RDS harus diaktifkan](#)

[\[GuardDuty.10\] Perlindungan GuardDuty S3 harus diaktifkan](#)

[\[GuardDuty.11\] GuardDuty Runtime Monitoring harus diaktifkan](#)

[\[GuardDuty.12\] GuardDuty ECS Runtime Monitoring harus diaktifkan](#)

[\[GuardDuty.13\] GuardDuty EC2 Runtime Monitoring harus diaktifkan](#)

[\[IAM.1\] Kebijakan IAM seharusnya tidak mengizinkan hak administratif “*” penuh](#)

[\[IAM.2\] Pengguna IAM seharusnya tidak memiliki kebijakan IAM yang dilampirkan](#)

[\[IAM.3\] Kunci akses pengguna IAM harus diputar setiap 90 hari atau kurang](#)

[\[IAM.4\] Kunci akses pengguna root IAM seharusnya tidak ada](#)

[\[IAM.5\] MFA harus diaktifkan untuk semua pengguna IAM yang memiliki kata sandi konsol](#)

[\[IAM.6\] MFA perangkat keras harus diaktifkan untuk pengguna root](#)

[\[IAM.7\] Kebijakan kata sandi untuk pengguna IAM harus memiliki konfigurasi yang kuat](#)

[\[IAM.8\] Kredensi pengguna IAM yang tidak digunakan harus dihapus](#)

[\[IAM.21\] Kebijakan terkelola pelanggan IAM yang Anda buat seharusnya tidak mengizinkan tindakan wildcard untuk layanan](#)

[\[Inspektor.1\] Pemindaian Amazon Inspector harus diaktifkan EC2](#)

[\[Inspektor.2\] Pemindaian ECR Amazon Inspector harus diaktifkan](#)

[\[Inspektor.3\] Pemindaian kode Amazon Inspector Lambda harus diaktifkan](#)

[\[Inspektor.4\] Pemindaian standar Amazon Inspector Lambda harus diaktifkan](#)

[\[Kinesis.1\] Aliran kinesis harus dienkripsi saat istirahat](#)

[\[Kinesis.3\] Aliran kinesis harus memiliki periode retensi data yang memadai](#)

[\[KMS.1\] Kebijakan yang dikelola pelanggan IAM tidak boleh mengizinkan tindakan dekripsi pada semua kunci KMS](#)

[\[KMS.2\] Prinsipal IAM tidak boleh memiliki kebijakan inline IAM yang memungkinkan tindakan dekripsi pada semua kunci KMS](#)

[\[KMS.3\] tidak AWS KMS keys boleh dihapus secara tidak sengaja](#)

[\[KMS.5\] Kunci KMS tidak boleh diakses publik](#)

[\[Lambda.1\] Kebijakan fungsi Lambda harus melarang akses publik](#)

[\[Lambda.2\] Fungsi Lambda harus menggunakan runtime yang didukung](#)

[\[Lambda.5\] Fungsi VPC Lambda harus beroperasi di beberapa Availability Zone](#)

[\[Macie.1\] Amazon Macie harus diaktifkan](#)

[\[Macie.2\] Penemuan data sensitif otomatis Macie harus diaktifkan](#)

[\[MQ.2\] Broker ActiveMQ harus mengalirkan log audit ke CloudWatch](#)

[\[MQ.3\] Broker Amazon MQ harus mengaktifkan peningkatan versi minor otomatis](#)

[\[MSK.1\] Kluster MSK harus dienkripsi saat transit di antara node broker](#)

[\[MSK.3\] Konektor MSK Connect harus dienkripsi saat transit](#)

[\[Neptunus.1\] Cluster DB Neptunus harus dienkripsi saat istirahat](#)

[\[Neptune.2\] Cluster DB Neptunus harus menerbitkan log audit ke Log CloudWatch](#)

[\[Neptune.3\] Snapshot cluster Neptunus DB seharusnya tidak publik](#)

[\[Neptunus.4\] Cluster DB Neptunus harus mengaktifkan perlindungan penghapusan](#)

[\[Neptunus.5\] Cluster DB Neptunus harus mengaktifkan cadangan otomatis](#)

[\[Neptune.6\] Snapshot cluster Neptunus DB harus dienkripsi saat istirahat](#)

[\[Neptune.7\] Cluster DB Neptunus harus mengaktifkan otentikasi basis data IAM](#)

[\[Neptunus.8\] Cluster DB Neptunus harus dikonfigurasi untuk menyalin tag ke snapshot](#)

[\[NetworkFirewall.2\] Pencatatan Firewall Jaringan harus diaktifkan](#)

[\[NetworkFirewall.3\] Kebijakan Network Firewall harus memiliki setidaknya satu kelompok aturan yang terkait](#)

[\[NetworkFirewall.4\] Tindakan stateless default untuk kebijakan Network Firewall harus drop atau forward untuk paket penuh](#)

[\[NetworkFirewall.5\] Tindakan stateless default untuk kebijakan Network Firewall harus drop atau forward untuk paket yang terfragmentasi](#)

[\[NetworkFirewall.6\] Grup aturan Stateless Network Firewall tidak boleh kosong](#)

[\[NetworkFirewall.9\] Firewall Jaringan harus mengaktifkan perlindungan penghapusan](#)

[\[NetworkFirewall.10\] Firewall Jaringan harus mengaktifkan perlindungan perubahan subnet](#)

[\[Opensearch.1\] OpenSearch domain harus mengaktifkan enkripsi saat istirahat](#)

[\[Opensearch.2\] OpenSearch domain tidak boleh diakses publik](#)

[\[Opensearch.3\] OpenSearch domain harus mengenkripsi data yang dikirim antar node](#)

[\[Opensearch.4\] login kesalahan OpenSearch domain ke Log harus diaktifkan CloudWatch](#)

[\[Opensearch.5\] OpenSearch domain harus mengaktifkan pencatatan audit](#)

[\[Opensearch.6\] OpenSearch domain harus memiliki setidaknya tiga node data](#)

[\[Opensearch.7\] OpenSearch domain harus mengaktifkan kontrol akses berbutir halus](#)

[\[Opensearch.8\] Koneksi ke OpenSearch domain harus dienkrpsi menggunakan kebijakan keamanan TLS terbaru](#)

[\[Opensearch.10\] OpenSearch domain harus menginstal pembaruan perangkat lunak terbaru](#)

[\[PCA.1\] otoritas sertifikat AWS Private CA root harus dinonaktifkan](#)

[\[Route53.2\] Route 53 zona yang dihosting publik harus mencatat kueri DNS](#)

[\[RDS.1\] Snapshot RDS harus bersifat pribadi](#)

[\[RDS.2\] Instans RDS DB harus melarang akses publik, sebagaimana ditentukan oleh konfigurasi PubliclyAccessible](#)

[\[RDS.3\] Instans RDS DB harus mengaktifkan enkripsi saat istirahat](#)

[\[RDS.4\] Snapshot cluster RDS dan snapshot database harus dienkrpsi saat istirahat](#)

[\[RDS.5\] Instans RDS DB harus dikonfigurasi dengan beberapa Availability Zone](#)

[\[RDS.6\] Pemantauan yang ditingkatkan harus dikonfigurasi untuk instans RDS DB](#)

[\[RDS.7\] Cluster RDS harus mengaktifkan perlindungan penghapusan](#)

[\[RDS.8\] Instans RDS DB harus mengaktifkan perlindungan penghapusan](#)

[\[RDS.9\] Instans RDS DB harus menerbitkan log ke Log CloudWatch](#)

[\[RDS.10\] Otentikasi IAM harus dikonfigurasi untuk instance RDS](#)

[\[RDS.11\] Instans RDS harus mengaktifkan pencadangan otomatis](#)

[\[RDS.12\] Otentikasi IAM harus dikonfigurasi untuk cluster RDS](#)

[\[RDS.13\] Peningkatan versi minor otomatis RDS harus diaktifkan](#)

[\[RDS.14\] Cluster Amazon Aurora seharusnya mengaktifkan backtracking](#)

[\[RDS.15\] Cluster RDS DB harus dikonfigurasi untuk beberapa Availability Zone](#)

[\[RDS.16\] Cluster RDS DB harus dikonfigurasi untuk menyalin tag ke snapshot](#)

[\[RDS.17\] Instans RDS DB harus dikonfigurasi untuk menyalin tag ke snapshot](#)

[\[RDS.19\] Langganan pemberitahuan acara RDS yang ada harus dikonfigurasi untuk peristiwa kluster penting](#)

[\[RDS.20\] Langganan pemberitahuan acara RDS yang ada harus dikonfigurasi untuk peristiwa instance basis data penting](#)

[\[RDS.21\] Langganan pemberitahuan acara RDS harus dikonfigurasi untuk peristiwa grup parameter basis data penting](#)

[\[RDS.22\] Langganan pemberitahuan acara RDS harus dikonfigurasi untuk acara grup keamanan basis data penting](#)

[\[RDS.23\] Instans RDS tidak boleh menggunakan port default mesin database](#)

[\[RDS.24\] Kluster Database RDS harus menggunakan nama pengguna administrator khusus](#)

[\[RDS.25\] Instans database RDS harus menggunakan nama pengguna administrator khusus](#)

[\[RDS.27\] Cluster RDS DB harus dienkripsi saat istirahat](#)

[\[RDS.34\] Kluster Aurora MySQL DB harus menerbitkan log audit ke Log CloudWatch](#)

[\[RDS.35\] Cluster RDS DB harus mengaktifkan peningkatan versi minor otomatis](#)

[\[RDS.36\] RDS untuk instance PostgreSQL DB harus menerbitkan log ke Log CloudWatch](#)

[\[RDS.37\] Cluster Aurora PostgreSQL DB harus menerbitkan log ke Log CloudWatch](#)

[\[RDS.40\] RDS untuk instance SQL Server DB harus menerbitkan log ke Log CloudWatch](#)

[\[RDS.41\] RDS untuk instance SQL Server DB harus dienkripsi saat transit](#)

[\[RDS.42\] RDS untuk instance MariaDB DB harus menerbitkan log ke Log CloudWatch](#)

[\[RDS.44\] RDS untuk instance MariaDB DB harus dienkripsi saat transit](#)

[\[Redshift.1\] Cluster Amazon Redshift harus melarang akses publik](#)

[\[Redshift.2\] Koneksi ke cluster Amazon Redshift harus dienkripsi saat transit](#)

[\[Redshift.3\] Cluster Amazon Redshift harus mengaktifkan snapshot otomatis](#)

[\[Redshift.4\] Cluster Amazon Redshift harus mengaktifkan pencatatan audit](#)

[\[Redshift.6\] Amazon Redshift harus mengaktifkan peningkatan otomatis ke versi utama](#)

[\[Redshift.7\] Cluster Redshift harus menggunakan perutean VPC yang ditingkatkan](#)

[\[Redshift.8\] Cluster Amazon Redshift tidak boleh menggunakan nama pengguna Admin default](#)

[\[Redshift.9\] Cluster Redshift tidak boleh menggunakan nama database default](#)

[\[Redshift.10\] Cluster Redshift harus dienkripsi saat istirahat](#)

[\[Redshift.15\] Grup keamanan Redshift harus mengizinkan masuknya port cluster hanya dari asal yang dibatasi](#)

[\[RedshiftServerless.1\] Grup kerja Amazon Redshift Tanpa Server harus menggunakan perutean VPC yang disempurnakan](#)

[\[RedshiftServerless.2\] Koneksi ke grup kerja Redshift Serverless harus diperlukan untuk menggunakan SSL](#)

[\[RedshiftServerless.3\] Kelompok kerja Redshift Tanpa Server harus melarang akses publik](#)

[\[RedshiftServerless.5\] Ruang nama Redshift Tanpa Server tidak boleh menggunakan nama pengguna admin default](#)

[\[RedshiftServerless.6\] Ruang nama Redshift Tanpa Server harus mengeksport log ke Log CloudWatch](#)

[\[RedshiftServerless.7\] Ruang nama Redshift Tanpa Server seharusnya tidak menggunakan nama database default](#)

[\[S3.1\] Bucket tujuan umum S3 harus mengaktifkan pengaturan akses publik blok](#)

[\[S3.2\] Bucket tujuan umum S3 harus memblokir akses baca publik](#)

[\[S3.3\] Bucket tujuan umum S3 harus memblokir akses tulis publik](#)

[\[S3.5\] Bucket tujuan umum S3 harus memerlukan permintaan untuk menggunakan SSL](#)

[\[S3.6\] Kebijakan bucket tujuan umum S3 harus membatasi akses ke yang lain Akun AWS](#)

[\[S3.8\] Bucket tujuan umum S3 harus memblokir akses publik](#)

[\[S3.9\] Bucket tujuan umum S3 harus mengaktifkan pencatatan akses server](#)

[\[S3.12\] tidak ACLs boleh digunakan untuk mengelola akses pengguna ke bucket tujuan umum S3](#)

[\[S3.13\] Bucket tujuan umum S3 harus memiliki konfigurasi Siklus Hidup](#)

[\[S3.19\] Titik akses S3 harus mengaktifkan pengaturan akses publik blok](#)

[\[S3.24\] Poin Akses Multi-Wilayah S3 harus mengaktifkan pengaturan akses publik blok](#)

[\[SageMaker.1\] Instans SageMaker notebook Amazon seharusnya tidak memiliki akses internet langsung](#)

[\[SageMaker.2\] instance SageMaker notebook harus diluncurkan dalam VPC khusus](#)

[\[SageMaker.3\] Pengguna seharusnya tidak memiliki akses root ke instance SageMaker notebook](#)

[\[SageMaker.4\] varian produksi SageMaker titik akhir harus memiliki jumlah instance awal yang lebih besar dari 1](#)

[\[SageMaker.5\] SageMaker model harus memblokir lalu lintas masuk](#)

[\[SageMaker.8\] instance SageMaker notebook harus berjalan pada platform yang didukung](#)

[\[SecretsManager.1\] Rahasia Secrets Manager harus mengaktifkan rotasi otomatis](#)

[\[SecretsManager.2\] Rahasia Secrets Manager yang dikonfigurasi dengan rotasi otomatis harus berhasil diputar](#)

[\[SecretsManager.3\] Hapus rahasia Secrets Manager yang tidak digunakan](#)

[\[SecretsManager.4\] Rahasia Secrets Manager harus diputar dalam jumlah hari tertentu](#)

[\[ServiceCatalog.1\] Portofolio Service Catalog harus dibagikan hanya dalam suatu organisasi AWS](#)

[\[SNS.4\] Kebijakan akses topik SNS seharusnya tidak mengizinkan akses publik](#)

[\[SQS.1\] Antrian Amazon SQS harus dienkripsi saat istirahat](#)

[\[SQS.3\] Kebijakan akses antrian SQS seharusnya tidak mengizinkan akses publik](#)

[\[SSM.1\] EC2 Instans Amazon harus dikelola oleh AWS Systems Manager](#)

[\[SSM.2\] EC2 Instans Amazon yang dikelola oleh Systems Manager harus memiliki status kepatuhan patch COMPLIANT setelah instalasi patch](#)

[\[SSM.3\] EC2 Instans Amazon yang dikelola oleh Systems Manager harus memiliki status kepatuhan asosiasi COMPLIANT](#)

[\[SSM.4\] Dokumen SSM seharusnya tidak bersifat publik](#)

[\[StepFunctions.1\] Mesin status Step Functions seharusnya mengaktifkan logging](#)

[\[Transfer.2\] Server Transfer Family tidak boleh menggunakan protokol FTP untuk koneksi titik akhir](#)

[\[Transfer.3\] Konektor Transfer Family seharusnya mengaktifkan logging](#)

[\[WAF.1\] Pencatatan ACL Web Global AWS WAF Klasik harus diaktifkan](#)

[\[WAF.2\] Aturan Regional AWS WAF Klasik harus memiliki setidaknya satu syarat](#)

[\[WAF.3\] Kelompok aturan Regional AWS WAF Klasik harus memiliki setidaknya satu aturan](#)

[\[WAF.4\] Web Regional AWS WAF Klasik ACLs harus memiliki setidaknya satu aturan atau kelompok aturan](#)

[\[WAF.6\] Aturan global AWS WAF klasik harus memiliki setidaknya satu syarat](#)

[\[WAF.7\] Kelompok aturan global AWS WAF klasik harus memiliki setidaknya satu aturan](#)

[\[WAF.8\] Web global AWS WAF klasik ACLs harus memiliki setidaknya satu aturan atau kelompok aturan](#)

[\[WAF.10\] AWS WAF web ACLs harus memiliki setidaknya satu aturan atau kelompok aturan](#)

[AWS WAF Aturan \[WAF.12\] harus mengaktifkan metrik CloudWatch](#)

[\[WorkSpaces.1\] volume WorkSpaces pengguna harus dienkrpsi saat istirahat](#)

[\[WorkSpaces.2\] volume WorkSpaces root harus dienkrpsi saat istirahat](#)

AWS Standar Penandaan Sumber Daya di Security Hub CSPM

Standar Penandaan AWS Sumber Daya, yang dikembangkan oleh AWS Security Hub Cloud Security Posture Management (CSPM), membantu Anda menentukan apakah AWS sumber daya Anda hilang tag. Tag adalah pasangan nilai kunci yang bertindak sebagai metadata untuk mengatur sumber daya. AWS Dengan sebagian besar AWS sumber daya, Anda memiliki opsi untuk menambahkan tag ke sumber daya saat Anda membuat sumber daya atau setelah Anda membuat sumber daya.

Contoh sumber daya termasuk CloudFront distribusi Amazon, instans Amazon Elastic Compute Cloud EC2 (Amazon), dan rahasia di. AWS Secrets Manager Tag dapat membantu Anda mengelola, mengidentifikasi, mengatur, mencari, dan memfilter AWS sumber daya.

Setiap tag memiliki dua bagian:

- Kunci tag—misalnya,, CostCenterEnvironment, atau. Project Kunci tag peka huruf besar dan kecil.
- Nilai tag—misalnya, atau. 111122223333 Production Seperti kunci tag, nilai tag peka huruf besar dan kecil.

Anda dapat menggunakan tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Untuk informasi tentang menambahkan tag ke AWS sumber daya, lihat [Panduan Pengguna AWS Sumber Daya Penandaan dan Editor Tag](#).

Untuk setiap kontrol yang berlaku untuk standar Penandaan AWS Sumber Daya di Security Hub CSPM, Anda dapat menggunakan parameter yang didukung secara opsional untuk menentukan kunci tag yang ingin diperiksa oleh kontrol. Jika Anda tidak menentukan kunci tag apa pun, kontrol hanya memeriksa keberadaan setidaknya satu kunci tag, dan gagal jika sumber daya tidak memiliki kunci tag.

Sebelum Anda mengaktifkan standar Penandaan AWS Sumber Daya, penting untuk mengaktifkan dan mengonfigurasi perekaman sumber daya terlebih dahulu. AWS Config Saat Anda mengonfigurasi perekaman sumber daya, pastikan juga untuk mengaktifkannya untuk semua jenis AWS sumber daya yang diperiksa oleh kontrol yang berlaku untuk standar. Jika tidak, Security Hub CSPM mungkin tidak dapat mengevaluasi sumber daya yang sesuai, dan menghasilkan temuan akurat untuk kontrol yang berlaku untuk standar. Untuk informasi selengkapnya, termasuk daftar jenis sumber daya yang akan direkam, lihat [AWS Config Sumber daya yang diperlukan untuk temuan kontrol](#).

 Note

Standar Penandaan AWS Sumber Daya tidak tersedia di Kanada Barat (Calgary), Tiongkok, dan Wilayah. AWS GovCloud (US)

Setelah Anda mengaktifkan standar Penandaan AWS Sumber Daya, Anda mulai menerima temuan untuk kontrol yang berlaku untuk standar. Perhatikan bahwa CSPM Security Hub dapat memakan waktu hingga 18 jam untuk menghasilkan temuan untuk kontrol yang menggunakan aturan AWS

Config terkait layanan yang sama dengan kontrol yang berlaku untuk standar lain yang diaktifkan. Untuk informasi selengkapnya, lihat [Jadwal untuk menjalankan pemeriksaan keamanan](#).

Standar Penandaan AWS Sumber Daya memiliki Nama Sumber Daya Amazon (ARN) berikut:
`arn:aws:securityhub:region::standards/aws-resource-tagging-standard/v/1.0.0`
Anda juga dapat menggunakan [GetEnabledStandards](#) pengoperasian Security Hub CSPM API untuk menemukan ARN dari standar yang diaktifkan.

Kontrol yang berlaku untuk standar

Daftar berikut menentukan kontrol AWS Security Hub Cloud Security Posture Management (CSPM) mana yang berlaku untuk standar AWS Resource Tagging (v1.0.0). Untuk meninjau detail kontrol, pilih kontrol.

- [\[ACM.3\] Sertifikat ACM harus ditandai](#)
- [\[Amplify.1\] Aplikasi Amplify harus diberi tag](#)
- [\[Amplify.2\] Amplify branch harus diberi tag](#)
- [\[AppConfig.1\] AWS AppConfig aplikasi harus diberi tag](#)
- [\[AppConfig.2\] profil AWS AppConfig konfigurasi harus ditandai](#)
- [\[AppConfig.3\] AWS AppConfig lingkungan harus ditandai](#)
- [\[AppConfig.4\] asosiasi AWS AppConfig ekstensi harus ditandai](#)
- [\[AppFlow.1\] AppFlow Aliran Amazon harus ditandai](#)
- [\[AppRunner.1\] Layanan App Runner harus diberi tag](#)
- [\[AppRunner.2\] Konektor VPC App Runner harus diberi tag](#)
- [\[AppSync.4\] AWS AppSync APIs GraphQL harus diberi tag](#)
- [\[Athena.2\] Katalog data Athena harus ditandai](#)
- [\[Athena.3\] Kelompok kerja Athena harus ditandai](#)
- [\[AutoScaling.10\] Grup EC2 Auto Scaling harus diberi tag](#)
- [\[Backup.2\] poin AWS Backup pemulihan harus ditandai](#)
- [\[Backup.3\] AWS Backup brankas harus ditandai](#)
- [\[Backup.4\] rencana AWS Backup laporan harus ditandai](#)
- [\[Backup.5\] rencana AWS Backup cadangan harus ditandai](#)
- [\[Batch.1\] Antrian pekerjaan batch harus ditandai](#)
- [\[Batch.2\] Kebijakan penjadwalan batch harus ditandai](#)

- [\[Batch.3\] Lingkungan komputasi Batch harus ditandai](#)
- [\[Batch.4\] Properti sumber daya komputasi di lingkungan komputasi Batch terkelola harus ditandai](#)
- [\[CloudFormation.2\] CloudFormation tumpukan harus ditandai](#)
- [\[CloudFront.14\] CloudFront distribusi harus ditandai](#)
- [\[CloudTrail.9\] CloudTrail jejak harus ditandai](#)
- [\[CodeArtifact.1\] CodeArtifact repositori harus ditandai](#)
- [\[CodeGuruProfiler.1\] Grup CodeGuru profil profiler harus diberi tag](#)
- [\[CodeGuruReviewer.1\] Asosiasi CodeGuru repositori peninjau harus diberi tag](#)
- [\[Connect.1\] Jenis objek Amazon Connect Customer Profiles harus diberi tag](#)
- [\[DataSync.2\] DataSync tugas harus ditandai](#)
- [\[Detective.1\] Grafik perilaku detektif harus diberi tag](#)
- [\[DMS.2\] Sertifikat DMS harus ditandai](#)
- [\[DMS.3\] Langganan acara DMS harus ditandai](#)
- [\[DMS.4\] Contoh replikasi DMS harus ditandai](#)
- [\[DMS.5\] Grup subnet replikasi DMS harus ditandai](#)
- [\[DynamoDB.5\] Tabel DynamoDB harus diberi tag](#)
- [\[EC2.33\] lampiran gateway EC2 transit harus ditandai](#)
- [\[EC2.34\] tabel rute gateway EC2 transit harus ditandai](#)
- [\[EC2.35\] antarmuka EC2 jaringan harus ditandai](#)
- [\[EC2.36\] gateway EC2 pelanggan harus ditandai](#)
- [\[EC2.37\] Alamat IP EC2 elastis harus ditandai](#)
- [\[EC2.38\] EC2 instance harus ditandai](#)
- [\[EC2.39\] gateway EC2 internet harus ditandai](#)
- [\[EC2.40\] Gateway EC2 NAT harus ditandai](#)
- [\[EC2.41\] EC2 jaringan ACLs harus ditandai](#)
- [\[EC2.42\] tabel EC2 rute harus ditandai](#)
- [\[EC2.43\] grup EC2 keamanan harus ditandai](#)
- [\[EC2.44\] EC2 subnet harus ditandai](#)
- [\[EC2.45\] EC2 volume harus ditandai](#)
- [\[EC2.46\] Amazon VPCs harus diberi tag](#)

- [\[EC2.47\] Layanan titik akhir Amazon VPC harus diberi tag](#)
- [\[EC2.48\] Log aliran VPC Amazon harus diberi tag](#)
- [\[EC2.49\] Koneksi peering VPC Amazon harus ditandai](#)
- [\[EC2.50\] Gateway EC2 VPN harus diberi tag](#)
- [\[EC2.52\] gateway EC2 transit harus ditandai](#)
- [\[EC2.174\] Set opsi EC2 DHCP harus ditandai](#)
- [\[EC2.175\] templat EC2 peluncuran harus diberi tag](#)
- [\[EC2.176\] daftar EC2 awalan harus ditandai](#)
- [\[EC2.177\] Sesi cermin EC2 lalu lintas harus ditandai](#)
- [\[EC2.178\] Filter cermin EC2 lalu lintas harus ditandai](#)
- [\[EC2.179\] Target cermin EC2 lalu lintas harus ditandai](#)
- [\[ECR.4\] Repositori publik ECR harus ditandai](#)
- [\[ECS.13\] Layanan ECS harus ditandai](#)
- [\[ECS.14\] Cluster ECS harus ditandai](#)
- [\[ECS.15\] Definisi tugas ECS harus ditandai](#)
- [\[EFS.5\] Titik akses EFS harus ditandai](#)
- [\[EKS.6\] Kluster EKS harus ditandai](#)
- [\[EKS.7\] Konfigurasi penyedia identitas EKS harus ditandai](#)
- [\[ES.9\] Domain Elasticsearch harus diberi tag](#)
- [\[EventBridge.2\] bus EventBridge acara harus diberi tag](#)
- [\[FraudDetector.1\] Jenis entitas Amazon Fraud Detector harus diberi tag](#)
- [\[FraudDetector.2\] Label Amazon Fraud Detector harus diberi tag](#)
- [\[FraudDetector.3\] Hasil Amazon Fraud Detector harus ditandai](#)
- [\[FraudDetector.4\] Variabel Amazon Fraud Detector harus diberi tag](#)
- [\[GlobalAccelerator.1\] Akselerator Akselerator Global harus diberi tag](#)
- [AWS Glue Pekerjaan \[Glue.1\] harus ditandai](#)
- [\[GuardDuty.2\] GuardDuty filter harus diberi tag](#)
- [\[GuardDuty.3\] GuardDuty IPSets harus ditandai](#)
- [\[GuardDuty.4\] GuardDuty detektor harus diberi tag](#)
- [\[IAM.23\] Penganalisis Akses IAM harus ditandai](#)

- [\[IAM.24\] Peran IAM harus ditandai](#)
- [\[IAM.25\] Pengguna IAM harus diberi tag](#)
- [\[IoT.1\] profil AWS IoT Device Defender keamanan harus ditandai](#)
- [\[IoT.2\] tindakan AWS IoT Core mitigasi harus ditandai](#)
- [AWS IoT Core Dimensi \[IoT.3\] harus ditandai](#)
- [\[IoT.4\] AWS IoT Core otorisasi harus diberi tag](#)
- [\[IoT.5\] alias AWS IoT Core peran harus ditandai](#)
- [AWS IoT Core Kebijakan \[IoT.6\] harus ditandai](#)
- [\[IoT Events .1\] Input Peristiwa AWS IoT harus diberi tag](#)
- [\[IoT Events .2\] Model detektor Acara AWS IoT harus diberi tag](#)
- [\[IoT Events .3\] Model alarm AWS IoT Events harus diberi tag](#)
- [\[IoT Site Wise.1\] Model aset AWS IoT harus ditandai SiteWise](#)
- [\[IoT Site Wise.2\] Dasbor AWS IoT harus diberi tag SiteWise](#)
- [\[IoT Site Wise.3\] Gateway AWS IoT harus diberi tag SiteWise](#)
- [\[IoT Site Wise.4\] Portal AWS IoT harus diberi tag SiteWise](#)
- [\[IoT Site Wise.5\] Proyek AWS IoT harus diberi tag SiteWise](#)
- [\[IoT Twin Maker.1\] Pekerjaan sinkronisasi AWS IoT harus ditandai TwinMaker](#)
- [\[IoT Twin Maker.2\] Ruang kerja AWS IoT harus diberi tag TwinMaker](#)
- [\[IoT Twin Maker.3\] Adegan AWS IoT harus diberi tag TwinMaker](#)
- [\[IoT Twin Maker.4\] Entitas AWS IoT harus diberi tag TwinMaker](#)
- [\[IoT Wireless .1\] Grup multicast Nirkabel AWS IoT harus diberi tag](#)
- [\[IoT Wireless .2\] Profil layanan AWS IoT Wireless harus diberi tag](#)
- [\[IoT Wireless .3\] Tugas AWS IoT FUOTA harus ditandai](#)
- [\[IVS.1\] Pasangan kunci pemutaran IVS harus ditandai](#)
- [\[IVS.2\] Konfigurasi perekaman IVS harus ditandai](#)
- [\[IVS.3\] Saluran IVS harus ditandai](#)
- [\[Keyspaces.1\] Ruang kunci Amazon Keyspaces harus diberi tag](#)
- [\[Kinesis.2\] Aliran kinesis harus ditandai](#)
- [\[Lambda.6\] Fungsi Lambda harus ditandai](#)
- [\[MQ.4\] Broker Amazon MQ harus diberi tag](#)

- [\[NetworkFirewall.7\] Firewall Jaringan harus diberi tag](#)
- [\[NetworkFirewall.8\] Kebijakan firewall Network Firewall harus ditandai](#)
- [\[Opensearch.9\] domain harus ditandai OpenSearch](#)
- [\[PCA.2\] Otoritas sertifikat CA AWS swasta harus ditandai](#)
- [\[RDS.28\] Cluster RDS DB harus ditandai](#)
- [\[RDS.29\] Snapshot cluster RDS DB harus ditandai](#)
- [\[RDS.30\] Instans RDS DB harus ditandai](#)
- [\[RDS.31\] Grup keamanan RDS DB harus ditandai](#)
- [\[RDS.32\] Snapshot RDS DB harus ditandai](#)
- [\[RDS.33\] Grup subnet RDS DB harus ditandai](#)
- [\[Redshift.11\] Cluster Redshift harus ditandai](#)
- [\[Redshift.12\] Langganan pemberitahuan acara Redshift harus ditandai](#)
- [\[Redshift.13\] Snapshot cluster Redshift harus ditandai](#)
- [\[Redshift.14\] Grup subnet cluster Redshift harus ditandai](#)
- [\[Redshift.17\] Grup parameter cluster Redshift harus ditandai](#)
- [\[Route53.1\] Pemeriksaan kesehatan rute 53 harus ditandai](#)
- [\[SageMaker.6\] konfigurasi gambar SageMaker aplikasi harus ditandai](#)
- [\[SageMaker.7\] SageMaker gambar harus diberi tag](#)
- [\[SecretsManager.5\] Rahasia Secrets Manager harus ditandai](#)
- [\[SES.1\] Daftar kontak SES harus ditandai](#)
- [\[SES.2\] Set konfigurasi SES harus ditandai](#)
- [\[SNS.3\] Topik SNS harus ditandai](#)
- [\[SQS.2\] Antrian SQS harus ditandai](#)
- [\[SSM.5\] Dokumen SSM harus ditandai](#)
- [\[StepFunctions.2\] Aktivitas Step Functions harus diberi tag](#)
- [\[Transfer.1\] AWS Transfer Family alur kerja harus ditandai](#)
- [\[Transfer.4\] Perjanjian Transfer Family harus ditandai](#)
- [\[Transfer.5\] Sertifikat Transfer Family harus diberi tag](#)
- [\[Transfer.6\] Konektor Transfer Family harus diberi tag](#)
- [\[Transfer.7\] Profil Transfer Family harus diberi tag](#)

Tolok Ukur AWS Yayasan CIS di Security Hub CSPM

Tolok Ukur AWS Yayasan Center for Internet Security (CIS) berfungsi sebagai seperangkat praktik terbaik konfigurasi keamanan untuk. AWS Praktik terbaik yang diterima industri ini memberi Anda prosedur step-by-step implementasi, dan penilaian yang jelas. Mulai dari sistem operasi hingga layanan cloud dan perangkat jaringan, kontrol dalam tolok ukur ini membantu Anda melindungi sistem spesifik yang digunakan organisasi Anda.

AWS Security Hub Cloud Security Posture Management (CSPM) mendukung CIS AWS Foundations Benchmark versi 3.0.0, 1.4.0, dan 1.2.0. Halaman ini mencantumkan kontrol keamanan yang didukung setiap versi. Ini juga menyediakan perbandingan versi.

Tolok Ukur AWS Yayasan CIS versi 3.0.0

Security Hub CSPM mendukung versi 3.0.0 (v3.0.0) dari CIS Foundations Benchmark. AWS Security Hub CSPM telah memenuhi persyaratan Sertifikasi Perangkat Lunak Keamanan CIS dan telah dianugerahi Sertifikasi Perangkat Lunak Keamanan CIS untuk Tolok Ukur CIS berikut:

- Tolok Ukur CIS untuk Tolok Ukur AWS Yayasan CIS, v3.0.0, Level 1
- Tolok Ukur CIS untuk Tolok Ukur AWS Yayasan CIS, v3.0.0, Level 2

Kontrol yang berlaku untuk CIS AWS Foundations Benchmark versi 3.0.0

[\[Akun.1\] Informasi kontak keamanan harus disediakan untuk Akun AWS](#)

[\[CloudTrail.1\] CloudTrail harus diaktifkan dan dikonfigurasi dengan setidaknya satu jejak Multi-wilayah yang mencakup acara manajemen baca dan tulis](#)

[\[CloudTrail.2\] CloudTrail harus mengaktifkan enkripsi saat istirahat](#)

[\[CloudTrail.4\] validasi file CloudTrail log harus diaktifkan](#)

[\[CloudTrail.7\] Pastikan pencatatan akses bucket S3 diaktifkan pada bucket CloudTrail S3](#)

[\[Config.1\] AWS Config harus diaktifkan dan menggunakan peran terkait layanan untuk perekaman sumber daya](#)

[\[EC2.2\] Grup keamanan default VPC tidak boleh mengizinkan lalu lintas masuk atau keluar](#)

[\[EC2.6\] Pencatatan aliran VPC harus diaktifkan di semua VPCs](#)

[\[EC2.7\] Enkripsi default EBS harus diaktifkan](#)

[\[EC2.8\] EC2 instans harus menggunakan Instance Metadata Service Versi 2 \(\) IMDSv2](#)

[\[EC2.21\] Jaringan ACLs seharusnya tidak mengizinkan masuknya dari 0.0.0.0/0 ke port 22 atau port 3389.](#)

[\[EC2.53\] grup EC2 keamanan seharusnya tidak mengizinkan masuknya dari 0.0.0.0/0 ke port administrasi server jarak jauh](#)

[\[EC2.54\] grup EC2 keamanan tidak boleh mengizinkan masuknya dari :/0 ke port administrasi server jarak jauh](#)

[\[EFS.1\] Sistem File Elastis harus dikonfigurasi untuk mengenkripsi data file saat istirahat menggunakan AWS KMS](#)

[\[IAM.2\] Pengguna IAM seharusnya tidak memiliki kebijakan IAM yang dilampirkan](#)

[\[IAM.3\] Kunci akses pengguna IAM harus diputar setiap 90 hari atau kurang](#)

[\[IAM.4\] Kunci akses pengguna root IAM seharusnya tidak ada](#)

[\[IAM.5\] MFA harus diaktifkan untuk semua pengguna IAM yang memiliki kata sandi konsol](#)

[\[IAM.6\] MFA perangkat keras harus diaktifkan untuk pengguna root](#)

[\[IAM.9\] MFA harus diaktifkan untuk pengguna root](#)

[\[IAM.15\] Pastikan kebijakan kata sandi IAM membutuhkan panjang kata sandi minimum 14 atau lebih](#)

[\[IAM.16\] Pastikan kebijakan kata sandi IAM mencegah penggunaan kembali kata sandi](#)

[\[IAM.18\] Memastikan peran dukungan telah dibuat untuk mengelola insiden dengan AWS Dukungan](#)

[\[IAM.22\] Kredensi pengguna IAM yang tidak digunakan selama 45 hari harus dihapus](#)

[\[IAM.26\] Sertifikat SSL/TLS kedaluwarsa yang dikelola di IAM harus dihapus](#)

[\[IAM.27\] Identitas IAM seharusnya tidak memiliki kebijakan yang dilampirkan AWSCloudShellFullAccess](#)

[\[IAM.28\] IAM Access Analyzer penganalisis akses eksternal harus diaktifkan](#)

[\[KMS.4\] rotasi AWS KMS tombol harus diaktifkan](#)

[\[RDS.2\] Instans RDS DB harus melarang akses publik, sebagaimana ditentukan oleh konfigurasi PubliclyAccessible](#)

[\[RDS.3\] Instans RDS DB harus mengaktifkan enkripsi saat istirahat](#)

[\[RDS.13\] Peningkatan versi minor otomatis RDS harus diaktifkan](#)

[\[S3.1\] Bucket tujuan umum S3 harus mengaktifkan pengaturan akses publik blok](#)

[\[S3.5\] Bucket tujuan umum S3 harus memerlukan permintaan untuk menggunakan SSL](#)

[\[S3.8\] Bucket tujuan umum S3 harus memblokir akses publik](#)

[\[S3.20\] Bucket tujuan umum S3 harus mengaktifkan penghapusan MFA](#)

[\[S3.22\] Bucket tujuan umum S3 harus mencatat peristiwa penulisan tingkat objek](#)

[\[S3.23\] Bucket tujuan umum S3 harus mencatat peristiwa pembacaan tingkat objek](#)

Tolok Ukur AWS Yayasan CIS versi 1.4.0

Security Hub CSPM mendukung versi 1.4.0 (v1.4.0) dari CIS Foundations Benchmark. AWS

Kontrol yang berlaku untuk CIS AWS Foundations Benchmark versi 1.4.0

[\[CloudTrail.1\] CloudTrail harus diaktifkan dan dikonfigurasi dengan setidaknya satu jejak Multi-wilayah yang mencakup acara manajemen baca dan tulis](#)

[\[CloudTrail.2\] CloudTrail harus mengaktifkan enkripsi saat istirahat](#)

[\[CloudTrail.4\] validasi file CloudTrail log harus diaktifkan](#)

[\[CloudTrail.5\] CloudTrail jalur harus diintegrasikan dengan Amazon Logs CloudWatch](#)

[\[CloudTrail.6\] Pastikan bucket S3 yang digunakan untuk menyimpan CloudTrail log tidak dapat diakses publik](#)

[\[CloudTrail.7\] Pastikan pencatatan akses bucket S3 diaktifkan pada bucket CloudTrail S3](#)

[\[CloudWatch.1\] Filter metrik log dan alarm harus ada untuk penggunaan pengguna "root"](#)

[\[CloudWatch.4\] Pastikan filter metrik log dan alarm ada untuk perubahan kebijakan IAM](#)

[\[CloudWatch.5\] Pastikan filter metrik log dan alarm ada untuk perubahan CloudTrail konfigurasi](#)

[\[CloudWatch.6\] Pastikan filter metrik log dan alarm ada untuk kegagalan AWS Management Console otentikasi](#)

[\[CloudWatch.7\] Pastikan filter metrik log dan alarm ada untuk menonaktifkan atau menjadwalkan penghapusan kunci yang dikelola pelanggan](#)

[\[CloudWatch.8\] Pastikan filter metrik log dan alarm ada untuk perubahan kebijakan bucket S3](#)

[\[CloudWatch.9\] Pastikan filter metrik log dan alarm ada untuk perubahan AWS Config konfigurasi](#)

[\[CloudWatch.10\] Pastikan filter metrik log dan alarm ada untuk perubahan grup keamanan](#)

[\[CloudWatch.11\] Pastikan filter metrik log dan alarm ada untuk perubahan pada Daftar Kontrol Akses Jaringan \(NACL\)](#)

[\[CloudWatch.12\] Pastikan filter metrik log dan alarm ada untuk perubahan pada gateway jaringan](#)

[\[CloudWatch.13\] Pastikan filter metrik log dan alarm ada untuk perubahan tabel rute](#)

[\[CloudWatch.14\] Pastikan filter metrik log dan alarm ada untuk perubahan VPC](#)

[\[Config.1\] AWS Config harus diaktifkan dan menggunakan peran terkait layanan untuk perekaman sumber daya](#)

[\[EC2.2\] Grup keamanan default VPC tidak boleh mengizinkan lalu lintas masuk atau keluar](#)

[\[EC2.6\] Pencatatan aliran VPC harus diaktifkan di semua VPCs](#)

[\[EC2.7\] Enkripsi default EBS harus diaktifkan](#)

[\[EC2.21\] Jaringan ACLs seharusnya tidak mengizinkan masuknya dari 0.0.0.0/0 ke port 22 atau port 3389.](#)

[\[IAM.1\] Kebijakan IAM seharusnya tidak mengizinkan hak administratif “*” penuh](#)

[\[IAM.3\] Kunci akses pengguna IAM harus diputar setiap 90 hari atau kurang](#)

[\[IAM.4\] Kunci akses pengguna root IAM seharusnya tidak ada](#)

[\[IAM.5\] MFA harus diaktifkan untuk semua pengguna IAM yang memiliki kata sandi konsol](#)

[\[IAM.6\] MFA perangkat keras harus diaktifkan untuk pengguna root](#)

[\[IAM.9\] MFA harus diaktifkan untuk pengguna root](#)

[\[IAM.15\] Pastikan kebijakan kata sandi IAM membutuhkan panjang kata sandi minimum 14 atau lebih](#)

[\[IAM.16\] Pastikan kebijakan kata sandi IAM mencegah penggunaan kembali kata sandi](#)

[\[IAM.18\] Memastikan peran dukungan telah dibuat untuk mengelola insiden dengan AWS Dukungan](#)

[\[IAM.22\] Kredensi pengguna IAM yang tidak digunakan selama 45 hari harus dihapus](#)

[\[KMS.4\] rotasi AWS KMS tombol harus diaktifkan](#)

[\[RDS.3\] Instans RDS DB harus mengaktifkan enkripsi saat istirahat](#)

[\[S3.1\] Bucket tujuan umum S3 harus mengaktifkan pengaturan akses publik blok](#)

[\[S3.5\] Bucket tujuan umum S3 harus memerlukan permintaan untuk menggunakan SSL](#)

[\[S3.8\] Bucket tujuan umum S3 harus memblokir akses publik](#)

[\[S3.20\] Bucket tujuan umum S3 harus mengaktifkan penghapusan MFA](#)

Tolok Ukur AWS Yayasan CIS versi 1.2.0

Security Hub CSPM mendukung versi 1.2.0 (v1.2.0) dari CIS Foundations Benchmark. AWS Security Hub CSPM telah memenuhi persyaratan Sertifikasi Perangkat Lunak Keamanan CIS dan telah dianugerahi Sertifikasi Perangkat Lunak Keamanan CIS untuk Tolok Ukur CIS berikut:

- Tolok Ukur CIS untuk Tolok Ukur AWS Yayasan CIS, v1.2.0, Level 1
- Tolok Ukur CIS untuk Tolok Ukur AWS Yayasan CIS, v1.2.0, Level 2

Kontrol yang berlaku untuk CIS AWS Foundations Benchmark versi 1.2.0

[\[CloudTrail.1\] CloudTrail harus diaktifkan dan dikonfigurasi dengan setidaknya satu jejak Multi-wilayah yang mencakup acara manajemen baca dan tulis](#)

[\[CloudTrail.2\] CloudTrail harus mengaktifkan enkripsi saat istirahat](#)

[\[CloudTrail.4\] validasi file CloudTrail log harus diaktifkan](#)

[\[CloudTrail.5\] CloudTrail jalur harus diintegrasikan dengan Amazon Logs CloudWatch](#)

[\[CloudTrail.6\] Pastikan bucket S3 yang digunakan untuk menyimpan CloudTrail log tidak dapat diakses publik](#)

[\[CloudTrail.7\] Pastikan pencatatan akses bucket S3 diaktifkan pada bucket CloudTrail S3](#)

[\[CloudWatch.1\] Filter metrik log dan alarm harus ada untuk penggunaan pengguna “root”](#)

[\[CloudWatch.2\] Pastikan filter metrik log dan alarm ada untuk panggilan API yang tidak sah](#)

[\[CloudWatch.3\] Pastikan filter metrik log dan alarm ada untuk login Konsol Manajemen tanpa MFA](#)

[\[CloudWatch.4\] Pastikan filter metrik log dan alarm ada untuk perubahan kebijakan IAM](#)

[\[CloudWatch.5\] Pastikan filter metrik log dan alarm ada untuk perubahan CloudTrail konfigurasi](#)

[\[CloudWatch.6\] Pastikan filter metrik log dan alarm ada untuk kegagalan AWS Management Console otentikasi](#)

[\[CloudWatch.7\] Pastikan filter metrik log dan alarm ada untuk menonaktifkan atau menjadwalkan penghapusan kunci yang dikelola pelanggan](#)

[\[CloudWatch.8\] Pastikan filter metrik log dan alarm ada untuk perubahan kebijakan bucket S3](#)

[\[CloudWatch.9\] Pastikan filter metrik log dan alarm ada untuk perubahan AWS Config konfigurasi](#)

[\[CloudWatch.10\] Pastikan filter metrik log dan alarm ada untuk perubahan grup keamanan](#)

[\[CloudWatch.11\] Pastikan filter metrik log dan alarm ada untuk perubahan pada Daftar Kontrol Akses Jaringan \(NACL\)](#)

[\[CloudWatch.12\] Pastikan filter metrik log dan alarm ada untuk perubahan pada gateway jaringan](#)

[\[CloudWatch.13\] Pastikan filter metrik log dan alarm ada untuk perubahan tabel rute](#)

[\[CloudWatch.14\] Pastikan filter metrik log dan alarm ada untuk perubahan VPC](#)

[\[Config.1\] AWS Config harus diaktifkan dan menggunakan peran terkait layanan untuk perekaman sumber daya](#)

[\[EC2.2\] Grup keamanan default VPC tidak boleh mengizinkan lalu lintas masuk atau keluar](#)

[\[EC2.6\] Pencatatan aliran VPC harus diaktifkan di semua VPCs](#)

[\[EC2.13\] Grup keamanan seharusnya tidak mengizinkan masuknya dari 0.0.0.0/0 atau ::/0 ke port 22](#)

[\[EC2.14\] Grup keamanan seharusnya tidak mengizinkan masuknya dari 0.0.0.0/0 atau :/0 ke port 3389](#)

[\[IAM.1\] Kebijakan IAM seharusnya tidak mengizinkan hak administratif “*” penuh](#)

[\[IAM.2\] Pengguna IAM seharusnya tidak memiliki kebijakan IAM yang dilampirkan](#)

[\[IAM.3\] Kunci akses pengguna IAM harus diputar setiap 90 hari atau kurang](#)

[\[IAM.4\] Kunci akses pengguna root IAM seharusnya tidak ada](#)

[\[IAM.5\] MFA harus diaktifkan untuk semua pengguna IAM yang memiliki kata sandi konsol](#)

[\[IAM.6\] MFA perangkat keras harus diaktifkan untuk pengguna root](#)

[\[IAM.8\] Kredensi pengguna IAM yang tidak digunakan harus dihapus](#)

[\[IAM.9\] MFA harus diaktifkan untuk pengguna root](#)

[\[IAM.11\] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu huruf besar](#)

[\[IAM.12\] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu huruf kecil](#)

[\[IAM.13\] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu simbol](#)

[\[IAM.14\] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu nomor](#)

[\[IAM.15\] Pastikan kebijakan kata sandi IAM membutuhkan panjang kata sandi minimum 14 atau lebih](#)

[\[IAM.16\] Pastikan kebijakan kata sandi IAM mencegah penggunaan kembali kata sandi](#)

[\[IAM.17\] Pastikan kebijakan kata sandi IAM kedaluwarsa kata sandi dalam waktu 90 hari atau kurang](#)

[\[IAM.18\] Memastikan peran dukungan telah dibuat untuk mengelola insiden dengan AWS Dukungan](#)

[\[KMS.4\] rotasi AWS KMS tombol harus diaktifkan](#)

Perbandingan versi untuk CIS AWS Foundations Benchmark

Bagian ini merangkum perbedaan antara versi spesifik dari Center for Internet Security (CIS) AWS Foundation Benchmark — v3.0.0, v1.4.0, dan v1.2.0. AWS Security Hub Cloud Security Posture Management (CSPM) mendukung masing-masing versi Tolok Ukur Yayasan CIS AWS ini. Namun, sebaiknya gunakan v3.0.0 agar tetap mengikuti praktik terbaik keamanan. Anda dapat mengaktifkan beberapa versi standar secara bersamaan. Untuk informasi tentang mengaktifkan

standar, lihat [Mengaktifkan standar keamanan](#). Jika Anda ingin meningkatkan ke v3.0.0, aktifkan sebelum Anda menonaktifkan versi yang lebih lama. Ini mencegah celah dalam pemeriksaan keamanan Anda. [Jika Anda menggunakan integrasi CSPM Security Hub dengan AWS Organizations dan ingin mengaktifkan batch v3.0.0 di beberapa akun, sebaiknya gunakan konfigurasi pusat.](#)

Pemetaan kontrol ke persyaratan CIS di setiap versi

Memahami kontrol mana yang mendukung setiap versi CIS AWS Foundations Benchmark.

Kontrol ID dan judul	Persyaratan CIS v3.0.0	Persyaratan CIS v1.4.0	Persyaratan CIS v1.2.0
[Akun.1] Informasi kontak keamanan harus disediakan untuk Akun AWS	1.2	1.2	1.18
[CloudTrail.1] CloudTrail harus diaktifkan dan dikonfigurasi dengan setidaknya satu jejak Multi-wilayah yang mencakup acara manajemen baca dan tulis	3.1	3.1	2.1
[CloudTrail.2] CloudTrail harus mengaktifkan enkripsi saat istirahat	3.5	3.7	2.7
[CloudTrail.4] validasi file CloudTrail log harus diaktifkan	3.2	3.2	2.2
[CloudTrail.5] CloudTrail jalur harus diintegrasikan dengan Amazon Logs CloudWatch	Tidak didukung - CIS menghapus persyaratan ini	3.4	2.4
[CloudTrail.6] Pastikan bucket S3 yang digunakan untuk menyimpan CloudTrail log tidak dapat diakses publik	Tidak didukung - CIS menghapus persyaratan ini	3.3	2.3
[CloudTrail.7] Pastikan pencatatan akses bucket S3 diaktifkan pada bucket CloudTrail S3	3.4	3.6	2.6

Kontrol ID dan judul	Persyaratan CIS v3.0.0	Persyaratan CIS v1.4.0	Persyaratan CIS v1.2.0
[CloudWatch.1] Filter metrik log dan alarm harus ada untuk penggunaan pengguna “root”	Tidak didukung - pemeriksaan manual	4.3	3.3
[CloudWatch.2] Pastikan filter metrik log dan alarm ada untuk panggilan API yang tidak sah	Tidak didukung - pemeriksaan manual	Tidak didukung - pemeriksaan manual	3.1
[CloudWatch.3] Pastikan filter metrik log dan alarm ada untuk login Konsol Manajemen tanpa MFA	Tidak didukung - pemeriksaan manual	Tidak didukung - pemeriksaan manual	3.2
[CloudWatch.4] Pastikan filter metrik log dan alarm ada untuk perubahan kebijakan IAM	Tidak didukung - pemeriksaan manual	4.4	3.4
[CloudWatch.5] Pastikan filter metrik log dan alarm ada untuk perubahan CloudTrail konfigurasi	Tidak didukung - pemeriksaan manual	4.5	3.5
[CloudWatch.6] Pastikan filter metrik log dan alarm ada untuk kegagalan AWS Management Console otentikasi	Tidak didukung - pemeriksaan manual	4.6	3.6
[CloudWatch.7] Pastikan filter metrik log dan alarm ada untuk menonaktifkan atau menjadwalkan penghapusan kunci yang dikelola pelanggan	Tidak didukung - pemeriksaan manual	4.7	3.7
[CloudWatch.8] Pastikan filter metrik log dan alarm ada untuk perubahan kebijakan bucket S3	Tidak didukung - pemeriksaan manual	4.8	3.8

Kontrol ID dan judul	Persyaratan CIS v3.0.0	Persyaratan CIS v1.4.0	Persyaratan CIS v1.2.0
[CloudWatch.9] Pastikan filter metrik log dan alarm ada untuk perubahan AWS Config konfigurasi	Tidak didukung - pemeriksaan manual	4.9	3.9
[CloudWatch.10] Pastikan filter metrik log dan alarm ada untuk perubahan grup keamanan	Tidak didukung - pemeriksaan manual	4.10	3.10
[CloudWatch.11] Pastikan filter metrik log dan alarm ada untuk perubahan pada Daftar Kontrol Akses Jaringan (NACL)	Tidak didukung - pemeriksaan manual	4.11	3.11
[CloudWatch.12] Pastikan filter metrik log dan alarm ada untuk perubahan pada gateway jaringan	Tidak didukung - pemeriksaan manual	4.12	3.12
[CloudWatch.13] Pastikan filter metrik log dan alarm ada untuk perubahan tabel rute	Tidak didukung - pemeriksaan manual	4.13	3.13
[CloudWatch.14] Pastikan filter metrik log dan alarm ada untuk perubahan VPC	Tidak didukung - pemeriksaan manual	4.14	3.14
[Config.1] AWS Config harus diaktifkan dan menggunakan peran terkait layanan untuk perekaman sumber daya	3.3	3.5	2.5
[EC2.2] Grup keamanan default VPC tidak boleh mengizinkan lalu lintas masuk atau keluar	5.4	5.3	4.3
[EC2.6] Pencatatan aliran VPC harus diaktifkan di semua VPCs	3.7	3.9	2.9

Kontrol ID dan judul	Persyaratan CIS v3.0.0	Persyaratan CIS v1.4.0	Persyaratan CIS v1.2.0
[EC2.7] Enkripsi default EBS harus diaktifkan	2.2.1	2.2.1	Tidak didukung
[EC2.8] EC2 instans harus menggunakan Instance Metadata Service Versi 2 () IMDSv2	5.6	Tidak didukung	Tidak didukung
[EC2.13] Grup keamanan seharusnya tidak mengizinkan masuknya dari 0.0.0.0/0 atau: :/0 ke port 22	Tidak didukung - digantikan oleh persyaratan 5.2 dan 5.3	Tidak didukung - digantikan oleh persyaratan 5.2 dan 5.3	4.1
[EC2.14] Grup keamanan seharusnya tidak mengizinkan masuknya dari 0.0.0.0/0 atau: :/0 ke port 3389	Tidak didukung - digantikan oleh persyaratan 5.2 dan 5.3	Tidak didukung - digantikan oleh persyaratan 5.2 dan 5.3	4.2
[EC2.21] Jaringan ACLs seharusnya tidak mengizinkan masuknya dari 0.0.0.0/0 ke port 22 atau port 3389.	5.1	5.1	Tidak didukung
[EC2.53] grup EC2 keamanan seharusnya tidak mengizinkan masuknya dari 0.0.0.0/0 ke port administrasi server jarak jauh	5.2	Tidak didukung	Tidak didukung
[EC2.54] grup EC2 keamanan tidak boleh mengizinkan masuknya dari: :/0 ke port administrasi server jarak jauh	5.3	Tidak didukung	Tidak didukung
[EFS.1] Sistem File Elastis harus dikonfigurasi untuk mengenkripsi data file saat istirahat menggunakan AWS KMS	2.4.1	Tidak didukung	Tidak didukung

Kontrol ID dan judul	Persyaratan CIS v3.0.0	Persyaratan CIS v1.4.0	Persyaratan CIS v1.2.0
[IAM.1] Kebijakan IAM seharusnya tidak mengizinkan hak administratif “*” penuh	Tidak didukung	1.16	1.22
[IAM.2] Pengguna IAM seharusnya tidak memiliki kebijakan IAM yang dilampirkan	1.15	Tidak didukung	1.16
[IAM.3] Kunci akses pengguna IAM harus diputar setiap 90 hari atau kurang	1.14	1.14	1.4
[IAM.4] Kunci akses pengguna root IAM seharusnya tidak ada	1.4	1.4	1.12
[IAM.5] MFA harus diaktifkan untuk semua pengguna IAM yang memiliki kata sandi konsol	1.10	1.10	1.2
[IAM.6] MFA perangkat keras harus diaktifkan untuk pengguna root	1.6	1.6	1.14
[IAM.8] Kredensi pengguna IAM yang tidak digunakan harus dihapus	Tidak didukung — lihat [IAM.22] Kredensi pengguna IAM yang tidak digunakan selama 45 hari harus dihapus sebagai gantinya	Tidak didukung — lihat [IAM.22] Kredensi pengguna IAM yang tidak digunakan selama 45 hari harus dihapus sebagai gantinya	1.3
[IAM.9] MFA harus diaktifkan untuk pengguna root	1.5	1.5	1.13

Kontrol ID dan judul	Persyaratan CIS v3.0.0	Persyaratan CIS v1.4.0	Persyaratan CIS v1.2.0
[IAM.11] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu huruf besar	Tidak didukung - CIS menghapus persyaratan ini	Tidak didukung - CIS menghapus persyaratan ini	1.5
[IAM.12] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu huruf kecil	Tidak didukung - CIS menghapus persyaratan ini	Tidak didukung - CIS menghapus persyaratan ini	1.6
[IAM.13] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu simbol	Tidak didukung - CIS menghapus persyaratan ini	Tidak didukung - CIS menghapus persyaratan ini	1.7
[IAM.14] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu nomor	Tidak didukung - CIS menghapus persyaratan ini	Tidak didukung - CIS menghapus persyaratan ini	1.8
[IAM.15] Pastikan kebijakan kata sandi IAM membutuhkan panjang kata sandi minimum 14 atau lebih	1.8	1.8	1.9
[IAM.16] Pastikan kebijakan kata sandi IAM mencegah penggunaan kembali kata sandi	1.9	1.9	1.10
[IAM.17] Pastikan kebijakan kata sandi IAM kedaluwarsa kata sandi dalam waktu 90 hari atau kurang	Tidak didukung - CIS menghapus persyaratan ini	Tidak didukung - CIS menghapus persyaratan ini	1.11
[IAM.18] Memastikan peran dukungan telah dibuat untuk mengelola insiden dengan AWS Dukungan	1.17	1.17	1.2
[IAM.20] Hindari penggunaan pengguna root	Tidak didukung - CIS menghapus persyaratan ini	Tidak didukung - CIS menghapus persyaratan ini	1.1

Kontrol ID dan judul	Persyaratan CIS v3.0.0	Persyaratan CIS v1.4.0	Persyaratan CIS v1.2.0
[IAM.22] Kredensi pengguna IAM yang tidak digunakan selama 45 hari harus dihapus	1.12	1.12	Tidak didukung - CIS menambahkan persyaratan ini di versi yang lebih baru
[IAM.26] Sertifikat SSL/TLS kedaluwarsa yang dikelola di IAM harus dihapus	1.19	Tidak didukung - CIS menambahkan persyaratan ini di versi yang lebih baru	Tidak didukung - CIS menambahkan persyaratan ini di versi yang lebih baru
[IAM.27] Identitas IAM seharusnya tidak memiliki kebijakan yang dilampirkan AWSCloud ShellFull Access	1.22	Tidak didukung - CIS menambahkan persyaratan ini di versi yang lebih baru	Tidak didukung - CIS menambahkan persyaratan ini di versi yang lebih baru
[IAM.28] IAM Access Analyzer peng analisis akses eksternal harus diaktifkan	1.20	Tidak didukung - CIS menambahkan persyaratan ini di versi yang lebih baru	Tidak didukung - CIS menambahkan persyaratan ini di versi yang lebih baru
[KMS.4] rotasi AWS KMS tombol harus diaktifkan	3.6	3.8	2.8
[Macie.1] Amazon Macie harus diaktifkan	Tidak didukung - pemeriksaan manual	Tidak didukung - pemeriksaan manual	Tidak didukung - pemeriksaan manual

Kontrol ID dan judul	Persyaratan CIS v3.0.0	Persyaratan CIS v1.4.0	Persyaratan CIS v1.2.0
[RDS.2] Instans RDS DB harus melarang akses publik, sebagaimana ditentukan oleh konfigurasi PubliclyAccessible	2.3.3	Tidak didukung - CIS menambahkan persyaratan ini di versi yang lebih baru	Tidak didukung - CIS menambahkan persyaratan ini di versi yang lebih baru
[RDS.3] Instans RDS DB harus mengaktifkan enkripsi saat istirahat	2.3.1	2.3.1	Tidak didukung - CIS menambahkan persyaratan ini di versi yang lebih baru
[RDS.13] Peningkatan versi minor otomatis RDS harus diaktifkan	2.3.2	Tidak didukung - CIS menambahkan persyaratan ini di versi yang lebih baru	Tidak didukung - CIS menambahkan persyaratan ini di versi yang lebih baru
[S3.1] Bucket tujuan umum S3 harus mengaktifkan pengaturan akses publik blok	2.1.4	2.1.5	Tidak didukung - CIS menambahkan persyaratan ini di versi yang lebih baru
[S3.5] Bucket tujuan umum S3 harus memerlukan permintaan untuk menggunakan SSL	2.1.1	2.1.2	Tidak didukung - CIS menambahkan persyaratan ini di versi yang lebih baru
[S3.8] Bucket tujuan umum S3 harus memblokir akses publik	2.1.4	2.1.5	Tidak didukung - CIS menambahkan persyaratan ini di versi yang lebih baru

Kontrol ID dan judul	Persyaratan CIS v3.0.0	Persyaratan CIS v1.4.0	Persyaratan CIS v1.2.0
[S3.20] Bucket tujuan umum S3 harus mengaktifkan penghapusan MFA	2.1.2	2.1.3	Tidak didukung - CIS menambahkan persyaratan ini di versi yang lebih baru

ARNs untuk Tolok Ukur AWS Yayasan CIS

Saat Anda mengaktifkan satu atau lebih versi Tolok Ukur AWS Yayasan CIS, Anda mulai menerima temuan di AWS Security Finding Format (ASFF). Di ASFF, setiap versi menggunakan Amazon Resource Name (ARN) berikut:

Tolok Ukur AWS Yayasan CIS v3.0.0

```
arn:aws:securityhub:region::standards/cis-aws-foundations-benchmark/v/3.0.0
```

Tolok Ukur AWS Yayasan CIS v1.4.0

```
arn:aws:securityhub:region::standards/cis-aws-foundations-benchmark/v/1.4.0
```

Tolok Ukur AWS Yayasan CIS v1.2.0

```
arn:aws:securityhub::ruleset/cis-aws-foundations-benchmark/v/1.2.0
```

Anda dapat menggunakan [GetEnabledStandards](#) pengoperasian Security Hub CSPM API untuk menemukan ARN dari standar yang diaktifkan.

Nilai-nilai sebelumnya adalah untuk `StandardsArn` Namun, `StandardsSubscriptionArn` mengacu pada sumber daya langganan standar yang dibuat CSPM Security Hub saat Anda berlangganan standar dengan menelepon [BatchEnableStandards](#) di Wilayah.

Note

Saat Anda mengaktifkan versi Tolok Ukur AWS Yayasan CIS, CSPM Security Hub dapat memakan waktu hingga 18 jam untuk menghasilkan temuan untuk kontrol yang

menggunakan aturan AWS Config terkait layanan yang sama dengan kontrol yang diaktifkan dalam standar lain yang diaktifkan. Untuk informasi lebih lanjut tentang jadwal untuk menghasilkan temuan kontrol, lihat [Jadwal untuk menjalankan pemeriksaan keamanan](#).

Menemukan bidang berbeda jika Anda mengaktifkan temuan kontrol konsolidasi. Untuk informasi tentang perbedaan-perbedaan ini, lihat [Dampak konsolidasi pada bidang dan nilai ASFF](#). Untuk temuan kontrol sampel, lihat [Sampel temuan kontrol](#).

Persyaratan CIS yang tidak didukung di Security Hub CSPM

Seperti disebutkan dalam tabel sebelumnya, Security Hub CSPM tidak mendukung setiap persyaratan CIS di setiap versi CIS Foundations Benchmark. AWS Banyak persyaratan yang tidak didukung hanya dapat dievaluasi dengan meninjau status sumber daya Anda secara manual. AWS

NIST SP 800-53 Revisi 5 di Security Hub CSPM

NIST Special Publication 800-53 Revision 5 (NIST SP 800-53 Rev. 5) adalah kerangka kerja keamanan siber dan kepatuhan yang dikembangkan oleh National Institute of Standards and Technology (NIST), sebuah lembaga yang merupakan bagian dari Departemen Perdagangan AS. Kerangka kepatuhan ini menyediakan katalog persyaratan keamanan dan privasi untuk melindungi kerahasiaan, integritas, dan ketersediaan sistem informasi dan sumber daya penting. Instansi dan kontraktor pemerintah federal AS harus mematuhi persyaratan ini untuk melindungi sistem dan organisasi mereka. Organisasi swasta juga dapat secara sukarela menggunakan persyaratan sebagai kerangka panduan untuk mengurangi risiko keamanan siber. Untuk informasi lebih lanjut tentang kerangka kerja dan persyaratannya, lihat [NIST SP 800-53 Rev. 5](#) di Pusat Sumber Daya Keamanan Komputer NIST.

AWS Security Hub Cloud Security Posture Management (CSPM) menyediakan kontrol keamanan yang mendukung subset persyaratan NIST SP 800-53 Revisi 5. Kontrol melakukan pemeriksaan keamanan otomatis untuk sumber daya tertentu Layanan AWS dan. Untuk mengaktifkan dan mengelola kontrol ini, Anda dapat mengaktifkan kerangka kerja NIST SP 800-53 Revisi 5 sebagai standar di Security Hub CSPM. Perhatikan bahwa kontrol tidak mendukung persyaratan NIST SP 800-53 Revisi 5 yang memerlukan pemeriksaan manual.

Tidak seperti kerangka kerja lainnya, kerangka kerja NIST SP 800-53 Revisi 5 tidak preskriptif tentang bagaimana persyaratannya harus dievaluasi. Sebaliknya, kerangka kerja memberikan pedoman. Dalam Security Hub CSPM, standar dan kontrol NIST SP 800-53 Revisi 5 mewakili pemahaman layanan tentang pedoman ini.

Topik

- [Mengkonfigurasi perekaman sumber daya untuk kontrol yang berlaku untuk standar](#)
- [Menentukan kontrol mana yang berlaku untuk standar](#)

Mengkonfigurasi perekaman sumber daya untuk kontrol yang berlaku untuk standar

Untuk mengoptimalkan cakupan dan keakuratan temuan, penting untuk mengaktifkan dan mengonfigurasi perekaman sumber daya AWS Config sebelum Anda mengaktifkan standar NIST SP 800-53 Revisi 5 di Security Hub AWS Cloud Security Posture Management (CSPM). Saat Anda mengonfigurasi perekaman sumber daya, pastikan juga untuk mengaktifkannya untuk semua jenis AWS sumber daya yang diperiksa oleh kontrol yang berlaku untuk standar. Ini terutama untuk kontrol yang memiliki jenis jadwal yang dipicu perubahan. Namun, beberapa kontrol dengan jenis jadwal berkala juga memerlukan perekaman sumber daya. Jika perekaman sumber daya tidak diaktifkan atau dikonfigurasi dengan benar, CSPM Security Hub mungkin tidak dapat mengevaluasi sumber daya yang sesuai, dan menghasilkan temuan akurat untuk kontrol yang berlaku pada standar.

Untuk informasi tentang cara Security Hub CSPM menggunakan rekaman sumber daya AWS Config, lihat [Mengaktifkan dan mengonfigurasi AWS Config untuk Security Hub CSPM](#). Untuk informasi tentang mengonfigurasi perekaman sumber daya AWS Config, lihat [Bekerja dengan perekam konfigurasi](#) di Panduan AWS Config Pengembang.

Tabel berikut menentukan jenis sumber daya untuk merekam kontrol yang berlaku untuk standar NIST SP 800-53 Revisi 5 di Security Hub CSPM.

Layanan AWS	Jenis sumber daya
Amazon API Gateway	AWS::ApiGateway::Stage , AWS::ApiGatewayV2::Stage
AWS AppSync	AWS::AppSync::GraphQLApi
AWS Backup	AWS::Backup::RecoveryPoint
AWS Certificate Manager (ACM)	AWS::ACM::Certificate
AWS CloudFormation	AWS::CloudFormation::Stack
Amazon CloudFront	AWS::CloudFront::Distribution

Layanan AWS	Jenis sumber daya
Amazon CloudWatch	<code>AWS::CloudWatch::Alarm</code>
AWS CodeBuild	<code>AWS::CodeBuild::Project</code>
AWS Database Migration Service (AWS DMS)	<code>AWS::DMS::Endpoint</code> , <code>AWS::DMS::ReplicationInstance</code> , <code>AWS::DMS::ReplicationTask</code>
Amazon DynamoDB	<code>AWS::DynamoDB::Table</code>
Amazon Elastic Compute Cloud (Amazon EC2)	<code>AWS::EC2::ClientVpnEndpoint</code> , <code>AWS::EC2::EIP</code> , <code>AWS::EC2::Instance</code> , <code>AWS::EC2::LaunchTemplate</code> , <code>AWS::EC2::NetworkAcl</code> , <code>AWS::EC2::NetworkInterface</code> , <code>AWS::EC2::SecurityGroup</code> , <code>AWS::EC2::Subnet</code> , <code>AWS::EC2::TransitGateway</code> , <code>AWS::EC2::VPNConnection</code> , <code>AWS::EC2::Volume</code>
EC2 Auto Scaling Amazon	<code>AWS::AutoScaling::AutoScalingGroup</code> , <code>AWS::AutoScaling::LaunchConfiguration</code>
Amazon Elastic Container Registry (Amazon ECR)	<code>AWS::ECR::Repository</code>
Amazon Elastic Container Service (Amazon ECS)	<code>AWS::ECS::Cluster</code> , <code>AWS::ECS::Service</code> , <code>AWS::ECS::TaskDefinition</code>
Amazon Elastic File System (Amazon EFS)	<code>AWS::EFS::AccessPoint</code>
Amazon Elastic Kubernetes Service (Amazon EKS)	<code>AWS::EKS::Cluster</code>

Layanan AWS	Jenis sumber daya
AWS Elastic Beanstalk	<code>AWS::ElasticBeanstalk::Environment</code>
Penyeimbang Beban Elastis	<code>AWS::ElasticLoadBalancing::LoadBalancer</code> , <code>AWS::ElasticLoadBalancingV2::Listener</code> , <code>AWS::ElasticLoadBalancingV2::LoadBalancer</code>
Amazon ElasticSearch	<code>AWS::Elasticsearch::Domain</code>
Amazon EMR	<code>AWS::EMR::SecurityConfiguration</code>
Amazon EventBridge	<code>AWS::Events::Endpoint</code> , <code>AWS::Events::EventBus</code>
AWS Glue	<code>AWS::Glue::Job</code>
AWS Identity and Access Management (IAM)	<code>AWS::IAM::Group</code> , <code>AWS::IAM::Policy</code> , <code>AWS::IAM::Role</code> , <code>AWS::IAM::User</code>
AWS Key Management Service (AWS KMS)	<code>AWS::KMS::Alias</code> , <code>AWS::KMS::Key</code>
Amazon Kinesis	<code>AWS::Kinesis::Stream</code>
AWS Lambda	<code>AWS::Lambda::Function</code>
Amazon Managed Streaming for Apache Kafka (Amazon MSK)	<code>AWS::MSK::Cluster</code>
Amazon MQ	<code>AWS::AmazonMQ::Broker</code>
AWS Network Firewall	<code>AWS::NetworkFirewall::Firewall</code> , <code>AWS::NetworkFirewall::FirewallPolicy</code> , <code>AWS::NetworkFirewall::RuleGroup</code>
OpenSearch Layanan Amazon	<code>AWS::OpenSearch::Domain</code>

Layanan AWS	Jenis sumber daya
Amazon Relational Database Service (Amazon RDS)	<code>AWS::RDS::DBCluster</code> , <code>AWS::RDS::DBClusterSnapshot</code> , <code>AWS::RDS::DBInstance</code> , <code>AWS::RDS::DBSnapshot</code> , <code>AWS::RDS::EventSubscription</code>
Amazon Redshift	<code>AWS::Redshift::Cluster</code> , <code>AWS::Redshift::ClusterSubnetGroup</code>
Amazon Route 53	<code>AWS::Route53::HostedZone</code>
Amazon Simple Storage Service (Amazon S3)	<code>AWS::S3::AccessPoint</code> , <code>AWS::S3::AccountPublicAccessBlock</code> , <code>AWS::S3::Bucket</code>
AWS Service Catalog	<code>AWS::ServiceCatalog::Portfolio</code>
Amazon Simple Notification Service (Amazon SNS)	<code>AWS::SNS::Topic</code>
Amazon Simple Queue Service (Amazon SQS)	<code>AWS::SQS::Queue</code>
Amazon EC2 Systems Manager (SSM)	<code>AWS::SSM::AssociationCompliance</code> , <code>AWS::SSM::ManagedInstanceInventory</code> , <code>AWS::SSM::PatchCompliance</code>
Amazon SageMaker AI	<code>AWS::SageMaker::NotebookInstance</code>
AWS Secrets Manager	<code>AWS::SecretsManager::Secret</code>
AWS Transfer Family	<code>AWS::Transfer::Connector</code>

Layanan AWS	Jenis sumber daya
AWS WAF	AWS::WAF::Rule , AWS::WAF::RuleGroup , AWS::WAF::WebACL , AWS::WAFRegional::Rule , AWS::WAFRegional::RuleGroup , AWS::WAFRegional::WebACL , AWS::WAFv2::RuleGroup , AWS::WAFv2::WebACL

Menentukan kontrol mana yang berlaku untuk standar

Daftar berikut menentukan kontrol yang mendukung persyaratan NIST SP 800-53 Revisi 5 dan berlaku untuk standar NIST SP 800-53 Revisi 5 di Security AWS Hub Cloud Security Posture Management (CSPM). Untuk detail tentang persyaratan spesifik yang didukung kontrol, pilih kontrol. Kemudian lihat bidang Persyaratan terkait di detail untuk kontrol. Bidang ini menentukan setiap persyaratan NIST yang didukung kontrol. Jika bidang tidak menentukan persyaratan NIST tertentu, kontrol tidak mendukung persyaratan.

- [\[Akun.1\] Informasi kontak keamanan harus disediakan untuk Akun AWS](#)
- [\[Akun.2\] Akun AWS harus menjadi bagian dari organisasi AWS Organizations](#)
- [\[ACM.1\] Sertifikat yang diimpor dan diterbitkan ACM harus diperbarui setelah jangka waktu tertentu](#)
- [\[APIGateway.1\] API Gateway REST dan pencatatan eksekusi WebSocket API harus diaktifkan](#)
- [\[APIGateway.2\] Tahapan API Gateway REST API harus dikonfigurasi untuk menggunakan sertifikat SSL untuk otentikasi backend](#)
- [\[APIGateway.3\] Tahapan API Gateway REST API harus mengaktifkan AWS X-Ray penelusuran](#)
- [\[APIGateway.4\] API Gateway harus dikaitkan dengan ACL Web WAF](#)
- [\[APIGateway.5\] Data cache API Gateway REST API harus dienkripsi saat istirahat](#)
- [\[APIGateway.8\] Rute API Gateway harus menentukan jenis otorisasi](#)
- [\[APIGateway.9\] Pencatatan akses harus dikonfigurasi untuk Tahap API Gateway V2](#)
- [\[AppSync.5\] AWS AppSync APIs GraphQL tidak boleh diautentikasi dengan kunci API](#)
- [\[AutoScaling.1\] Grup Auto Scaling yang terkait dengan penyeimbang beban harus menggunakan pemeriksaan kesehatan ELB](#)
- [\[AutoScaling.2\] Grup EC2 Auto Scaling Amazon harus mencakup beberapa Availability Zone](#)

- [\[AutoScaling.3\] Konfigurasi peluncuran grup Auto Scaling harus EC2 mengonfigurasi instance agar memerlukan Layanan Metadata Instance Versi 2 \(\) IMDSv2](#)
- [\[Autoscaling.5\] Instans EC2 Amazon yang diluncurkan menggunakan konfigurasi peluncuran grup Auto Scaling seharusnya tidak memiliki alamat IP Publik](#)
- [\[AutoScaling.6\] Grup Auto Scaling harus menggunakan beberapa jenis instance di beberapa Availability Zone](#)
- [\[AutoScaling.9\] Grup EC2 Auto Scaling Amazon harus menggunakan templat peluncuran Amazon EC2](#)
- [\[Backup.1\] titik AWS Backup pemulihan harus dienkripsi saat istirahat](#)
- [\[CloudFront.1\] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi](#)
- [\[CloudFront.3\] CloudFront distribusi harus memerlukan enkripsi dalam perjalanan](#)
- [\[CloudFront.4\] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi](#)
- [\[CloudFront.5\] CloudFront distribusi seharusnya mengaktifkan logging](#)
- [\[CloudFront.6\] CloudFront distribusi harus mengaktifkan WAF](#)
- [\[CloudFront.7\] CloudFront distribusi harus menggunakan sertifikat SSL/TLS khusus](#)
- [\[CloudFront.8\] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS](#)
- [\[CloudFront.9\] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus](#)
- [\[CloudFront.10\] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal kustom](#)
- [\[CloudFront.12\] CloudFront distribusi seharusnya tidak menunjukkan asal S3 yang tidak ada](#)
- [\[CloudTrail.1\] CloudTrail harus diaktifkan dan dikonfigurasi dengan setidaknya satu jejak Multi-wilayah yang mencakup acara manajemen baca dan tulis](#)
- [\[CloudTrail.2\] CloudTrail harus mengaktifkan enkripsi saat istirahat](#)
- [\[CloudTrail.4\] validasi file CloudTrail log harus diaktifkan](#)
- [\[CloudTrail.5\] CloudTrail jalur harus diintegrasikan dengan Amazon Logs CloudWatch](#)
- [\[CloudTrail.10\] Penyimpanan data acara CloudTrail danau harus dienkripsi dengan pelanggan yang dikelola AWS KMS keys](#)
- [\[CloudWatch.15\] CloudWatch alarm harus memiliki tindakan tertentu yang dikonfigurasi](#)
- [\[CloudWatch.16\] grup CloudWatch log harus dipertahankan untuk jangka waktu tertentu](#)
- [\[CloudWatch.17\] tindakan CloudWatch alarm harus diaktifkan](#)
- [\[CodeBuild.1\] Repositori sumber CodeBuild Bitbucket tidak URLs boleh berisi kredensial sensitif](#)
- [\[CodeBuild.2\] variabel lingkungan CodeBuild proyek tidak boleh berisi kredensial teks yang jelas](#)

- [\[CodeBuild.3\] Log CodeBuild S3 harus dienkripsi](#)
- [\[CodeBuild.4\] lingkungan CodeBuild proyek harus memiliki urasi logging AWS Config](#)
- [\[Config.1\] AWS Config harus diaktifkan dan menggunakan peran terkait layanan untuk perekaman sumber daya](#)
- [\[DataFirehose.1\] Aliran pengiriman Firehose harus dienkripsi saat istirahat](#)
- [\[DMS.1\] Instans replikasi Layanan Migrasi Database tidak boleh bersifat publik](#)
- [\[DMS.6\] Instans replikasi DMS harus mengaktifkan peningkatan versi minor otomatis](#)
- [\[DMS.7\] Tugas replikasi DMS untuk database target seharusnya mengaktifkan logging](#)
- [\[DMS.8\] Tugas replikasi DMS untuk database sumber seharusnya mengaktifkan logging](#)
- [\[DMS.9\] Titik akhir DMS harus menggunakan SSL](#)
- [\[DMS.10\] Titik akhir DMS untuk database Neptune harus mengaktifkan otorisasi IAM](#)
- [\[DMS.11\] Titik akhir DMS untuk MongoDB harus mengaktifkan mekanisme otentikasi](#)
- [\[DMS.12\] Titik akhir DMS untuk Redis OSS seharusnya mengaktifkan TLS](#)
- [\[DocumentDB.1\] Cluster Amazon DocumentDB harus dienkripsi saat istirahat](#)
- [\[DocumentDB.2\] Cluster Amazon DocumentDB harus memiliki periode retensi cadangan yang memadai](#)
- [\[DocumentDB.3\] Cuplikan cluster manual Amazon DocumentDB seharusnya tidak bersifat publik](#)
- [\[DocumentDB.4\] Cluster Amazon DocumentDB harus mempublikasikan log audit ke Log CloudWatch](#)
- [\[DocumentDB.5\] Cluster Amazon DocumentDB harus mengaktifkan perlindungan penghapusan](#)
- [\[DynamoDB.1\] Tabel DynamoDB harus secara otomatis menskalakan kapasitas sesuai permintaan](#)
- [\[DynamoDB.2\] Tabel DynamoDB harus mengaktifkan pemulihan point-in-time](#)
- [\[DynamoDB.3\] Cluster DynamoDB Accelerator \(DAX\) harus dienkripsi saat istirahat](#)
- [\[DynamoDB.4\] Tabel DynamoDB harus ada dalam rencana cadangan](#)
- [\[DynamoDB.6\] Tabel DynamoDB harus mengaktifkan perlindungan penghapusan](#)
- [\[DynamoDB.7\] Cluster DynamoDB Accelerator harus dienkripsi saat transit](#)
- [\[EC2.1\] Cuplikan Amazon EBS tidak boleh dipulihkan secara publik](#)
- [\[EC2.2\] Grup keamanan default VPC tidak boleh mengizinkan lalu lintas masuk atau keluar](#)
- [\[EC2.3\] Volume Amazon EBS yang terlampir harus dienkripsi saat istirahat](#)
- [\[EC2.4\] EC2 Instans yang dihentikan harus dihapus setelah periode waktu tertentu](#)
- [\[EC2.6\] Pencatatan aliran VPC harus diaktifkan di semua VPCs](#)

- [\[EC2.7\] Enkripsi default EBS harus diaktifkan](#)
- [\[EC2.8\] EC2 instans harus menggunakan Instance Metadata Service Versi 2 \(\) IMDSv2](#)
- [\[EC2.9\] EC2 Instans Amazon seharusnya tidak memiliki alamat publik IPv4](#)
- [\[EC2.10\] Amazon EC2 harus dikonfigurasi untuk menggunakan titik akhir VPC yang dibuat untuk layanan Amazon EC2](#)
- [\[EC2.12\] Amazon yang tidak terpakai EC2 EIPs harus dihapus](#)
- [\[EC2.13\] Grup keamanan seharusnya tidak mengizinkan masuknya dari 0.0.0.0/0 atau :/0 ke port 22](#)
- [\[EC2.15\] EC2 Subnet Amazon seharusnya tidak secara otomatis menetapkan alamat IP publik](#)
- [\[EC2.16\] Daftar Kontrol Akses Jaringan yang Tidak Digunakan harus dihapus](#)
- [\[EC2.17\] EC2 Instans Amazon seharusnya tidak menggunakan banyak ENIs](#)
- [\[EC2.18\] Grup keamanan seharusnya hanya mengizinkan lalu lintas masuk yang tidak terbatas untuk port resmi](#)
- [\[EC2.19\] Kelompok keamanan tidak boleh mengizinkan akses tidak terbatas ke port dengan risiko tinggi](#)
- [\[EC2.20\] Kedua terowongan VPN untuk koneksi AWS Site-to-Site VPN harus siap](#)
- [\[EC2.21\] Jaringan ACLs seharusnya tidak mengizinkan masuknya dari 0.0.0.0/0 ke port 22 atau port 3389.](#)
- [\[EC2.23\] Amazon EC2 Transit Gateways seharusnya tidak secara otomatis menerima permintaan lampiran VPC](#)
- [\[EC2.24\] Jenis instance EC2 paravirtual Amazon tidak boleh digunakan](#)
- [\[EC2.25\] Templat EC2 peluncuran Amazon tidak boleh menetapkan publik IPs ke antarmuka jaringan](#)
- [\[EC2.28\] Volume EBS harus dicakup oleh rencana cadangan](#)
- [\[EC2.51\] Titik akhir EC2 Client VPN harus mengaktifkan pencatatan koneksi klien](#)
- [\[EC2.55\] VPCs harus dikonfigurasi dengan titik akhir antarmuka untuk ECR API](#)
- [\[EC2.56\] VPCs harus dikonfigurasi dengan titik akhir antarmuka untuk Docker Registry](#)
- [\[EC2.57\] VPCs harus dikonfigurasi dengan titik akhir antarmuka untuk Systems Manager](#)
- [\[EC2.58\] VPCs harus dikonfigurasi dengan titik akhir antarmuka untuk Kontak Manajer Insiden Systems Manager](#)
- [\[EC2.60\] VPCs harus dikonfigurasi dengan titik akhir antarmuka untuk Systems Manager Incident Manager](#)

- [\[ECR.1\] Repositori pribadi ECR harus memiliki pemindaian gambar yang dikonfigurasi](#)
- [\[ECR.2\] Repositori pribadi ECR harus memiliki kekekalan tag yang dikonfigurasi](#)
- [\[ECR.3\] Repositori ECR harus memiliki setidaknya satu kebijakan siklus hidup yang dikonfigurasi](#)
- [\[ECR.5\] Repositori ECR harus dienkripsi dengan pelanggan yang dikelola AWS KMS keys](#)
- [\[ECS.1\] Definisi tugas Amazon ECS harus memiliki mode jaringan yang aman dan definisi pengguna](#)
- [\[ECS.2\] Layanan ECS seharusnya tidak memiliki alamat IP publik yang ditetapkan kepadanya secara otomatis](#)
- [\[ECS.3\] Definisi tugas ECS tidak boleh membagikan namespace proses host](#)
- [\[ECS.4\] Kontainer ECS harus berjalan sebagai non-hak istimewa](#)
- [\[ECS.5\] Wadah ECS harus dibatasi pada akses hanya-baca ke sistem file root](#)
- [\[ECS.8\] Rahasia tidak boleh diteruskan sebagai variabel lingkungan kontainer](#)
- [\[ECS.9\] Definisi tugas ECS harus memiliki konfigurasi logging](#)
- [\[ECS.10\] Layanan ECS Fargate harus berjalan pada versi platform Fargate terbaru](#)
- [\[ECS.12\] Cluster ECS harus menggunakan Wawasan Kontainer](#)
- [\[ECS.17\] Definisi tugas ECS tidak boleh menggunakan mode jaringan host](#)
- [\[EFS.1\] Sistem File Elastis harus dikonfigurasi untuk mengenkripsi data file saat istirahat menggunakan AWS KMS](#)
- [\[EFS.2\] Volume Amazon EFS harus dalam rencana cadangan](#)
- [\[EFS.3\] Titik akses EFS harus menegakkan direktori root](#)
- [\[EFS.4\] Titik akses EFS harus menegakkan identitas pengguna](#)
- [\[EFS.6\] Target pemasangan EFS tidak boleh dikaitkan dengan subnet publik](#)
- [\[EKS.1\] Titik akhir kluster EKS seharusnya tidak dapat diakses publik](#)
- [\[EKS.2\] Kluster EKS harus berjalan pada versi Kubernetes yang didukung](#)
- [\[EKS.3\] Kluster EKS harus menggunakan rahasia Kubernetes terenkripsi](#)
- [\[EKS.8\] Kluster EKS harus mengaktifkan pencatatan audit](#)
- [\[ElastiCache.1\] Cluster ElastiCache \(Redis OSS\) harus mengaktifkan pencadangan otomatis](#)
- [\[ElastiCache.2\] ElastiCache cluster harus mengaktifkan peningkatan versi minor otomatis](#)
- [\[ElastiCache.3\] grup ElastiCache replikasi harus mengaktifkan failover otomatis](#)
- [\[ElastiCache.4\] grup ElastiCache replikasi harus dienkripsi saat istirahat](#)

- [\[ElastiCache.5\] grup ElastiCache replikasi harus dienkrpsi saat transit](#)
- [\[ElastiCache.6\] ElastiCache \(Redis OSS\) grup replikasi dari versi sebelumnya harus mengaktifkan Redis OSS AUTH](#)
- [\[ElastiCache.7\] ElastiCache cluster tidak boleh menggunakan grup subnet default](#)
- [\[ElasticBeanstalk.1\] Lingkungan Elastic Beanstalk seharusnya mengaktifkan pelaporan kesehatan yang ditingkatkan](#)
- [\[ElasticBeanstalk.2\] Pembaruan platform yang dikelola Elastic Beanstalk harus diaktifkan](#)
- [\[ELB.1\] Application Load Balancer harus dikonfigurasi untuk mengalihkan semua permintaan HTTP ke HTTPS](#)
- [\[ELB.2\] Classic Load Balancer dengan pendengar SSL/HTTPS harus menggunakan sertifikat yang disediakan oleh AWS Certificate Manager](#)
- [\[ELB.3\] Pendengar Classic Load Balancer harus dikonfigurasi dengan penghentian HTTPS atau TLS](#)
- [\[ELB.4\] Application Load Balancer harus dikonfigurasi untuk menjatuhkan header http yang tidak valid](#)
- [\[ELB.5\] Pencatatan aplikasi dan Classic Load Balancer harus diaktifkan](#)
- [\[ELB.6\] Aplikasi, Gateway, dan Network Load Balancer harus mengaktifkan perlindungan penghapusan](#)
- [\[ELB.7\] Classic Load Balancers harus mengaktifkan pengurusan koneksi](#)
- [\[ELB.8\] Classic Load Balancer dengan pendengar SSL harus menggunakan kebijakan keamanan yang telah ditentukan sebelumnya yang memiliki urasi yang kuat AWS Config](#)
- [\[ELB.9\] Classic Load Balancer harus mengaktifkan penyeimbangan beban lintas zona](#)
- [\[ELB.10\] Classic Load Balancer harus menjangkau beberapa Availability Zone](#)
- [\[ELB.12\] Application Load Balancer harus dikonfigurasi dengan mode mitigasi desync defensif atau paling ketat](#)
- [\[ELB.13\] Penyeimbang Beban Aplikasi, Jaringan, dan Gateway harus mencakup beberapa Availability Zone](#)
- [\[ELB.14\] Classic Load Balancer harus dikonfigurasi dengan mode mitigasi desync defensif atau paling ketat](#)
- [\[ELB.16\] Application Load Balancers harus dikaitkan dengan ACL web AWS WAF](#)
- [\[ELB.17\] Aplikasi dan Penyeimbang Beban Jaringan dengan pendengar harus menggunakan kebijakan keamanan yang direkomendasikan](#)

- [\[EMR.1\] Node primer kluster EMR Amazon seharusnya tidak memiliki alamat IP publik](#)
- [\[EMR.2\] Pengaturan akses publik blok EMR Amazon harus diaktifkan](#)
- [\[EMR.3\] Konfigurasi keamanan Amazon EMR harus dienkripsi saat istirahat](#)
- [\[EMR.4\] Konfigurasi keamanan Amazon EMR harus dienkripsi saat transit](#)
- [\[ES.1\] Domain Elasticsearch harus mengaktifkan enkripsi saat istirahat](#)
- [\[ES.2\] Domain Elasticsearch tidak boleh diakses publik](#)
- [\[ES.3\] Domain Elasticsearch harus mengenkripsi data yang dikirim antar node](#)
- [\[ES.4\] Kesalahan domain Elasticsearch yang masuk ke CloudWatch Log harus diaktifkan](#)
- [\[ES.5\] Domain Elasticsearch harus mengaktifkan pencatatan audit](#)
- [\[ES.6\] Domain Elasticsearch harus memiliki setidaknya tiga node data](#)
- [\[ES.7\] Domain Elasticsearch harus dikonfigurasi dengan setidaknya tiga node master khusus](#)
- [\[ES.8\] Koneksi ke domain Elasticsearch harus dienkripsi menggunakan kebijakan keamanan TLS terbaru](#)
- [\[EventBridge.3\] bus acara EventBridge khusus harus memiliki kebijakan berbasis sumber daya terlampir](#)
- [\[EventBridge.4\] titik akhir EventBridge global harus mengaktifkan replikasi acara](#)
- [\[FSx.1\] FSx untuk sistem file OpenZFS harus dikonfigurasi untuk menyalin tag ke cadangan dan volume](#)
- [\[FSx.2\] FSx untuk sistem file Lustre harus dikonfigurasi untuk menyalin tag ke cadangan](#)
- [\[Glue.4\] Pekerjaan AWS Glue percikan harus berjalan pada versi yang didukung AWS Glue](#)
- [\[GuardDuty.1\] GuardDuty harus diaktifkan](#)
- [\[IAM.1\] Kebijakan IAM seharusnya tidak mengizinkan hak administratif “*” penuh](#)
- [\[IAM.2\] Pengguna IAM seharusnya tidak memiliki kebijakan IAM yang dilampirkan](#)
- [\[IAM.3\] Kunci akses pengguna IAM harus diputar setiap 90 hari atau kurang](#)
- [\[IAM.4\] Kunci akses pengguna root IAM seharusnya tidak ada](#)
- [\[IAM.5\] MFA harus diaktifkan untuk semua pengguna IAM yang memiliki kata sandi konsol](#)
- [\[IAM.6\] MFA perangkat keras harus diaktifkan untuk pengguna root](#)
- [\[IAM.7\] Kebijakan kata sandi untuk pengguna IAM harus memiliki konfigurasi yang kuat](#)
- [\[IAM.8\] Kredensi pengguna IAM yang tidak digunakan harus dihapus](#)
- [\[IAM.9\] MFA harus diaktifkan untuk pengguna root](#)

- [\[IAM.19\] MFA harus diaktifkan untuk semua pengguna IAM](#)
- [\[IAM.21\] Kebijakan terkelola pelanggan IAM yang Anda buat seharusnya tidak mengizinkan tindakan wildcard untuk layanan](#)
- [\[Kinesis.1\] Aliran kinesis harus dienkrpsi saat istirahat](#)
- [\[KMS.1\] Kebijakan yang dikelola pelanggan IAM tidak boleh mengizinkan tindakan dekripsi pada semua kunci KMS](#)
- [\[KMS.2\] Prinsipal IAM tidak boleh memiliki kebijakan inline IAM yang memungkinkan tindakan dekripsi pada semua kunci KMS](#)
- [\[KMS.3\] tidak AWS KMS keys boleh dihapus secara tidak sengaja](#)
- [\[KMS.4\] rotasi AWS KMS tombol harus diaktifkan](#)
- [\[Lambda.1\] Kebijakan fungsi Lambda harus melarang akses publik](#)
- [\[Lambda.2\] Fungsi Lambda harus menggunakan runtime yang didukung](#)
- [\[Lambda.3\] Fungsi Lambda harus dalam VPC](#)
- [\[Lambda.5\] Fungsi VPC Lambda harus beroperasi di beberapa Availability Zone](#)
- [\[Macie.1\] Amazon Macie harus diaktifkan](#)
- [\[Macie.2\] Penemuan data sensitif otomatis Macie harus diaktifkan](#)
- [\[MSK.1\] Kluster MSK harus dienkrpsi saat transit di antara node broker](#)
- [\[MSK.2\] Kluster MSK seharusnya telah meningkatkan pemantauan yang dikonfigurasi](#)
- [\[MQ.2\] Broker ActiveMQ harus mengalirkan log audit ke CloudWatch](#)
- [\[MQ.3\] Broker Amazon MQ harus mengaktifkan peningkatan versi minor otomatis](#)
- [\[MQ.5\] Broker ActiveMQ harus menggunakan mode penerapan aktif/siaga](#)
- [\[MQ.6\] Broker RabbitMQ harus menggunakan mode penerapan cluster](#)
- [\[Neptunus.1\] Cluster DB Neptunus harus dienkrpsi saat istirahat](#)
- [\[Neptune.2\] Cluster DB Neptunus harus menerbitkan log audit ke Log CloudWatch](#)
- [\[Neptune.3\] Snapshot cluster Neptunus DB seharusnya tidak publik](#)
- [\[Neptunus.4\] Cluster DB Neptunus harus mengaktifkan perlindungan penghapusan](#)
- [\[Neptunus.5\] Cluster DB Neptunus harus mengaktifkan cadangan otomatis](#)
- [\[Neptune.6\] Snapshot cluster Neptunus DB harus dienkrpsi saat istirahat](#)
- [\[Neptune.7\] Cluster DB Neptunus harus mengaktifkan otentikasi basis data IAM](#)
- [\[Neptunus.8\] Cluster DB Neptunus harus dikonfigurasi untuk menyalin tag ke snapshot](#)

- [\[Neptunus.9\] Cluster DB Neptunus harus digunakan di beberapa Availability Zone](#)
- [\[NetworkFirewall.1\] Firewall Jaringan harus digunakan di beberapa Availability Zone](#)
- [\[NetworkFirewall.2\] Pencatatan Firewall Jaringan harus diaktifkan](#)
- [\[NetworkFirewall.3\] Kebijakan Network Firewall harus memiliki setidaknya satu kelompok aturan yang terkait](#)
- [\[NetworkFirewall.4\] Tindakan stateless default untuk kebijakan Network Firewall harus drop atau forward untuk paket penuh](#)
- [\[NetworkFirewall.5\] Tindakan stateless default untuk kebijakan Network Firewall harus drop atau forward untuk paket yang terfragmentasi](#)
- [\[NetworkFirewall.6\] Grup aturan Stateless Network Firewall tidak boleh kosong](#)
- [\[NetworkFirewall.9\] Firewall Jaringan harus mengaktifkan perlindungan penghapusan](#)
- [\[NetworkFirewall.10\] Firewall Jaringan harus mengaktifkan perlindungan perubahan subnet](#)
- [\[Opensearch.1\] OpenSearch domain harus mengaktifkan enkripsi saat istirahat](#)
- [\[Opensearch.2\] OpenSearch domain tidak boleh diakses publik](#)
- [\[Opensearch.3\] OpenSearch domain harus mengenkripsi data yang dikirim antar node](#)
- [\[Opensearch.4\] Login kesalahan OpenSearch domain ke Log harus diaktifkan CloudWatch](#)
- [\[Opensearch.5\] OpenSearch domain harus mengaktifkan pencatatan audit](#)
- [\[Opensearch.6\] OpenSearch domain harus memiliki setidaknya tiga node data](#)
- [\[Opensearch.7\] OpenSearch domain harus mengaktifkan kontrol akses berbutir halus](#)
- [\[Opensearch.8\] Koneksi ke OpenSearch domain harus dienkripsi menggunakan kebijakan keamanan TLS terbaru](#)
- [\[Opensearch.10\] OpenSearch domain harus menginstal pembaruan perangkat lunak terbaru](#)
- [\[Opensearch.11\] OpenSearch domain harus memiliki setidaknya tiga node primer khusus](#)
- [\[PCA.1\] otoritas sertifikat AWS Private CA root harus dinonaktifkan](#)
- [\[RDS.1\] Snapshot RDS harus bersifat pribadi](#)
- [\[RDS.2\] Instans RDS DB harus melarang akses publik, sebagaimana ditentukan oleh konfigurasi PubliclyAccessible](#)
- [\[RDS.3\] Instans RDS DB harus mengaktifkan enkripsi saat istirahat](#)
- [\[RDS.4\] Snapshot cluster RDS dan snapshot database harus dienkripsi saat istirahat](#)
- [\[RDS.5\] Instans RDS DB harus dikonfigurasi dengan beberapa Availability Zone](#)
- [\[RDS.6\] Pemantauan yang ditingkatkan harus dikonfigurasi untuk instans RDS DB](#)

- [\[RDS.7\] Cluster RDS harus mengaktifkan perlindungan penghapusan](#)
- [\[RDS.8\] Instans RDS DB harus mengaktifkan perlindungan penghapusan](#)
- [\[RDS.9\] Instans RDS DB harus menerbitkan log ke Log CloudWatch](#)
- [\[RDS.10\] Otentikasi IAM harus dikonfigurasi untuk instance RDS](#)
- [\[RDS.11\] Instans RDS harus mengaktifkan pencadangan otomatis](#)
- [\[RDS.12\] Otentikasi IAM harus dikonfigurasi untuk cluster RDS](#)
- [\[RDS.13\] Peningkatan versi minor otomatis RDS harus diaktifkan](#)
- [\[RDS.14\] Cluster Amazon Aurora seharusnya mengaktifkan backtracking](#)
- [\[RDS.15\] Cluster RDS DB harus dikonfigurasi untuk beberapa Availability Zone](#)
- [\[RDS.16\] Cluster RDS DB harus dikonfigurasi untuk menyalin tag ke snapshot](#)
- [\[RDS.17\] Instans RDS DB harus dikonfigurasi untuk menyalin tag ke snapshot](#)
- [\[RDS.19\] Langganan pemberitahuan acara RDS yang ada harus dikonfigurasi untuk peristiwa klaster penting](#)
- [\[RDS.20\] Langganan pemberitahuan acara RDS yang ada harus dikonfigurasi untuk peristiwa instance basis data penting](#)
- [\[RDS.21\] Langganan pemberitahuan acara RDS harus dikonfigurasi untuk peristiwa grup parameter basis data penting](#)
- [\[RDS.22\] Langganan pemberitahuan acara RDS harus dikonfigurasi untuk acara grup keamanan basis data penting](#)
- [\[RDS.23\] Instans RDS tidak boleh menggunakan port default mesin database](#)
- [\[RDS.24\] Kluster Database RDS harus menggunakan nama pengguna administrator khusus](#)
- [\[RDS.25\] Instans database RDS harus menggunakan nama pengguna administrator khusus](#)
- [\[RDS.26\] Instans RDS DB harus dilindungi oleh rencana cadangan](#)
- [\[RDS.27\] Cluster RDS DB harus dienkrpsi saat istirahat](#)
- [\[RDS.34\] Kluster Aurora MySQL DB harus menerbitkan log audit ke Log CloudWatch](#)
- [\[RDS.35\] Cluster RDS DB harus mengaktifkan peningkatan versi minor otomatis](#)
- [\[RDS.40\] RDS untuk instance SQL Server DB harus menerbitkan log ke Log CloudWatch](#)
- [\[RDS.42\] RDS untuk instance MariaDB DB harus menerbitkan log ke Log CloudWatch](#)
- [\[Redshift.1\] Cluster Amazon Redshift harus melarang akses publik](#)
- [\[Redshift.2\] Koneksi ke cluster Amazon Redshift harus dienkrpsi saat transit](#)
- [\[Redshift.3\] Cluster Amazon Redshift harus mengaktifkan snapshot otomatis](#)

- [\[Redshift.4\] Cluster Amazon Redshift harus mengaktifkan pencatatan audit](#)
- [\[Redshift.6\] Amazon Redshift harus mengaktifkan peningkatan otomatis ke versi utama](#)
- [\[Redshift.7\] Cluster Redshift harus menggunakan perutean VPC yang ditingkatkan](#)
- [\[Redshift.8\] Cluster Amazon Redshift tidak boleh menggunakan nama pengguna Admin default](#)
- [\[Redshift.9\] Cluster Redshift tidak boleh menggunakan nama database default](#)
- [\[Redshift.10\] Cluster Redshift harus dienkripsi saat istirahat](#)
- [\[RedshiftServerless.4\] Ruang nama Redshift Tanpa Server harus dienkripsi dengan pengelolaan pelanggan AWS KMS keys](#)
- [\[RedshiftServerless.7\] Ruang nama Redshift Tanpa Server seharusnya tidak menggunakan nama database default](#)
- [\[Route53.2\] Route 53 zona yang dihosting publik harus mencatat kueri DNS](#)
- [\[S3.1\] Bucket tujuan umum S3 harus mengaktifkan pengaturan akses publik blok](#)
- [\[S3.2\] Bucket tujuan umum S3 harus memblokir akses baca publik](#)
- [\[S3.3\] Bucket tujuan umum S3 harus memblokir akses tulis publik](#)
- [\[S3.5\] Bucket tujuan umum S3 harus memerlukan permintaan untuk menggunakan SSL](#)
- [\[S3.6\] Kebijakan bucket tujuan umum S3 harus membatasi akses ke yang lain Akun AWS](#)
- [\[S3.7\] Ember tujuan umum S3 harus menggunakan replikasi lintas wilayah](#)
- [\[S3.8\] Bucket tujuan umum S3 harus memblokir akses publik](#)
- [\[S3.9\] Bucket tujuan umum S3 harus mengaktifkan pencatatan akses server](#)
- [\[S3.10\] Bucket tujuan umum S3 dengan versi diaktifkan harus memiliki konfigurasi Siklus Hidup](#)
- [\[S3.11\] Bucket tujuan umum S3 harus mengaktifkan pemberitahuan acara](#)
- [\[S3.12\] tidak ACLs boleh digunakan untuk mengelola akses pengguna ke bucket tujuan umum S3](#)
- [\[S3.13\] Bucket tujuan umum S3 harus memiliki konfigurasi Siklus Hidup](#)
- [\[S3.14\] Bucket tujuan umum S3 harus mengaktifkan versi](#)
- [\[S3.15\] Bucket tujuan umum S3 harus mengaktifkan Object Lock](#)
- [\[S3.17\] Ember tujuan umum S3 harus dienkripsi saat istirahat AWS KMS keys](#)
- [\[S3.19\] Titik akses S3 harus mengaktifkan pengaturan akses publik blok](#)
- [\[S3.20\] Bucket tujuan umum S3 harus mengaktifkan penghapusan MFA](#)
- [\[SageMaker.1\] Instans SageMaker notebook Amazon seharusnya tidak memiliki akses internet langsung](#)

- [\[SageMaker.2\] instance SageMaker notebook harus diluncurkan dalam VPC khusus](#)
- [\[SageMaker.3\] Pengguna seharusnya tidak memiliki akses root ke instance SageMaker notebook](#)
- [\[SageMaker.4\] varian produksi SageMaker titik akhir harus memiliki jumlah instance awal yang lebih besar dari 1](#)
- [\[SecretsManager.1\] Rahasia Secrets Manager harus mengaktifkan rotasi otomatis](#)
- [\[SecretsManager.2\] Rahasia Secrets Manager yang dikonfigurasi dengan rotasi otomatis harus berhasil diputar](#)
- [\[SecretsManager.3\] Hapus rahasia Secrets Manager yang tidak digunakan](#)
- [\[SecretsManager.4\] Rahasia Secrets Manager harus diputar dalam jumlah hari tertentu](#)
- [\[ServiceCatalog.1\] Portofolio Service Catalog harus dibagikan hanya dalam suatu organisasi AWS](#)
- [\[SNS.1\] Topik SNS harus dienkripsi saat istirahat menggunakan AWS KMS](#)
- [\[SQS.1\] Antrian Amazon SQS harus dienkripsi saat istirahat](#)
- [\[SSM.1\] EC2 Instans Amazon harus dikelola oleh AWS Systems Manager](#)
- [\[SSM.2\] EC2 Instans Amazon yang dikelola oleh Systems Manager harus memiliki status kepatuhan patch COMPLIANT setelah instalasi patch](#)
- [\[SSM.3\] EC2 Instans Amazon yang dikelola oleh Systems Manager harus memiliki status kepatuhan asosiasi COMPLIANT](#)
- [\[SSM.4\] Dokumen SSM seharusnya tidak bersifat publik](#)
- [\[Transfer.2\] Server Transfer Family tidak boleh menggunakan protokol FTP untuk koneksi titik akhir](#)
- [\[Transfer.3\] Konektor Transfer Family seharusnya mengaktifkan logging](#)
- [\[WAF.1\] Pencatatan ACL Web Global AWS WAF Klasik harus diaktifkan](#)
- [\[WAF.2\] Aturan Regional AWS WAF Klasik harus memiliki setidaknya satu syarat](#)
- [\[WAF.3\] Kelompok aturan Regional AWS WAF Klasik harus memiliki setidaknya satu aturan](#)
- [\[WAF.4\] Web Regional AWS WAF Klasik ACLs harus memiliki setidaknya satu aturan atau kelompok aturan](#)
- [\[WAF.6\] Aturan global AWS WAF klasik harus memiliki setidaknya satu syarat](#)
- [\[WAF.7\] Kelompok aturan global AWS WAF klasik harus memiliki setidaknya satu aturan](#)
- [\[WAF.8\] Web global AWS WAF klasik ACLs harus memiliki setidaknya satu aturan atau kelompok aturan](#)
- [\[WAF.10\] AWS WAF web ACLs harus memiliki setidaknya satu aturan atau kelompok aturan](#)
- [\[WAF.11\] pencatatan ACL AWS WAF web harus diaktifkan](#)

- [AWS WAF Aturan \[WAF.12\] harus mengaktifkan metrik CloudWatch](#)

NIST SP 800-171 Revisi 2 di Security Hub CSPM

NIST Special Publication 800-171 Revision 2 (NIST SP 800-171 Rev. 2) adalah kerangka kerja keamanan siber dan kepatuhan yang dikembangkan oleh National Institute of Standards and Technology (NIST), sebuah lembaga yang merupakan bagian dari Departemen Perdagangan AS. Kerangka kepatuhan ini memberikan persyaratan keamanan yang direkomendasikan untuk melindungi kerahasiaan Informasi Tidak Diklasifikasikan Terkendali dalam sistem dan organisasi yang bukan bagian dari pemerintah federal AS. Controlled Unclassified Information, juga disebut sebagai CUI, adalah informasi sensitif yang tidak memenuhi kriteria pemerintah untuk klasifikasi tetapi harus dilindungi. Ini adalah informasi yang dianggap sensitif dan dibuat atau dimiliki oleh pemerintah federal AS atau entitas lain atas nama pemerintah federal AS.

NIST SP 800-171 Rev. 2 memberikan persyaratan keamanan yang direkomendasikan untuk melindungi kerahasiaan CUI ketika:

- Informasi berada dalam sistem dan organisasi non-federal,
- Organisasi non-federal tidak mengumpulkan atau memelihara informasi atas nama agen federal atau menggunakan atau mengoperasikan sistem atas nama agen, dan
- Tidak ada persyaratan pengamanan khusus untuk melindungi kerahasiaan CUI yang ditentukan oleh undang-undang otorisasi, peraturan, atau kebijakan pemerintah untuk kategori CUI yang tercantum dalam Registri CUI.

Persyaratan berlaku untuk semua komponen sistem dan organisasi non-federal yang memproses, menyimpan, atau mengirimkan CUI, atau memberikan perlindungan keamanan untuk komponen. Untuk informasi lebih lanjut, lihat [NIST SP 800-171 Rev. 2](#) di Pusat Sumber Daya Keamanan Komputer NIST.

AWS Security Hub Cloud Security Posture Management (CSPM) menyediakan kontrol keamanan yang mendukung subset persyaratan NIST SP 800-171 Revisi 2. Kontrol melakukan pemeriksaan keamanan otomatis untuk sumber daya tertentu Layanan AWS dan. Untuk mengaktifkan dan mengelola kontrol ini, Anda dapat mengaktifkan kerangka kerja NIST SP 800-171 Revisi 2 sebagai standar di Security Hub CSPM. Perhatikan bahwa kontrol tidak mendukung persyaratan NIST SP 800-171 Revisi 2 yang memerlukan pemeriksaan manual.

Topik

- [Mengkonfigurasi perekaman sumber daya untuk kontrol yang berlaku untuk standar](#)
- [Menentukan kontrol mana yang berlaku untuk standar](#)

Mengkonfigurasi perekaman sumber daya untuk kontrol yang berlaku untuk standar

Untuk mengoptimalkan cakupan dan keakuratan temuan, penting untuk mengaktifkan dan mengonfigurasi perekaman sumber daya AWS Config sebelum Anda mengaktifkan standar NIST SP 800-171 Revisi 2 di Security Hub Cloud Security Posture AWS Management (CSPM). Saat Anda mengonfigurasi perekaman sumber daya, pastikan juga untuk mengaktifkannya untuk semua jenis AWS sumber daya yang diperiksa oleh kontrol yang berlaku untuk standar. Jika tidak, Security Hub CSPM mungkin tidak dapat mengevaluasi sumber daya yang sesuai, dan menghasilkan temuan akurat untuk kontrol yang berlaku untuk standar.

Untuk informasi tentang cara Security Hub CSPM menggunakan rekaman sumber daya AWS Config, lihat [Mengaktifkan dan mengonfigurasi AWS Config untuk Security Hub CSPM](#). Untuk informasi tentang mengonfigurasi perekaman sumber daya AWS Config, lihat [Bekerja dengan perekam konfigurasi](#) di Panduan AWS Config Pengembang.

Tabel berikut menentukan jenis sumber daya untuk merekam kontrol yang berlaku untuk standar NIST SP 800-171 Revisi 2 di Security Hub CSPM.

Layanan AWS	Jenis sumber daya
AWS Certificate Manager(ACM)	AWS::ACM::Certificate
Amazon API Gateway	AWS::ApiGateway::Stage
Amazon CloudFront	AWS::CloudFront::Distribution
Amazon CloudWatch	AWS::CloudWatch::Alarm
Amazon Elastic Compute Cloud (Amazon EC2)	AWS::EC2::ClientVpnEndpoint , AWS::EC2::NetworkAcl , AWS::EC2: :SecurityGroup , AWS::EC2::VPC , AWS::EC2::VPNConnection
Penyeimbang Beban Elastis	AWS::ElasticLoadBalancing:: LoadBalancer

Layanan AWS	Jenis sumber daya
AWS Identity and Access Management(IAM)	AWS::IAM::Policy , AWS::IAM::User
AWS Key Management Service (AWS KMS)	AWS::KMS::Alias , AWS::KMS::Key
AWS Network Firewall	AWS::NetworkFirewall::FirewallPolicy , AWS::NetworkFirewall::RuleGroup
Layanan Penyimpanan Sederhana Amazon (Amazon S3)	AWS::S3::Bucket
Layanan Pemberitahuan Sederhana Amazon (Amazon SNS)	AWS::SNS::Topic
AWS Systems Manager(SSM)	AWS::SSM::PatchCompliance
AWS WAF	AWS::WAFv2::RuleGroup

Menentukan kontrol mana yang berlaku untuk standar

Daftar berikut menentukan kontrol yang mendukung persyaratan NIST SP 800-171 Revisi 2 dan berlaku untuk standar NIST SP 800-171 Revisi 2 di Security Hub Cloud AWS Security Posture Management (CSPM). Untuk detail tentang persyaratan spesifik yang didukung kontrol, pilih kontrol. Kemudian lihat bidang Persyaratan terkait di detail untuk kontrol. Bidang ini menentukan setiap persyaratan NIST yang didukung kontrol. Jika bidang tidak menentukan persyaratan NIST tertentu, kontrol tidak mendukung persyaratan.

- [\[ACM.1\] Sertifikat yang diimpor dan diterbitkan ACM harus diperbarui setelah jangka waktu tertentu](#)
- [\[APIGateway.2\] Tahapan API Gateway REST API harus dikonfigurasi untuk menggunakan sertifikat SSL untuk otentikasi backend](#)
- [\[CloudFront.7\] CloudFront distribusi harus menggunakan sertifikat SSL/TLS khusus](#)
- [\[CloudFront.10\] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal kustom](#)
- [\[CloudTrail.2\] CloudTrail harus mengaktifkan enkripsi saat istirahat](#)
- [\[CloudTrail.3\] Setidaknya satu CloudTrail jejak harus diaktifkan](#)

- [\[CloudTrail.4\] validasi file CloudTrail log harus diaktifkan](#)
- [\[CloudWatch.1\] Filter metrik log dan alarm harus ada untuk penggunaan pengguna “root”](#)
- [\[CloudWatch.2\] Pastikan filter metrik log dan alarm ada untuk panggilan API yang tidak sah](#)
- [\[CloudWatch.4\] Pastikan filter metrik log dan alarm ada untuk perubahan kebijakan IAM](#)
- [\[CloudWatch.5\] Pastikan filter metrik log dan alarm ada untuk perubahan CloudTrail konfigurasi](#)
- [\[CloudWatch.6\] Pastikan filter metrik log dan alarm ada untuk kegagalan AWS Management Console otentikasi](#)
- [\[CloudWatch.7\] Pastikan filter metrik log dan alarm ada untuk menonaktifkan atau menjadwalkan penghapusan kunci yang dikelola pelanggan](#)
- [\[CloudWatch.8\] Pastikan filter metrik log dan alarm ada untuk perubahan kebijakan bucket S3](#)
- [\[CloudWatch.9\] Pastikan filter metrik log dan alarm ada untuk perubahan AWS Config konfigurasi](#)
- [\[CloudWatch.10\] Pastikan filter metrik log dan alarm ada untuk perubahan grup keamanan](#)
- [\[CloudWatch.11\] Pastikan filter metrik log dan alarm ada untuk perubahan pada Daftar Kontrol Akses Jaringan \(NACL\)](#)
- [\[CloudWatch.12\] Pastikan filter metrik log dan alarm ada untuk perubahan pada gateway jaringan](#)
- [\[CloudWatch.13\] Pastikan filter metrik log dan alarm ada untuk perubahan tabel rute](#)
- [\[CloudWatch.14\] Pastikan filter metrik log dan alarm ada untuk perubahan VPC](#)
- [\[CloudWatch.15\] CloudWatch alarm harus memiliki tindakan tertentu yang dikonfigurasi](#)
- [\[EC2.6\] Pencatatan aliran VPC harus diaktifkan di semua VPCs](#)
- [\[EC2.10\] Amazon EC2 harus dikonfigurasi untuk menggunakan titik akhir VPC yang dibuat untuk layanan Amazon EC2](#)
- [\[EC2.13\] Grup keamanan seharusnya tidak mengizinkan masuknya dari 0.0.0.0/0 atau :/0 ke port 22](#)
- [\[EC2.16\] Daftar Kontrol Akses Jaringan yang Tidak Digunakan harus dihapus](#)
- [\[EC2.18\] Grup keamanan seharusnya hanya mengizinkan lalu lintas masuk yang tidak terbatas untuk port resmi](#)
- [\[EC2.19\] Kelompok keamanan tidak boleh mengizinkan akses tidak terbatas ke port dengan risiko tinggi](#)
- [\[EC2.20\] Kedua terowongan VPN untuk koneksi AWS Site-to-Site VPN harus siap](#)
- [\[EC2.21\] Jaringan ACLs seharusnya tidak mengizinkan masuknya dari 0.0.0.0/0 ke port 22 atau port 3389.](#)

- [\[EC2.51\] Titik akhir EC2 Client VPN harus mengaktifkan pencatatan koneksi klien](#)
- [\[ELB.2\] Classic Load Balancer dengan pendengar SSL/HTTPS harus menggunakan sertifikat yang disediakan oleh AWS Certificate Manager](#)
- [\[ELB.3\] Pendengar Classic Load Balancer harus dikonfigurasi dengan penghentian HTTPS atau TLS](#)
- [\[ELB.8\] Classic Load Balancer dengan pendengar SSL harus menggunakan kebijakan keamanan yang telah ditentukan sebelumnya yang memiliki urasi yang kuat AWS Config](#)
- [\[GuardDuty.1\] GuardDuty harus diaktifkan](#)
- [\[IAM.1\] Kebijakan IAM seharusnya tidak mengizinkan hak administratif “*” penuh](#)
- [\[IAM.2\] Pengguna IAM seharusnya tidak memiliki kebijakan IAM yang dilampirkan](#)
- [\[IAM.7\] Kebijakan kata sandi untuk pengguna IAM harus memiliki konfigurasi yang kuat](#)
- [\[IAM.8\] Kredensi pengguna IAM yang tidak digunakan harus dihapus](#)
- [\[IAM.10\] Kebijakan kata sandi untuk pengguna IAM harus memiliki konfigurasi yang kuat](#)
- [\[IAM.11\] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu huruf besar](#)
- [\[IAM.12\] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu huruf kecil](#)
- [\[IAM.13\] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu simbol](#)
- [\[IAM.14\] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu nomor](#)
- [\[IAM.15\] Pastikan kebijakan kata sandi IAM membutuhkan panjang kata sandi minimum 14 atau lebih](#)
- [\[IAM.16\] Pastikan kebijakan kata sandi IAM mencegah penggunaan kembali kata sandi](#)
- [\[IAM.17\] Pastikan kebijakan kata sandi IAM kedaluwarsa kata sandi dalam waktu 90 hari atau kurang](#)
- [\[IAM.18\] Memastikan peran dukungan telah dibuat untuk mengelola insiden dengan AWS Dukungan](#)
- [\[IAM.19\] MFA harus diaktifkan untuk semua pengguna IAM](#)
- [\[IAM.21\] Kebijakan terkelola pelanggan IAM yang Anda buat seharusnya tidak mengizinkan tindakan wildcard untuk layanan](#)
- [\[IAM.22\] Kredensi pengguna IAM yang tidak digunakan selama 45 hari harus dihapus](#)
- [\[NetworkFirewall.2\] Pencatatan Firewall Jaringan harus diaktifkan](#)
- [\[NetworkFirewall.3\] Kebijakan Network Firewall harus memiliki setidaknya satu kelompok aturan yang terkait](#)

- [\[NetworkFirewall.5\]](#) Tindakan stateless default untuk kebijakan Network Firewall harus drop atau forward untuk paket yang terfragmentasi
- [\[NetworkFirewall.6\]](#) Grup aturan Stateless Network Firewall tidak boleh kosong
- [\[S3.5\]](#) Bucket tujuan umum S3 harus memerlukan permintaan untuk menggunakan SSL
- [\[S3.6\]](#) Kebijakan bucket tujuan umum S3 harus membatasi akses ke yang lain Akun AWS
- [\[S3.9\]](#) Bucket tujuan umum S3 harus mengaktifkan pencatatan akses server
- [\[S3.11\]](#) Bucket tujuan umum S3 harus mengaktifkan pemberitahuan acara
- [\[S3.14\]](#) Bucket tujuan umum S3 harus mengaktifkan versi
- [\[S3.17\]](#) Ember tujuan umum S3 harus dienkripsi saat istirahat AWS KMS keys
- [\[SNS.1\]](#) Topik SNS harus dienkripsi saat istirahat menggunakan AWS KMS
- [\[SSM.2\]](#) EC2 Instans Amazon yang dikelola oleh Systems Manager harus memiliki status kepatuhan patch COMPLIANT setelah instalasi patch
- [AWS WAF Aturan \[WAF.12\]](#) harus mengaktifkan metrik CloudWatch

PCI DSS di Security Hub CSPM

Standar Keamanan Data Industri Kartu Pembayaran (PCI DSS) adalah kerangka kepatuhan pihak ketiga yang menyediakan seperangkat aturan dan pedoman untuk menangani informasi kartu kredit dan debit dengan aman. Dewan Standar Keamanan PCI (SSC) membuat dan memperbarui kerangka kerja ini.

AWS Security Hub Cloud Security Posture Management (CSPM) menyediakan standar PCI DSS yang dapat membantu Anda tetap mematuhi kerangka kerja pihak ketiga ini. Anda dapat menggunakan standar ini untuk menemukan kerentanan keamanan dalam AWS sumber daya yang menangani data pemegang kartu. Sebaiknya aktifkan standar ini Akun AWS yang memiliki sumber daya yang menyimpan, memproses, atau mengirimkan data pemegang kartu atau data otentikasi sensitif. Penilaian oleh PCI SSC memvalidasi standar ini.

Security Hub CSPM menawarkan dukungan untuk PCI DSS v3.2.1 dan PCI DSS v4.0.1. Sebaiknya gunakan v4.0.1 agar tetap mengikuti praktik terbaik keamanan. Anda dapat mengaktifkan kedua versi standar secara bersamaan. Untuk informasi tentang mengaktifkan standar, lihat [Mengaktifkan standar keamanan](#). Jika saat ini Anda menggunakan v3.2.1 tetapi hanya ingin menggunakan v4.0.1, aktifkan versi yang lebih baru sebelum menonaktifkan versi yang lebih lama. Ini mencegah celah dalam pemeriksaan keamanan Anda. Jika Anda menggunakan integrasi CSPM Security Hub dengan AWS

Organizations dan ingin mengaktifkan v4.0.1 secara batch di beberapa akun, sebaiknya gunakan [konfigurasi pusat](#) untuk melakukannya.

Bagian berikut menentukan kontrol mana yang berlaku untuk PCI DSS v3.2.1 dan PCI DSS v4.0.1.

Kontrol yang berlaku untuk PCI DSS v3.2.1

Daftar berikut menentukan kontrol AWS Security Hub Cloud Security Posture Management (CSPM) mana yang berlaku untuk PCI DSS v3.2.1. Untuk meninjau detail kontrol, pilih kontrol.

[\[AutoScaling.1\] Grup Auto Scaling yang terkait dengan penyeimbang beban harus menggunakan pemeriksaan kesehatan ELB](#)

[\[CloudTrail.2\] CloudTrail harus mengaktifkan enkripsi saat istirahat](#)

[\[CloudTrail.3\] Setidaknya satu CloudTrail jejak harus diaktifkan](#)

[\[CloudTrail.4\] validasi file CloudTrail log harus diaktifkan](#)

[\[CloudTrail.5\] CloudTrail jalur harus diintegrasikan dengan Amazon Logs CloudWatch](#)

[\[CloudWatch.1\] Filter metrik log dan alarm harus ada untuk penggunaan pengguna "root"](#)

[\[CodeBuild.1\] Repositori sumber CodeBuild Bitbucket tidak URLs boleh berisi kredensial sensitif](#)

[\[CodeBuild.2\] variabel lingkungan CodeBuild proyek tidak boleh berisi kredensial teks yang jelas](#)

[\[Config.1\] AWS Config harus diaktifkan dan menggunakan peran terkait layanan untuk perekaman sumber daya](#)

[\[DMS.1\] Instans replikasi Layanan Migrasi Database tidak boleh bersifat publik](#)

[\[EC2.1\] Cuplikan Amazon EBS tidak boleh dipulihkan secara publik](#)

[\[EC2.2\] Grup keamanan default VPC tidak boleh mengizinkan lalu lintas masuk atau keluar](#)

[\[EC2.6\] Pencatatan aliran VPC harus diaktifkan di semua VPCs](#)

[\[EC2.12\] Amazon yang tidak terpakai EC2 EIPs harus dihapus](#)

[\[EC2.13\] Grup keamanan seharusnya tidak mengizinkan masuknya dari 0.0.0.0/0 atau :/0 ke port 22](#)

[\[ELB.1\] Application Load Balancer harus dikonfigurasi untuk mengalihkan semua permintaan HTTP ke HTTPS](#)

[\[ES.1\] Domain Elasticsearch harus mengaktifkan enkripsi saat istirahat](#)

[\[ES.2\] Domain Elasticsearch tidak boleh diakses publik](#)

[\[GuardDuty.1\] GuardDuty harus diaktifkan](#)

[\[IAM.1\] Kebijakan IAM seharusnya tidak mengizinkan hak administratif “*” penuh](#)

[\[IAM.2\] Pengguna IAM seharusnya tidak memiliki kebijakan IAM yang dilampirkan](#)

[\[IAM.4\] Kunci akses pengguna root IAM seharusnya tidak ada](#)

[\[IAM.6\] MFA perangkat keras harus diaktifkan untuk pengguna root](#)

[\[IAM.8\] Kredensi pengguna IAM yang tidak digunakan harus dihapus](#)

[\[IAM.9\] MFA harus diaktifkan untuk pengguna root](#)

[\[IAM.10\] Kebijakan kata sandi untuk pengguna IAM harus memiliki konfigurasi yang kuat](#)

[\[IAM.19\] MFA harus diaktifkan untuk semua pengguna IAM](#)

[\[KMS.4\] rotasi AWS KMS tombol harus diaktifkan](#)

[\[Lambda.1\] Kebijakan fungsi Lambda harus melarang akses publik](#)

[\[Lambda.3\] Fungsi Lambda harus dalam VPC](#)

[\[Opensearch.1\] OpenSearch domain harus mengaktifkan enkripsi saat istirahat](#)

[\[Opensearch.2\] OpenSearch domain tidak boleh diakses publik](#)

[\[RDS.1\] Snapshot RDS harus bersifat pribadi](#)

[\[RDS.2\] Instans RDS DB harus melarang akses publik, sebagaimana ditentukan oleh konfigurasi PubliclyAccessible](#)

[\[Redshift.1\] Cluster Amazon Redshift harus melarang akses publik](#)

[\[S3.1\] Bucket tujuan umum S3 harus mengaktifkan pengaturan akses publik blok](#)

[\[S3.2\] Bucket tujuan umum S3 harus memblokir akses baca publik](#)

[\[S3.3\] Bucket tujuan umum S3 harus memblokir akses tulis publik](#)

[\[S3.5\] Bucket tujuan umum S3 harus memerlukan permintaan untuk menggunakan SSL](#)

[\[S3.7\] Ember tujuan umum S3 harus menggunakan replikasi lintas wilayah](#)

[\[SageMaker.1\] Instans SageMaker notebook Amazon seharusnya tidak memiliki akses internet langsung](#)

[\[SSM.1\] EC2 Instans Amazon harus dikelola oleh AWS Systems Manager](#)

[\[SSM.2\] EC2 Instans Amazon yang dikelola oleh Systems Manager harus memiliki status kepatuhan patch COMPLIANT setelah instalasi patch](#)

[\[SSM.3\] EC2 Instans Amazon yang dikelola oleh Systems Manager harus memiliki status kepatuhan asosiasi COMPLIANT](#)

Kontrol yang berlaku untuk PCI DSS v4.0.1

Daftar berikut menentukan kontrol AWS Security Hub Cloud Security Posture Management (CSPM) mana yang berlaku untuk PCI DSS v4.0.1. Untuk meninjau detail kontrol, pilih kontrol.

[\[ACM.1\] Sertifikat yang diimpor dan diterbitkan ACM harus diperbarui setelah jangka waktu tertentu](#)

[\[ACM.2\] Sertifikat RSA yang dikelola oleh ACM harus menggunakan panjang kunci minimal 2.048 bit](#)

[\[APIGateway.9\] Pencatatan akses harus dikonfigurasi untuk Tahap API Gateway V2](#)

[\[AppSync.2\] AWS AppSync harus mengaktifkan logging tingkat lapangan](#)

[\[AutoScaling.3\] Konfigurasi peluncuran grup Auto Scaling harus EC2 mengonfigurasi instance agar memerlukan Layanan Metadata Instance Versi 2 \(\) IMDSv2](#)

[\[Autoscaling.5\] Instans EC2 Amazon yang diluncurkan menggunakan konfigurasi peluncuran grup Auto Scaling seharusnya tidak memiliki alamat IP Publik](#)

[\[CloudFront.1\] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi](#)

[\[CloudFront.10\] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal kustom](#)

[\[CloudFront.12\] CloudFront distribusi seharusnya tidak menunjukkan asal S3 yang tidak ada](#)

[\[CloudFront.3\] CloudFront distribusi harus memerlukan enkripsi dalam perjalanan](#)

[\[CloudFront.5\] CloudFront distribusi seharusnya mengaktifkan logging](#)

[\[CloudFront.6\] CloudFront distribusi harus mengaktifkan WAF](#)

[\[CloudFront.9\] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus](#)

[\[CloudTrail.2\] CloudTrail harus mengaktifkan enkripsi saat istirahat](#)

[\[CloudTrail.3\] Setidaknya satu CloudTrail jejak harus diaktifkan](#)

[\[CloudTrail.4\] validasi file CloudTrail log harus diaktifkan](#)

[\[CloudTrail.6\] Pastikan bucket S3 yang digunakan untuk menyimpan CloudTrail log tidak dapat diakses publik](#)

[\[CloudTrail.7\] Pastikan pencatatan akses bucket S3 diaktifkan pada bucket CloudTrail S3](#)

[\[CodeBuild.1\] Repositori sumber CodeBuild Bitbucket tidak URLs boleh berisi kredensial sensitif](#)

[\[CodeBuild.2\] variabel lingkungan CodeBuild proyek tidak boleh berisi kredensial teks yang jelas](#)

[\[CodeBuild.3\] Log CodeBuild S3 harus dienkripsi](#)

[\[DMS.1\] Instans replikasi Layanan Migrasi Database tidak boleh bersifat publik](#)

[\[DMS.10\] Titik akhir DMS untuk database Neptune harus mengaktifkan otorisasi IAM](#)

[\[DMS.11\] Titik akhir DMS untuk MongoDB harus mengaktifkan mekanisme otentikasi](#)

[\[DMS.12\] Titik akhir DMS untuk Redis OSS seharusnya mengaktifkan TLS](#)

[\[DMS.6\] Instans replikasi DMS harus mengaktifkan peningkatan versi minor otomatis](#)

[\[DMS.7\] Tugas replikasi DMS untuk database target seharusnya mengaktifkan logging](#)

[\[DMS.8\] Tugas replikasi DMS untuk database sumber seharusnya mengaktifkan logging](#)

[\[DMS.9\] Titik akhir DMS harus menggunakan SSL](#)

[\[DocumentDB.2\] Cluster Amazon DocumentDB harus memiliki periode retensi cadangan yang memadai](#)

[\[DocumentDB.3\] Cuplikan cluster manual Amazon DocumentDB seharusnya tidak bersifat publik](#)

[\[DocumentDB.4\] Cluster Amazon DocumentDB harus mempublikasikan log audit ke Log CloudWatch](#)

[\[DynamoDB.7\] Cluster DynamoDB Accelerator harus dienkripsi saat transit](#)

[\[EC2.13\] Grup keamanan seharusnya tidak mengizinkan masuknya dari 0.0.0.0/0 atau :/0 ke port 22](#)

[\[EC2.14\] Grup keamanan seharusnya tidak mengizinkan masuknya dari 0.0.0.0/0 atau :/0 ke port 3389](#)

[\[EC2.15\] EC2 Subnet Amazon seharusnya tidak secara otomatis menetapkan alamat IP publik](#)

[\[EC2.16\] Daftar Kontrol Akses Jaringan yang Tidak Digunakan harus dihapus](#)

[\[EC2.170\] templat EC2 peluncuran harus menggunakan Layanan Metadata Instance Versi 2 \(\) IMDSv2](#)

[\[EC2.171\] Koneksi EC2 VPN seharusnya mengaktifkan logging](#)

[\[EC2.21\] Jaringan ACLs seharusnya tidak mengizinkan masuknya dari 0.0.0.0/0 ke port 22 atau port 3389.](#)

[\[EC2.25\] Templat EC2 peluncuran Amazon tidak boleh menetapkan publik IPs ke antarmuka jaringan](#)

[\[EC2.51\] Titik akhir EC2 Client VPN harus mengaktifkan pencatatan koneksi klien](#)

[\[EC2.53\] grup EC2 keamanan seharusnya tidak mengizinkan masuknya dari 0.0.0.0/0 ke port administrasi server jarak jauh](#)

[\[EC2.54\] grup EC2 keamanan tidak boleh mengizinkan masuknya dari :/0 ke port administrasi server jarak jauh](#)

[\[EC2.8\] EC2 instans harus menggunakan Instance Metadata Service Versi 2 \(\) IMDSv2](#)

[\[ECR.1\] Repositori pribadi ECR harus memiliki pemindaian gambar yang dikonfigurasi](#)

[\[ECS.10\] Layanan ECS Fargate harus berjalan pada versi platform Fargate terbaru](#)

[\[ECS.16\] Set tugas ECS seharusnya tidak secara otomatis menetapkan alamat IP publik](#)

[\[ECS.2\] Layanan ECS seharusnya tidak memiliki alamat IP publik yang ditetapkan kepadanya secara otomatis](#)

[\[ECS.8\] Rahasia tidak boleh diteruskan sebagai variabel lingkungan kontainer](#)

[\[EFS.4\] Titik akses EFS harus menegakkan identitas pengguna](#)

[\[EKS.1\] Titik akhir kluster EKS seharusnya tidak dapat diakses publik](#)

[\[EKS.2\] Kluster EKS harus berjalan pada versi Kubernetes yang didukung](#)

[\[EKS.3\] Kluster EKS harus menggunakan rahasia Kubernetes terenkripsi](#)

[\[EKS.8\] Kluster EKS harus mengaktifkan pencatatan audit](#)

[\[ElastiCache.2\] ElastiCache cluster harus mengaktifkan peningkatan versi minor otomatis](#)

[\[ElastiCache.5\] grup ElastiCache replikasi harus dienkripsi saat transit](#)

[\[ElastiCache.6\] ElastiCache \(Redis OSS\) grup replikasi dari versi sebelumnya harus mengaktifkan Redis OSS AUTH](#)

[\[ElasticBeanstalk.2\] Pembaruan platform yang dikelola Elastic Beanstalk harus diaktifkan](#)

[\[ElasticBeanstalk.3\] Elastic Beanstalk harus mengalirkan log ke CloudWatch](#)

[\[ELB.12\] Application Load Balancer harus dikonfigurasi dengan mode mitigasi desync defensif atau paling ketat](#)

[\[ELB.14\] Classic Load Balancer harus dikonfigurasi dengan mode mitigasi desync defensif atau paling ketat](#)

[\[ELB.3\] Pendengar Classic Load Balancer harus dikonfigurasi dengan penghentian HTTPS atau TLS](#)

[\[ELB.4\] Application Load Balancer harus dikonfigurasi untuk menjatuhkan header http yang tidak valid](#)

[\[ELB.8\] Classic Load Balancer dengan pendengar SSL harus menggunakan kebijakan keamanan yang telah ditentukan sebelumnya yang memiliki urasi yang kuat AWS Config](#)

[\[EMR.1\] Node primer kluster EMR Amazon seharusnya tidak memiliki alamat IP publik](#)

[\[EMR.2\] Pengaturan akses publik blok EMR Amazon harus diaktifkan](#)

[\[ES.2\] Domain Elasticsearch tidak boleh diakses publik](#)

[\[ES.3\] Domain Elasticsearch harus mengenkripsi data yang dikirim antar node](#)

[\[ES.5\] Domain Elasticsearch harus mengaktifkan pencatatan audit](#)

[\[ES.8\] Koneksi ke domain Elasticsearch harus dienkripsi menggunakan kebijakan keamanan TLS terbaru](#)

[\[EventBridge.3\] bus acara EventBridge khusus harus memiliki kebijakan berbasis sumber daya terlampir](#)

[\[GuardDuty.1\] GuardDuty harus diaktifkan](#)

[\[GuardDuty.10\] Perlindungan GuardDuty S3 harus diaktifkan](#)

[\[GuardDuty.6\] Perlindungan GuardDuty Lambda harus diaktifkan](#)

[\[GuardDuty.7\] GuardDuty EKS Runtime Monitoring harus diaktifkan](#)

[\[GuardDuty.9\] Perlindungan GuardDuty RDS harus diaktifkan](#)

[\[IAM.11\] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu huruf besar](#)

[\[IAM.12\] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu huruf kecil](#)

[\[IAM.13\] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu simbol](#)

[\[IAM.14\] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu nomor](#)

[\[IAM.16\] Pastikan kebijakan kata sandi IAM mencegah penggunaan kembali kata sandi](#)

[\[IAM.17\] Pastikan kebijakan kata sandi IAM kedaluwarsa kata sandi dalam waktu 90 hari atau kurang](#)

[\[IAM.18\] Memastikan peran dukungan telah dibuat untuk mengelola insiden dengan AWS Dukungan](#)

[\[IAM.19\] MFA harus diaktifkan untuk semua pengguna IAM](#)

[\[IAM.3\] Kunci akses pengguna IAM harus diputar setiap 90 hari atau kurang](#)

[\[IAM.5\] MFA harus diaktifkan untuk semua pengguna IAM yang memiliki kata sandi konsol](#)

[\[IAM.6\] MFA perangkat keras harus diaktifkan untuk pengguna root](#)

[\[IAM.7\] Kebijakan kata sandi untuk pengguna IAM harus memiliki konfigurasi yang kuat](#)

[\[IAM.8\] Kredensi pengguna IAM yang tidak digunakan harus dihapus](#)

[\[IAM.9\] MFA harus diaktifkan untuk pengguna root](#)

[\[Inspektor.1\] Pemindaian Amazon Inspector harus diaktifkan EC2](#)

[\[Inspektor.2\] Pemindaian ECR Amazon Inspector harus diaktifkan](#)

[\[Inspektor.3\] Pemindaian kode Amazon Inspector Lambda harus diaktifkan](#)

[\[Inspektor.4\] Pemindaian standar Amazon Inspector Lambda harus diaktifkan](#)

[\[KMS.4\] rotasi AWS KMS tombol harus diaktifkan](#)

[\[Lambda.1\] Kebijakan fungsi Lambda harus melarang akses publik](#)

[\[Lambda.2\] Fungsi Lambda harus menggunakan runtime yang didukung](#)

[\[MQ.2\] Broker ActiveMQ harus mengalirkan log audit ke CloudWatch](#)

[\[MQ.3\] Broker Amazon MQ harus mengaktifkan peningkatan versi minor otomatis](#)

[\[MSK.1\] Kluster MSK harus dienkrpsi saat transit di antara node broker](#)

[\[MSK.3\] Konektor MSK Connect harus dienkrpsi saat transit](#)

[\[Neptune.2\] Cluster DB Neptunus harus menerbitkan log audit ke Log CloudWatch](#)

[\[Neptune.3\] Snapshot cluster Neptunus DB seharusnya tidak publik](#)

[\[Opensearch.10\] OpenSearch domain harus menginstal pembaruan perangkat lunak terbaru](#)

[\[Opensearch.5\] OpenSearch domain harus mengaktifkan pencatatan audit](#)

[\[RDS.13\] Peningkatan versi minor otomatis RDS harus diaktifkan](#)

[\[RDS.2\] Instans RDS DB harus melarang akses publik, sebagaimana ditentukan oleh konfigurasi PubliclyAccessible](#)

[\[RDS.20\] Langganan pemberitahuan acara RDS yang ada harus dikonfigurasi untuk peristiwa instance basis data penting](#)

[\[RDS.21\] Langganan pemberitahuan acara RDS harus dikonfigurasi untuk peristiwa grup parameter basis data penting](#)

[\[RDS.22\] Langganan pemberitahuan acara RDS harus dikonfigurasi untuk acara grup keamanan basis data penting](#)

[\[RDS.24\] Kluster Database RDS harus menggunakan nama pengguna administrator khusus](#)

[\[RDS.25\] Instans database RDS harus menggunakan nama pengguna administrator khusus](#)

[\[RDS.34\] Kluster Aurora MySQL DB harus menerbitkan log audit ke Log CloudWatch](#)

[\[RDS.35\] Cluster RDS DB harus mengaktifkan peningkatan versi minor otomatis](#)

[\[RDS.36\] RDS untuk instance PostgreSQL DB harus menerbitkan log ke Log CloudWatch](#)

[\[RDS.37\] Cluster Aurora PostgreSQL DB harus menerbitkan log ke Log CloudWatch](#)

[\[RDS.9\] Instans RDS DB harus menerbitkan log ke Log CloudWatch](#)

[\[Redshift.1\] Cluster Amazon Redshift harus melarang akses publik](#)

[\[Redshift.15\] Grup keamanan Redshift harus mengizinkan masuknya port cluster hanya dari asal yang dibatasi](#)

[\[Redshift.2\] Koneksi ke cluster Amazon Redshift harus dienkripsi saat transit](#)

[\[Redshift.4\] Cluster Amazon Redshift harus mengaktifkan pencatatan audit](#)

[\[Route53.2\] Route 53 zona yang dihosting publik harus mencatat kueri DNS](#)

[\[S3.1\] Bucket tujuan umum S3 harus mengaktifkan pengaturan akses publik blok](#)

[\[S3.15\] Bucket tujuan umum S3 harus mengaktifkan Object Lock](#)

[\[S3.17\] Ember tujuan umum S3 harus dienkripsi saat istirahat AWS KMS keys](#)

[\[S3.19\] Titik akses S3 harus mengaktifkan pengaturan akses publik blok](#)

[\[S3.22\] Bucket tujuan umum S3 harus mencatat peristiwa penulisan tingkat objek](#)

[\[S3.23\] Bucket tujuan umum S3 harus mencatat peristiwa pembacaan tingkat objek](#)

[\[S3.24\] Poin Akses Multi-Wilayah S3 harus mengaktifkan pengaturan akses publik blok](#)

[\[S3.5\] Bucket tujuan umum S3 harus memerlukan permintaan untuk menggunakan SSL](#)

[\[S3.8\] Bucket tujuan umum S3 harus memblokir akses publik](#)

[\[S3.9\] Bucket tujuan umum S3 harus mengaktifkan pencatatan akses server](#)

[\[SageMaker.1\] Instans SageMaker notebook Amazon seharusnya tidak memiliki akses internet langsung](#)

[\[SecretsManager.1\] Rahasia Secrets Manager harus mengaktifkan rotasi otomatis](#)

[\[SecretsManager.2\] Rahasia Secrets Manager yang dikonfigurasi dengan rotasi otomatis harus berhasil diputar](#)

[\[SecretsManager.4\] Rahasia Secrets Manager harus diputar dalam jumlah hari tertentu](#)

[\[SSM.2\] EC2 Instans Amazon yang dikelola oleh Systems Manager harus memiliki status kepatuhan patch COMPLIANT setelah instalasi patch](#)

[\[SSM.3\] EC2 Instans Amazon yang dikelola oleh Systems Manager harus memiliki status kepatuhan asosiasi COMPLIANT](#)

[\[StepFunctions.1\] Mesin status Step Functions seharusnya mengaktifkan logging](#)

[\[Transfer.2\] Server Transfer Family tidak boleh menggunakan protokol FTP untuk koneksi titik akhir](#)

[\[WAF.1\] Pencatatan ACL Web Global AWS WAF Klasik harus diaktifkan](#)

[\[WAF.11\] pencatatan ACL AWS WAF web harus diaktifkan](#)

Standar yang dikelola layanan di Security Hub CSPM

Standar yang dikelola layanan adalah standar keamanan yang Layanan AWS dikelola orang lain tetapi dapat Anda lihat di Security Hub CSPM. Misalnya, [Service-Managed Standard: AWS Control Tower](#) adalah standar yang dikelola layanan yang mengelola. AWS Control Tower Standar yang dikelola layanan berbeda dari standar keamanan yang dikelola Security Hub Cloud AWS Security Posture Management (CSPM) dengan cara berikut:

- Pembuatan dan penghapusan standar — Anda membuat dan menghapus standar yang dikelola layanan dengan konsol atau API layanan pengelola, atau dengan. AWS CLI Sampai Anda membuat standar dalam layanan pengelolaan dengan salah satu cara tersebut, standar tidak

muncul di konsol CSPM Security Hub dan tidak dapat diakses oleh Security Hub CSPM API atau AWS CLI

- Tidak ada pengaktifan kontrol otomatis — Saat Anda membuat standar yang dikelola layanan, CSPM Security Hub dan layanan pengelola tidak secara otomatis mengaktifkan kontrol yang berlaku pada standar. Selain itu, ketika Security Hub CSPM merilis kontrol baru untuk standar, kontrol tersebut tidak diaktifkan secara otomatis. Ini adalah penyimpangan dari standar yang dikelola Security Hub CSPM. Untuk informasi selengkapnya tentang cara biasa mengonfigurasi kontrol di Security Hub CSPM, lihat. [Memahami kontrol keamanan di Security Hub CSPM](#)
- Mengaktifkan dan menonaktifkan kontrol — Kami menyarankan untuk mengaktifkan dan menonaktifkan kontrol dalam layanan pengelolaan untuk menghindari penyimpangan.
- Ketersediaan kontrol — Layanan pengelola memilih kontrol mana yang tersedia sebagai bagian dari standar yang dikelola layanan. Kontrol yang tersedia dapat mencakup semua, atau sebagian dari, kontrol CSPM Security Hub yang ada.

Setelah mengelola layanan membuat standar yang dikelola layanan dan menyediakan kontrol untuk itu, Anda dapat mengakses temuan kontrol, status kontrol, dan skor keamanan standar di konsol CSPM Security Hub, Security Hub CSPM API, atau AWS CLI Beberapa atau semua informasi ini mungkin juga tersedia di layanan pengelolaan.

Pilih standar yang dikelola layanan dari daftar berikut untuk melihat detail selengkapnya.

Standar yang dikelola layanan

- [Standar yang Dikelola Layanan: AWS Control Tower](#)

Standar yang Dikelola Layanan: AWS Control Tower

Bagian ini memberikan informasi tentang Standar yang Dikelola Layanan: AWS Control Tower

Apa itu Standar yang Dikelola Layanan? AWS Control Tower

Standar ini dirancang untuk pengguna AWS Security Hub Cloud Security Posture Management (CSPM) dan AWS Control Tower. Ini memungkinkan Anda mengonfigurasi kontrol proaktif AWS Control Tower di samping kontrol detektif Security Hub CSPM dalam layanan. AWS Control Tower

Kontrol proaktif membantu memastikan bahwa Akun AWS mempertahankan kepatuhan karena mereka menandai tindakan yang dapat menyebabkan pelanggaran kebijakan atau kesalahan konfigurasi. Kontrol Detektif mendeteksi ketidakpatuhan sumber daya (misalnya, kesalahan

konfigurasi) di dalam Anda. Akun AWS Dengan mengaktifkan kontrol proaktif dan detektif untuk AWS lingkungan Anda, Anda dapat meningkatkan postur keamanan Anda pada berbagai tahap pengembangan.

 Tip

Standar yang dikelola layanan berbeda dari standar yang dikelola AWS Security Hub Cloud Security Posture Management (CSPM). Misalnya, Anda harus membuat dan menghapus standar yang dikelola layanan di layanan pengelolaan. Untuk informasi selengkapnya, lihat [Standar yang dikelola layanan di Security Hub CSPM](#).

Di konsol dan API CSPM Security Hub, Anda dapat melihat Standar yang Dikelola Layanan: bersama standar CSPM AWS Control Tower Security Hub lainnya.

Menciptakan standar

Standar ini hanya tersedia jika Anda membuat standar di AWS Control Tower. AWS Control Tower membuat standar saat Anda pertama kali mengaktifkan kontrol yang berlaku dengan menggunakan salah satu metode berikut:

- AWS Control Tower konsol
- AWS Control Tower API (panggil [EnableControl](#)API)
- AWS CLI (jalankan [enable-control](#)perintah)

Kontrol CSPM Security Hub diidentifikasi di AWS Control Tower konsol sebagai SH.

ControlID(misalnya, SH. CodeBuild.1).

Ketika Anda membuat standar, jika Anda belum mengaktifkan Security Hub CSPM, AWS Control Tower juga mengaktifkan Security Hub CSPM untuk Anda.

Jika belum menyiapkan AWS Control Tower, Anda tidak dapat melihat atau mengakses standar ini di konsol CSPM Security Hub, Security Hub CSPM API, atau. AWS CLI Bahkan jika Anda telah menyiapkan AWS Control Tower, Anda tidak dapat melihat atau mengakses standar ini di Security Hub CSPM tanpa terlebih dahulu membuat standar dalam AWS Control Tower menggunakan salah satu metode sebelumnya.

Standar ini hanya tersedia di [Wilayah AWS tempat yang AWS Control Tower tersedia](#), termasuk AWS GovCloud (US).

Mengaktifkan dan menonaktifkan kontrol dalam standar

Setelah Anda membuat standar di AWS Control Tower konsol, Anda dapat melihat standar dan kontrol yang tersedia di kedua layanan.

Setelah Anda pertama kali membuat standar, itu tidak memiliki kontrol apa pun yang diaktifkan secara otomatis. Selain itu, ketika Security Hub CSPM menambahkan kontrol baru, kontrol tersebut tidak diaktifkan secara otomatis untuk Standar yang Dikelola Layanan:. AWS Control Tower Anda harus mengaktifkan dan menonaktifkan kontrol untuk standar AWS Control Tower dengan menggunakan salah satu metode berikut:

- AWS Control Tower konsol
- AWS Control Tower API (panggil [EnableControl](#) dan [DisableControl](#) APIs)
- AWS CLI (jalankan [enable-control](#) dan [disable-control](#) perintah)

Saat Anda mengubah status pengaktifan kontrol AWS Control Tower, perubahan tersebut juga tercermin dalam Security Hub CSPM.

Namun, menonaktifkan kontrol di Security Hub CSPM yang diaktifkan AWS Control Tower menghasilkan penyimpangan kontrol. Status kontrol di AWS Control Tower menunjukkan sebagai *Drifted*. Anda dapat mengatasi penyimpangan ini dengan memilih [Registrasi ulang OU](#) di AWS Control Tower konsol, atau dengan menonaktifkan dan mengaktifkan kembali kontrol dalam AWS Control Tower menggunakan salah satu metode sebelumnya.

Menyelesaikan tindakan pemberdayaan dan penonaktifan AWS Control Tower membantu Anda menghindari penyimpangan kontrol.

Saat Anda mengaktifkan atau menonaktifkan kontrol AWS Control Tower, tindakan akan berlaku di seluruh akun dan Wilayah. Jika Anda mengaktifkan dan menonaktifkan kontrol di Security Hub CSPM (tidak disarankan untuk standar ini), tindakan hanya berlaku untuk akun saat ini dan Wilayah.

Note

[Konfigurasi pusat](#) tidak dapat digunakan untuk mengelola Standar yang Dikelola Layanan:. AWS Control Tower Jika Anda menggunakan konfigurasi pusat, Anda hanya dapat menggunakan AWS Control Tower layanan untuk mengaktifkan dan menonaktifkan kontrol dalam standar ini untuk akun yang dikelola secara terpusat.

Melihat status pemberdayaan dan status kontrol

Anda dapat melihat status pemberdayaan kontrol dengan menggunakan salah satu metode berikut:

- Konsol CSPM Security Hub, Security Hub CSPM API, atau AWS CLI
- AWS Control Tower konsol
- AWS Control Tower API untuk melihat daftar kontrol yang diaktifkan (panggil [ListEnabledControlsAPI](#))
- AWS CLI untuk melihat daftar kontrol yang diaktifkan (jalankan [list-enabled-controls](#) perintah)

Kontrol yang Anda nonaktifkan AWS Control Tower memiliki status pengaktifan Disabled di Security Hub CSPM kecuali Anda secara eksplisit mengaktifkan kontrol tersebut di Security Hub CSPM.

Security Hub CSPM menghitung status kontrol berdasarkan status alur kerja dan status kepatuhan dari temuan kontrol. Untuk informasi selengkapnya tentang status pemberdayaan dan status kontrol, lihat [Meninjau rincian kontrol di Security Hub CSPM](#).

Berdasarkan status kontrol, Security Hub CSPM menghitung [skor keamanan](#) untuk Service-Managed Standard. AWS Control Tower Skor ini hanya tersedia di Security Hub CSPM. Selain itu, Anda hanya dapat melihat [temuan kontrol](#) di Security Hub CSPM. Skor keamanan standar dan temuan kontrol tidak tersedia di AWS Control Tower.

Note

Saat Anda mengaktifkan kontrol untuk Standar yang Dikelola Layanan: AWS Control Tower, CSPM Security Hub dapat memakan waktu hingga 18 jam untuk menghasilkan temuan untuk kontrol yang menggunakan aturan terkait layanan yang ada. AWS Config Anda mungkin memiliki aturan terkait layanan yang ada jika Anda telah mengaktifkan standar dan kontrol lain di CSPM Security Hub. Untuk informasi selengkapnya, lihat [Jadwal untuk menjalankan pemeriksaan keamanan](#).

Menghapus standar

Anda dapat menghapus standar ini AWS Control Tower dengan menonaktifkan semua kontrol yang berlaku menggunakan salah satu metode berikut:

- AWS Control Tower konsol
- AWS Control Tower API (panggil [DisableControlAPI](#))
- AWS CLI (jalankan [disable-control](#) perintah)

Menonaktifkan semua kontrol akan menghapus standar di semua akun terkelola dan Wilayah yang diatur di. AWS Control Tower Menghapus standar di AWS Control Tower menghapusnya dari halaman Standar konsol CSPM Security Hub, dan Anda tidak dapat lagi mengaksesnya dengan menggunakan Security Hub CSPM API atau. AWS CLI

 Note

Menonaktifkan semua kontrol dari standar di Security Hub CSPM tidak menonaktifkan atau menghapus standar.

Menonaktifkan layanan CSPM Security Hub akan menghapus Standar yang Dikelola Layanan: AWS Control Tower dan standar lain yang telah Anda aktifkan.

Menemukan format bidang untuk Standar yang Dikelola Layanan: AWS Control Tower

Ketika Anda membuat Service-Managed Standard: AWS Control Tower dan mengaktifkan kontrol untuk itu, Anda akan mulai menerima temuan kontrol di Security Hub CSPM. Security Hub CSPM melaporkan temuan kontrol di. [AWS Format Pencarian Keamanan \(ASFF\)](#) Ini adalah nilai ASFF untuk Amazon Resource Name (ARN) standar ini dan: GeneratorId

- ARN standar — `arn:aws:us-east-1:securityhub:::standards/service-managed-aws-control-tower/v/1.0.0`
- GeneratorId – `service-managed-aws-control-tower/v/1.0.0/CodeBuild.1`

Untuk contoh temuan Standar yang Dikelola Layanan: AWS Control Tower, lihat. [Sampel temuan kontrol](#)

Kontrol yang berlaku untuk Standar yang Dikelola Layanan: AWS Control Tower

Service-Managed Standard: AWS Control Tower mendukung subset kontrol yang merupakan bagian dari standar AWS Foundational Security Best Practices (FSBP). Pilih kontrol untuk melihat informasi tentangnya, termasuk langkah-langkah remediasi untuk temuan yang gagal.

Daftar berikut menunjukkan kontrol yang tersedia untuk Standar yang Dikelola Layanan: AWS Control Tower Batas regional pada kontrol cocok dengan batas Regional pada kontrol wajar dalam standar FSBP. Daftar ini menunjukkan kontrol keamanan agnostik standar. IDs Di AWS Control Tower konsol, kontrol IDs diformat sebagai SH. **ControlID**(misalnya SH. CodeBuild.1). Di Security Hub CSPM, jika [temuan kontrol konsolidasi](#) dimatikan di akun Anda, `ProductFields.ControlId` bidang tersebut menggunakan ID kontrol berbasis standar. ID kontrol berbasis standar diformat sebagai CT. **ControlId**(misalnya, CT. CodeBuild.1).

- [\[Akun.1\] Informasi kontak keamanan harus disediakan untuk Akun AWS](#)
- [\[ACM.1\] Sertifikat yang diimpor dan diterbitkan ACM harus diperbarui setelah jangka waktu tertentu](#)
- [\[ACM.2\] Sertifikat RSA yang dikelola oleh ACM harus menggunakan panjang kunci minimal 2.048 bit](#)
- [\[APIGateway.1\] API Gateway REST dan pencatatan eksekusi WebSocket API harus diaktifkan](#)
- [\[APIGateway.2\] Tahapan API Gateway REST API harus dikonfigurasi untuk menggunakan sertifikat SSL untuk otentikasi backend](#)
- [\[APIGateway.3\] Tahapan API Gateway REST API harus mengaktifkan AWS X-Ray penelusuran](#)
- [\[APIGateway.4\] API Gateway harus dikaitkan dengan ACL Web WAF](#)
- [\[APIGateway.5\] Data cache API Gateway REST API harus dienkripsi saat istirahat](#)
- [\[APIGateway.8\] Rute API Gateway harus menentukan jenis otorisasi](#)
- [\[APIGateway.9\] Pencatatan akses harus dikonfigurasi untuk Tahap API Gateway V2](#)
- [\[AppSync.5\] AWS AppSync APIs GraphQL tidak boleh diautentikasi dengan kunci API](#)
- [\[AutoScaling.1\] Grup Auto Scaling yang terkait dengan penyeimbang beban harus menggunakan pemeriksaan kesehatan ELB](#)
- [\[AutoScaling.2\] Grup EC2 Auto Scaling Amazon harus mencakup beberapa Availability Zone](#)
- [\[AutoScaling.3\] Konfigurasi peluncuran grup Auto Scaling harus EC2 mengonfigurasi instance agar memerlukan Layanan Metadata Instance Versi 2 \(\) IMDSv2](#)
- [\[Autoscaling.5\] Instans EC2 Amazon yang diluncurkan menggunakan konfigurasi peluncuran grup Auto Scaling seharusnya tidak memiliki alamat IP Publik](#)
- [\[AutoScaling.6\] Grup Auto Scaling harus menggunakan beberapa jenis instance di beberapa Availability Zone](#)
- [\[AutoScaling.9\] Grup EC2 Auto Scaling Amazon harus menggunakan templat peluncuran Amazon EC2](#)

- [\[CloudTrail.1\] CloudTrail harus diaktifkan dan dikonfigurasi dengan setidaknya satu jejak Multi-wilayah yang mencakup acara manajemen baca dan tulis](#)
- [\[CloudTrail.2\] CloudTrail harus mengaktifkan enkripsi saat istirahat](#)
- [\[CloudTrail.4\] validasi file CloudTrail log harus diaktifkan](#)
- [\[CloudTrail.5\] CloudTrail jalur harus diintegrasikan dengan Amazon Logs CloudWatch](#)
- [\[CloudTrail.6\] Pastikan bucket S3 yang digunakan untuk menyimpan CloudTrail log tidak dapat diakses publik](#)
- [\[CodeBuild.1\] Repositori sumber CodeBuild Bitbucket tidak URLs boleh berisi kredensial sensitif](#)
- [\[CodeBuild.2\] variabel lingkungan CodeBuild proyek tidak boleh berisi kredensial teks yang jelas](#)
- [\[CodeBuild.3\] Log CodeBuild S3 harus dienkripsi](#)
- [\[CodeBuild.4\] lingkungan CodeBuild proyek harus memiliki urasi logging AWS Config](#)
- [\[DMS.1\] Instans replikasi Layanan Migrasi Database tidak boleh bersifat publik](#)
- [\[DMS.9\] Titik akhir DMS harus menggunakan SSL](#)
- [\[DocumentDB.1\] Cluster Amazon DocumentDB harus dienkripsi saat istirahat](#)
- [\[DocumentDB.2\] Cluster Amazon DocumentDB harus memiliki periode retensi cadangan yang memadai](#)
- [\[DocumentDB.3\] Cuplikan cluster manual Amazon DocumentDB seharusnya tidak bersifat publik](#)
- [\[DynamoDB.1\] Tabel DynamoDB harus secara otomatis menskalakan kapasitas sesuai permintaan](#)
- [\[DynamoDB.2\] Tabel DynamoDB harus mengaktifkan pemulihan point-in-time](#)
- [\[DynamoDB.3\] Cluster DynamoDB Accelerator \(DAX\) harus dienkripsi saat istirahat](#)
- [\[EC2.1\] Cuplikan Amazon EBS tidak boleh dipulihkan secara publik](#)
- [\[EC2.2\] Grup keamanan default VPC tidak boleh mengizinkan lalu lintas masuk atau keluar](#)
- [\[EC2.3\] Volume Amazon EBS yang terlampir harus dienkripsi saat istirahat](#)
- [\[EC2.4\] EC2 Instans yang dihentikan harus dihapus setelah periode waktu tertentu](#)
- [\[EC2.6\] Pencatatan aliran VPC harus diaktifkan di semua VPCs](#)
- [\[EC2.7\] Enkripsi default EBS harus diaktifkan](#)
- [\[EC2.8\] EC2 instans harus menggunakan Instance Metadata Service Versi 2 \(\) IMDSv2](#)
- [\[EC2.9\] EC2 Instans Amazon seharusnya tidak memiliki alamat publik IPv4](#)
- [\[EC2.10\] Amazon EC2 harus dikonfigurasi untuk menggunakan titik akhir VPC yang dibuat untuk layanan Amazon EC2](#)
- [\[EC2.15\] EC2 Subnet Amazon seharusnya tidak secara otomatis menetapkan alamat IP publik](#)

- [\[EC2.16\] Daftar Kontrol Akses Jaringan yang Tidak Digunakan harus dihapus](#)
- [\[EC2.17\] EC2 Instans Amazon seharusnya tidak menggunakan banyak ENIs](#)
- [\[EC2.18\] Grup keamanan seharusnya hanya mengizinkan lalu lintas masuk yang tidak terbatas untuk port resmi](#)
- [\[EC2.19\] Kelompok keamanan tidak boleh mengizinkan akses tidak terbatas ke port dengan risiko tinggi](#)
- [\[EC2.20\] Kedua terowongan VPN untuk koneksi AWS Site-to-Site VPN harus siap](#)
- [\[EC2.21\] Jaringan ACLs seharusnya tidak mengizinkan masuknya dari 0.0.0.0/0 ke port 22 atau port 3389.](#)
- [\[EC2.22\] Grup EC2 keamanan Amazon yang tidak digunakan harus dihapus](#)
- [\[EC2.23\] Amazon EC2 Transit Gateways seharusnya tidak secara otomatis menerima permintaan lampiran VPC](#)
- [\[EC2.25\] Templat EC2 peluncuran Amazon tidak boleh menetapkan publik IPs ke antarmuka jaringan](#)
- [\[ECR.1\] Repositori pribadi ECR harus memiliki pemindaian gambar yang dikonfigurasi](#)
- [\[ECR.2\] Repositori pribadi ECR harus memiliki kekekalan tag yang dikonfigurasi](#)
- [\[ECR.3\] Repositori ECR harus memiliki setidaknya satu kebijakan siklus hidup yang dikonfigurasi](#)
- [\[ECS.1\] Definisi tugas Amazon ECS harus memiliki mode jaringan yang aman dan definisi pengguna](#)
- [\[ECS.2\] Layanan ECS seharusnya tidak memiliki alamat IP publik yang ditetapkan kepadanya secara otomatis](#)
- [\[ECS.3\] Definisi tugas ECS tidak boleh membagikan namespace proses host](#)
- [\[ECS.4\] Kontainer ECS harus berjalan sebagai non-hak istimewa](#)
- [\[ECS.5\] Wadah ECS harus dibatasi pada akses hanya-baca ke sistem file root](#)
- [\[ECS.8\] Rahasia tidak boleh diteruskan sebagai variabel lingkungan kontainer](#)
- [\[ECS.10\] Layanan ECS Fargate harus berjalan pada versi platform Fargate terbaru](#)
- [\[ECS.12\] Cluster ECS harus menggunakan Wawasan Kontainer](#)
- [\[EFS.1\] Sistem File Elastis harus dikonfigurasi untuk mengenkripsi data file saat istirahat menggunakan AWS KMS](#)
- [\[EFS.2\] Volume Amazon EFS harus dalam rencana cadangan](#)
- [\[EFS.3\] Titik akses EFS harus menegakkan direktori root](#)
- [\[EFS.4\] Titik akses EFS harus menegakkan identitas pengguna](#)

- [\[EKS.1\] Titik akhir kluster EKS seharusnya tidak dapat diakses publik](#)
- [\[EKS.2\] Kluster EKS harus berjalan pada versi Kubernetes yang didukung](#)
- [\[ElastiCache.3\] grup ElastiCache replikasi harus mengaktifkan failover otomatis](#)
- [\[ElastiCache.4\] grup ElastiCache replikasi harus dienkripsi saat istirahat](#)
- [\[ElastiCache.5\] grup ElastiCache replikasi harus dienkripsi saat transit](#)
- [\[ElastiCache.6\] ElastiCache \(Redis OSS\) grup replikasi dari versi sebelumnya harus mengaktifkan Redis OSS AUTH](#)
- [\[ElasticBeanstalk.1\] Lingkungan Elastic Beanstalk seharusnya mengaktifkan pelaporan kesehatan yang ditingkatkan](#)
- [\[ElasticBeanstalk.2\] Pembaruan platform yang dikelola Elastic Beanstalk harus diaktifkan](#)
- [\[ELB.1\] Application Load Balancer harus dikonfigurasi untuk mengalihkan semua permintaan HTTP ke HTTPS](#)
- [\[ELB.2\] Classic Load Balancer dengan pendengar SSL/HTTPS harus menggunakan sertifikat yang disediakan oleh AWS Certificate Manager](#)
- [\[ELB.3\] Pendengar Classic Load Balancer harus dikonfigurasi dengan penghentian HTTPS atau TLS](#)
- [\[ELB.4\] Application Load Balancer harus dikonfigurasi untuk menjatuhkan header http yang tidak valid](#)
- [\[ELB.5\] Pencatatan aplikasi dan Classic Load Balancer harus diaktifkan](#)
- [\[ELB.6\] Aplikasi, Gateway, dan Network Load Balancer harus mengaktifkan perlindungan penghapusan](#)
- [\[ELB.7\] Classic Load Balancers harus mengaktifkan pengurusan koneksi](#)
- [\[ELB.8\] Classic Load Balancer dengan pendengar SSL harus menggunakan kebijakan keamanan yang telah ditentukan sebelumnya yang memiliki urasi yang kuat AWS Config](#)
- [\[ELB.9\] Classic Load Balancer harus mengaktifkan penyeimbangan beban lintas zona](#)
- [\[ELB.10\] Classic Load Balancer harus menjangkau beberapa Availability Zone](#)
- [\[ELB.12\] Application Load Balancer harus dikonfigurasi dengan mode mitigasi desync defensif atau paling ketat](#)
- [\[ELB.13\] Penyeimbang Beban Aplikasi, Jaringan, dan Gateway harus mencakup beberapa Availability Zone](#)
- [\[ELB.14\] Classic Load Balancer harus dikonfigurasi dengan mode mitigasi desync defensif atau paling ketat](#)

- [\[EMR.1\] Node primer kluster EMR Amazon seharusnya tidak memiliki alamat IP publik](#)
- [\[ES.1\] Domain Elasticsearch harus mengaktifkan enkripsi saat istirahat](#)
- [\[ES.2\] Domain Elasticsearch tidak boleh diakses publik](#)
- [\[ES.3\] Domain Elasticsearch harus mengenkripsi data yang dikirim antar node](#)
- [\[ES.4\] Kesalahan domain Elasticsearch yang masuk ke CloudWatch Log harus diaktifkan](#)
- [\[ES.5\] Domain Elasticsearch harus mengaktifkan pencatatan audit](#)
- [\[ES.6\] Domain Elasticsearch harus memiliki setidaknya tiga node data](#)
- [\[ES.7\] Domain Elasticsearch harus dikonfigurasi dengan setidaknya tiga node master khusus](#)
- [\[ES.8\] Koneksi ke domain Elasticsearch harus dienkripsi menggunakan kebijakan keamanan TLS terbaru](#)
- [\[EventBridge.3\] bus acara EventBridge khusus harus memiliki kebijakan berbasis sumber daya terlampir](#)
- [\[GuardDuty.1\] GuardDuty harus diaktifkan](#)
- [\[IAM.1\] Kebijakan IAM seharusnya tidak mengizinkan hak administratif “*” penuh](#)
- [\[IAM.2\] Pengguna IAM seharusnya tidak memiliki kebijakan IAM yang dilampirkan](#)
- [\[IAM.3\] Kunci akses pengguna IAM harus diputar setiap 90 hari atau kurang](#)
- [\[IAM.4\] Kunci akses pengguna root IAM seharusnya tidak ada](#)
- [\[IAM.5\] MFA harus diaktifkan untuk semua pengguna IAM yang memiliki kata sandi konsol](#)
- [\[IAM.6\] MFA perangkat keras harus diaktifkan untuk pengguna root](#)
- [\[IAM.7\] Kebijakan kata sandi untuk pengguna IAM harus memiliki konfigurasi yang kuat](#)
- [\[IAM.8\] Kredensi pengguna IAM yang tidak digunakan harus dihapus](#)
- [\[IAM.21\] Kebijakan terkelola pelanggan IAM yang Anda buat seharusnya tidak mengizinkan tindakan wildcard untuk layanan](#)
- [\[Kinesis.1\] Aliran kinesis harus dienkripsi saat istirahat](#)
- [\[KMS.1\] Kebijakan yang dikelola pelanggan IAM tidak boleh mengizinkan tindakan dekripsi pada semua kunci KMS](#)
- [\[KMS.2\] Prinsipal IAM tidak boleh memiliki kebijakan inline IAM yang memungkinkan tindakan dekripsi pada semua kunci KMS](#)
- [\[KMS.3\] tidak AWS KMS keys boleh dihapus secara tidak sengaja](#)
- [\[KMS.4\] rotasi AWS KMS tombol harus diaktifkan](#)
- [\[Lambda.1\] Kebijakan fungsi Lambda harus melarang akses publik](#)

- [\[Lambda.2\] Fungsi Lambda harus menggunakan runtime yang didukung](#)
- [\[Lambda.3\] Fungsi Lambda harus dalam VPC](#)
- [\[Lambda.5\] Fungsi VPC Lambda harus beroperasi di beberapa Availability Zone](#)
- [\[MSK.1\] Kluster MSK harus dienkripsi saat transit di antara node broker](#)
- [\[MQ.5\] Broker ActiveMQ harus menggunakan mode penerapan aktif/siaga](#)
- [\[MQ.6\] Broker RabbitMQ harus menggunakan mode penerapan cluster](#)
- [\[Neptunus.1\] Cluster DB Neptunus harus dienkripsi saat istirahat](#)
- [\[Neptune.2\] Cluster DB Neptunus harus menerbitkan log audit ke Log CloudWatch](#)
- [\[Neptune.3\] Snapshot cluster Neptunus DB seharusnya tidak publik](#)
- [\[Neptunus.4\] Cluster DB Neptunus harus mengaktifkan perlindungan penghapusan](#)
- [\[Neptunus.5\] Cluster DB Neptunus harus mengaktifkan cadangan otomatis](#)
- [\[Neptune.6\] Snapshot cluster Neptunus DB harus dienkripsi saat istirahat](#)
- [\[Neptune.7\] Cluster DB Neptunus harus mengaktifkan otentikasi basis data IAM](#)
- [\[Neptunus.8\] Cluster DB Neptunus harus dikonfigurasi untuk menyalin tag ke snapshot](#)
- [\[NetworkFirewall.3\] Kebijakan Network Firewall harus memiliki setidaknya satu kelompok aturan yang terkait](#)
- [\[NetworkFirewall.4\] Tindakan stateless default untuk kebijakan Network Firewall harus drop atau forward untuk paket penuh](#)
- [\[NetworkFirewall.5\] Tindakan stateless default untuk kebijakan Network Firewall harus drop atau forward untuk paket yang terfragmentasi](#)
- [\[NetworkFirewall.6\] Grup aturan Stateless Network Firewall tidak boleh kosong](#)
- [\[Opensearch.1\] OpenSearch domain harus mengaktifkan enkripsi saat istirahat](#)
- [\[Opensearch.2\] OpenSearch domain tidak boleh diakses publik](#)
- [\[Opensearch.3\] OpenSearch domain harus mengenkripsi data yang dikirim antar node](#)
- [\[Opensearch.4\] login kesalahan OpenSearch domain ke Log harus diaktifkan CloudWatch](#)
- [\[Opensearch.5\] OpenSearch domain harus mengaktifkan pencatatan audit](#)
- [\[Opensearch.6\] OpenSearch domain harus memiliki setidaknya tiga node data](#)
- [\[Opensearch.7\] OpenSearch domain harus mengaktifkan kontrol akses berbutir halus](#)
- [\[Opensearch.8\] Koneksi ke OpenSearch domain harus dienkripsi menggunakan kebijakan keamanan TLS terbaru](#)

- [\[RDS.1\] Snapshot RDS harus bersifat pribadi](#)
- [\[RDS.2\] Instans RDS DB harus melarang akses publik, sebagaimana ditentukan oleh konfigurasi `PubliclyAccessible`](#)
- [\[RDS.3\] Instans RDS DB harus mengaktifkan enkripsi saat istirahat](#)
- [\[RDS.4\] Snapshot cluster RDS dan snapshot database harus dienkrpsi saat istirahat](#)
- [\[RDS.5\] Instans RDS DB harus dikonfigurasi dengan beberapa Availability Zone](#)
- [\[RDS.6\] Pemantauan yang ditingkatkan harus dikonfigurasi untuk instans RDS DB](#)
- [\[RDS.8\] Instans RDS DB harus mengaktifkan perlindungan penghapusan](#)
- [\[RDS.9\] Instans RDS DB harus menerbitkan log ke Log CloudWatch](#)
- [\[RDS.10\] Otentikasi IAM harus dikonfigurasi untuk instance RDS](#)
- [\[RDS.11\] Instans RDS harus mengaktifkan pencadangan otomatis](#)
- [\[RDS.12\] Otentikasi IAM harus dikonfigurasi untuk cluster RDS](#)
- [\[RDS.13\] Peningkatan versi minor otomatis RDS harus diaktifkan](#)
- [\[RDS.15\] Cluster RDS DB harus dikonfigurasi untuk beberapa Availability Zone](#)
- [\[RDS.17\] Instans RDS DB harus dikonfigurasi untuk menyalin tag ke snapshot](#)
- [\[RDS.18\] Instans RDS harus digunakan di VPC](#)
- [\[RDS.19\] Langganan pemberitahuan acara RDS yang ada harus dikonfigurasi untuk peristiwa klaster penting](#)
- [\[RDS.20\] Langganan pemberitahuan acara RDS yang ada harus dikonfigurasi untuk peristiwa instance basis data penting](#)
- [\[RDS.21\] Langganan pemberitahuan acara RDS harus dikonfigurasi untuk peristiwa grup parameter basis data penting](#)
- [\[RDS.22\] Langganan pemberitahuan acara RDS harus dikonfigurasi untuk acara grup keamanan basis data penting](#)
- [\[RDS.23\] Instans RDS tidak boleh menggunakan port default mesin database](#)
- [\[RDS.25\] Instans database RDS harus menggunakan nama pengguna administrator khusus](#)
- [\[RDS.27\] Cluster RDS DB harus dienkrpsi saat istirahat](#)
- [\[Redshift.1\] Cluster Amazon Redshift harus melarang akses publik](#)
- [\[Redshift.2\] Koneksi ke cluster Amazon Redshift harus dienkrpsi saat transit](#)
- [\[Redshift.4\] Cluster Amazon Redshift harus mengaktifkan pencatatan audit](#)
- [\[Redshift.6\] Amazon Redshift harus mengaktifkan peningkatan otomatis ke versi utama](#)

- [\[Redshift.7\] Cluster Redshift harus menggunakan perutean VPC yang ditingkatkan](#)
- [\[Redshift.8\] Cluster Amazon Redshift tidak boleh menggunakan nama pengguna Admin default](#)
- [\[Redshift.9\] Cluster Redshift tidak boleh menggunakan nama database default](#)
- [\[Redshift.10\] Cluster Redshift harus dienkripsi saat istirahat](#)
- [\[S3.1\] Bucket tujuan umum S3 harus mengaktifkan pengaturan akses publik blok](#)
- [\[S3.2\] Bucket tujuan umum S3 harus memblokir akses baca publik](#)
- [\[S3.3\] Bucket tujuan umum S3 harus memblokir akses tulis publik](#)
- [\[S3.5\] Bucket tujuan umum S3 harus memerlukan permintaan untuk menggunakan SSL](#)
- [\[S3.6\] Kebijakan bucket tujuan umum S3 harus membatasi akses ke yang lain Akun AWS](#)
- [\[S3.8\] Bucket tujuan umum S3 harus memblokir akses publik](#)
- [\[S3.9\] Bucket tujuan umum S3 harus mengaktifkan pencatatan akses server](#)
- [\[S3.12\] tidak ACLs boleh digunakan untuk mengelola akses pengguna ke bucket tujuan umum S3](#)
- [\[S3.13\] Bucket tujuan umum S3 harus memiliki konfigurasi Siklus Hidup](#)
- [\[S3.17\] Ember tujuan umum S3 harus dienkripsi saat istirahat AWS KMS keys](#)
- [\[SageMaker.1\] Instans SageMaker notebook Amazon seharusnya tidak memiliki akses internet langsung](#)
- [\[SageMaker.2\] instance SageMaker notebook harus diluncurkan dalam VPC khusus](#)
- [\[SageMaker.3\] Pengguna seharusnya tidak memiliki akses root ke instance SageMaker notebook](#)
- [\[SecretsManager.1\] Rahasia Secrets Manager harus mengaktifkan rotasi otomatis](#)
- [\[SecretsManager.2\] Rahasia Secrets Manager yang dikonfigurasi dengan rotasi otomatis harus berhasil diputar](#)
- [\[SecretsManager.3\] Hapus rahasia Secrets Manager yang tidak digunakan](#)
- [\[SecretsManager.4\] Rahasia Secrets Manager harus diputar dalam jumlah hari tertentu](#)
- [\[SQS.1\] Antrian Amazon SQS harus dienkripsi saat istirahat](#)
- [\[SSM.1\] EC2 Instans Amazon harus dikelola oleh AWS Systems Manager](#)
- [\[SSM.2\] EC2 Instans Amazon yang dikelola oleh Systems Manager harus memiliki status kepatuhan patch COMPLIANT setelah instalasi patch](#)
- [\[SSM.3\] EC2 Instans Amazon yang dikelola oleh Systems Manager harus memiliki status kepatuhan asosiasi COMPLIANT](#)
- [\[SSM.4\] Dokumen SSM seharusnya tidak bersifat publik](#)

- [\[WAF.2\] Aturan Regional AWS WAF Klasik harus memiliki setidaknya satu syarat](#)
- [\[WAF.3\] Kelompok aturan Regional AWS WAF Klasik harus memiliki setidaknya satu aturan](#)
- [\[WAF.4\] Web Regional AWS WAF Klasik ACLs harus memiliki setidaknya satu aturan atau kelompok aturan](#)
- [\[WAF.10\] AWS WAF web ACLs harus memiliki setidaknya satu aturan atau kelompok aturan](#)

Untuk informasi selengkapnya tentang standar ini, lihat [Kontrol CSPM Security Hub](#) di AWS Control Tower Panduan Pengguna.

Mengaktifkan standar keamanan

Saat Anda mengaktifkan standar keamanan di AWS Security Hub Cloud Security Posture Management (CSPM), Security Hub CSPM secara otomatis membuat dan mengaktifkan semua kontrol yang berlaku untuk standar. Security Hub CSPM juga mulai menjalankan pemeriksaan keamanan dan menghasilkan temuan untuk kontrol.

Untuk mengoptimalkan cakupan dan keakuratan temuan, aktifkan dan konfigurasi perekaman sumber daya AWS Config sebelum Anda mengaktifkan standar. Saat Anda mengonfigurasi perekaman sumber daya, pastikan juga untuk mengaktifkannya untuk semua jenis sumber daya yang diperiksa oleh kontrol yang berlaku untuk standar. Jika tidak, Security Hub CSPM mungkin tidak dapat mengevaluasi sumber daya yang sesuai, dan menghasilkan temuan akurat untuk kontrol yang berlaku untuk standar. Untuk informasi selengkapnya, lihat [Mengaktifkan dan mengonfigurasi AWS Config untuk Security Hub CSPM](#).

Setelah Anda mengaktifkan standar, Anda dapat menonaktifkan atau kemudian mengaktifkan kembali kontrol individual yang berlaku untuk standar. Jika Anda menonaktifkan kontrol untuk standar, Security Hub CSPM berhenti menghasilkan temuan untuk kontrol. Selain itu, Security Hub CSPM mengabaikan kontrol saat menghitung skor keamanan untuk standar. Skor keamanan adalah persentase kontrol yang lulus evaluasi, relatif terhadap jumlah total kontrol yang berlaku untuk standar, diaktifkan, dan memiliki data evaluasi.

Saat Anda mengaktifkan standar, Security Hub CSPM menghasilkan skor keamanan awal untuk standar tersebut, biasanya dalam waktu 30 menit setelah kunjungan pertama Anda ke halaman Ringkasan atau Standar Keamanan di konsol CSPM Security Hub. Skor keamanan dibuat hanya untuk standar yang diaktifkan saat Anda mengunjungi halaman tersebut di konsol. Selain itu, perekaman sumber daya harus AWS Config dikonfigurasi agar skor muncul. Di Wilayah Tiongkok AWS GovCloud (US) Regions dan, dibutuhkan waktu hingga 24 jam bagi Security Hub CSPM untuk

menghasilkan skor keamanan awal untuk standar. Setelah Security Hub CSPM menghasilkan skor awal, itu memperbarui skor setiap 24 jam. Untuk menentukan kapan skor keamanan terakhir diperbarui, Anda dapat merujuk ke stempel waktu yang disediakan Security Hub CSPM untuk skor tersebut. Untuk informasi selengkapnya, lihat [Menghitung skor keamanan](#).

Cara Anda mengaktifkan standar tergantung pada apakah Anda menggunakan [konfigurasi pusat](#) untuk mengelola Security Hub CSPM untuk beberapa akun dan Wilayah AWS. Wilayah AWS Sebaiknya gunakan konfigurasi pusat jika Anda ingin mengaktifkan standar di lingkungan multi-akun, Multi-wilayah. Anda dapat menggunakan konfigurasi pusat jika Anda mengintegrasikan Security Hub CSPM dengan AWS Organizations. Jika Anda tidak menggunakan konfigurasi pusat, Anda harus mengaktifkan setiap standar secara terpisah di setiap akun dan setiap Wilayah.

Topik

- [Mengaktifkan standar di beberapa akun dan Wilayah AWS](#)
- [Mengaktifkan standar dalam satu akun dan Wilayah AWS](#)
- [Memeriksa status standar](#)

Mengaktifkan standar di beberapa akun dan Wilayah AWS

Untuk mengaktifkan dan mengonfigurasi standar keamanan di beberapa akun dan Wilayah AWS, gunakan [konfigurasi pusat](#). Dengan konfigurasi pusat, administrator CSPM Security Hub yang didelegasikan dapat membuat kebijakan konfigurasi CSPM Security Hub yang mengaktifkan satu atau beberapa standar. Administrator kemudian dapat mengaitkan kebijakan konfigurasi dengan akun individu, unit organisasi (OUs), atau root. Kebijakan konfigurasi memengaruhi Wilayah asal, juga disebut sebagai Wilayah agregasi, dan semua Wilayah yang ditautkan.

Kebijakan konfigurasi menawarkan opsi penyesuaian. Misalnya, Anda dapat memilih untuk hanya mengaktifkan standar AWS Foundational Security Best Practices (FSBP) untuk satu OU. Untuk OU lain, Anda dapat memilih untuk mengaktifkan standar FSBP dan standar Center for Internet Security (CIS) AWS Foundations Benchmark v1.4.0. Untuk informasi tentang membuat kebijakan konfigurasi yang memungkinkan standar tertentu yang Anda tentukan, lihat [Membuat dan mengaitkan kebijakan konfigurasi](#).

Jika Anda menggunakan konfigurasi pusat, Security Hub CSPM tidak secara otomatis mengaktifkan standar apa pun di akun baru atau yang sudah ada. Sebagai gantinya, administrator CSPM Security Hub menentukan standar mana yang akan diaktifkan di akun yang berbeda saat mereka membuat kebijakan konfigurasi CSPM Security Hub untuk organisasi mereka. Security Hub CSPM

menawarkan kebijakan konfigurasi yang direkomendasikan di mana hanya standar FSBP yang diaktifkan. Untuk informasi selengkapnya, lihat [Jenis kebijakan konfigurasi](#).

Note

Administrator CSPM Security Hub dapat menggunakan kebijakan konfigurasi untuk mengaktifkan standar apa pun kecuali standar yang dikelola [AWS Control Tower layanan](#). Untuk mengaktifkan standar ini, administrator harus menggunakan AWS Control Tower secara langsung. Mereka juga harus menggunakan AWS Control Tower untuk mengaktifkan atau menonaktifkan kontrol individu dalam standar ini untuk akun yang dikelola secara terpusat.

Jika Anda ingin beberapa akun mengaktifkan dan mengonfigurasi standar untuk akun mereka sendiri, administrator CSPM Security Hub dapat menetapkan akun tersebut sebagai akun yang dikelola sendiri. Akun yang dikelola sendiri harus mengaktifkan dan mengonfigurasi standar secara terpisah di setiap Wilayah.

Mengaktifkan standar dalam satu akun dan Wilayah AWS

Jika Anda tidak menggunakan konfigurasi pusat atau memiliki akun yang dikelola sendiri, Anda tidak dapat menggunakan kebijakan konfigurasi untuk mengaktifkan standar keamanan secara terpusat di beberapa akun atau Wilayah AWS. Namun, Anda dapat mengaktifkan standar dalam satu akun dan Wilayah. Anda dapat melakukannya dengan menggunakan konsol CSPM Security Hub atau Security Hub CSPM API.

Security Hub CSPM console

Ikuti langkah-langkah ini untuk mengaktifkan standar dalam satu akun dan Wilayah dengan menggunakan konsol CSPM Security Hub.

Untuk mengaktifkan standar dalam satu akun dan Wilayah

1. Buka konsol AWS Security Hub Cloud Security Posture Management (CSPM) di <https://console.aws.amazon.com/securityhub/>
2. Dengan menggunakan Wilayah AWS pemilih di sudut kanan atas halaman, pilih Wilayah di mana Anda ingin mengaktifkan standar.
3. Di panel navigasi, pilih Standar keamanan. Halaman standar Keamanan mencantumkan semua standar yang didukung Security Hub CSPM saat ini. Jika Anda sudah mengaktifkan

standar, bagian untuk standar mencakup skor keamanan saat ini dan detail tambahan untuk standar.

4. Di bagian untuk standar yang ingin Anda aktifkan, pilih Aktifkan standar.

Untuk mengaktifkan standar di Wilayah tambahan, ulangi langkah-langkah sebelumnya di setiap Wilayah tambahan.

Security Hub CSPM API

Untuk mengaktifkan standar secara terprogram dalam satu akun dan Wilayah, gunakan operasi [BatchEnableStandards](#). Atau, jika Anda menggunakan AWS Command Line Interface (AWS CLI), jalankan [batch-enable-standards](#) perintah.

Dalam permintaan Anda, gunakan `StandardsArn` parameter untuk menentukan Nama Sumber Daya Amazon (ARN) dari standar yang ingin Anda aktifkan. Tentukan juga Wilayah tempat permintaan Anda berlaku. Misalnya, perintah berikut memungkinkan standar AWS Foundational Security Best Practices (FSBP):

```
$ aws securityhub batch-enable-standards \
--standards-subscription-requests '{"StandardsArn":"arn:aws:securityhub:us-
east-1::standards/aws-foundational-security-best-practices/v/1.0.0"}' \
--region us-east-1
```

Di `arn:aws:securityhub:us-east-1::standards/aws-foundational-security-best-practices/v/1.0.0` mana ARN dari standar FSBP di Wilayah AS Timur (Virginia N.), dan `us-east-1` merupakan Wilayah untuk mengaktifkannya.

Untuk mendapatkan ARN untuk standar, gunakan [DescribeStandards](#) operasi atau, jika Anda menggunakan AWS CLI, jalankan perintah. [describe-standards](#)

Untuk terlebih dahulu meninjau daftar standar yang saat ini diaktifkan di akun Anda, Anda dapat menggunakan [GetEnabledStandards](#) operasi. Jika Anda menggunakan AWS CLI, Anda dapat menjalankan [get-enabled-standards](#) perintah untuk mengambil daftar ini.

Setelah Anda mengaktifkan standar, Security Hub CSPM mulai melakukan tugas untuk mengaktifkan standar di akun dan Wilayah yang ditentukan. Ini termasuk membuat semua kontrol yang berlaku untuk standar. Untuk memantau status tugas-tugas ini, Anda dapat memeriksa status standar untuk akun dan Wilayah.

Memeriksa status standar

Saat Anda mengaktifkan standar keamanan untuk akun, Security Hub CSPM mulai membuat semua kontrol yang berlaku untuk standar di akun. Security Hub CSPM juga melakukan tugas-tugas tambahan untuk mengaktifkan standar untuk akun, seperti menghasilkan skor keamanan awal untuk standar. Sementara Security Hub CSPM melakukan tugas-tugas ini, status standar adalah Pending untuk akun. Status standar kemudian melewati status tambahan, yang dapat Anda pantau dan periksa.

Note

Perubahan pada kontrol individual untuk standar tidak memengaruhi status keseluruhan standar. Misalnya, jika Anda mengaktifkan kontrol yang sebelumnya dinonaktifkan, perubahan Anda tidak akan memengaruhi status standar. Demikian pula, jika Anda mengubah nilai parameter untuk kontrol yang diaktifkan, perubahan Anda tidak akan memengaruhi status standar.

Untuk memeriksa status standar menggunakan konsol CSPM Security Hub, pilih Standar keamanan di panel navigasi. Halaman standar Keamanan mencantumkan semua standar yang didukung Security Hub CSPM saat ini. Jika Security Hub CSPM saat ini melakukan tugas untuk mengaktifkan standar, bagian untuk standar menunjukkan bahwa Security Hub CSPM masih menghasilkan skor keamanan untuk standar. Jika standar diaktifkan, bagian untuk standar mencakup skor saat ini. Pilih Lihat hasil untuk meninjau detail tambahan, termasuk status kontrol individual yang berlaku untuk standar. Untuk informasi selengkapnya, lihat [Jadwal untuk menjalankan pemeriksaan keamanan](#).

Untuk memeriksa status standar secara terprogram dengan Security Hub CSPM API, gunakan operasi [GetEnabledStandards](#). Dalam permintaan Anda, secara opsional gunakan `StandardsSubscriptionArns` parameter untuk menentukan Nama Sumber Daya Amazon (ARN) dari standar yang statusnya ingin Anda periksa. Jika Anda menggunakan AWS Command Line Interface (AWS CLI), Anda dapat menjalankan [get-enabled-standards](#) perintah untuk memeriksa status standar. Untuk menentukan ARN standar yang akan diperiksa, gunakan parameter `standards-subscription-arns`. Untuk menentukan ARN mana yang akan ditentukan, Anda dapat menggunakan [DescribeStandards](#) operasi atau, untuk AWS CLI, jalankan perintah. [describe-standards](#)

Jika permintaan Anda berhasil, Security Hub CSPM merespons dengan array objek. `StandardsSubscription` Langganan standar adalah AWS sumber daya yang dibuat CSPM

Security Hub di akun saat standar diaktifkan untuk akun tersebut. Setiap `StandardsSubscription` objek memberikan rincian tentang standar yang saat ini diaktifkan atau sedang diaktifkan atau dinonaktifkan untuk akun. Dalam setiap objek, `StandardsStatus` bidang menentukan status standar saat ini untuk akun.

Status standar (`StandardsStatus`) dapat menjadi salah satu dari berikut ini.

PENDING

Security Hub CSPM saat ini sedang melakukan tugas untuk mengaktifkan standar untuk akun. Ini termasuk membuat kontrol yang berlaku untuk standar, dan menghasilkan skor keamanan awal untuk standar. Diperlukan beberapa menit untuk Security Hub CSPM untuk menyelesaikan semua tugas. Standar juga dapat memiliki status ini jika sudah diaktifkan untuk akun dan Security Hub CSPM saat ini menambahkan kontrol baru ke standar.

Jika standar memiliki status ini, Anda mungkin tidak dapat mengambil rincian kontrol individual yang berlaku untuk standar. Selain itu, Anda mungkin tidak dapat mengonfigurasi atau menonaktifkan kontrol individual untuk standar. Misalnya, jika Anda mencoba menonaktifkan kontrol dengan menggunakan [UpdateStandardsControl](#) operasi, kesalahan terjadi.

Untuk menentukan apakah Anda dapat mengonfigurasi atau mengelola kontrol individual untuk standar, lihat nilai untuk `StandardsControlsUpdatable` bidang tersebut. Jika nilai untuk bidang ini `READY_FOR_UPDATES`, Anda dapat mulai mengelola kontrol individual untuk standar. Jika tidak, tunggu hingga Security Hub CSPM menyelesaikan tugas pemrosesan tambahan untuk mengaktifkan standar.

READY

Standar saat ini diaktifkan untuk akun. Security Hub CSPM dapat menjalankan pemeriksaan keamanan dan menghasilkan temuan untuk semua kontrol yang berlaku untuk standar dan saat ini diaktifkan. Security Hub CSPM juga dapat menghitung skor keamanan untuk standar.

Jika standar memiliki status ini, Anda dapat mengambil rincian kontrol individual yang berlaku untuk standar. Selain itu, Anda dapat mengonfigurasi, menonaktifkan, atau mengaktifkan kembali kontrol. Anda juga dapat menonaktifkan standar.

INCOMPLETE

Security Hub CSPM tidak dapat mengaktifkan standar sepenuhnya untuk akun. Security Hub CSPM tidak dapat menjalankan pemeriksaan keamanan dan menghasilkan temuan untuk semua kontrol yang berlaku untuk standar dan saat ini diaktifkan. Selain itu, Security Hub CSPM tidak dapat menghitung skor keamanan untuk standar.

Untuk menentukan mengapa standar tidak diaktifkan sepenuhnya, lihat informasi dalam `StandardsStatusReason` array. Array ini menentukan masalah yang mencegah CSPM Security Hub mengaktifkan standar. Jika terjadi kesalahan internal, coba aktifkan standar untuk akun lagi. Untuk jenis masalah lainnya, [periksa AWS Config pengaturan Anda](#). Anda juga dapat [menonaktifkan kontrol individual](#) yang tidak ingin Anda periksa, atau menonaktifkan standar sepenuhnya.

DELETING

Security Hub CSPM saat ini sedang memproses permintaan untuk menonaktifkan standar untuk akun. Ini termasuk menonaktifkan kontrol yang berlaku untuk standar, dan menghapus skor keamanan terkait. Diperlukan beberapa menit untuk Security Hub CSPM untuk menyelesaikan pemrosesan permintaan.

Jika standar memiliki status ini, Anda tidak dapat mengaktifkan kembali standar atau mencoba menonaktifkannya lagi untuk akun tersebut. Security Hub CSPM harus menyelesaikan pemrosesan permintaan saat ini terlebih dahulu. Selain itu, Anda tidak dapat mengambil detail kontrol individual yang berlaku untuk standar atau mengelola kontrol.

FAILED

Security Hub CSPM tidak dapat menonaktifkan standar untuk akun tersebut. Satu atau beberapa kesalahan terjadi ketika Security Hub CSPM mencoba untuk menonaktifkan standar. Selain itu, Security Hub CSPM tidak dapat menghitung skor keamanan untuk standar.

Untuk menentukan mengapa standar tidak dinonaktifkan sepenuhnya, lihat informasi dalam `StandardsStatusReason` array. Array ini menentukan masalah yang mencegah CSPM Security Hub menonaktifkan standar.

Jika standar memiliki status ini, Anda tidak dapat mengambil detail kontrol individual yang berlaku untuk standar atau mengelola kontrol. Namun, Anda dapat mengaktifkan kembali standar untuk akun tersebut. Jika Anda mengatasi masalah yang mencegah CSPM Security Hub menonaktifkan standar, Anda juga dapat mencoba menonaktifkan standar lagi.

Jika status standar adalah `READY`, Security Hub CSPM menjalankan pemeriksaan keamanan dan menghasilkan temuan untuk semua kontrol yang berlaku untuk standar dan saat ini diaktifkan. Untuk status lain, Security Hub CSPM mungkin menjalankan pemeriksaan dan menghasilkan temuan untuk beberapa, tetapi tidak semua, kontrol yang diaktifkan. Diperlukan waktu hingga 24 jam untuk menghasilkan atau memperbarui temuan kontrol. Untuk informasi selengkapnya, lihat [Jadwal untuk menjalankan pemeriksaan keamanan](#).

Meninjau detail standar keamanan

Setelah Anda mengaktifkan standar keamanan di AWS Security Hub Cloud Security Posture Management (CSPM), Anda dapat menggunakan konsol untuk meninjau detail standar. Di konsol, halaman detail untuk standar mencakup informasi berikut:

- Skor keamanan saat ini untuk standar.
- Tabel kontrol yang berlaku untuk standar.
- Statistik agregat untuk kontrol yang berlaku untuk standar.
- Ringkasan visual status kontrol yang berlaku untuk standar.
- Ringkasan visual pemeriksaan keamanan untuk kontrol yang diaktifkan dan berlaku untuk standar. Jika Anda mengintegrasikan dengan AWS Organizations, kontrol yang diaktifkan di setidaknya satu akun organisasi dianggap diaktifkan.

Untuk meninjau detail ini, pilih Standar keamanan di panel navigasi di konsol. Kemudian, di bagian untuk standar, pilih Lihat hasil. Untuk analisis yang lebih dalam, Anda dapat memfilter dan mengurutkan data, dan menelusuri untuk meninjau detail kontrol individual yang berlaku untuk standar.

Topik

- [Memahami skor keamanan standar](#)
- [Meninjau kontrol untuk standar](#)

Memahami skor keamanan standar

Pada konsol AWS Security Hub Cloud Security Posture Management (CSPM), halaman detail untuk standar menampilkan skor keamanan untuk standar. Skor adalah persentase kontrol yang lulus evaluasi, relatif terhadap jumlah total kontrol yang berlaku untuk standar, diaktifkan, dan memiliki data evaluasi. Di bawah skor adalah bagan yang merangkum pemeriksaan keamanan untuk kontrol yang diaktifkan untuk standar. Ini termasuk jumlah pemeriksaan keamanan yang lulus dan gagal. Untuk akun administrator, skor dan bagan standar digabungkan di seluruh akun administrator dan semua akun anggota. Untuk meninjau pemeriksaan keamanan yang gagal untuk kontrol yang memiliki tingkat keparahan tertentu, pilih tingkat keparahannya.

Saat Anda mengaktifkan standar, Security Hub CSPM menghasilkan skor keamanan awal untuk standar, biasanya dalam waktu 30 menit setelah kunjungan pertama Anda ke halaman Ringkasan

atau halaman standar Keamanan di konsol CSPM Security Hub. Skor dihasilkan hanya untuk standar yang diaktifkan saat Anda mengunjungi halaman tersebut. Selain itu, perekaman AWS Config sumber daya harus dikonfigurasi agar skor muncul. Di Wilayah Tiongkok AWS GovCloud (US) Regions dan, dibutuhkan waktu hingga 24 jam bagi Security Hub CSPM untuk menghasilkan skor awal. Setelah Security Hub CSPM menghasilkan skor awal untuk standar, itu memperbarui skor setiap 24 jam. Untuk informasi selengkapnya, lihat [Menghitung skor keamanan](#).

Semua data pada halaman detail standar Keamanan khusus untuk saat ini Wilayah AWS kecuali Anda menetapkan Wilayah agregasi. Jika Anda menetapkan Wilayah agregasi, skor keamanan berlaku di seluruh Wilayah dan menyertakan temuan untuk semua Wilayah yang ditautkan. Selain itu, status kepatuhan kontrol mencerminkan temuan dari Wilayah terkait, dan jumlah pemeriksaan keamanan mencakup temuan dari Wilayah terkait.

Meninjau kontrol untuk standar

Saat Anda menggunakan konsol AWS Security Hub Cloud Security Posture Management (CSPM) Security Hub untuk meninjau detail standar yang diaktifkan, Anda dapat meninjau tabel kontrol keamanan yang berlaku untuk standar. Untuk setiap kontrol, tabel mencakup informasi berikut:

- ID kontrol dan judul.
- Status kontrol. Untuk informasi selengkapnya, lihat [Mengevaluasi status kepatuhan dan status kontrol](#).
- Tingkat keparahan yang ditugaskan untuk kontrol.
- Jumlah cek yang gagal dan jumlah total cek. Jika berlaku, bidang Pemeriksaan gagal juga menentukan jumlah temuan dengan status Tidak Diketahui.
- Apakah kontrol mendukung parameter khusus. Untuk informasi selengkapnya, lihat [Memahami parameter kontrol di Security Hub CSPM](#).

Security Hub CSPM memperbarui status kontrol dan hitungan pemeriksaan keamanan setiap 24 jam. Stempel waktu di bagian atas halaman menunjukkan kapan Security Hub CSPM terbaru memperbarui data ini.

Untuk akun administrator, status kontrol dan jumlah pemeriksaan keamanan dikumpulkan di seluruh akun administrator dan semua akun anggota. Jumlah kontrol yang diaktifkan mencakup kontrol yang diaktifkan untuk standar di akun administrator atau setidaknya satu akun anggota. Hitungan kontrol yang dinonaktifkan mencakup kontrol yang dinonaktifkan untuk standar di akun administrator dan semua akun anggota.

Anda dapat memfilter tabel kontrol yang berlaku untuk standar. Dengan menggunakan opsi Filter menurut tabel, Anda dapat memilih untuk melihat hanya kontrol yang diaktifkan atau hanya dinonaktifkan untuk standar. Jika Anda hanya menampilkan kontrol yang diaktifkan, Anda dapat memfilter tabel lebih lanjut berdasarkan status kontrol. Anda kemudian dapat fokus pada kontrol yang memiliki status kontrol tertentu. Selain Filter menurut opsi, Anda dapat memasukkan kriteria filter di kotak Kontrol filter. Misalnya, Anda dapat memfilter berdasarkan ID kontrol atau judul.

Pilih metode akses pilihan Anda. Kemudian ikuti langkah-langkah untuk meninjau kontrol yang berlaku untuk standar yang Anda aktifkan.

Security Hub CSPM console

Untuk meninjau kontrol untuk standar yang diaktifkan

1. Buka konsol AWS Security Hub Cloud Security Posture Management (CSPM) di <https://console.aws.amazon.com/securityhub/>
2. Pilih Standar keamanan di panel navigasi.
3. Di bagian untuk standar, pilih Lihat hasil.

Tabel di bagian bawah halaman mencantumkan semua kontrol yang berlaku untuk standar. Anda dapat memfilter dan mengurutkan tabel. Anda juga dapat mengunduh halaman tabel saat ini sebagai file CSV. Untuk melakukan ini, pilih Unduh di atas tabel. Jika Anda memfilter tabel, file yang diunduh hanya menyertakan kontrol yang cocok dengan pengaturan filter Anda saat ini.

Security Hub CSPM API

Untuk meninjau kontrol untuk standar yang diaktifkan

1. Gunakan [ListSecurityControlDefinitions](#) pengoperasian Security Hub CSPM API. Jika Anda menggunakan AWS CLI, jalankan [list-security-control-definitions](#) perintah.

Tentukan Nama Sumber Daya Amazon (ARN) dari standar yang ingin Anda tinjau kontrol. ARNs Untuk mendapatkan standar, gunakan [DescribeStandards](#) operasi atau jalankan [perintah deskripsi-standar](#). Jika Anda tidak menentukan ARN untuk standar, Security Hub CSPM mengembalikan semua kontrol keamanan. IDs

2. Gunakan [ListStandardsControlAssociations](#) pengoperasian Security Hub CSPM API, atau jalankan perintah. [list-standards-control-associations](#) Operasi ini memberi tahu Anda standar mana kontrol diaktifkan.

Identifikasi kontrol dengan memberikan ID kontrol keamanan atau ARN. Parameter pagination adalah opsional.

Contoh berikut memberi tahu Anda standar mana kontrol Config.1 diaktifkan.

```
$ aws securityhub list-standards-control-associations --region us-east-1 --security-control-id Config.1
```

Mematikan standar keamanan yang diaktifkan secara otomatis

Jika organisasi Anda tidak menggunakan konfigurasi pusat, ia menggunakan jenis konfigurasi yang disebut konfigurasi lokal. Dengan konfigurasi lokal, AWS Security Hub Cloud Security Posture Management (CSPM) dapat secara otomatis mengaktifkan standar keamanan default untuk akun anggota baru saat akun bergabung dengan organisasi Anda. Semua kontrol yang berlaku untuk standar default ini juga diaktifkan secara otomatis.

Saat ini, standar keamanan default adalah standar Praktik Terbaik Keamanan AWS Dasar dan standar Center for Internet Security (CIS) AWS Foundations Benchmark v1.2.0. Untuk informasi tentang standar ini, lihat [Referensi standar untuk Security Hub CSPM](#).

Jika Anda memilih untuk mengaktifkan standar keamanan secara manual untuk akun anggota baru, Anda dapat mematikan pengaktifan otomatis standar default. Anda dapat melakukan ini hanya jika Anda mengintegrasikan dengan AWS Organizations dan menggunakan konfigurasi lokal. Jika Anda menggunakan konfigurasi pusat, Anda dapat membuat kebijakan konfigurasi yang mengaktifkan standar default dan mengaitkan kebijakan dengan root. Semua akun organisasi Anda OUs kemudian mewarisi kebijakan konfigurasi ini kecuali jika dikaitkan dengan kebijakan yang berbeda atau dikelola sendiri. Jika Anda tidak berintegrasi dengan AWS Organizations, Anda dapat menonaktifkan standar default ketika Anda awalnya mengaktifkan Security Hub CSPM atau yang lebih baru. Untuk mempelajari caranya, lihat [Menonaktifkan standar](#).

Untuk menonaktifkan pengaktifan otomatis standar default untuk akun anggota baru, Anda dapat menggunakan konsol CSPM Security Hub atau Security Hub CSPM API.

Security Hub CSPM console

Ikuti langkah-langkah berikut untuk mematikan pengaktifan otomatis standar default dengan menggunakan konsol CSPM Security Hub.

Untuk mematikan pengaktifan otomatis standar default

1. Buka konsol AWS Security Hub Cloud Security Posture Management (CSPM) di <https://console.aws.amazon.com/securityhub/>

Masuk menggunakan kredensi akun administrator.

2. Di panel navigasi, di bawah Pengaturan, pilih Konfigurasi.
3. Di bagian Ikhtisar, pilih Edit.
4. Di bawah Pengaturan akun baru, kosongkan kotak centang Aktifkan standar keamanan default.
5. Pilih Konfirmasi.

Security Hub CSPM API

Untuk mematikan pengaktifan otomatis standar default secara terprogram, dari akun administrator CSPM Security Hub, gunakan pengoperasian Security Hub CSPM API. [UpdateOrganizationConfiguration](#) Dalam permintaan Anda, tentukan NONE `AutoEnableStandards` parameternya.

Jika Anda menggunakan AWS CLI, jalankan [update-organization-configuration](#) perintah untuk mematikan pengaktifan otomatis standar default. Untuk parameter `auto-enable-standards`, tentukan NONE. Misalnya, perintah berikut secara otomatis mengaktifkan Security Hub CSPM untuk akun anggota baru, dan mematikan pengaktifan otomatis standar default untuk akun tersebut.

```
$ aws securityhub update-organization-configuration --auto-enable --auto-enable-standards NONE
```

Menonaktifkan standar keamanan

Saat Anda menonaktifkan standar keamanan di AWS Security Hub Cloud Security Posture Management (CSPM), hal berikut akan terjadi:

- Semua kontrol yang berlaku untuk standar dinonaktifkan, kecuali jika diasosiasikan dengan standar lain yang saat ini diaktifkan.
- Pemeriksaan keamanan untuk kontrol yang dinonaktifkan tidak lagi dilakukan, dan tidak ada temuan tambahan yang dihasilkan untuk kontrol yang dinonaktifkan.

- Temuan yang ada untuk kontrol yang dinonaktifkan diarsipkan secara otomatis setelah sekitar 3-5 hari.
- AWS Config aturan bahwa Security Hub CSPM dibuat untuk kontrol yang dinonaktifkan dihapus.

Penghapusan AWS Config aturan yang sesuai biasanya terjadi dalam beberapa menit setelah menonaktifkan standar. Namun, mungkin butuh waktu lebih lama. Jika permintaan pertama gagal menghapus aturan, Security Hub CSPM mencoba lagi setiap 12 jam. Namun, jika Anda menonaktifkan CSPM Security Hub atau tidak mengaktifkan standar lain, CSPM Security Hub tidak dapat mencoba lagi, yang berarti tidak dapat menghapus aturan. Jika ini terjadi dan Anda perlu menghapus aturan, hubungi AWS Dukungan.

Topik

- [Menonaktifkan standar di beberapa akun dan Wilayah AWS](#)
- [Menonaktifkan standar dalam satu akun dan Wilayah AWS](#)

Menonaktifkan standar di beberapa akun dan Wilayah AWS

Untuk menonaktifkan standar keamanan di beberapa akun dan Wilayah AWS, gunakan [konfigurasi pusat](#). Dengan konfigurasi pusat, administrator CSPM Security Hub yang didelegasikan dapat membuat kebijakan konfigurasi CSPM Security Hub yang menonaktifkan satu atau beberapa standar. Administrator kemudian dapat mengaitkan kebijakan konfigurasi dengan akun individu, unit organisasi (OUs), atau root. Kebijakan konfigurasi memengaruhi Wilayah asal, juga disebut sebagai Wilayah agregasi, dan semua Wilayah yang ditautkan.

Kebijakan konfigurasi menawarkan opsi penyesuaian. Misalnya, Anda dapat memilih untuk menonaktifkan Standar Keamanan Data Industri Kartu Pembayaran (PCI DSS) dalam satu OU. Untuk OU lain, Anda dapat memilih untuk menonaktifkan standar PCI DSS dan National Institute of Standards and Technology (NIST) SP 800-53 Rev. 5. Untuk informasi tentang membuat kebijakan konfigurasi yang mengaktifkan atau menonaktifkan standar individual yang Anda tentukan, lihat [Membuat dan mengaitkan kebijakan konfigurasi](#).

Note

Administrator CSPM Security Hub dapat menggunakan kebijakan konfigurasi untuk menonaktifkan standar apa pun kecuali standar yang dikelola [AWS Control Tower layanan](#). Untuk menonaktifkan standar ini, administrator harus menggunakan AWS Control Tower secara langsung. Mereka juga harus menggunakan AWS Control Tower untuk menonaktifkan

atau mengaktifkan kontrol individu dalam standar ini untuk akun yang dikelola secara terpusat.

Jika Anda ingin beberapa akun mengonfigurasi atau menonaktifkan standar untuk akun mereka sendiri, administrator CSPM Security Hub dapat menetapkan akun tersebut sebagai akun yang dikelola sendiri. Akun yang dikelola sendiri harus menonaktifkan standar secara terpisah di setiap Wilayah.

Menonaktifkan standar dalam satu akun dan Wilayah AWS

Jika Anda tidak menggunakan konfigurasi pusat atau memiliki akun yang dikelola sendiri, Anda tidak dapat menggunakan kebijakan konfigurasi untuk menonaktifkan standar keamanan secara terpusat di beberapa akun atau Wilayah AWS. Namun, Anda dapat menonaktifkan standar dalam satu akun dan Wilayah. Anda dapat melakukannya dengan menggunakan konsol CSPM Security Hub atau Security Hub CSPM API.

Security Hub CSPM console

Ikuti langkah-langkah ini untuk menonaktifkan standar dalam satu akun dan Wilayah dengan menggunakan konsol CSPM Security Hub.

Untuk menonaktifkan standar dalam satu akun dan Wilayah

1. Buka konsol AWS Security Hub Cloud Security Posture Management (CSPM) di <https://console.aws.amazon.com/securityhub/>
2. Dengan menggunakan Wilayah AWS pemilih di sudut kanan atas halaman, pilih Wilayah di mana Anda ingin menonaktifkan standar.
3. Di panel navigasi, pilih Standar keamanan.
4. Di bagian untuk standar yang ingin Anda nonaktifkan, pilih Nonaktifkan standar.

Untuk menonaktifkan standar di Wilayah tambahan, ulangi langkah-langkah sebelumnya di setiap Wilayah tambahan.

Security Hub CSPM API

Untuk menonaktifkan standar secara terprogram dalam satu akun dan Wilayah, gunakan operasi [BatchDisableStandards](#). Atau, jika Anda menggunakan AWS Command Line Interface (AWS CLI), jalankan [batch-disable-standards](#) perintah.

Dalam permintaan Anda, gunakan `StandardsSubscriptionArns` parameter untuk menentukan Nama Sumber Daya Amazon (ARN) dari standar yang ingin Anda nonaktifkan. Jika Anda menggunakan AWS CLI, gunakan `standards-subscription-arns` parameter untuk menentukan ARN. Tentukan juga Wilayah tempat permintaan Anda berlaku. Misalnya, perintah berikut menonaktifkan standar Praktik Terbaik Keamanan AWS Dasar (FSBP) untuk akun (`123456789012`):

```
$ aws securityhub batch-disable-standards \
--standards-subscription-arns "arn:aws:securityhub:us-east-1:123456789012:subscription/aws-foundational-security-best-practices/v/1.0.0" \
--region us-east-1
```

Di *arn:aws:securityhub:us-east-1:123456789012:subscription/aws-foundational-security-best-practices/v/1.0.0* mana ARN standar FSBP untuk akun di Wilayah AS Timur (Virginia N.), dan *us-east-1* merupakan Wilayah untuk menonaktifkannya.

Untuk mendapatkan ARN untuk standar, Anda dapat menggunakan operasi.

[GetEnabledStandards](#) Operasi ini mengambil informasi tentang standar yang saat ini diaktifkan di akun Anda. Jika Anda menggunakan AWS CLI, Anda dapat menjalankan [get-enabled-standards](#) perintah untuk mengambil informasi ini.

Setelah Anda menonaktifkan standar, Security Hub CSPM mulai melakukan tugas untuk menonaktifkan standar di akun dan Wilayah yang ditentukan. Ini termasuk menonaktifkan semua kontrol yang berlaku untuk standar. Untuk memantau status tugas-tugas ini, Anda dapat [memeriksa status standar](#) untuk akun dan Wilayah.

Memahami kontrol keamanan di Security Hub CSPM

Dalam AWS Security Hub Cloud Security Posture Management (CSPM), kontrol keamanan, juga disebut sebagai kontrol, adalah perlindungan dalam standar keamanan yang membantu organisasi melindungi kerahasiaan, integritas, dan ketersediaan informasinya. Di Security Hub CSPM, kontrol terkait dengan sumber daya tertentu AWS .

Ketika Anda mengaktifkan kontrol dalam satu atau beberapa standar, Security Hub CSPM mulai menjalankan pemeriksaan keamanan di atasnya. Pemeriksaan keamanan menghasilkan temuan CSPM Security Hub. Saat Anda menonaktifkan kontrol, Security Hub CSPM berhenti menjalankan pemeriksaan keamanan di dalamnya, dan temuan tidak lagi dihasilkan.

Anda dapat mengaktifkan atau menonaktifkan kontrol satu per satu untuk satu akun dan Wilayah AWS. Untuk menghemat waktu dan mengurangi penyimpangan konfigurasi di lingkungan multi-akun, sebaiknya gunakan [konfigurasi pusat](#) untuk mengaktifkan atau menonaktifkan kontrol. Dengan konfigurasi pusat, administrator CSPM Security Hub yang didelegasikan dapat membuat kebijakan yang menentukan bagaimana kontrol harus dikonfigurasi di beberapa akun dan Wilayah. Untuk informasi selengkapnya tentang mengaktifkan dan menonaktifkan kontrol, lihat. [Mengaktifkan kontrol di Security Hub CSPM](#)

Tampilan kontrol terkonsolidasi

Halaman Kontrol konsol CSPM Security Hub menampilkan semua kontrol yang tersedia saat ini Wilayah AWS (Anda dapat melihat kontrol dalam konteks standar dengan mengunjungi halaman standar Keamanan dan memilih standar yang diaktifkan). Security Hub CSPM menetapkan kontrol ID kontrol keamanan yang konsisten, judul, dan deskripsi di seluruh standar. Kontrol IDs termasuk nomor yang relevan Layanan AWS dan unik (misalnya, CodeBuild .3).

Informasi berikut tersedia di halaman Kontrol konsol [CSPM Security Hub](#):

- Skor keamanan keseluruhan berdasarkan proporsi kontrol yang dilewati dibandingkan dengan jumlah total kontrol yang diaktifkan dengan data
- Rincian status kontrol di semua kontrol CSPM Security Hub yang didukung
- Jumlah total pemeriksaan keamanan yang lulus dan gagal.
- Jumlah pemeriksaan keamanan yang gagal untuk kontrol dengan tingkat keparahan yang berbeda-beda, dan tautan untuk melihat detail lebih lanjut tentang pemeriksaan yang gagal tersebut.
- Daftar kontrol CSPM Security Hub, dengan filter untuk melihat subset kontrol tertentu.

Dari halaman Kontrol, Anda dapat memilih kontrol untuk melihat detailnya dan mengambil tindakan atas temuan yang dihasilkan oleh kontrol. Dari halaman ini, Anda juga dapat mengaktifkan atau menonaktifkan kontrol keamanan saat ini Akun AWS dan Wilayah AWS. Tindakan pemberdayaan dan penonaktifan dari halaman Kontrol berlaku di seluruh standar. Untuk informasi selengkapnya, lihat [Mengaktifkan kontrol di Security Hub CSPM](#).

Untuk akun administrator, halaman Kontrol mencerminkan status kontrol di seluruh akun anggota. Jika pemeriksaan kontrol gagal di setidaknya satu akun anggota, status kontrol Gagal. Jika Anda telah menetapkan [Wilayah agregasi](#), halaman Kontrol mencerminkan status kontrol di semua Wilayah tertaut. Jika pemeriksaan kontrol gagal di setidaknya satu Wilayah tertaut, status kontrol Gagal.

Tampilan kontrol terkonsolidasi menyebabkan perubahan mengontrol bidang pencarian di Format Pencarian AWS Keamanan (ASFF) yang dapat memengaruhi alur kerja. Untuk informasi selengkapnya, lihat [Tampilan kontrol konsolidasi - perubahan ASFF](#).

Skor keamanan ringkasan untuk kontrol

Halaman Kontrol menampilkan skor keamanan ringkasan dari 0-100 persen. Skor keamanan ringkasan dihitung berdasarkan proporsi kontrol yang diteruskan dibandingkan dengan jumlah total kontrol yang diaktifkan dengan data di seluruh standar.

Note

Untuk melihat skor keamanan keseluruhan untuk kontrol, Anda harus menambahkan izin untuk memanggil **BatchGetControlEvaluations** ke peran IAM yang Anda gunakan untuk mengakses CSPM Security Hub. Izin ini tidak diperlukan untuk melihat skor keamanan untuk standar tertentu.

Saat Anda mengaktifkan Security Hub CSPM, Security Hub CSPM menghitung skor keamanan awal dalam waktu 30 menit setelah kunjungan pertama Anda ke halaman Ringkasan atau halaman standar Keamanan di konsol CSPM Security Hub. Diperlukan waktu hingga 24 jam untuk skor keamanan pertama kali dihasilkan di Wilayah Tiongkok dan. AWS GovCloud (US) Regions

Selain skor keamanan keseluruhan, Security Hub CSPM menghitung skor keamanan standar untuk setiap standar yang diaktifkan dalam waktu 30 menit setelah kunjungan pertama Anda ke halaman Ringkasan atau halaman standar Keamanan. Untuk melihat daftar standar yang saat ini diaktifkan, gunakan operasi [GetEnabledStandards](#) API.

AWS Config harus diaktifkan dengan perekaman sumber daya agar skor muncul. Untuk informasi tentang cara Security Hub CSPM menghitung skor keamanan, lihat. [Menghitung skor keamanan](#)

Setelah menghasilkan skor pertama kali, Security Hub CSPM memperbarui skor keamanan setiap 24 jam. Security Hub CSPM menampilkan stempel waktu untuk menunjukkan kapan skor keamanan terakhir diperbarui.

Jika Anda telah menetapkan Wilayah agregasi, skor keamanan keseluruhan mencerminkan temuan kontrol di seluruh Wilayah yang ditautkan.

Referensi kontrol untuk Security Hub CSPM

Referensi kontrol ini menyediakan daftar kontrol AWS Security Hub Cloud Security Posture Management (CSPM) yang tersedia dengan tautan ke informasi lebih lanjut tentang setiap kontrol. Tabel ikhtisar menampilkan kontrol dalam urutan abjad dengan ID kontrol. Hanya kontrol dalam penggunaan aktif oleh Security Hub CSPM yang disertakan di sini. Kontrol pensiun dikecualikan dari daftar ini. Tabel memberikan informasi berikut untuk setiap kontrol:

- ID kontrol keamanan — ID ini berlaku di seluruh standar dan menunjukkan Layanan AWS dan sumber daya yang terkait dengan kontrol. Konsol CSPM Security Hub menampilkan kontrol keamanan IDs, terlepas dari apakah [temuan kontrol konsolidasi](#) diaktifkan atau dimatikan di akun Anda. Namun, temuan CSPM Security Hub IDs hanya mengacu pada kontrol keamanan jika temuan kontrol konsolidasi diaktifkan di akun Anda. Jika temuan kontrol konsolidasi dimatikan di akun Anda, beberapa kontrol IDs bervariasi menurut standar dalam temuan kontrol Anda. Untuk pemetaan kontrol khusus standar IDs ke kontrol keamanan, lihat. IDs [Bagaimana konsolidasi memengaruhi kontrol IDs dan judul](#)

Jika Anda ingin mengatur [otomatisasi](#) untuk kontrol keamanan, sebaiknya filter berdasarkan ID kontrol daripada judul atau deskripsi. Sementara Security Hub CSPM kadang-kadang dapat memperbarui judul kontrol atau deskripsi, kontrol IDs tetap sama.

Kontrol IDs dapat melewati angka. Ini adalah placeholder untuk kontrol masa depan.

- Standar yang berlaku - Menunjukkan standar mana yang berlaku untuk kontrol. Pilih kontrol untuk meninjau persyaratan spesifik dari kerangka kerja kepatuhan pihak ketiga.
- Judul kontrol keamanan - Judul ini berlaku di seluruh standar. Konsol CSPM Security Hub menampilkan judul kontrol keamanan, terlepas dari apakah temuan kontrol konsolidasi diaktifkan atau dinonaktifkan di akun Anda. Namun, temuan CSPM Security Hub merujuk judul kontrol keamanan hanya jika temuan kontrol konsolidasi diaktifkan di akun Anda. Jika temuan kontrol

konsolidasi dimatikan di akun Anda, beberapa judul kontrol bervariasi menurut standar dalam temuan kontrol Anda. Untuk pemetaan kontrol khusus standar IDs ke kontrol keamanan, lihat [IDs Bagaimana konsolidasi memengaruhi kontrol IDs dan judul](#)

- **Keparahan** — Tingkat keparahan kontrol mengidentifikasi pentingnya dari sudut pandang keamanan. Untuk informasi tentang cara CSPM Security Hub menentukan tingkat keparahan kontrol, lihat [Tingkat keparahan untuk temuan kontrol](#)
- **Jenis jadwal** - Menunjukkan kapan kontrol dievaluasi. Untuk informasi selengkapnya, lihat [Jadwal untuk menjalankan pemeriksaan keamanan](#).
- **Mendukung parameter kustom** - Menunjukkan apakah kontrol mendukung nilai kustom untuk satu atau beberapa parameter. Pilih kontrol untuk meninjau detail parameter. Untuk informasi selengkapnya, lihat [Memahami parameter kontrol di Security Hub CSPM](#).

Pilih kontrol untuk meninjau detail tambahan. Kontrol tercantum dalam urutan abjad oleh ID kontrol keamanan.

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
Akun.1	Informasi kontak keamanan harus disediakan untuk Akun AWS	CIS AWS Foundations Benchmark v3.0.0, Praktik Terbaik Keamanan AWS Dasar v1.0.0, Standar yang Dikelola Layanan:, NIST SP 800-53 Rev. 5 AWS Control Tower	MEDIUM	 Tidak	Berkala
Akun.2	Akun AWS harus menjadi bagian dari sebuah AWS Organizations organisasi	NIST SP 800-53 Wahyu 5	TINGGI	 Tidak	Berkala

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
ACM.1	Sertifikat yang diimpor dan diterbitkan ACM harus diperpanjang setelah jangka waktu tertentu	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan:, NIST SP 800-53 Rev. 5 AWS Control Tower, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1	MEDIUM	 Ya	Perubahan dipicu dan periodik
ACM.2	Sertifikat RSA yang dikelola oleh ACM harus menggunakan panjang kunci minimal 2.048 bit	AWS Praktik Terbaik Keamanan Dasar v1.0.0, PCI DSS v4.0.1	TINGGI	 Tidak	Perubahan dipicu
ACM.3	Sertifikat ACM harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
Amplify.1	Aplikasi Amplify harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
Amplify.2	Amplify branch harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
APIGateway y.1	API Gateway REST dan pencatatan eksekusi WebSocket API harus diaktifkan	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Ya	Perubahan dipicu
APIGateway y.2	Tahapan API Gateway REST API harus dikonfigurasi untuk menggunakan sertifikat SSL untuk otentikasi backend	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: NIST SP 800-53 Rev. 5 AWS Control Tower, NIST SP 800-171 Rev. 2	MEDIUM	 Tidak	Perubahan dipicu
APIGateway y.3	Tahapan API Gateway REST API harus mengaktifkan AWS X-Ray penelusuran	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	RENDAH	 Tidak	Perubahan dipicu
APIGateway y.4	API Gateway harus dikaitkan dengan WAF Web ACL	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
APIGateway.y.5	Data cache API Gateway REST API harus dienkripsi saat istirahat	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
APIGateway.y.8	Rute API Gateway harus menentukan jenis otorisasi	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Ya	Berkala
APIGateway.y.9	Pencatatan akses harus dikonfigurasi untuk Tahap API Gateway V2	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: NIST SP 800-53 Rev. 5 AWS Control Tower, PCI DSS v4.0.1	MEDIUM	 Tidak	Perubahan dipicu
AppConfig.y.1	AWS AppConfig aplikasi harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
AppConfig.y.2	AWS AppConfig profil konfigurasi harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
AppConfig .3	AWS AppConfig lingkungan harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
AppConfig .4	AWS AppConfig asosiasi ekstensi harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
AppFlow.1	AppFlow Aliran Amazon harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
AppRunner .1	Layanan App Runner harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
AppRunner .2	Konektor VPC App Runner harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
AppSync.1	AWS AppSync Cache API harus dienkripsi saat istirahat	AWS Praktik Terbaik Keamanan Dasar	MEDIUM	 Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
AppSync.2	AWS AppSync harus mengaktifkan logging tingkat lapangan	AWS Praktik Terbaik Keamanan Dasar v1.0.0, PCI DSS v4.0.1	MEDIUM	 Ya	Perubahan dipicu
AppSync.4	AWS AppSync APIs GraphQL harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
AppSync.5	AWS AppSync APIs GraphQL tidak boleh diautentikasi dengan kunci API	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	TINGGI	 Tidak	Perubahan dipicu
AppSync.6	AWS AppSync Cache API harus dienkrpsi saat transit	AWS Praktik Terbaik Keamanan Dasar	MEDIUM	 Tidak	Perubahan dipicu
Athena.2	Katalog data Athena harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
Athena.3	Kelompok kerja Athena harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
Athena.4	Kelompok kerja Athena seharusnya mengaktifkan logging	AWS Praktik Terbaik Keamanan Dasar	MEDIUM	 Tidak	Perubahan dipicu
AutoScaling.1	Grup Auto Scaling yang terkait dengan penyeimbang beban harus menggunakan pemeriksaan kesehatan ELB	AWS Praktik Terbaik Keamanan Dasar, Standar yang Dikelola Layanan:, PCI DSS v3.2.1 AWS Control Tower, NIST SP 800-53 Rev. 5	RENDAH	 Tidak	Perubahan dipicu
AutoScaling.2	Grup EC2 Auto Scaling Amazon harus mencakup beberapa Availability Zone	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Ya	Perubahan dipicu
AutoScaling.3	Konfigurasi peluncuran grup Auto Scaling harus mengonfigurasi EC2 instance agar memerlukan Layanan Metadata Instance Versi 2 () IMDSv2	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan:, NIST SP 800-53 Rev. 5 AWS Control Tower, PCI DSS v4.0.1	TINGGI	 Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
AutoScaling.5	EC2 Instans Amazon yang diluncurkan menggunakan konfigurasi peluncuran grup Auto Scaling seharusnya tidak memiliki alamat IP Publik	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan:, NIST SP 800-53 Rev. 5 AWS Control Tower, PCI DSS v4.0.1	TINGGI	 Tidak	Perubahan dipicu
AutoScaling.6	Grup Auto Scaling harus menggunakan beberapa jenis instance di beberapa Availability Zone	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
AutoScaling.9	EC2 Grup Auto Scaling harus menggunakan template peluncuran EC2	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
AutoScaling.10	EC2 Grup Auto Scaling harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
Backup.1	AWS Backup titik pemulihan harus dienkripsi saat istirahat	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
Backup.2	AWS Backup poin pemulihan harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
Backup.3	AWS Backup brankas harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
Backup.4	AWS Backup rencana laporan harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
Backup.5	AWS Backup rencana cadangan harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
Batch.1	Antrian pekerjaan batch harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
Batch.2	Kebijakan penjadwalan Batch harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
Batch.3	Lingkungan komputasi Batch harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
Batch.4	Properti sumber daya komputasi di lingkungan komputasi Batch terkelola harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
CloudFormation.2	CloudFormation tumpukan harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
CloudFront.1	CloudFront distribusi harus memiliki objek root default yang dikonfigurasi	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	TINGGI	 Tidak	Perubahan dipicu
CloudFront.3	CloudFront distribusi harus memerlukan enkripsi dalam perjalanan	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIUM	 Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
CloudFront t.4	CloudFront distribusi harus memiliki failover asal yang dikonfigurasi	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	RENDAH	 Tidak	Perubahan dipicu
CloudFront t.5	CloudFront distribusi harus mengaktifkan logging	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIUM	 Tidak	Perubahan dipicu
CloudFront t.6	CloudFront distribusi harus mengaktifkan WAF	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIUM	 Tidak	Perubahan dipicu
CloudFront t.7	CloudFront distribusi harus menggunakan sertifikat khusus SSL/TLS	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2	MEDIUM	 Tidak	Perubahan dipicu
CloudFront t.8	CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	RENDAH	 Tidak	Perubahan dipicu
CloudFront t.9	CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIUM	 Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
CloudFront t.10	CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal kustom	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1	MEDIUM	 Tidak	Perubahan dipicu
CloudFront t.12	CloudFront distribusi seharusnya tidak menunjukkan asal S3 yang tidak ada	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	TINGGI	 Tidak	Berkala
CloudFront t.13	CloudFront distribusi harus menggunakan kontrol akses asal	AWS Praktik Terbaik Keamanan Dasar v1.0.0	MEDIUM	 Tidak	Perubahan dipicu
CloudFront t.14	CloudFront distribusi harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
CloudTrail I.1	CloudTrail harus diaktifkan dan dikonfigurasi dengan setidaknya satu jejak Multi-wilayah yang mencakup acara manajemen baca dan tulis	Tolok Ukur AWS Yayasan CIS v3.0.0, Tolok Ukur AWS Yayasan CIS v1.4.0, Tolok Ukur Yayasan CIS v1.2.0, Praktik Terbaik Keamanan AWS Dasar, Standar yang AWS Dikelola Layanan:, NIST SP 800-53 Rev. 5 AWS Control Tower	TINGGI	 Tidak	Berkala
CloudTrail I.2	CloudTrail harus mengaktifkan enkripsi saat istirahat	Tolok Ukur AWS Yayasan CIS v3.0.0, Tolok Ukur Yayasan CIS v1.2.0, Tolok Ukur AWS Yayasan CIS v1.4.0 Praktik Terbaik Keamanan AWS Dasar v1.0.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v3.2.1, PCI DSS v4.0.1, Standar yang Dikelola Layanan: AWS AWS Control Tower	MEDIUM	 Tidak	Berkala

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
CloudTrail I.3	Setidaknya satu CloudTrail jejak harus diaktifkan	NIST SP 800-171 Rev. 2, PCI DSS v4.0.1, PCI DSS v3.2.1	TINGGI	 Tidak	Berkala
CloudTrail I.4	CloudTrail validasi file log harus diaktifkan	Tolok Ukur AWS Yayasan CIS v3.0.0, Tolok Ukur Yayasan CIS v1.4.0, Tolok Ukur AWS Yayasan CIS v1.2.0, Praktik Terbaik Keamanan AWS Dasar v1.0.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1, PCI DSS v3.2.1, Standar yang Dikelola Layanan: AWS AWS Control Tower	RENDAH	 Tidak	Berkala

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
CloudTrail I.5	CloudTrail jalur harus diintegrasikan dengan Amazon Logs CloudWatch	Tolok Ukur AWS Yayasan CIS v1.2.0, Tolok Ukur AWS Yayasan CIS v1.4.0, Praktik Terbaik Keamanan AWS Dasar v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v3.2.1, PCI DSS v4.0.1, Standar yang Dikelola Layanan: AWS Control Tower	RENDAH	 Tidak	Berkala
CloudTrail I.6	Pastikan bucket S3 yang digunakan untuk menyimpan CloudTrail log tidak dapat diakses publik	Tolok Ukur AWS Yayasan CIS v1.2.0, Tolok Ukur AWS Yayasan CIS v1.4.0, PCI DSS v4.0.1	KRITIS	 Tidak	Perubahan dipicu dan periodik
CloudTrail I.7	Pastikan pencatatan akses bucket S3 diaktifkan pada bucket CloudTrail S3	Tolok Ukur AWS Yayasan CIS v1.2.0, Tolok Ukur AWS Yayasan CIS v1.4.0, Tolok Ukur Yayasan CIS v3.0.0, PCI DSS v4.0.1 AWS	RENDAH	 Tidak	Berkala
CloudTrail I.9	CloudTrail jalan setapak harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
CloudTrail I.10	CloudTrail Penyimpanan data acara danau harus dienkripsi dengan pelanggan yang dikelola AWS KMS keys	NIST SP 800-53 Wahyu 5	MEDIUM	 Ya	Berkala
CloudWatch h.1	Filter metrik log dan alarm harus ada untuk penggunaan pengguna "root"	Tolok Ukur AWS Yayasan CIS v1.4.0, Tolok Ukur AWS Yayasan CIS v1.2.0, NIST SP 800-171 Rev. 2, PCI DSS v3.2.1	RENDAH	 Tidak	Berkala
CloudWatch h.2	Pastikan filter metrik log dan alarm ada untuk panggilan API yang tidak sah	Tolok Ukur AWS Yayasan CIS v1.2.0, NIST SP 800-171 Rev. 2	RENDAH	 Tidak	Berkala
CloudWatch h.3	Pastikan ada filter metrik log dan alarm untuk login Management Console tanpa MFA	Tolok Ukur AWS Yayasan CIS v1.2.0	RENDAH	 Tidak	Berkala
CloudWatch h.4	Pastikan filter metrik log dan alarm ada untuk perubahan kebijakan IAM	Tolok Ukur AWS Yayasan CIS v1.4.0, Tolok Ukur AWS Yayasan CIS v1.2.0, NIST SP 800-171 Rev. 2	RENDAH	 Tidak	Berkala

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
CloudWatch h.5	Pastikan filter metrik log dan alarm ada untuk perubahan CloudTrail konfigurasi	Tolok Ukur AWS Yayasan CIS v1.4.0, Tolok Ukur AWS Yayasan CIS v1.2.0, NIST SP 800-171 Rev. 2	RENDAH	 Tidak	Berkala
CloudWatch h.6	Pastikan filter metrik log dan alarm ada untuk kegagalan AWS Management Console otentikasi	Tolok Ukur AWS Yayasan CIS v1.4.0, Tolok Ukur AWS Yayasan CIS v1.2.0, NIST SP 800-171 Rev. 2	RENDAH	 Tidak	Berkala
CloudWatch h.7	Pastikan filter metrik log dan alarm ada untuk menonaktifkan atau terjadwal penghapusan pelanggan yang dibuat CMKs	Tolok Ukur AWS Yayasan CIS v1.4.0, Tolok Ukur AWS Yayasan CIS v1.2.0, NIST SP 800-171 Rev. 2	RENDAH	 Tidak	Berkala
CloudWatch h.8	Pastikan filter metrik log dan alarm ada untuk perubahan kebijakan bucket S3	Tolok Ukur AWS Yayasan CIS v1.4.0, Tolok Ukur AWS Yayasan CIS v1.2.0, NIST SP 800-171 Rev. 2	RENDAH	 Tidak	Berkala

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
CloudWatch h.9	Pastikan filter metrik log dan alarm ada untuk perubahan AWS Config konfigurasi	Tolok Ukur AWS Yayasan CIS v1.4.0, Tolok Ukur AWS Yayasan CIS v1.2.0, NIST SP 800-171 Rev. 2	RENDAH	 Tidak	Berkala
CloudWatch h.10	Pastikan filter metrik log dan alarm ada untuk perubahan grup keamanan	Tolok Ukur AWS Yayasan CIS v1.4.0, Tolok Ukur AWS Yayasan CIS v1.2.0, NIST SP 800-171 Rev. 2	RENDAH	 Tidak	Berkala
CloudWatch h.11	Pastikan filter metrik log dan alarm ada untuk perubahan pada Daftar Kontrol Akses Jaringan (NACL)	Tolok Ukur AWS Yayasan CIS v1.4.0, Tolok Ukur AWS Yayasan CIS v1.2.0, NIST SP 800-171 Rev. 2	RENDAH	 Tidak	Berkala
CloudWatch h.12	Pastikan filter metrik log dan alarm ada untuk perubahan gateway jaringan	Tolok Ukur AWS Yayasan CIS v1.4.0, Tolok Ukur AWS Yayasan CIS v1.2.0, NIST SP 800-171 Rev. 2	RENDAH	 Tidak	Berkala

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
CloudWatch h.13	Pastikan filter metrik log dan alarm ada untuk perubahan tabel rute	Tolok Ukur AWS Yayasan CIS v1.4.0, Tolok Ukur AWS Yayasan CIS v1.2.0, NIST SP 800-171 Rev. 2	RENDAH	 Tidak	Berkala
CloudWatch h.14	Pastikan filter metrik log dan alarm ada untuk perubahan VPC	Tolok Ukur AWS Yayasan CIS v1.4.0, Tolok Ukur AWS Yayasan CIS v1.2.0, NIST SP 800-171 Rev. 2	RENDAH	 Tidak	Berkala
CloudWatch h.15	CloudWatch alarm harus memiliki tindakan tertentu yang dikonfigurasi	NIST SP 800-53 Wahyu 5, NIST SP 800-171 Wahyu 2	TINGGI	 Ya	Perubahan dipicu
CloudWatch h.16	CloudWatch grup log harus dipertahankan untuk jangka waktu tertentu	NIST SP 800-53 Wahyu 5	MEDIUM	 Ya	Berkala
CloudWatch h.17	CloudWatch tindakan alarm harus diaktifkan	NIST SP 800-53 Wahyu 5	TINGGI	 Tidak	Perubahan dipicu
CodeArtifact act.1	CodeArtifact repositori harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
CodeBuild .1	CodeBuild Repositori sumber Bitbucket tidak URLs boleh berisi kredensial sensitif	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v3.2.1, PCI DSS v4.0.1, Standar yang Dikelola Layanan: AWS Control Tower	KRITIS	 Tidak	Perubahan dipicu
CodeBuild .2	CodeBuild variabel lingkungan proyek tidak boleh berisi kredensial teks yang jelas	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v3.2.1, PCI DSS v4.0.1, Standar yang Dikelola Layanan: AWS Control Tower	KRITIS	 Tidak	Perubahan dipicu
CodeBuild .3	CodeBuild Log S3 harus dienkripsi	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, Standar yang Dikelola Layanan: AWS Control Tower	RENDAH	 Tidak	Perubahan dipicu
CodeBuild .4	CodeBuild lingkungan proyek harus memiliki konfigurasi logging	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
CodeBuild.7	CodeBuild ekspor kelompok laporan harus dienkripsi saat istirahat	AWS Praktik Terbaik Keamanan Dasar	MEDIUM	 Tidak	Perubahan dipicu
CodeGuruProfiler.1	CodeGuru Grup profil profiler harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
CodeGuruReviewer.1	CodeGuru Asosiasi repositori reviewer harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
Kognito.1	Kumpulan pengguna Cognito harus mengaktifkan perlindungan ancaman dengan mode penegakan fungsi penuh untuk otentikasi standar	AWS Praktik Terbaik Keamanan Dasar	MEDIUM	 Ya	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
Konfigurasi.1	AWS Config harus diaktifkan dan menggunakan peran terkait layanan untuk perekaman sumber daya	Tolok Ukur AWS Yayasan CIS v3.0.0, Tolok Ukur AWS Yayasan CIS v1.4.0, Tolok Ukur Yayasan CIS v1.2.0, Praktik Terbaik Keamanan AWS Dasar, NIST AWS SP 800-53 Rev. 5, PCI DSS v3.2.1	KRITIS	 Ya	Berkala
Hubungkan.1	Jenis objek Amazon Connect Customer Profiles harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
Hubungkan.2	Instans Amazon Connect seharusnya mengaktifkan CloudWatch logging	AWS Praktik Terbaik Keamanan Dasar	MEDIUM	 Tidak	Perubahan dipicu
DataFirehose.1	Aliran pengiriman Firehose harus dienkripsi saat istirahat	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Berkala
DataSync.1	DataSync tugas harus mengaktifkan pencatatan	AWS Praktik Terbaik Keamanan Dasar	MEDIUM	 Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
DataSync.2	DataSync tugas harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
Detektif.1	Grafik perilaku Detektif harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
DMS.1	Contoh replikasi Database Migration Service tidak boleh bersifat publik	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v3.2.1, PCI DSS v4.0.1, Standar yang Dikelola Layanan: AWS Control Tower	KRITIS	 Tidak	Berkala
DMS.2	Sertifikat DMS harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
DMS.3	Langganan acara DMS harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
DMS.4	Instans replikasi DMS harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
DMS.5	Grup subnet replikasi DMS harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
DMS.6	Instans replikasi DMS harus mengaktifkan peningkatan versi minor otomatis	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIUM	 Tidak	Perubahan dipicu
DMS.7	Tugas replikasi DMS untuk database target harus mengaktifkan logging	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIUM	 Tidak	Perubahan dipicu
DMS.8	Tugas replikasi DMS untuk database sumber harus mengaktifkan logging	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIUM	 Tidak	Perubahan dipicu
DMS.9	Titik akhir DMS harus menggunakan SSL	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIUM	 Tidak	Perubahan dipicu
DMS.10	Titik akhir DMS untuk database Neptunus harus mengaktifkan otorisasi IAM	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIUM	 Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
DMS.11	Titik akhir DMS untuk MongoDB harus mengaktifkan mekanisme otentikasi	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIUM	 Tidak	Perubahan dipicu
DMS.12	Titik akhir DMS untuk Redis OSS harus mengaktifkan TLS	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIUM	 Tidak	Perubahan dipicu
Dokumentasi.1	Cluster Amazon DocumentDB harus dienkripsi saat istirahat	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5, Standar yang Dikelola Layanan: AWS Control Tower	MEDIUM	 Tidak	Perubahan dipicu
Dokumentasi.2	Cluster Amazon DocumentDB harus memiliki periode retensi cadangan yang memadai	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, Standar yang Dikelola Layanan: AWS Control Tower	MEDIUM	 Ya	Perubahan dipicu
Dokumentasi.3	Cuplikan cluster manual Amazon DocumentDB seharusnya tidak bersifat publik	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	KRITIS	 Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
DokumenD.4	Cluster Amazon DocumentDB harus mempublikasikan log audit ke Log CloudWatch	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIUM	 Tidak	Perubahan dipicu
DokumenD.5	Cluster Amazon DocumentDB harus mengaktifkan perlindungan penghapusan	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
DokumenD.6	Cluster Amazon DocumentDB harus dienkripsi saat transit	AWS Praktik Terbaik Keamanan Dasar	MEDIUM	 Tidak	Berkala
DynamoDB 1	Tabel DynamoDB harus secara otomatis menskalakan kapasitas dengan permintaan	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Ya	Berkala
DynamoDB 2	Tabel DynamoDB harus mengaktifkan pemulihan point-in-time	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
DynamoDB 3	Cluster DynamoDB Accelerator (DAX) harus dienkripsi saat istirahat	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Berkala
DynamoDB 4	Tabel DynamoDB harus ada dalam rencana cadangan	NIST SP 800-53 Wahyu 5	MEDIUM	 Ya	Berkala
DynamoDB 5	Tabel DynamoDB harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
DynamoDB 6	Tabel DynamoDB harus mengaktifkan perlindungan penghapusan	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
DynamoDB 7	Cluster DynamoDB Accelerator harus dienkripsi saat transit	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIUM	 Tidak	Berkala
EC2.1	Snapshot EBS tidak boleh dipulihkan secara publik	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan:, PCI DSS v3.2.1 AWS Control Tower, NIST SP 800-53 Rev. 5	KRITIS	 Tidak	Berkala

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
EC2.2	Grup keamanan default VPC tidak boleh mengizinkan lalu lintas masuk atau keluar	Tolok Ukur AWS Yayasan CIS v3.0.0, Tolok Ukur AWS Yayasan CIS v1.2.0, Praktik Terbaik Keamanan AWS Dasar v1.0.0, Standar yang Dikelola Layanan:, PCI DSS v3.2.1, Tolok Ukur Yayasan CIS v1.4.0, NIST SP 800-53 AWS Control Tower Rev. 5 AWS	TINGGI	 Tidak	Perubahan dipicu
EC2.3	Volume EBS yang terpasang harus dienkripsi saat istirahat	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
EC2.4	EC2 Instans yang dihentikan harus dihapus setelah periode waktu tertentu	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Ya	Berkala

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
EC2.6	Pencatatan aliran VPC harus diaktifkan di semua VPCs	Tolok Ukur AWS Yayasan CIS v3.0.0, Tolok Ukur AWS Yayasan CIS v1.2.0, Praktik Terbaik Keamanan AWS Dasar v1.0.0, Standar yang Dikelola Layanan:, PCI DSS v3.2.1, Tolok Ukur Yayasan CIS v1.4.0, NIST SP 800-53 Rev. 5 AWS Control Tower, NIST SP 800-171 Rev. 2 AWS	MEDIUM	 Tidak	Berkala
EC2.7	Enkripsi default EBS harus diaktifkan	Tolok Ukur AWS Yayasan CIS v3.0.0, Praktik Terbaik Keamanan AWS Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, Tolok Ukur Yayasan CIS v1.4.0, NIST SP 800-53 Rev. 5 AWS	MEDIUM	 Tidak	Berkala

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
EC2.8	EC2 instance harus menggunakan Instance Metadata Service Version 2 () IMDSv2	Tolok Ukur AWS Yayasan CIS v3.0.0, Praktik Terbaik Keamanan AWS Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, Standar yang Dikelola Layanan: AWS Control Tower	TINGGI	 Tidak	Perubahan dipicu
EC2.9	EC2 instans seharusnya tidak memiliki alamat publik IPv4	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	TINGGI	 Tidak	Perubahan dipicu
EC2.10	Amazon EC2 harus dikonfigurasi untuk menggunakan titik akhir VPC yang dibuat untuk layanan Amazon EC2	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan:, NIST SP 800-53 Rev. 5 AWS Control Tower, NIST SP 800-171 Rev. 2	MEDIUM	 Tidak	Berkala
EC2.12	Tidak terpakai EC2 EIPs harus dihapus	PCI DSS v3.2.1, NIST SP 800-53 Wahyu 5	RENDAH	 Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
EC2.13	Grup keamanan tidak boleh mengizinkan masuknya dari 0.0.0.0/0 atau :/0 ke port 22	Tolok Ukur AWS Yayasan CIS v1.2.0, PCI DSS v3.2.1, PCI DSS v4.0.1, NIST SP 800-53 Rev. 5, NIST SP 800-171 Wahyu 2	TINGGI	 Tidak	Perubahan dipicu dan periodik
EC2.14	Grup keamanan tidak boleh mengizinkan masuknya dari 0.0.0.0/0 atau :/0 ke port 3389	Tolok Ukur AWS Yayasan CIS v1.2.0, PCI DSS v4.0.1	TINGGI	 Tidak	Perubahan dipicu dan periodik
EC2.15	EC2 subnet seharusnya tidak secara otomatis menetapkan alamat IP publik	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, Standar yang Dikelola Layanan:, AWS Control Tower	MEDIUM	 Tidak	Perubahan dipicu
EC2.16	Daftar Kontrol Akses Jaringan yang Tidak Digunakan harus dihapus	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1, Standar yang Dikelola Layanan:, AWS Control Tower	RENDAH	 Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
EC2.17	EC2 instance tidak boleh menggunakan banyak ENIs	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	RENDAH	 Tidak	Perubahan dipicu
EC2.18	Grup keamanan hanya boleh mengizinkan lalu lintas masuk yang tidak terbatas untuk port resmi	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan:, NIST SP 800-53 Rev. 5 AWS Control Tower, NIST SP 800-171 Rev. 2	TINGGI	 Ya	Perubahan dipicu
EC2.19	Kelompok keamanan tidak boleh mengizinkan akses tidak terbatas ke port dengan risiko tinggi	AWS Praktik Terbaik Keamanan Dasar, Standar yang Dikelola Layanan:, NIST SP 800-53 Rev. 5 AWS Control Tower, NIST SP 800-171 Rev. 2	KRITIS	 Tidak	Perubahan dipicu dan periodik
EC2.20	Kedua terowongan VPN untuk koneksi AWS Site-to-Site VPN harus siap	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan:, NIST SP 800-53 Rev. 5 AWS Control Tower, NIST SP 800-171 Rev. 2	MEDIUM	 Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
EC2.21	Jaringan ACLs seharusnya tidak mengizinkan masuknya dari 0.0.0.0/0 ke port 22 atau port 3389	Tolok Ukur AWS Yayasan CIS v3.0.0, Tolok Ukur AWS Yayasan CIS v1.4.0, Praktik Terbaik Keamanan AWS Dasar, Standar yang Dikelola Layanan:, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2 AWS Control Tower, PCI DSS v4.0.1	MEDIUM	 Tidak	Perubahan dipicu
EC2.22	Kelompok EC2 keamanan yang tidak digunakan harus dihapus	Standar yang Dikelola Layanan: AWS Control Tower	MEDIUM	 Tidak	Berkala
EC2.23	EC2 Transit Gateways seharusnya tidak secara otomatis menerima permintaan lampiran VPC	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	TINGGI	 Tidak	Perubahan dipicu
EC2.24	EC2 tipe instance paravirtual tidak boleh digunakan	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
EC2.25	EC2 template peluncuran tidak boleh menetapkan n publik IPs ke antarmuka jaringan	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, Standar yang Dikelola Layanan: AWS Control Tower	TINGGI	 Tidak	Perubahan dipicu
EC2.28	Volume EBS harus dalam rencana cadangan	NIST SP 800-53 Wahyu 5	RENDAH	 Ya	Berkala
EC2.33	EC2 lampiran transit gateway harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
EC2.34	EC2 tabel rute gateway transit harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
EC2.35	EC2 antarmuka jaringan harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
EC2.36	EC2 gateway pelanggan harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
EC2.37	EC2 Alamat IP elastis harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
EC2.38	EC2 instance harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
EC2.39	EC2 gateway internet harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
EC2.40	EC2 Gateway NAT harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
EC2.41	EC2 jaringan ACLs harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
EC2.42	EC2 tabel rute harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
EC2.43	EC2 kelompok keamanan harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
EC2.44	EC2 subnet harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
EC2.45	EC2 volume harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
EC2.46	Amazon VPCs harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
EC2.47	Layanan endpoint Amazon VPC harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
EC2.48	Log aliran VPC Amazon harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
EC2.49	Koneksi peering VPC Amazon harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
EC2.50	EC2 Gateway VPN harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
EC2.51	EC2 Titik akhir Client VPN harus mengaktifkan pencatatan koneksi klien	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1	RENDAH	 Tidak	Perubahan dipicu
EC2.52	EC2 gateway transit harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
EC2.53	EC2 grup keamanan tidak boleh mengizinkan masuknya dari 0.0.0.0/0 ke port administrasi server jarak jauh	Tolok Ukur AWS Yayasan CIS v3.0.0, PCI DSS v4.0.1	TINGGI	 Tidak	Berkala

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
EC2.54	EC2 grup keamanan tidak boleh mengizinkan masuknya dari :/0 ke port administrasi server jarak jauh	Tolok Ukur AWS Yayasan CIS v3.0.0, PCI DSS v4.0.1	TINGGI	 Tidak	Berkala
EC2.55	VPCs harus dikonfigurasi dengan titik akhir antarmuka untuk ECR API	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5	MEDIUM	 Ya	Berkala
EC2.56	VPCs harus dikonfigurasi dengan titik akhir antarmuka untuk Docker Registry	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5	MEDIUM	 Ya	Berkala
EC2.57	VPCs harus dikonfigurasi dengan titik akhir antarmuka untuk Systems Manager	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5	MEDIUM	 Ya	Berkala
EC2.58	VPCs harus dikonfigurasi dengan titik akhir antarmuka untuk Kontak Manajer Insiden Systems Manager	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5	MEDIUM	 Ya	Berkala
EC2.60	VPCs harus dikonfigurasi dengan titik akhir antarmuka untuk Systems Manager Incident Manager	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5	MEDIUM	 Ya	Berkala

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
EC2.170	EC2 template peluncuran harus menggunakan Instance Metadata Service Version 2 () IMDSv2	AWS Praktik Terbaik Keamanan Dasar, PCI DSS v4.0.1	RENDAH	 Tidak	Perubahan dipicu
EC2.171	EC2 Koneksi VPN seharusnya mengaktifkan logging	AWS Praktik Terbaik Keamanan Dasar, PCI DSS v4.0.1	MEDIUM	 Tidak	Perubahan dipicu
EC2.172	EC2 Pengaturan Akses Publik Blok VPC harus memblokir lalu lintas gateway internet	AWS Praktik Terbaik Keamanan Dasar	MEDIUM	 Ya	Perubahan dipicu
EC2.173	EC2 Permintaan Armada Spot harus mengaktifkan enkripsi untuk volume EBS terlampir	AWS Praktik Terbaik Keamanan Dasar	MEDIUM	 Tidak	Perubahan dipicu
EC2.174	EC2 Set opsi DHCP harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
EC2.175	EC2 template peluncuran harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
EC2.176	EC2 daftar awalan harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
EC2.177	EC2 Sesi cermin lalu lintas harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
EC2.178	EC2 filter cermin lalu lintas harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
EC2.179	EC2 target cermin lalu lintas harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
ECR.1	Repositori pribadi ECR harus memiliki pemindaian gambar yang dikonfigurasi	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, Standar yang Dikelola Layanan: AWS Control Tower	TINGGI	 Tidak	Berkala

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
ECR.2	Repositori pribadi ECR harus memiliki kekekalan tag yang dikonfigurasi	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
ECR.3	Repositori ECR harus memiliki setidaknya satu kebijakan siklus hidup yang dikonfigurasi	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
ECR.4	Repositori publik ECR harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
ECR.5	Repositori ECR harus dienkripsi dengan pelanggan yang dikelola AWS KMS keys	NIST SP 800-53 Wahyu 5	MEDIUM	 Ya	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
ECS.1	Definisi tugas Amazon ECS harus memiliki mode jaringan yang aman dan definisi pengguna.	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	TINGGI	 Tidak	Perubahan dipicu
ECS.2	Layanan ECS seharusnya tidak memiliki alamat IP publik yang ditetapkan kepadanya secara otomatis	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, Standar yang Dikelola Layanan: AWS Control Tower	TINGGI	 Tidak	Perubahan dipicu
ECS.3	Definisi tugas ECS tidak boleh berbagi namespace proses host	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	TINGGI	 Tidak	Perubahan dipicu
ECS.4	Kontainer ECS harus berjalan sebagai non-hak istimewa	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	TINGGI	 Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
ECS.5	Kontainer ECS harus dibatasi pada akses hanya-baca ke sistem file root	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	TINGGI	 Tidak	Perubahan dipicu
ECS.8	Rahasia tidak boleh diteruskan sebagai variabel lingkungan kontainer	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, Standar yang Dikelola Layanan: AWS Control Tower	TINGGI	 Tidak	Perubahan dipicu
ECS.9	Definisi tugas ECS harus memiliki konfigurasi logging	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	TINGGI	 Tidak	Perubahan dipicu
ECS.10	Layanan ECS Fargate harus berjalan pada versi platform Fargate terbaru	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, Standar yang Dikelola Layanan: AWS Control Tower	MEDIUM	 Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
ECS.12	Cluster ECS harus menggunakan Wawasan Kontainer	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
ECS.13	Layanan ECS harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
ECS.14	Cluster ECS harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
ECS.15	Definisi tugas ECS harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
ECS.16	Set tugas ECS seharusnya tidak secara otomatis menetapkan alamat IP publik	AWS Praktik Terbaik Keamanan Dasar, PCI DSS v4.0.1	TINGGI	 Tidak	Perubahan dipicu
ECS.17	Definisi tugas ECS tidak boleh menggunakan mode jaringan host	NIST SP 800-53 Wahyu 5	MEDIUM	 Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
EFS.1	Sistem File Elastis harus dikonfigurasi untuk mengenkripsi data file saat istirahat menggunakan AWS KMS	CIS AWS Foundations Benchmark v3.0.0, Praktik Terbaik Keamanan AWS Dasar v1.0.0, Standar yang Dikelola Layanan:, NIST SP 800-53 Rev. 5 AWS Control Tower	MEDIUM	 Tidak	Berkala
EFS.2	Volume Amazon EFS harus ada dalam paket cadangan	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Berkala
EFS.3	Titik akses EFS harus menerapkan direktori root	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
EFS.4	Titik akses EFS harus menegakkan identitas pengguna	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, Standar yang Dikelola Layanan: AWS Control Tower	MEDIUM	 Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
EFS.5	Titik akses EFS harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
EFS.6	Target pemasangan EFS tidak boleh dikaitkan dengan subnet publik	AWS Praktik Terbaik Keamanan Dasar	MEDIUM	 Tidak	Berkala
EFS.7	Sistem file EFS harus mengaktifkan pencadangan otomatis	AWS Praktik Terbaik Keamanan Dasar	MEDIUM	 Tidak	Perubahan dipicu
EFS.8	Sistem file EFS harus dienkripsi saat istirahat	AWS Praktik Terbaik Keamanan Dasar	MEDIUM	 Ya	Perubahan dipicu
EKS.1	Titik akhir kluster EKS tidak boleh diakses publik	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	TINGGI	 Tidak	Berkala
EKS.2	Kluster EKS harus berjalan pada versi Kubernetes yang didukung	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, Standar yang Dikelola Layanan: AWS Control Tower	TINGGI	 Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
EKS.3	Kluster EKS harus menggunakan rahasia Kubernetes terenkripsi	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIUM	 Tidak	Berkala
EKS.6	Kluster EKS harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
EKS.7	Konfigurasi penyedia identitas EKS harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
EKS.8	Kluster EKS harus mengaktifkan pencatatan audit	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIUM	 Tidak	Perubahan dipicu
ElastiCache.1	ElastiCache Cluster (Redis OSS) harus mengaktifkan pencadangan otomatis	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	TINGGI	 Ya	Berkala
ElastiCache.2	ElastiCache cluster harus mengaktifkan peningkatan versi minor otomatis	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	TINGGI	 Tidak	Berkala

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
ElastiCac he.3	ElastiCache grup replikasi harus mengaktifkan failover otomatis	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Berkala
ElastiCac he.4	ElastiCache kelompok replikasi harus encrypted-at-rest	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Berkala
ElastiCac he.5	ElastiCache kelompok replikasi harus encrypted-in-transit	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIUM	 Tidak	Berkala
ElastiCac he.6	ElastiCache (Redis OSS) grup replikasi dari versi sebelumnya harus mengaktifkan Redis OSS AUTH	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIUM	 Tidak	Berkala
ElastiCac he.7	ElastiCache cluster tidak boleh menggunakan grup subnet default	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	TINGGI	 Tidak	Berkala
ElasticBeanstalk.1	Lingkungan Elastic Beanstalk seharusnya mengaktifkan pelaporan kesehatan yang ditingkatkan	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	RENDAH	 Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
ElasticBeanstalk.2	Pembaruan platform yang dikelola Elastic Beanstalk harus diaktifkan	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, Standar yang Dikelola Layanan: AWS Control Tower	TINGGI	 Ya	Perubahan dipicu
ElasticBeanstalk.3	Elastic Beanstalk harus mengalirkan log ke CloudWatch	AWS Praktik Terbaik Keamanan Dasar, PCI DSS v4.0.1	TINGGI	 Ya	Perubahan dipicu
ELB.1	Application Load Balancer harus dikonfigurasi untuk mengalihkan semua permintaan HTTP ke HTTPS	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan:, PCI DSS v3.2.1 AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Berkala
ELB.2	Classic Load Balancer dengan SSL/HTTPS pendengar harus menggunakan sertifikat yang disediakan oleh AWS Certificate Manager	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan:, NIST SP 800-53 Rev. 5 AWS Control Tower, NIST SP 800-171 Rev. 2	MEDIUM	 Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
ELB.3	Pendengar Classic Load Balancer harus dikonfigurasi dengan penghentian HTTPS atau TLS	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1, Standar yang Dikelola Layanan: AWS Control Tower	MEDIUM	 Tidak	Perubahan dipicu
ELB.4	Application Load Balancer harus dikonfigurasi untuk menjatuhkan header http	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, Standar yang Dikelola Layanan: AWS Control Tower	MEDIUM	 Tidak	Perubahan dipicu
ELB.5	Pencatatan aplikasi dan Classic Load Balancer harus diaktifkan	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
ELB.6	Aplikasi, Gateway, dan Network Load Balancers harus mengaktifkan perlindungan penghapusan	AWS Praktik Terbaik Keamanan Dasar, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
ELB.7	Classic Load Balancers harus mengaktifkan pengurusan koneksi	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
ELB.8	Classic Load Balancer dengan pendengar SSL harus menggunakan kebijakan keamanan yang telah ditentukan sebelumnya yang memiliki konfigurasi yang kuat	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1, Standar yang Dikelola Layanan: AWS Control Tower	MEDIUM	 Tidak	Perubahan dipicu
ELB.9	Penyeimbang Beban Klasik harus mengaktifkan penyeimbangan beban lintas zona	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
ELB.10	Classic Load Balancer harus menjangkau beberapa Availability Zone	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Ya	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
ELB.12	Application Load Balancer harus dikonfigurasi dengan mode mitigasi desync defensif atau paling ketat	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, Standar yang Dikelola Layanan: AWS Control Tower	MEDIUM	 Tidak	Perubahan dipicu
ELB.13	Penyeimbang Beban Aplikasi, Jaringan, dan Gateway harus menjangkau beberapa Availability Zone	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Ya	Perubahan dipicu
ELB.14	Classic Load Balancer harus dikonfigurasi dengan mode mitigasi desync defensif atau paling ketat	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, Standar yang Dikelola Layanan: AWS Control Tower	MEDIUM	 Tidak	Perubahan dipicu
ELB.16	Application Load Balancers harus dikaitkan dengan ACL web AWS WAF	NIST SP 800-53 Wahyu 5	MEDIUM	 Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
ELB.17	Aplikasi dan Network Load Balancer dengan pendengar harus menggunakan kebijakan keamanan yang direkomen dasikan	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
EMR.1	Node primer klaster EMR Amazon seharusnya tidak memiliki alamat IP publik	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, Standar yang Dikelola Layanan: AWS Control Tower	TINGGI	 Tidak	Berkala
EMR.2	Amazon EMR memblokir pengaturan akses publik harus diaktifkan	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	KRITIS	 Tidak	Berkala
EMR.3	Konfigurasi keamanan Amazon EMR harus dienkripsi saat istirahat	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
EMR.4	Konfigurasi keamanan Amazon EMR harus dienkripsi saat transit	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
ES.1	Domain Elasticsearch harus mengaktifkan enkripsi saat istirahat	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan:, PCI DSS v3.2.1 AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Berkala
ES.2	Domain Elasticsearch tidak boleh diakses publik	AWS Praktik Terbaik Keamanan Dasar, PCI DSS v3.2.1, PCI DSS v4.0.1, NIST SP 800-53 Rev. 5, Standar yang Dikelola Layanan: AWS Control Tower	KRITIS	 Tidak	Berkala
ES.3	Domain Elasticsearch harus mengenkripsi data yang dikirim antar node	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, Standar yang Dikelola Layanan:, AWS Control Tower	MEDIUM	 Tidak	Perubahan dipicu
ES.4	Kesalahan domain Elasticsearch yang masuk ke CloudWatch Log harus diaktifkan	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
ES.5	Domain Elasticsearch harus mengaktifkan pencatatan audit	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, Standar yang Dikelola Layanan: AWS Control Tower	MEDIUM	 Tidak	Perubahan dipicu
ES.6	Domain Elasticsearch harus memiliki setidaknya tiga node data	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
ES.7	Domain Elasticsearch harus dikonfigurasi dengan setidaknya tiga node master khusus	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
ES.8	Koneksi ke domain Elasticsearch harus dienkripsi menggunakan kebijakan keamanan TLS terbaru	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, Standar yang Dikelola Layanan: AWS Control Tower	MEDIUM	 Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
ES.9	Domain Elasticsearch harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
EventBridge.2	EventBridge bus acara harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
EventBridge.3	EventBridge bus acara khusus harus memiliki kebijakan berbasis sumber daya terlampir	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	RENDAH	 Tidak	Perubahan dipicu
EventBridge.4	EventBridge titik akhir global harus mengaktifkan replikasi acara	NIST SP 800-53 Wahyu 5	MEDIUM	 Tidak	Perubahan dipicu
FraudDetector.1	Jenis entitas Amazon Fraud Detector harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
FraudDetector.2	Label Amazon Fraud Detector harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
FraudDetector.3	Hasil Amazon Fraud Detector harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
FraudDetector.4	Variabel Amazon Fraud Detector harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
FSx.1	FSx untuk sistem file OpenZFS harus dikonfigurasi untuk menyalin tag ke backup dan volume	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	RENDAH	 Tidak	Berkala
FSx.2	FSx untuk sistem file Lustre harus dikonfigurasi untuk menyalin tag ke cadangan	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5	RENDAH	 Tidak	Berkala
FSx.3	FSx untuk sistem file OpenZFS harus dikonfigurasi untuk penyebaran Multi-AZ	AWS Praktik Terbaik Keamanan Dasar	MEDIUM	 Tidak	Berkala
FSx.4	FSx untuk sistem file NetApp ONTAP harus dikonfigurasi untuk penyebaran Multi-AZ	AWS Praktik Terbaik Keamanan Dasar	MEDIUM	 Ya	Berkala

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
FSx.5	FSx untuk sistem file Windows File Server harus dikonfigurasi untuk penyebaran Multi-AZ	AWS Praktik Terbaik Keamanan Dasar	MEDIUM	 Tidak	Berkala
Lem. 1	AWS Glue pekerjaan harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
Lem.3	AWS Glue transformasi pembelajaran mesin harus dienkripsi saat istirahat	AWS Praktik Terbaik Keamanan Dasar	MEDIUM	 Tidak	Perubahan dipicu
Lem.4	AWS Glue Pekerjaan percikan harus berjalan pada versi yang didukung AWS Glue	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
GlobalAccelerator.1	Akselerator Global Accelerator harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
GuardDuty .1	GuardDuty harus diaktifkan	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v3.2.1, PCI DSS v4.0.1, Standar yang Dikelola Layanan: AWS Control Tower	TINGGI	 Tidak	Berkala
GuardDuty .2	GuardDuty filter harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
GuardDuty .3	GuardDuty IPSets harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
GuardDuty .4	GuardDuty detektor harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
GuardDuty .5	GuardDuty Pemantauan Log Audit EKS harus diaktifkan	AWS Praktik Terbaik Keamanan Dasar	TINGGI	 Tidak	Berkala

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
GuardDuty .6	GuardDuty Perlindungan Lambda harus diaktifkan	AWS Praktik Terbaik Keamanan Dasar, PCI DSS v4.0.1	TINGGI	 Tidak	Berkala
GuardDuty .7	GuardDuty EKS Runtime Monitoring harus diaktifkan	AWS Praktik Terbaik Keamanan Dasar, PCI DSS v4.0.1	MEDIUM	 Tidak	Berkala
GuardDuty .8	GuardDuty Perlindungan Malware untuk EC2 harus diaktifkan	AWS Praktik Terbaik Keamanan Dasar	TINGGI	 Tidak	Berkala
GuardDuty .9	GuardDuty Perlindungan RDS harus diaktifkan	AWS Praktik Terbaik Keamanan Dasar, PCI DSS v4.0.1	TINGGI	 Tidak	Berkala
GuardDuty .10	GuardDuty Perlindungan S3 harus diaktifkan	AWS Praktik Terbaik Keamanan Dasar, PCI DSS v4.0.1	TINGGI	 Tidak	Berkala
GuardDuty .11	GuardDuty Runtime Monitoring harus diaktifkan	AWS Praktik Terbaik Keamanan Dasar	TINGGI	 Tidak	Berkala

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
GuardDuty .12	GuardDuty ECS Runtime Monitoring harus diaktifkan	AWS Praktik Terbaik Keamanan Dasar	MEDIUM	 Tidak	Berkala
GuardDuty .13	GuardDuty EC2 Runtime Monitoring harus diaktifkan	AWS Praktik Terbaik Keamanan Dasar	MEDIUM	 Tidak	Berkala
IAM.1	Kebijakan IAM seharusnya tidak mengizinkan hak administratif “*” penuh	Tolok Ukur AWS Yayasan CIS v1.2.0, Praktik Terbaik Keamanan AWS Dasar v1.0.0, Standar yang Dikelola Layanan:, PCI DSS v3.2.1, Tolok Ukur AWS Yayasan CIS v1.4.0 AWS Control Tower, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2	TINGGI	 Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
IAM.2	Pengguna IAM seharusnya tidak memiliki kebijakan IAM yang dilampirkan	Tolok Ukur AWS Yayasan CIS v3.0.0, Tolok Ukur AWS Yayasan CIS v1.2.0, Praktik Terbaik Keamanan AWS Dasar v1.0.0, Standar yang Dikelola Layanan:, PCI DSS v3.2.1, NIST SP 800-53 Rev. 5, NIST SP AWS Control Tower 800-171 Rev. 2	RENDAH	 Tidak	Perubahan dipicu
IAM.3	Kunci akses pengguna IAM harus diputar setiap 90 hari atau kurang	Tolok Ukur AWS Yayasan CIS v3.0.0, Tolok Ukur AWS Yayasan CIS v1.4.0, Tolok Ukur Yayasan CIS v1.2.0, Praktik Terbaik Keamanan AWS Dasar, NIST AWS SP 800-53 Rev. 5, PCI DSS v4.0.1, Standar yang Dikelola Layanan: AWS Control Tower	MEDIUM	 Tidak	Berkala

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
IAM.4	Kunci akses pengguna root IAM seharusnya tidak ada	Tolok Ukur AWS Yayasan CIS v3.0.0, Tolok Ukur Yayasan CIS v1.4.0, Tolok Ukur AWS Yayasan CIS v1.2.0, Praktik Terbaik Keamanan AWS Dasar v1.0.0, AWS Standar yang Dikelola Layanan:, PCI DSS v3.2.1, NIST SP 800-53 Rev. 5 AWS Control Tower	KRITIS	 Tidak	Berkala
IAM.5	MFA harus diaktifkan untuk semua pengguna IAM yang memiliki kata sandi konsol	Tolok Ukur AWS Yayasan CIS v3.0.0, Tolok Ukur AWS Yayasan CIS v1.4.0, Tolok Ukur Yayasan CIS v1.2.0, Praktik Terbaik Keamanan AWS Dasar, NIST AWS SP 800-53 Rev. 5, PCI DSS v4.0.1, Standar yang Dikelola Layanan: AWS Control Tower	MEDIUM	 Tidak	Berkala

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
IAM.6	MFA perangkat keras harus diaktifkan untuk pengguna root	Tolok Ukur AWS Yayasan CIS v3.0.0, Tolok Ukur AWS Yayasan CIS v1.4.0, Tolok Ukur Yayasan CIS AWS v1.2.0, Praktik Terbaik Keamanan AWS Dasar, NIST SP 800-53 Rev. 5, PCI DSS v3.2.1, PCI DSS v4.0.1, Standar yang Dikelola Layanan: AWS Control Tower	KRITIS	 Tidak	Berkala
IAM.7	Kebijakan kata sandi untuk pengguna IAM harus memiliki konfigurasi yang kuat	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1, Standar yang Dikelola Layanan: AWS Control Tower	MEDIUM	 Ya	Berkala

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
IAM.8	Kredensyal pengguna IAM yang tidak digunakan harus dihapus	Tolok Ukur AWS Yayasan CIS v1.2.0, Praktik Terbaik Keamanan AWS Dasar, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v3.2.1, PCI DSS v4.0.1, Standar yang Dikelola Layanan: AWS Control Tower	MEDIUM	 Tidak	Berkala
IAM.9	MFA harus diaktifkan untuk pengguna root	Tolok Ukur AWS Yayasan CIS v3.0.0, Tolok Ukur Yayasan CIS v1.4.0, Tolok Ukur AWS Yayasan CIS v1.2.0, NIST SP 800-53 AWS Rev. 5, PCI DSS v3.2.1, PCI DSS v4.0.1	KRITIS	 Tidak	Berkala
IAM.10	Kebijakan kata sandi untuk pengguna IAM harus memiliki konfigurasi yang kuat	NIST SP 800-171 Wahyu 2, PCI DSS v3.2.1	MEDIUM	 Tidak	Berkala
IAM.11	Pastikan kebijakan kata sandi IAM memerlukan setidaknya satu huruf besar	Tolok Ukur AWS Yayasan CIS v1.2.0, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1	MEDIUM	 Tidak	Berkala

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
IAM.12	Pastikan kebijakan kata sandi IAM memerlukan setidaknya satu huruf kecil	Tolok Ukur AWS Yayasan CIS v1.2.0, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1	MEDIUM	 Tidak	Berkala
IAM.13	Pastikan kebijakan kata sandi IAM memerlukan setidaknya satu simbol	Tolok Ukur AWS Yayasan CIS v1.2.0, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1	MEDIUM	 Tidak	Berkala
IAM.14	Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu nomor	Tolok Ukur AWS Yayasan CIS v1.2.0, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1	MEDIUM	 Tidak	Berkala
IAM.15	Pastikan kebijakan kata sandi IAM memerlukan panjang kata sandi minimum 14 atau lebih	Tolok Ukur AWS Yayasan CIS v3.0.0, Tolok Ukur Yayasan CIS v1.4.0, Tolok Ukur AWS Yayasan CIS v1.2.0, NIST SP 800-171 AWS Rev. 2	MEDIUM	 Tidak	Berkala

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
IAM.16	Pastikan kebijakan kata sandi IAM mencegah penggunaan kembali kata sandi	Tolok Ukur AWS Yayasan CIS v3.0.0, Tolok Ukur Yayasan CIS v1.4.0, Tolok Ukur AWS Yayasan CIS v1.2.0, NIST SP 800-171 AWS Rev. 2, PCI DSS v4.0.1	RENDAH	 Tidak	Berkala
IAM.17	Pastikan kebijakan kata sandi IAM kedaluwarsa kata sandi dalam waktu 90 hari atau kurang	Tolok Ukur AWS Yayasan CIS v1.2.0, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1	RENDAH	 Tidak	Berkala
IAM.18	Pastikan peran dukungan telah dibuat untuk mengelola insiden dengan AWS Dukungan	Tolok Ukur AWS Yayasan CIS v3.0.0, Tolok Ukur Yayasan CIS v1.4.0, Tolok Ukur AWS Yayasan CIS v1.2.0, NIST SP 800-171 AWS Rev. 2, PCI DSS v4.0.1	RENDAH	 Tidak	Berkala
IAM.19	MFA harus diaktifkan untuk semua pengguna IAM	NIST SP 800-53 Wahyu 5, NIST SP 800-171 Wahyu 2, PCI DSS v3.2.1, PCI DSS v4.0.1	MEDIUM	 Tidak	Berkala

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
IAM.21	Kebijakan terkelola pelanggan IAM yang Anda buat tidak boleh mengizinkan tindakan wildcard untuk layanan	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan:, NIST SP 800-53 Rev. 5 AWS Control Tower, NIST SP 800-171 Rev. 2	RENDAH	 Tidak	Perubahan dipicu
IAM.22	Kredensi pengguna IAM yang tidak digunakan selama 45 hari harus dihapus	Tolok Ukur AWS Yayasan CIS v3.0.0, Tolok Ukur Yayasan CIS v1.4.0, NIST SP AWS 800-171 Rev. 2	MEDIUM	 Tidak	Berkala
IAM.23	Alat analisis IAM Access Analyzer harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
IAM.24	Peran IAM harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
IAM.25	Pengguna IAM harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
IAM.26	SSL/TLS Sertifikat kedaluwarsa yang dikelola di IAM harus dihapus	Tolok Ukur AWS Yayasan CIS v3.0.0	MEDIUM	 Tidak	Berkala
IAM.27	Identitas IAM seharusnya tidak memiliki kebijakan yang dilampirkan AWSCloud ShellFull Access	Tolok Ukur AWS Yayasan CIS v3.0.0	MEDIUM	 Tidak	Perubahan dipicu
IAM.28	IAM Access Analyzer penganalisis akses eksternal harus diaktifkan	Tolok Ukur AWS Yayasan CIS v3.0.0	TINGGI	 Tidak	Berkala
Inspektor .1	EC2 Pemindaian Amazon Inspector harus diaktifkan	AWS Praktik Terbaik Keamanan Dasar, PCI DSS v4.0.1	TINGGI	 Tidak	Berkala
Inspektor .2	Pemindaian ECR Amazon Inspector harus diaktifkan	AWS Praktik Terbaik Keamanan Dasar, PCI DSS v4.0.1	TINGGI	 Tidak	Berkala
Inspektor .3	Pemindaian kode Amazon Inspector Lambda harus diaktifkan	AWS Praktik Terbaik Keamanan Dasar, PCI DSS v4.0.1	TINGGI	 Tidak	Berkala

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
Inspektor .4	Pemindaian standar Amazon Inspector Lambda harus diaktifkan	AWS Praktik Terbaik Keamanan Dasar, PCI DSS v4.0.1	TINGGI	 Tidak	Berkala
IoT.1	AWS IoT Device Defender profil keamanan harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
IoT.2	AWS IoT Core tindakan mitigasi harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
IoT.3	AWS IoT Core dimensi harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
IoT.4	AWS IoT Core otorisasi harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
IoT.5	AWS IoT Core alias peran harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
IoT.6	AWS IoT Core kebijakan harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
IoTEvents .1	AWS IoT Events input harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
IoTEvents .2	AWS IoT Events model detektor harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
IoTEvents .3	AWS IoT Events model alarm harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
IoT Site Bijak.1	AWS IoT SiteWise model aset harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
IoT Site Bijak.2	AWS IoT SiteWise dasbor harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
Io TSite Bijak.3	AWS IoT SiteWise gateway harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
Io TSite Bijak.4	AWS IoT SiteWise portal harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
Io TSite Bijak.5	AWS IoT SiteWise proyek harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
TTwinPemuat lo. 1	AWS Pekerjaan TwinMaker sinkronisasi IoT harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
TTwinPemuat lo.2	AWS TwinMaker Ruang kerja IoT harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
TTwinPemuat lo.3	AWS TwinMaker Adegan IoT harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
TwinMaker uat lo.4	AWS TwinMaker Entitas IoT harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
IoT Wireless	AWS Grup multicast Nirkabel IoT harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
IoT Wireless	AWS Profil layanan IoT Wireless harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
IoT Wireless	AWS Tugas FUOTA IoT Wireless harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
IVS.1	Pasangan kunci pemutaran IVS harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
IVS.2	Konfigurasi perekaman IVS harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
IVS.3	Saluran IVS harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
Ruang kunci.1	Ruang kunci Amazon Keyspaces harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
Kinesis.1	Aliran Kinesis harus dienkripsi saat istirahat	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
Kinesis.2	Aliran Kinesis harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
Kinesis.3	Aliran Kinesis harus memiliki periode retensi data yang memadai	AWS Praktik Terbaik Keamanan Dasar	MEDIUM	 Ya	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
KMS.1	Kebijakan yang dikelola pelanggan IAM tidak boleh mengizinkan tindakan dekripsi pada semua kunci KMS	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
KMS.2	Prinsipal IAM seharusnya tidak memiliki kebijakan inline IAM yang memungkinkan tindakan dekripsi pada semua kunci KMS	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
KMS.3	AWS KMS keys tidak boleh dihapus secara tidak sengaja	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	KRITIS	 Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
KMS.4	AWS KMS key rotasi harus diaktifkan	Tolok Ukur AWS Yayasan CIS v3.0.0, Tolok Ukur Yayasan CIS v1.4.0, Tolok Ukur AWS Yayasan CIS v1.2.0, NIST SP 800-53 AWS Rev. 5, PCI DSS v3.2.1, PCI DSS v4.0.1	MEDIUM	 Tidak	Berkala
KMS.5	Kunci KMS tidak boleh diakses publik	AWS Praktik Terbaik Keamanan Dasar	KRITIS	 Tidak	Perubahan dipicu
Lambda.1	Kebijakan fungsi Lambda harus melarang akses publik	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v3.2.1, PCI DSS v4.0.1, Standar yang Dikelola Layanan: AWS Control Tower	KRITIS	 Tidak	Perubahan dipicu
Lambda.2	Fungsi Lambda harus menggunakan runtime yang didukung	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, Standar yang Dikelola Layanan: AWS Control Tower	MEDIUM	 Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
Lambda.3	Fungsi Lambda harus dalam VPC	PCI DSS v3.2.1, NIST SP 800-53 Wahyu 5	RENDAH	 Tidak	Perubahan dipicu
Lambda.5	Fungsi VPC Lambda harus beroperasi di beberapa Availability Zone	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Ya	Perubahan dipicu
Lambda.6	Fungsi Lambda harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
Macie.1	Amazon Macie harus diaktifkan	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Berkala
Macie.2	Penemuan data sensitif otomatis Macie harus diaktifkan	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	TINGGI	 Tidak	Berkala
MSK.1	Cluster MSK harus dienkripsi dalam perjalanan di antara node broker	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIUM	 Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
MSK.2	Cluster MSK harus memiliki pemantauan yang ditingkatkan yang dikonfigurasi	NIST SP 800-53 Wahyu 5	RENDAH	 Tidak	Perubahan dipicu
MSK.3	Konektor MSK Connect harus dienkripsi saat transit	AWS Praktik Terbaik Keamanan Dasar, PCI DSS v4.0.1	MEDIUM	 Tidak	Perubahan dipicu
MQ.2	Broker ActiveMQ harus mengalirkan log audit ke CloudWatch	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIUM	 Tidak	Perubahan dipicu
MQ.3	Broker Amazon MQ harus mengaktifkan peningkatan versi minor otomatis	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	RENDAH	 Tidak	Perubahan dipicu
MQ.4	Broker Amazon MQ harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
MQ.5	Broker ActiveMQ harus menggunakan mode penerapan active/standby	NIST SP 800-53 Rev. 5, Standar yang Dikelola Layanan: AWS Control Tower	RENDAH	 Tidak	Perubahan dipicu
MQ.6	Broker RabbitMQ harus menggunakan mode penerapan cluster	NIST SP 800-53 Rev. 5, Standar yang Dikelola Layanan: AWS Control Tower	RENDAH	 Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
Neptunus. 1	Cluster DB Neptunus harus dienkripsi saat istirahat	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5, Standar yang Dikelola Layanan: AWS Control Tower	MEDIUM	 Tidak	Perubahan dipicu
Neptunus. 2	Cluster DB Neptunus harus mempublikasikan log audit ke Log CloudWatch	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, Standar yang Dikelola Layanan: AWS Control Tower	MEDIUM	 Tidak	Perubahan dipicu
Neptunus. 3	Snapshot cluster Neptunus DB seharusnya tidak bersifat publik	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, Standar yang Dikelola Layanan: AWS Control Tower	KRITIS	 Tidak	Perubahan dipicu
Neptunus. 4	Cluster DB Neptunus harus mengaktifkan perlindungan penghapusan	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5, Standar yang Dikelola Layanan: AWS Control Tower	RENDAH	 Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
Neptunus. 5	Cluster DB Neptunus harus mengaktifkan cadangan otomatis	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5, Standar yang Dikelola Layanan: AWS Control Tower	MEDIUM	 Ya	Perubahan dipicu
Neptunus. 6	Snapshot cluster Neptunus DB harus dienkripsi saat istirahat	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5, Standar yang Dikelola Layanan: AWS Control Tower	MEDIUM	 Tidak	Perubahan dipicu
Neptunus. 7	Cluster DB Neptunus harus mengaktifkan otentikasi database IAM	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5, Standar yang Dikelola Layanan: AWS Control Tower	MEDIUM	 Tidak	Perubahan dipicu
Neptunus. 8	Cluster DB Neptunus harus dikonfigurasi untuk menyalin tag ke snapshot	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5, Standar yang Dikelola Layanan: AWS Control Tower	RENDAH	 Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
Neptunus.9	Cluster DB Neptunus harus digunakan di beberapa Availability Zone	NIST SP 800-53 Wahyu 5	MEDIUM	 Tidak	Perubahan dipicu
NetworkFirewall.1	Firewall Network Firewall harus digunakan di beberapa Availability Zone	NIST SP 800-53 Wahyu 5	MEDIUM	 Tidak	Perubahan dipicu
NetworkFirewall.2	Pencatatan Network Firewall harus diaktifkan	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2	MEDIUM	 Tidak	Berkala
NetworkFirewall.3	Kebijakan Network Firewall harus memiliki setidaknya satu kelompok aturan yang terkait	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan:, NIST SP 800-53 Rev. 5 AWS Control Tower, NIST SP 800-171 Rev. 2	MEDIUM	 Tidak	Perubahan dipicu
NetworkFirewall.4	Tindakan stateless default untuk kebijakan Network Firewall harus dijatuhkan atau diteruskan untuk paket lengkap	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
NetworkFirewall.5	Tindakan stateless default untuk kebijakan Network Firewall harus dijatuhkan atau diteruskan untuk paket yang terfragmentasi	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan:, NIST SP 800-53 Rev. 5 AWS Control Tower, NIST SP 800-171 Rev. 2	MEDIUM	 Tidak	Perubahan dipicu
NetworkFirewall.6	Grup aturan firewall jaringan stateless tidak boleh kosong	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan:, NIST SP 800-53 Rev. 5 AWS Control Tower, NIST SP 800-171 Rev. 2	MEDIUM	 Tidak	Perubahan dipicu
NetworkFirewall.7	Firewall Network Firewall harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
NetworkFirewall.8	Kebijakan firewall Network Firewall harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
NetworkFirewall.9	Firewall Network Firewall harus mengaktifkan perlindungan penghapusan	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
NetworkFirewall.10	Firewall Network Firewall harus mengaktifkan perlindungan perubahan subnet	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
OpenSearch.h.1	OpenSearch domain harus mengaktifkan enkripsi saat istirahat	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan:, PCI DSS v3.2.1 AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
OpenSearch.h.2	OpenSearch domain tidak boleh diakses publik	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan:, PCI DSS v3.2.1 AWS Control Tower, NIST SP 800-53 Rev. 5	KRITIS	 Tidak	Perubahan dipicu
OpenSearch.h.3	OpenSearch domain harus mengenkripsi data yang dikirim antar node	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
Opensearch h.4	OpenSearch kesalahan domain saat masuk ke CloudWatch Log harus diaktifkan	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
Opensearch h.5	OpenSearch domain harus mengaktifkan pencatatan audit	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, Standar yang Dikelola Layanan: AWS Control Tower	MEDIUM	 Tidak	Perubahan dipicu
Opensearch h.6	OpenSearch domain harus memiliki setidaknya tiga node data	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
Opensearch h.7	OpenSearch domain harus mengaktifkan kontrol akses berbutir halus	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	TINGGI	 Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
Opensearch h.8	Koneksi ke OpenSearch domain harus dienkripsi i menggunakan kebijakan keamanan TLS terbaru	AWS Praktik Terbaik Keamanan Dasar, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
Opensearch h.9	OpenSearch domain harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
Opensearch h.10	OpenSearch domain harus memiliki pembaruan perangkat lunak terbaru yang diinstal	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	RENDAH	 Tidak	Perubahan dipicu
Opensearch h.11	OpenSearch domain harus memiliki setidaknya tiga node primer khusus	NIST SP 800-53 Wahyu 5	RENDAH	 Tidak	Berkala
PCA.1	AWS Private CA otoritas sertifikat root harus dinonaktifkan	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	RENDAH	 Tidak	Berkala
PCA.2	AWS Otoritas sertifikat CA swasta harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
RDS.1	Snapshot RDS harus bersifat pribadi	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan:, PCI DSS v3.2.1 AWS Control Tower, NIST SP 800-53 Rev. 5	KRITIS	 Tidak	Perubahan dipicu
RDS.2	Instans RDS DB harus melarang akses publik, sebagaimana ditentukan oleh konfigurasi PubliclyAccessible	Tolok Ukur AWS Yayasan CIS v3.0.0, Praktik Terbaik Keamanan AWS Dasar, Standar yang Dikelola Layanan:, NIST SP 800-53 Rev. 5, PCI DSS v3.2.1 AWS Control Tower, PCI DSS v4.0.1	KRITIS	 Tidak	Perubahan dipicu
RDS.3	Instans RDS DB harus mengaktifkan enkripsi saat istirahat	Tolok Ukur AWS Yayasan CIS v3.0.0, Tolok Ukur AWS Yayasan CIS v1.4.0, Praktik Terbaik Keamanan AWS Dasar v1.0.0, Standar yang Dikelola Layanan:, NIST SP 800-53 Rev. 5 AWS Control Tower	MEDIUM	 Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
RDS.4	Snapshot cluster RDS dan snapshot database harus dienkripsi saat istirahat	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
RDS.5	Instans RDS DB harus dikonfigurasi dengan beberapa Availability Zone	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
RDS.6	Pemantauan yang ditingkatkan harus dikonfigurasi untuk instans RDS DB	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	RENDAH	 Ya	Perubahan dipicu
RDS.7	Cluster RDS harus mengaktifkan perlindungan penghapusan	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	RENDAH	 Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
RDS.8	Instans RDS DB harus mengaktifkan perlindungan penghapusan	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	RENDAH	 Tidak	Perubahan dipicu
RDS.9	Instans RDS DB harus menerbitkan log ke Log CloudWatch	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, Standar yang Dikelola Layanan: AWS Control Tower	MEDIUM	 Tidak	Perubahan dipicu
RDS.10	Autentikasi IAM harus dikonfigurasi untuk instance RDS	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
RDS.11	Instans RDS harus mengaktifkan pencadangan otomatis	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Ya	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
RDS.12	Autentikasi IAM harus dikonfigurasi untuk cluster RDS	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
RDS.13	Peningkatan versi minor otomatis RDS harus diaktifkan	Tolok Ukur AWS Yayasan CIS v3.0.0, Praktik Terbaik Keamanan AWS Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, Standar yang Dikelola Layanan: AWS Control Tower	TINGGI	 Tidak	Perubahan dipicu
RDS.14	Cluster Amazon Aurora seharusnya mengaktifkan backtracking	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	MEDIUM	 Ya	Perubahan dipicu
RDS.15	Cluster RDS DB harus dikonfigurasi untuk beberapa Availability Zone	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
RDS.16	Cluster RDS DB harus dikonfigurasi untuk menyalin tag ke snapshot	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	RENDAH	 Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
RDS.17	Instans RDS DB harus dikonfigurasi untuk menyalin tag ke snapshot	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	RENDAH	 Tidak	Perubahan dipicu
RDS.18	Instans RDS harus digunakan dalam VPC	Standar yang Dikelola Layanan: AWS Control Tower	TINGGI	 Tidak	Perubahan dipicu
RDS.19	Langganan pemberitahuan acara RDS yang ada harus dikonfigurasi untuk peristiwa klaster kritis	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	RENDAH	 Tidak	Perubahan dipicu
RDS.20	Langganan pemberitahuan acara RDS yang ada harus dikonfigurasi untuk peristiwa instance database penting	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, Standar yang Dikelola Layanan: AWS Control Tower	RENDAH	 Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
RDS.21	Langganan pemberitahuan acara RDS harus dikonfigurasi untuk peristiwa grup parameter basis data kritis	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, Standar yang Dikelola Layanan: AWS Control Tower	RENDAH	 Tidak	Perubahan dipicu
RDS.22	Langganan pemberitahuan acara RDS harus dikonfigurasi untuk peristiwa grup keamanan basis data penting	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, Standar yang Dikelola Layanan: AWS Control Tower	RENDAH	 Tidak	Perubahan dipicu
RDS.23	Instans RDS tidak boleh menggunakan port default mesin database	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	RENDAH	 Tidak	Perubahan dipicu
RDS.24	Cluster Database RDS harus menggunakan nama pengguna administrator khusus	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIUM	 Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
RDS.25	Instans database RDS harus menggunakan nama pengguna administrator khusus	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, Standar yang Dikelola Layanan: AWS Control Tower	MEDIUM	 Tidak	Perubahan dipicu
RDS.26	Instans RDS DB harus dilindungi oleh rencana cadangan	NIST SP 800-53 Wahyu 5	MEDIUM	 Ya	Berkala
RDS.27	Cluster RDS DB harus dienkripsi saat istirahat	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5, Standar yang Dikelola Layanan: AWS Control Tower	MEDIUM	 Tidak	Perubahan dipicu
RDS.28	Cluster RDS DB harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
RDS.29	Snapshot cluster RDS DB harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
RDS.30	Instans RDS DB harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
RDS.31	Grup keamanan RDS DB harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
RDS.32	Snapshot RDS DB harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
RDS.33	Grup subnet RDS DB harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
RDS.34	Cluster Aurora MySQL DB harus mempublikasikan log audit ke Log CloudWatch	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIUM	 Tidak	Perubahan dipicu
RDS.35	Cluster RDS DB harus mengaktifkan peningkatan versi minor otomatis	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIUM	 Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
RDS.36	RDS untuk instance PostgreSQL DB harus mempublikasikan log ke Log CloudWatch	AWS Praktik Terbaik Keamanan Dasar, PCI DSS v4.0.1	MEDIUM	 Ya	Perubahan dipicu
RDS.37	Cluster Aurora PostgreSQL DB harus mempublikasikan log ke Log CloudWatch	AWS Praktik Terbaik Keamanan Dasar, PCI DSS v4.0.1	MEDIUM	 Tidak	Perubahan dipicu
RDS.38	RDS untuk instance PostgreSQL DB harus dienkripsi saat transit	AWS Praktik Terbaik Keamanan Dasar	MEDIUM	 Tidak	Berkala
RDS.39	RDS untuk instance MySQL DB harus dienkripsi saat transit	AWS Praktik Terbaik Keamanan Dasar	MEDIUM	 Tidak	Berkala
RDS.40	RDS untuk instance SQL Server DB harus mempublikasikan log ke Log CloudWatch	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5	MEDIUM	 Ya	Perubahan dipicu
RDS.41	RDS untuk instans SQL Server DB harus dienkripsi saat transit	AWS Praktik Terbaik Keamanan Dasar	MEDIUM	 Tidak	Berkala

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
RDS.42	RDS untuk instance MariaDB DB harus mempublikasikan log ke Log CloudWatch	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5	MEDIUM	 Ya	Berkala
RDS.44	RDS untuk instance MariaDB DB harus dienkripsi saat transit	AWS Praktik Terbaik Keamanan Dasar	MEDIUM	 Tidak	Berkala
Pergeseran merah.1	Cluster Amazon Redshift harus melarang akses publik	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v3.2.1, PCI DSS v4.0.1, Standar yang Dikelola Layanan: AWS Control Tower	KRITIS	 Tidak	Perubahan dipicu
Pergeseran merah.2	Koneksi ke cluster Amazon Redshift harus dienkripsi saat transit	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, Standar yang Dikelola Layanan: AWS Control Tower	MEDIUM	 Tidak	Perubahan dipicu
Pergeseran merah.3	Cluster Amazon Redshift harus mengaktifkan snapshot otomatis	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	MEDIUM	 Ya	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
Pergeseran merah.4	Cluster Amazon Redshift harus mengaktifkan pencatatan audit	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, Standar yang Dikelola Layanan: AWS Control Tower	MEDIUM	 Tidak	Perubahan dipicu
Pergeseran merah.6	Amazon Redshift harus mengaktifkan peningkatan otomatis ke versi utama	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
Pergeseran merah.7	Cluster Redshift harus menggunakan perutean VPC yang ditingkatkan	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
Pergeseran merah.8	Cluster Amazon Redshift tidak boleh menggunakan nama pengguna Admin default	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
Pergeseran Merah.9	Cluster Redshift tidak boleh menggunakan nama database default	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
Pergeseran Merah.10	Cluster Redshift harus dienkripsi saat istirahat	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
Pergeseran Merah.11	Cluster Redshift harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
Pergeseran Merah.12	Pemberitahuan berlangganan acara Redshift harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
Pergeseran Merah.13	Cuplikan klaster Redshift harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
Pergeseran Merah.14	Grup subnet cluster Redshift harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
Pergeseran Merah.15	Grup keamanan Redshift harus mengizinkan masuknya pada port cluster hanya dari asal yang dibatasi	AWS Praktik Terbaik Keamanan Dasar, PCI DSS v4.0.1	TINGGI	 Tidak	Berkala
Pergeseran Merah.16	Grup subnet cluster Redshift harus memiliki subnet dari beberapa Availability Zone	NIST SP 800-53 Wahyu 5	MEDIUM	 Tidak	Perubahan dipicu
Pergeseran Merah.17	Grup parameter cluster Redshift harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
Redshift Serverless.1	Grup kerja Amazon Redshift Tanpa Server harus menggunakan perutean VPC yang disempurnakan	AWS Praktik Terbaik Keamanan Dasar	TINGGI	 Tidak	Berkala

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
RedshiftServerless.2	Koneksi ke grup kerja Redshift Serverless harus diperlukan untuk menggunakan SSL	AWS Praktik Terbaik Keamanan Dasar	MEDIUM	 Tidak	Berkala
RedshiftServerless.3	Kelompok kerja Redshift Tanpa Server harus melarang akses publik	AWS Praktik Terbaik Keamanan Dasar	TINGGI	 Tidak	Berkala
RedshiftServerless.4	Ruang nama Redshift Tanpa Server harus dienkripsi dengan pengelolaan pelanggan AWS KMS keys	NIST SP 800-53 Wahyu 5	MEDIUM	 Ya	Berkala
RedshiftServerless.5	Ruang nama Redshift Tanpa Server tidak boleh menggunakan nama pengguna admin default	AWS Praktik Terbaik Keamanan Dasar	MEDIUM	 Ya	Berkala
RedshiftServerless.6	Ruang nama Redshift Tanpa Server harus mengeksport log ke Log CloudWatch	AWS Praktik Terbaik Keamanan Dasar	MEDIUM	 Tidak	Berkala

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
RedshiftServerless.7	Ruang nama Redshift Tanpa Server tidak boleh menggunakan nama database default	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Berkala
Route53.1	Pemeriksaan kesehatan Route 53 harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
Route53.2	Rute 53 zona yang dihosting publik harus mencatat kueri DNS	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIUM	 Tidak	Perubahan dipicu
S3.1	Bucket tujuan umum S3 harus mengaktifkan pengaturan akses publik blok	Tolok Ukur AWS Yayasan CIS v3.0.0, Tolok Ukur AWS Yayasan CIS v1.4.0, Praktik Terbaik Keamanan AWS Dasar, NIST SP 800-53 Rev. 5, PCI DSS v3.2.1, PCI DSS v4.0.1, Standar yang Dikelola Layanan: AWS Control Tower	MEDIUM	 Tidak	Berkala

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
S3.2	Bucket tujuan umum S3 harus memblokir akses baca publik	AWS Praktik Terbaik Keamanan Dasar, Standar yang Dikelola Layanan:, PCI DSS v3.2.1 AWS Control Tower, NIST SP 800-53 Rev. 5	KRITIS	 Tidak	Perubahan dipicu dan periodik
S3.3	Bucket tujuan umum S3 harus memblokir akses tulis publik	AWS Praktik Terbaik Keamanan Dasar, Standar yang Dikelola Layanan:, PCI DSS v3.2.1 AWS Control Tower, NIST SP 800-53 Rev. 5	KRITIS	 Tidak	Perubahan dipicu dan periodik
S3.5	Bucket tujuan umum S3 harus memerlukan permintaan untuk menggunakan SSL	Tolok Ukur AWS Yayasan CIS v3.0.0, Tolok Ukur AWS Yayasan CIS v1.4.0, Praktik Terbaik Keamanan AWS Dasar, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v3.2.1, PCI DSS v4.0.1, Standar yang Dikelola Layanan: AWS Control Tower	MEDIUM	 Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
S3.6	Kebijakan bucket tujuan umum S3 harus membatasi akses ke yang lain Akun AWS	AWS Praktik Terbaik Keamanan Dasar, Standar yang Dikelola Layanan:, NIST SP 800-53 Rev. 5 AWS Control Tower, NIST SP 800-171 Rev. 2	TINGGI	 Tidak	Perubahan dipicu
S3.7	Bucket tujuan umum S3 harus menggunakan replikasi lintas wilayah	PCI DSS v3.2.1, NIST SP 800-53 Wahyu 5	RENDAH	 Tidak	Perubahan dipicu
S3.8	Bucket tujuan umum S3 harus memblokir akses publik	Tolok Ukur AWS Yayasan CIS v3.0.0, Tolok Ukur AWS Yayasan CIS v1.4.0, Praktik Terbaik Keamanan AWS Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, Standar yang Dikelola Layanan: AWS Control Tower	TINGGI	 Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
S3.9	Bucket tujuan umum S3 harus mengaktifkan pencatatan akses server	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1, Standar yang Dikelola Layanan: AWS Control Tower	MEDIUM	 Tidak	Perubahan dipicu
S3.10	Bucket tujuan umum S3 dengan versi diaktifkan harus memiliki konfigurasi Siklus Hidup	NIST SP 800-53 Wahyu 5	MEDIUM	 Tidak	Perubahan dipicu
S3.11	Bucket tujuan umum S3 harus mengaktifkan pemberitahuan acara	NIST SP 800-53 Wahyu 5, NIST SP 800-171 Wahyu 2	MEDIUM	 Ya	Perubahan dipicu
S3.12	ACLs tidak boleh digunakan untuk mengelola akses pengguna ke bucket tujuan umum S3	AWS Praktik Terbaik Keamanan Dasar, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
S3.13	Bucket tujuan umum S3 harus memiliki konfigurasi Siklus Hidup	AWS Praktik Terbaik Keamanan Dasar, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	RENDAH	 Ya	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
S3.14	Bucket tujuan umum S3 harus mengaktifkan versi	NIST SP 800-53 Wahyu 5, NIST SP 800-171 Wahyu 2	RENDAH	 Tidak	Perubahan dipicu
S3.15	Bucket tujuan umum S3 harus mengaktifkan Object Lock	NIST SP 800-53 Wahyu 5, PCI DSS v4.0.1	MEDIUM	 Ya	Perubahan dipicu
S3.17	Ember tujuan umum S3 harus dienkripsi saat istirahat AWS KMS keys	NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1, Standar yang Dikelola Layanan: AWS Control Tower	MEDIUM	 Tidak	Perubahan dipicu
S3.19	Titik akses S3 harus mengaktifkan pengaturan akses publik blok	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	KRITIS	 Tidak	Perubahan dipicu
S3.20	Bucket tujuan umum S3 harus mengaktifkan penghapusan MFA	Tolok Ukur AWS Yayasan CIS v3.0.0, Tolok Ukur AWS Yayasan CIS v1.4.0, NIST SP 800-53 Rev. 5	RENDAH	 Tidak	Perubahan dipicu
S3.22	Bucket tujuan umum S3 harus mencatat peristiwa penulisan tingkat objek	Tolok Ukur AWS Yayasan CIS v3.0.0, PCI DSS v4.0.1	MEDIUM	 Tidak	Berkala

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
S3.23	Bucket tujuan umum S3 harus mencatat peristiwa pembacaan tingkat objek	Tolok Ukur AWS Yayasan CIS v3.0.0, PCI DSS v4.0.1	MEDIUM	 Tidak	Berkala
S3.24	Titik Akses Multi-Wilayah S3 harus mengaktifkan pengaturan akses publik yang diblokir	AWS Praktik Terbaik Keamanan Dasar, PCI DSS v4.0.1	TINGGI	 Tidak	Perubahan dipicu
SageMaker .1	Instans SageMaker notebook Amazon seharusnya tidak memiliki akses internet langsung	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v3.2.1, PCI DSS v4.0.1, Standar yang Dikelola Layanan: AWS Control Tower	TINGGI	 Tidak	Berkala
SageMaker .2	SageMaker instance notebook harus diluncurkan dalam VPC khusus	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	TINGGI	 Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
SageMaker .3	Pengguna seharusnya tidak memiliki akses root ke instance SageMaker notebook	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	TINGGI	 Tidak	Perubahan dipicu
SageMaker .4	SageMaker varian produksi endpoint harus memiliki jumlah instance awal yang lebih besar dari 1	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Berkala
SageMaker .5	SageMaker model harus memblokir lalu lintas masuk	AWS Praktik Terbaik Keamanan Dasar	MEDIUM	 Tidak	Perubahan dipicu
SageMaker .6	SageMaker konfigurasi gambar aplikasi harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
SageMaker .7	SageMaker gambar harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
SageMaker .8	SageMaker instance notebook harus berjalan pada platform yang didukung	AWS Praktik Terbaik Keamanan Dasar	MEDIUM	 Tidak	Berkala

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
SecretsManager.1	Rahasia Secrets Manager harus mengaktifkan rotasi otomatis	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, Standar yang Dikelola Layanan: AWS Control Tower	MEDIUM	 Ya	Perubahan dipicu
SecretsManager.2	Rahasia Secrets Manager yang dikonfigurasi dengan rotasi otomatis harus berhasil diputar	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, Standar yang Dikelola Layanan: AWS Control Tower	MEDIUM	 Tidak	Perubahan dipicu
SecretsManager.3	Hapus rahasia Secrets Manager yang tidak digunakan	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, Standar yang Dikelola Layanan: AWS Control Tower	MEDIUM	 Ya	Berkala
SecretsManager.4	Rahasia Secrets Manager harus diputar dalam jumlah hari tertentu	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, Standar yang Dikelola Layanan: AWS Control Tower	MEDIUM	 Ya	Berkala

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
SecretsManager.5	Rahasia Secrets Manager harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
ServiceCatalog.1	Portofolio Service Catalog harus dibagikan hanya dalam suatu organisasi AWS	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5	TINGGI	 Tidak	Berkala
SES.1	Daftar kontak SES harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
SES.2	Set konfigurasi SES harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
SNS.1	Topik SNS harus dienkripsi saat istirahat menggunakan AWS KMS	NIST SP 800-53 Wahyu 5, NIST SP 800-171 Wahyu 2	MEDIUM	 Tidak	Perubahan dipicu
SNS.3	Topik SNS harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
SNS.4	Kebijakan akses topik SNS seharusnya tidak mengizinkan akses publik	AWS Praktik Terbaik Keamanan Dasar	TINGGI	 Tidak	Perubahan dipicu
SQS.1	Antrian Amazon SQS harus dienkripsi saat istirahat	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
SQ.2	Antrian SQS harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
SQS.3	Kebijakan akses antrian SQS seharusnya tidak mengizinkan akses publik	AWS Praktik Terbaik Keamanan Dasar	TINGGI	 Tidak	Perubahan dipicu
SSM.1	EC2 contoh harus dikelola oleh AWS Systems Manager	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan:, PCI DSS v3.2.1 AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
SSM.2	EC2 instans yang dikelola oleh Systems Manager harus memiliki status kepatuhan patch COMPLIANT setelah instalasi patch	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v3.2.1, PCI DSS v4.0.1, Standar yang Dikelola Layanan: AWS Control Tower	TINGGI	 Tidak	Perubahan dipicu
SSM.3	EC2 instans yang dikelola oleh Systems Manager harus memiliki status kepatuhan asosiasi COMPLIANT	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v3.2.1, PCI DSS v4.0.1, Standar yang Dikelola Layanan: AWS Control Tower	RENDAH	 Tidak	Perubahan dipicu
SSM.4	Dokumen SSM tidak boleh bersifat publik	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	KRITIS	 Tidak	Berkala
SSM.5	Dokumen SSM harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
StepFunctions.1	Mesin status Step Functions harus mengaktifkan logging	AWS Praktik Terbaik Keamanan Dasar, PCI DSS v4.0.1	MEDIUM	 Ya	Perubahan dipicu
StepFunctions.2	Aktivitas Step Functions harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
Transfer.1	Alur kerja Transfer Family harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
Transfer.2	Server Transfer Family tidak boleh menggunakan protokol FTP untuk koneksi endpoint	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIUM	 Tidak	Berkala
Transfer.3	Konektor Transfer Family seharusnya mengaktifkan logging	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
Transfer.4	Perjanjian Transfer Family harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
Transfer.5	Sertifikat Transfer Family harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
Transfer.6	Konektor Transfer Family harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
Transfer.7	Profil Transfer Family harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
WAF.1	AWS Pencatatan ACL Web Global WAF Classic harus diaktifkan	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIUM	 Tidak	Berkala
WAF.2	AWS Aturan WAF Classic Regional harus memiliki setidaknya satu syarat	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
WAF.3	AWS Kelompok aturan WAF Classic Regional harus memiliki setidaknya satu aturan	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
WAF.4	AWS Web WAF Classic Regional ACLs harus memiliki setidaknya satu aturan atau kelompok aturan	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
WAF.6	AWS Aturan global WAF Classic harus memiliki setidaknya satu syarat	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
WAF.7	AWS Grup aturan global WAF Classic harus memiliki setidaknya satu aturan	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
WAF.8	AWS Web global WAF Classic ACLs harus memiliki setidaknya satu aturan atau grup aturan	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
WAF.10	AWS Web WAF ACLs harus memiliki setidaknya satu aturan atau kelompok aturan	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
WAF.11	AWS Pencatatan ACL web WAF harus diaktifkan	NIST SP 800-53 Wahyu 5, PCI DSS v4.0.1	RENDAH	 Tidak	Berkala
WAF.12	AWS Aturan WAF harus mengaktifkan CloudWatch metrik	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2	MEDIUM	 Tidak	Perubahan dipicu
WorkSpace s.1	WorkSpaces volume pengguna harus dienkripsi saat istirahat	AWS Praktik Terbaik Keamanan Dasar	MEDIUM	 Tidak	Perubahan dipicu
WorkSpace s.2	WorkSpaces volume root harus dienkripsi saat istirahat	AWS Praktik Terbaik Keamanan Dasar	MEDIUM	 Tidak	Perubahan dipicu

Ubah log untuk kontrol CSPM Security Hub

Log perubahan berikut melacak perubahan material pada kontrol AWS keamanan Security Hub Cloud Security Posture Management (CSPM) Security Hub yang ada, yang dapat mengakibatkan

perubahan pada status keseluruhan kontrol dan status kepatuhan temuannya. Untuk informasi tentang cara CSPM Security Hub mengevaluasi status kontrol, lihat. [Mengevaluasi status kepatuhan dan status kontrol](#) Perubahan dapat memakan waktu beberapa hari setelah entri mereka di log ini untuk memengaruhi semua Wilayah AWS kontrol yang tersedia.

Log ini melacak perubahan yang terjadi sejak April 2023. Pilih kontrol untuk meninjau detail tambahan tentangnya. Perubahan judul dicatat dalam deskripsi rinci kontrol selama 90 hari.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
30 Mei 2025	[IAM.10] Kebijakan kata sandi untuk pengguna IAM harus memiliki konfigurasi yang kuat	Security Hub CSPM menghapus kontrol ini dari standar PCI DSS v4.0.1. Kontrol ini memeriksa apakah kebijakan kata sandi akun untuk pengguna IAM memenuhi persyaratan minimum, termasuk panjang kata sandi minimum 7 karakter. PCI DSS v4.0.1 sekarang membutuhkan kata sandi untuk memiliki minimal 8 karakter. Kontrol terus berlaku untuk standar PCI DSS v3.2.1, yang memiliki persyaratan kata sandi yang berbeda. Untuk mengevaluasi kebijakan kata sandi akun terhadap persyaratan PCI DSS

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
		v4.0.1, Anda dapat menggunakan kontrol IAM.7. Kontrol ini membutuhkan kata sandi untuk memiliki minimal 8 karakter. Ini juga mendukung nilai khusus untuk panjang kata sandi dan parameter lainnya. Kontrol IAM.7 adalah bagian dari standar PCI DSS v4.0.1 di Security Hub CSPM.
8 Mei 2025	[RDS.46] Instans RDS DB tidak boleh digunakan di subnet publik dengan rute ke gateway internet	Security Hub CSPM memutar kembali rilis kontrol RDS.46 secara keseluruhan. Wilayah AWS Sebelumnya, kontrol ini mendukung standar AWS Foundational Security Best Practices (FSBP).

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
April 7, 2025	[ELB.17] Aplikasi dan Penyeimbang Beban Jaringan dengan pendengar harus menggunakan kebijakan keamanan yang direkomendasikan	Kontrol ini memeriksa apakah pendengar HTTPS untuk Application Load Balancer atau pendengar TLS untuk Network Load Balancer dikonfigurasi untuk mengenkripsi data dalam perjalanan menggunakan kebijakan keamanan yang direkomendasikan. Security Hub CSPM sekarang mendukung dua nilai parameter tambahan untuk kontrol ini: <code>ELBSecurityPolicy-TLS13-1-2-Res-2021-06</code> dan <code>ELBSecurityPolicy-TLS13-1-2-Res-FIPS-2023-04</code>

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
Maret 27, 2025	[Lambda.2] Fungsi Lambda harus menggunakan runtime yang didukung	Kontrol ini memeriksa apakah setelah runtime untuk AWS Lambda fungsi cocok dengan nilai yang diharapkan untuk runtime yang didukung dalam setiap bahasa. Security Hub CSPM sekarang mendukung ruby3.4 sebagai nilai parameter untuk kontrol ini. AWS Lambda menambahkan dukungan untuk runtime ini.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
Maret 26, 2025	[EKS.2] Kluster EKS harus berjalan pada versi Kubernetes yang didukung	Kontrol ini memeriksa apakah kluster Amazon Elastic Kubernetes Service (Amazon EKS) berjalan pada versi Kubernetes yang didukung. Untuk <code>oldestVersionSupported</code> parameter, Security Hub CSPM mengubah nilai dari 1.29 ke 1.30. Versi Kubernetes tertua yang didukung sekarang 1.30.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
10 Maret 2025	[Lambda.2] Fungsi Lambda harus menggunakan runtime yang didukung	Kontrol ini memeriksa apakah setelah runtime untuk AWS Lambda fungsi cocok dengan nilai yang diharapkan untuk runtime yang didukung dalam setiap bahasa. Security Hub CSPM tidak lagi mendukung dotnet6 dan python3.8 sebagai nilai parameter untuk kontrol ini. AWS Lambda tidak lagi mendukung runtime ini.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
7 Maret 2025	[RDS.18] Instans RDS harus digunakan di VPC	Security Hub CSPM menghapus kontrol ini dari standar Praktik Terbaik Keamanan AWS Dasar dan pemeriksaan otomatis untuk persyaratan NIST SP 800-53 Rev. 5. Sejak jaringan Amazon EC2 -Classic dihentikan, instans Amazon Relational Database Service (Amazon RDS) tidak dapat lagi digunakan di luar VPC. Kontrol terus menjadi bagian dari standar yang AWS Control Tower dikelola layanan .
Januari 10, 2025	[Glue.2] Pekerjaan AWS Glue seharusnya mengaktifkan logging	Security Hub CSPM menghentikan kontrol ini dan menghapusnya dari semua standar.
Desember 20, 2024	EC2.61 hingga EC2 .169	Security Hub CSPM memutar kembali rilis kontrol EC2 .61 hingga EC2 .169.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
Desember 12, 2024	[RDS.23] Instans RDS tidak boleh menggunakan port default mesin database	RDS.23 memeriksa apakah cluster atau instance Amazon Relational Database Service (Amazon RDS) menggunakan port selain port default mesin database. Kami memperbaiki kontrol sehingga AWS Config aturan yang mendasarinya mengembalikan hasil NOT_APPLICABLE untuk instance RDS yang merupakan bagian dari cluster.
Desember 2, 2024	[Lambda.2] Fungsi Lambda harus menggunakan runtime yang didukung	Lambda.2 memeriksa apakah setelan AWS Lambda fungsi untuk runtime cocok dengan nilai yang diharapkan yang ditetapkan untuk runtime yang didukung dalam setiap bahasa. Security Hub CSPM sekarang mendukung nodejs22.x sebagai parameter.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
November 26, 2024	[EKS.2] Kluster EKS harus berjalan pada versi Kubernetes yang didukung	Kontrol ini memeriksa apakah kluster Amazon Elastic Kubernetes Service (Amazon EKS) berjalan pada versi Kubernetes yang didukung. Versi tertua yang didukung sekarang 1.29.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
November 20, 2024	[Config.1] AWS Config harus diaktifkan dan menggunakan peran terkait layanan untuk perekaman sumber daya	Config.1 memeriksa apakah AWS Config diaktifkan, menggunakan peran terkait layanan, dan merekam sumber daya untuk kontrol yang diaktifkan. Security Hub CSPM meningkatkan tingkat keparahan kontrol ini dari keMEDIUM. CRITICAL Security Hub CSPM juga menambahkan kode status baru dan alasan status untuk temuan Config.1 yang gagal. Perubahan ini mencerminkan pentingnya Config.1 untuk pengoperasian kontrol CSPM Security Hub. Jika Anda memiliki AWS Config atau perekaman sumber daya dinonaktifkan, Anda dapat menerima temuan kontrol yang tidak akurat. Untuk menerima PASSED temuan untuk Config.1,

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
		aktifkan perekaman sumber daya untuk sumber daya yang sesuai dengan kontrol CSPM Security Hub yang diaktifkan, dan nonaktifkan kontrol yang tidak diperlukan di organisasi Anda. Untuk petunjuk tentang mengonfigurasi AWS Config CSPM Security Hub, lihat. Mengaktifkan dan mengonfigurasi AWS Config untuk Security Hub CSPM Untuk daftar kontrol CSPM Security Hub dan sumber daya yang sesuai, lihat. AWS Config Sumber daya yang diperlukan untuk temuan kontrol

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
November 12, 2024	[Lambda.2] Fungsi Lambda harus menggunakan runtime yang didukung	Lambda.2 memeriksa apakah setelah AWS Lambda fungsi untuk runtime cocok dengan nilai yang diharapkan yang ditetapkan untuk runtime yang didukung dalam setiap bahasa. Security Hub CSPM sekarang mendukung python3.13 sebagai parameter.
Oktober 11, 2024	ElastiCache kontrol	Mengubah judul kontrol untuk ElastiCache .3, ElastiCache .4, ElastiCache .5, dan .7. ElastiCache Judul tidak lagi menyebutkan Redis OSS karena kontrol juga berlaku ElastiCache untuk Valkey.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
September 27, 2024	[ELB.4] Application Load Balancer harus dikonfigurasi untuk menjatuhkan header http yang tidak valid	Judul kontrol yang diubah dari Application Load Balancer harus dikonfigurasi untuk menjatuhkan header http ke Application Load Balancer harus dikonfigurasi untuk menjatuhkan header http yang tidak valid.
Agustus 19, 2024	Judul berubah ke DMS.12 dan kontrol ElastiCache	Mengubah judul kontrol untuk DMS.12 dan .1 hingga ElastiCache .7. ElastiCache Kami mengubah judul-judul ini untuk mencerminkan perubahan nama di layanan Amazon ElastiCache (Redis OSS).

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
Agustus 15, 2024	[Config.1] AWS Config harus diaktifkan dan menggunakan peran terkait layanan untuk perekaman sumber daya	Config.1 memeriksa apakah AWS Config diaktifkan, menggunakan peran terkait layanan, dan merekam sumber daya untuk kontrol yang diaktifkan. Security Hub CSPM menambahkan parameter kontrol kustom bernama <code>includeConfigServiceLinkedRoleCheck</code> . Dengan menyetel parameter ini <code>false</code> , Anda dapat memilih untuk tidak memeriksa apakah AWS Config menggunakan peran terkait layanan.
Juli 31, 2024	[IoT.1] profil AWS IoT Device Defender keamanan harus ditandai	Judul kontrol yang diubah dari profil AWS IoT Core keamanan harus ditandai ke profil AWS IoT Device Defender keamanan harus ditandai.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
Juli 29, 2024	[Lambda.2] Fungsi Lambda harus menggunakan runtime yang didukung	Lambda.2 memeriksa apakah setelan AWS Lambda fungsi untuk runtime cocok dengan nilai yang diharapkan yang ditetapkan untuk runtime yang didukung dalam setiap bahasa. Security Hub CSPM tidak lagi mendukung <code>nodejs16.x</code> sebagai parameter.
Juli 29, 2024	[EKS.2] Kluster EKS harus berjalan pada versi Kubernetes yang didukung	Kontrol ini memeriksa apakah kluster Amazon Elastic Kubernetes Service (Amazon EKS) berjalan pada versi Kubernetes yang didukung. Versi tertua yang didukung adalah <code>1.28</code> .

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
Juni 25, 2024	[Config.1] AWS Config harus diaktifkan dan menggunakan peran terkait layanan untuk perekaman sumber daya	Kontrol ini memeriksa apakah AWS Config diaktifkan, menggunakan peran terkait layanan, dan merekam sumber daya untuk kontrol yang diaktifkan. Security Hub CSPM memperbarui judul kontrol untuk mencerminkan apa yang dievaluasi oleh kontrol.
Juni 14, 2024	[RDS.34] Kluster Aurora MySQL DB harus menerbitkan log audit ke Log CloudWatch	Kontrol ini memeriksa apakah kluster DB MySQL Amazon Aurora dikonfigurasi untuk mempublikasikan log audit ke Amazon Logs. CloudWatch Security Hub CSPM memperbarui kontrol sehingga tidak menghasilkan temuan untuk cluster Aurora Serverless v1 DB.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
Juni 11, 2024	[EKS.2] Kluster EKS harus berjalan pada versi Kubernetes yang didukung	Kontrol ini memeriksa apakah kluster Amazon Elastic Kubernetes Service (Amazon EKS) berjalan pada versi Kubernetes yang didukung. Versi tertua yang didukung adalah 1.27.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
Juni 10, 2024	[Config.1] AWS Config harus diaktifkan dan menggunakan peran terkait layanan untuk perekaman sumber daya	Kontrol ini memeriksa apakah AWS Config diaktifkan dan perekaman AWS Config sumber daya diaktifkan. Sebelumnya, kontrol menghasilkan PASSED temuan hanya jika Anda mengonfigurasi rekaman untuk semua sumber daya. Security Hub CSPM memperbarui kontrol untuk menghasilkan PASSED temuan saat perekaman diaktifkan untuk sumber daya yang diperlukan untuk kontrol yang diaktifkan. Kontrol juga telah diperbarui untuk memeriksa apakah peran AWS Config terkait layanan digunakan, yang memberikan izin untuk merekam sumber daya yang diperlukan.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
8 Mei 2024	[S3.20] Bucket tujuan umum S3 harus mengaktifkan penghapusan MFA	Kontrol ini memeriksa apakah bucket berversi tujuan umum Amazon S3 telah mengaktifkan penghapusan autentikasi multi-faktor (MFA). Sebelumnya, kontrol menghasilkan FAILED temuan untuk bucket yang memiliki konfigurasi Siklus Hidup. Namun, penghapusan MFA dengan pembuatan versi tidak dapat diaktifkan pada bucket yang memiliki konfigurasi Siklus Hidup. Security Hub CSPM memperbarui kontrol agar tidak menghasilkan temuan untuk bucket yang memiliki konfigurasi Siklus Hidup. Deskripsi kontrol telah diperbarui untuk mencerminkan perilaku saat ini.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
2 Mei 2024	[EKS.2] Kluster EKS harus berjalan pada versi Kubernetes yang didukung	Security Hub CSPM memperbarui versi Kubernetes tertua yang didukung yang dapat dijalankan oleh kluster Amazon EKS untuk menghasilkan temuan yang lewat. Versi tertua yang didukung saat ini adalah Kubernetes 1.26.
April 30, 2024	[CloudTrail.3] Setidaknya satu CloudTrail jejak harus diaktifkan	Judul kontrol yang diubah dari CloudTrail harus diaktifkan ke Setidaknya satu CloudTrail jejak harus diaktifkan. Kontrol ini saat ini menghasilkan PASSED temuan jika Akun AWS memiliki setidaknya satu CloudTrail jejak diaktifkan. Judul dan deskripsi telah diubah untuk secara akurat mencerminkan perilaku saat ini.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
April 29, 2024	[AutoScaling.1] Grup Auto Scaling yang terkait dengan penyeimbang beban harus menggunakan pemeriksaan kesehatan ELB	Judul kontrol yang diubah dari grup Auto Scaling yang terkait dengan Classic Load Balancer harus menggunakan pemeriksaan kesehatan penyeimbang beban ke grup Auto Scaling yang terkait dengan penyeimbang beban harus menggunakan pemeriksaan kesehatan ELB. Kontrol ini saat ini mengevaluasi Application, Gateway, Network, dan Classic Load Balancer. Judul dan deskripsi telah diubah untuk secara akurat mencerminkan perilaku saat ini.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
April 19, 2024	[CloudTrail.1] CloudTrail harus diaktifkan dan dikonfigurasi dengan setidaknya satu jejak Multi-wilayah yang mencakup acara manajemen baca dan tulis	Kontrol memeriksa apakah AWS CloudTrail diaktifkan dan dikonfigurasi dengan setidaknya satu jejak Multi-wilayah yang mencakup peristiwa manajemen baca dan tulis. Sebelumnya, kontrol salah menghasilkan PASSED temuan ketika akun telah CloudTrail diaktifkan dan dikonfigurasi dengan setidaknya satu jejak Multi-wilayah, bahkan jika tidak ada jejak yang menangkap peristiwa manajemen baca dan tulis. Kontrol sekarang menghasilkan PASSED temuan hanya ketika CloudTrail diaktifkan dan dikonfigurasi dengan setidaknya satu jejak Multi-wilayah yang menangkap peristiwa manajemen baca dan tulis.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
April 10, 2024	[Athena.1] Kelompok kerja Athena harus dienkripsi saat istirahat	Security Hub CSPM menghentikan kontrol ini dan menghapusnya dari semua standar. Workgroup Athena mengirim log ke bucket Amazon Simple Storage Service (Amazon S3). Amazon S3 sekarang menyediakan enkripsi default dengan kunci terkelola S3 (SS3-S3) pada bucket S3 baru dan yang sudah ada.
April 10, 2024	[AutoScaling.4] Konfigurasi peluncuran grup Auto Scaling seharusnya tidak memiliki batas hop respons metadata yang lebih besar dari 1	Security Hub CSPM menghentikan kontrol ini dan menghapusnya dari semua standar. Batas hop respons metadata untuk instans Amazon Elastic Compute Cloud (Amazon EC2) bergantung pada beban kerja.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
April 10, 2024	[CloudFormation.1] CloudFormation tumpukan harus diintegrasikan dengan Simple Notification Service (SNS)	Security Hub CSPM menghentikan kontrol ini dan menghapusnya dari semua standar. Mengintegrasikan AWS CloudFormation tumpukan dengan topik Amazon SNS bukan lagi praktik terbaik keamanan. Meskipun mengintegrasikan CloudFormation tumpukan penting dengan topik SNS dapat bermanfaat, itu tidak diperlukan untuk semua tumpukan.
April 10, 2024	[CodeBuild.5] lingkungan CodeBuild proyek seharusnya tidak mengaktifkan mode istimewa	Security Hub CSPM menghentikan kontrol ini dan menghapusnya dari semua standar. Mengaktifkan mode istimewa dalam CodeBuild proyek tidak menimbulkan risiko tambahan bagi lingkungan pelanggan.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
April 10, 2024	[IAM.20] Hindari penggunaan pengguna root	Security Hub CSPM menghentikan kontrol ini dan menghapusnya dari semua standar. Tujuan dari kontrol ini dicakup oleh kontrol lain, [CloudWatch.1] Filter metrik log dan alarm harus ada untuk penggunaan pengguna "root" .
April 10, 2024	[SNS.2] Pencatatan status pengiriman harus diaktifkan untuk pesan notifikasi yang dikirim ke suatu topik	Security Hub CSPM menghentikan kontrol ini dan menghapusnya dari semua standar. Mencatat status pengiriman untuk topik SNS bukan lagi praktik terbaik keamanan. Meskipun mencatat status pengiriman untuk topik SNS penting dapat berguna, itu tidak diperlukan untuk semua topik.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
April 10, 2024	[S3.10] Bucket tujuan umum S3 dengan versi diaktifkan harus memiliki konfigurasi Siklus Hidup	Security Hub CSPM menghapus kontrol ini dari Praktik Terbaik Keamanan AWS Dasar dan Standar yang Dikelola Layanan:. AWS Control Tower Tujuan dari kontrol ini dicakup oleh dua kontrol lainnya: [S3.13] Bucket tujuan umum S3 harus memiliki konfigurasi Siklus Hidup dan [S3.14] Bucket tujuan umum S3 harus mengaktifkan versi . Kontrol ini masih merupakan bagian dari NIST SP 800-53 Rev. 5.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
April 10, 2024	[S3.11] Bucket tujuan umum S3 harus mengaktifkan pemberitahuan acara	Security Hub CSPM menghapus kontrol ini dari Praktik Terbaik Keamanan AWS Dasar dan Standar yang Dikelola Layanan:. AWS Control Tower Meskipun ada beberapa kasus di mana pemberitahuan acara untuk bucket S3 berguna, ini bukan praktik terbaik keamanan universal . Kontrol ini masih merupakan bagian dari NIST SP 800-53 Rev. 5.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
April 10, 2024	[SNS.1] Topik SNS harus dienkripsi saat istirahat menggunakan AWS KMS	Security Hub CSPM menghapus kontrol ini dari Praktik Terbaik Keamanan AWS Dasar dan Standar yang Dikelola Layanan:. AWS Control Tower Secara default, SNS mengenkripsi topik saat istirahat dengan enkripsi disk. Untuk informasi selengkapnya tentang enkripsi saat istirahat , lihat. Menggunakan AWS KMS untuk mengenkripsi topik tidak lagi direkomendasikan sebagai praktik terbaik keamanan. Kontrol ini masih merupakan bagian dari NIST SP 800-53 Rev. 5.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
April 8, 2024	[ELB.6] Aplikasi, Gateway, dan Network Load Balancer harus mengaktifkan perlindungan penghapusan	Judul kontrol yang diubah dari perlindungan penghapusan Application Load Balancer harus diaktifkan ke Application, Gateway, dan Network Load Balancer harus mengaktifkan perlindungan penghapusan. Kontrol ini saat ini mengevaluasi Application, Gateway, dan Network Load Balancers. Judul dan deskripsi telah diubah untuk secara akurat mencerminkan perilaku saat ini.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
Maret 22, 2024	[Opensearch.8] Koneksi ke OpenSearch domain harus dienkripsi menggunakan kebijakan keamanan TLS terbaru	Judul kontrol yang diubah dari Koneksi ke OpenSearch domain harus dienkripsi menggunakan TLS 1.2 hingga Koneksi ke OpenSearch domain harus dienkripsi menggunakan kebijakan keamanan TLS terbaru. Sebelumnya, kontrol hanya memeriksa apakah koneksi ke OpenSearch domain menggunakan TLS 1.2. Kontrol sekarang menghasilkan PASSED temuan jika OpenSearch domain dienkripsi menggunakan kebijakan keamanan TLS terbaru. Judul kontrol dan deskripsi telah diperbarui untuk mencerminkan perilaku saat ini.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
Maret 22, 2024	[ES.8] Koneksi ke domain Elasticsearch harus dienkripsi menggunakan kebijakan keamanan TLS terbaru	Judul kontrol yang diubah dari Connections ke domain Elasticsearch harus dienkripsi i menggunakan TLS 1.2 ke Connections to Elasticsearch domain harus dienkripsi i menggunakan kebijakan keamanan TLS terbaru. Sebelumnya, kontrol hanya memeriksa apakah koneksi ke domain Elasticsearch menggunakan TLS 1.2. Kontrol sekarang menghasilkan PASSED temuan jika domain Elasticsearch dienkripsi i menggunakan kebijakan keamanan TLS terbaru. Judul kontrol dan deskripsi telah diperbarui untuk mencerminkan perilaku saat ini.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
Maret 12, 2024	[S3.1] Bucket tujuan umum S3 harus mengaktifkan pengaturan akses publik blok	Judul yang diubah dari pengaturan Akses Publik Blok S3 harus diaktifkan ke bucket tujuan umum S3 harus mengaktifkan pengaturan akses publik blok. Security Hub CSPM mengubah judul menjadi akun untuk jenis bucket S3 baru.
Maret 12, 2024	[S3.2] Bucket tujuan umum S3 harus memblokir akses baca publik	Judul yang diubah dari bucket S3 harus melarang akses baca publik ke bucket tujuan umum S3 harus memblokir akses baca publik. Security Hub CSPM mengubah judul menjadi akun untuk jenis bucket S3 baru.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
Maret 12, 2024	[S3.3] Bucket tujuan umum S3 harus memblokir akses tulis publik	Judul yang diubah dari bucket S3 harus melarang akses tulis publik ke bucket tujuan umum S3 harus memblokir akses tulis publik. Security Hub CSPM mengubah judul menjadi akun untuk jenis bucket S3 baru.
Maret 12, 2024	[S3.5] Bucket tujuan umum S3 harus memerlukan permintaan untuk menggunakan SSL	Judul yang diubah dari bucket S3 harus memerlukan permintaan untuk menggunakan Secure Socket Layer ke bucket tujuan umum S3 harus memerlukan permintaan untuk menggunakan SSL. Security Hub CSPM mengubah judul menjadi akun untuk jenis bucket S3 baru.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
Maret 12, 2024	[S3.6] Kebijakan bucket tujuan umum S3 harus membatasi akses ke yang lain Akun AWS	Judul yang diubah dari izin S3 yang diberikan ke kebijakan bucket lainnya harus dibatasi Akun AWS pada kebijakan bucket tujuan umum S3 yang harus membatasi akses ke yang lain. Akun AWS Security Hub CSPM mengubah judul menjadi akun untuk jenis bucket S3 baru.
Maret 12, 2024	[S3.7] Ember tujuan umum S3 harus menggunakan replikasi lintas wilayah	Judul yang diubah dari bucket S3 harus mengaktifkan replikasi lintas wilayah ke bucket tujuan umum S3 harus menggunakan replikasi lintas wilayah. Security Hub CSPM mengubah judul menjadi akun untuk jenis bucket S3 baru.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
Maret 12, 2024	[S3.7] Ember tujuan umum S3 harus menggunakan replikasi lintas wilayah	Judul yang diubah dari bucket S3 harus mengaktifkan replikasi lintas wilayah ke bucket tujuan umum S3 harus menggunakan replikasi lintas wilayah. Security Hub CSPM mengubah judul menjadi akun untuk jenis bucket S3 baru.
Maret 12, 2024	[S3.8] Bucket tujuan umum S3 harus memblokir akses publik	Judul yang diubah dari pengaturan Akses Publik Blok S3 harus diaktifkan pada bucket tujuan umum tingkat ember ke S3 harus memblokir akses publik. Security Hub CSPM mengubah judul menjadi akun untuk jenis bucket S3 baru.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
Maret 12, 2024	[S3.9] Bucket tujuan umum S3 harus mengaktifkan pencatatan akses server	Judul yang diubah dari pencatatan akses server bucket S3 harus diaktifkan ke Pencatatan akses Server harus diaktifkan untuk bucket tujuan umum S3. Security Hub CSPM mengubah judul menjadi akun untuk jenis bucket S3 baru.
Maret 12, 2024	[S3.10] Bucket tujuan umum S3 dengan versi diaktifkan harus memiliki konfigurasi Siklus Hidup	Judul yang diubah dari bucket S3 dengan versi diaktifkan harus memiliki kebijakan siklus hidup yang dikonfigurasi ke bucket tujuan umum S3 dengan versi yang diaktifkan harus memiliki konfigurasi Siklus Hidup. Security Hub CSPM mengubah judul menjadi akun untuk jenis bucket S3 baru.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
Maret 12, 2024	[S3.11] Bucket tujuan umum S3 harus mengaktifkan pemberitahuan acara	Judul yang diubah dari bucket S3 harus mengaktifkan notifikasi acara ke bucket tujuan umum S3 harus mengaktifkan pemberitahuan acara. Security Hub CSPM mengubah judul menjadi akun untuk jenis bucket S3 baru.
Maret 12, 2024	[S3.12] tidak ACLs boleh digunakan untuk mengelola akses pengguna ke bucket tujuan umum S3	Judul yang diubah dari daftar kontrol akses S3 (ACLs) tidak boleh digunakan untuk mengelola akses pengguna ke bucket agar ACLs tidak digunakan untuk mengelola akses pengguna ke bucket tujuan umum S3. Security Hub CSPM mengubah judul menjadi akun untuk jenis bucket S3 baru.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
Maret 12, 2024	[S3.13] Bucket tujuan umum S3 harus memiliki konfigurasi Siklus Hidup	Judul yang diubah dari bucket S3 harus memiliki kebijakan siklus hidup yang dikonfigurasi ke bucket tujuan umum S3 harus memiliki konfigurasi Siklus Hidup. Security Hub CSPM mengubah judul menjadi akun untuk jenis bucket S3 baru.
Maret 12, 2024	[S3.14] Bucket tujuan umum S3 harus mengaktifkan versi	Judul yang diubah dari bucket S3 harus menggunakan pembuatan versi ke bucket tujuan umum S3 harus mengaktifkan versi. Security Hub CSPM mengubah judul menjadi akun untuk jenis bucket S3 baru.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
Maret 12, 2024	[S3.15] Bucket tujuan umum S3 harus mengaktifkan Object Lock	Judul yang diubah dari bucket S3 harus dikonfigurasi untuk menggunakan Object Lock ke bucket tujuan umum S3 harus mengaktifkan Object Lock. Security Hub CSPM mengubah judul menjadi akun untuk jenis bucket S3 baru.
Maret 12, 2024	[S3.17] Ember tujuan umum S3 harus dienkripsi i saat istirahat AWS KMS keys	Judul yang diubah dari bucket S3 harus dienkripsi saat istirahat dengan AWS KMS keys bucket tujuan umum S3 harus dienkripsi saat istirahat. AWS KMS keys Security Hub CSPM mengubah judul menjadi akun untuk jenis bucket S3 baru.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
7 Maret 2024	[Lambda.2] Fungsi Lambda harus menggunakan runtime yang didukung	Lambda.2 memeriksa apakah setelah AWS Lambda fungsi untuk runtime cocok dengan nilai yang diharapkan yang ditetapkan untuk runtime yang didukung dalam setiap bahasa. Security Hub CSPM sekarang mendukung <code>nodejs20.x</code> dan <code>ruby3.3</code> sebagai parameter.
Februari 22, 2024	[Lambda.2] Fungsi Lambda harus menggunakan runtime yang didukung	Lambda.2 memeriksa apakah setelah AWS Lambda fungsi untuk runtime cocok dengan nilai yang diharapkan yang ditetapkan untuk runtime yang didukung dalam setiap bahasa. Security Hub CSPM sekarang mendukung <code>dotnet8</code> sebagai parameter.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
Februari 5, 2024	[EKS.2] Kluster EKS harus berjalan pada versi Kubernetes yang didukung	Security Hub CSPM memperbarui versi Kubernetes tertua yang didukung yang dapat dijalankan oleh kluster Amazon EKS untuk menghasilkan temuan yang lewat. Versi tertua yang didukung saat ini adalah Kubernetes 1.25.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
10 Januari 2024	[CodeBuild.1] Repositori sumber CodeBuild Bitbucket tidak URLs boleh berisi kredensial sensitif	Judul yang diubah dari CodeBuild GitHub atau repositori sumber Bitbucket URLs harus digunakan OAuth untuk repositori sumber CodeBuild Bitbucket tidak boleh berisi kredensial URLs sensitif. Security Hub CSPM menghapus penyebutan OAuth karena metode koneksi lain juga bisa aman. Security Hub CSPM menghapus penyebutan GitHub karena tidak mungkin lagi memiliki token akses pribadi atau nama pengguna dan kata sandi di repositori GitHub sumber. URLs

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
8 Januari 2024	[Lambda.2] Fungsi Lambda harus menggunakan runtime yang didukung	Lambda.2 memeriksa apakah setelah AWS Lambda fungsi untuk runtime cocok dengan nilai yang diharapkan yang ditetapkan untuk runtime yang didukung dalam setiap bahasa. Security Hub CSPM tidak lagi mendukung go1.x dan java8 sebagai parameter karena ini adalah runtime yang sudah pensiun.
Desember 29, 2023	[RDS.8] Instans RDS DB harus mengaktifkan perlindungan penghapusan	RDS.8 memeriksa apakah instans Amazon RDS DB yang menggunakan salah satu mesin database yang didukung telah mengaktifkan perlindungan penghapusan. Security Hub CSPM sekarang mendukung custom-oracle-ee,oracle-ee-cdb, dan oracle-se2-cdb sebagai mesin database.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
22 Desember 2023	[Lambda.2] Fungsi Lambda harus menggunakan runtime yang didukung	Lambda.2 memeriksa apakah setelah AWS Lambda fungsi untuk runtime cocok dengan nilai yang diharapkan yang ditetapkan untuk runtime yang didukung dalam setiap bahasa. Security Hub CSPM sekarang mendukung java21 dan python3.12 sebagai parameter. Security Hub CSPM tidak lagi mendukung ruby2.7 sebagai parameter.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
15 Desember 2023	[CloudFront.1] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi	CloudFront.1 memeriksa apakah CloudFront distribus i Amazon memiliki objek root default yang dikonfigurasi. Security Hub CSPM menurunkan tingkat keparahan kontrol ini dari CRITICAL ke HIGH karena menambahkan objek root default adalah rekomendasi yang bergantung pada aplikasi pengguna dan persyaratan spesifik.
5 Desember 2023	[EC2.13] Grup keamanan seharusnya tidak mengizinkan masuknya dari 0.0.0.0/0 atau: :/0 ke port 22	Judul kontrol yang diubah dari Grup keamanan tidak boleh mengizink an masuknya dari 0.0.0.0/0 ke port 22 ke Grup keamanan tidak boleh mengizink an masuknya dari 0.0.0.0/0 atau: :/0 ke port 22.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
5 Desember 2023	[EC2.14] Grup keamanan seharusnya tidak mengizinkan masuknya dari 0.0.0.0/0 atau: :/0 ke port 3389	Judul kontrol yang diubah dari Pastikan tidak ada grup keamanan yang mengizinkan masuknya dari 0.0.0.0/0 ke port 3389 ke Grup keamanan tidak boleh mengizinkan masuknya dari 0.0.0.0/0 atau: :/0 ke port 3389.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
5 Desember 2023	[RDS.9] Instans RDS DB harus menerbitkan log ke Log CloudWatch	Judul kontrol yang diubah dari pencatatan Database harus diaktifkan ke instans RDS DB harus menerbitkan log ke CloudWatch Log. Security Hub CSPM mengidentifikasi bahwa kontrol ini hanya memeriksa apakah log dipublikasikan ke Amazon CloudWatch Logs dan tidak memeriksa apakah log RDS diaktifkan. Kontrol menghasilkan PASSED temuan jika instans RDS DB dikonfigurasi untuk menerbitkan log ke CloudWatch Log. Judul kontrol telah diperbarui untuk mencerminkan perilaku saat ini.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
5 Desember 2023	[EKS.8] Kluster EKS harus mengaktifkan pencatatan audit	Kontrol ini memeriksa apakah kluster Amazon EKS mengaktifkan pencatatan audit. AWS Config Aturan yang digunakan Security Hub CSPM untuk mengevaluasi kontrol ini berubah dari eks-cluster-logging-enabled ke. eks-cluster-log-enabled

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
17 November 2023	[EC2.19] Kelompok keamanan tidak boleh mengizinkan akses tidak terbatas ke port dengan risiko tinggi	EC2.19 memeriksa apakah lalu lintas masuk yang tidak dibatasi untuk grup keamanan dapat diakses ke port tertentu yang dianggap berisiko tinggi. Security Hub CSPM memperbarui kontrol ini untuk memperhitungkan daftar awalan terkelola saat dipasok sebagai sumber untuk aturan grup keamanan. Kontrol menghasilkan FAILED temuan jika daftar awalan berisi string '0.0.0.0/0' atau ': :/0'.
16 November 2023	[CloudWatch.15] CloudWatch alarm harus memiliki tindakan tertentu yang dikonfigurasi	Judul kontrol yang diubah dari CloudWatch alarm harus memiliki tindakan yang dikonfigurasi untuk status ALARM ke CloudWatch alarm harus memiliki tindakan tertentu yang dikonfigurasi.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
16 November 2023	[CloudWatch.16] grup CloudWatch log harus dipertahankan untuk jangka waktu tertentu	Judul kontrol yang diubah dari grup CloudWatch log harus dipertahankan setidaknya selama 1 tahun untuk grup CloudWatch log harus dipertahankan untuk jangka waktu tertentu.
16 November 2023	[Lambda.5] Fungsi VPC Lambda harus beroperasi di beberapa Availability Zone	Judul kontrol yang diubah dari fungsi VPC Lambda harus beroperasi di lebih dari satu Availability Zone ke VPC Lambda fungsi harus beroperasi di beberapa Availability Zone.
16 November 2023	[AppSync.2] AWS AppSync harus mengaktifkan logging tingkat lapangan	Judul kontrol yang diubah dari AWS AppSync seharusnya mengaktifkan pencatatan tingkat permintaan dan tingkat bidang harus mengaktifkan logging tingkat bidang.AWS AppSync

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
16 November 2023	[EMR.1] Node primer klaster EMR Amazon seharusnya tidak memiliki alamat IP publik	Judul kontrol yang diubah dari node master MapReduce cluster Amazon Elastic seharusnya tidak memiliki alamat IP publik ke node primer klaster EMR Amazon tidak boleh memiliki alamat IP publik.
16 November 2023	[Opensearch.2] OpenSearch domain tidak boleh diakses publik	Judul kontrol yang diubah dari OpenSearch domain harus dalam VPC OpenSearch ke domain tidak boleh diakses publik.
16 November 2023	[ES.2] Domain Elasticsearch tidak boleh diakses publik	Judul kontrol yang diubah dari domain Elasticsearch harus dalam VPC ke domain Elasticsearch tidak boleh diakses publik.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
31 Oktober 2023	[ES.4] Kesalahan domain Elasticsearch yang masuk ke CloudWatch Log harus diaktifkan	ES.4 memeriksa apakah domain Elasticsearch dikonfigurasi untuk mengirim log kesalahan ke Amazon Logs. CloudWatch Kontrol sebelumnya menghasilkan PASSED temuan untuk domain Elasticsearch yang memiliki log yang dikonfigurasi untuk dikirim ke CloudWatch Log. Security Hub CSPM memperbarui kontrol untuk menghasilkan PASSED temuan hanya untuk domain Elasticsearch yang dikonfigurasi untuk mengirim log kesalahan ke Log. CloudWatch Kontrol juga diperbarui untuk mengecualikan versi Elasticsearch yang tidak mendukung log kesalahan dari evaluasi.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
16 Oktober 2023	[EC2.13] Grup keamanan seharusnya tidak mengizinkan masuknya dari 0.0.0.0/0 atau :/0 ke port 22	EC2.13 memeriksa apakah grup keamanan mengizinkan akses masuk tidak terbatas ke port 22. Security Hub CSPM memperbarui kontrol ini untuk memperhitungkan daftar awalan terkelola saat dipasok sebagai sumber untuk aturan grup keamanan. Kontrol menghasilkan FAILED temuan jika daftar awalan berisi string '0.0.0.0/0' atau ': /0'.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
16 Oktober 2023	[EC2.14] Grup keamanan seharusnya tidak mengizinkan masuknya dari 0.0.0.0/0 atau :/0 ke port 3389	EC2.14 memeriksa apakah grup keamanan mengizinkan akses masuk tidak terbatas ke port 3389. Security Hub CSPM memperbarui kontrol ini untuk memperhitungkan daftar awalan terkelola saat dipasok sebagai sumber untuk aturan grup keamanan. Kontrol menghasilkan FAILED temuan jika daftar awalan berisi string '0.0.0.0/0' atau ': :/0'.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
16 Oktober 2023	[EC2.18] Grup keamanan seharusnya hanya mengizinkan lalu lintas masuk yang tidak terbatas untuk port resmi	EC2.18 memeriksa apakah grup keamanan yang digunakan mengizinkan lalu lintas masuk yang tidak dibatasi. Security Hub CSPM memperbarui kontrol ini untuk memperhitungkan daftar awalan terkelola saat dipasok sebagai sumber untuk aturan grup keamanan. Kontrol menghasilkan FAILED temuan jika daftar awalan berisi string '0.0.0.0/0' atau ': :/0'.
16 Oktober 2023	[Lambda.2] Fungsi Lambda harus menggunakan runtime yang didukung	Lambda.2 memeriksa apakah setelan AWS Lambda fungsi untuk runtime cocok dengan nilai yang diharapkan yang ditetapkan untuk runtime yang didukung dalam setiap bahasa. Security Hub CSPM sekarang mendukung python3.11 sebagai parameter.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
4 Oktober 2023	[S3.7] Ember tujuan umum S3 harus menggunakan replikasi lintas wilayah	Security Hub CSPM menambahkan parameter <code>ReplicationType</code> dengan nilai <code>CROSS-REGION</code> untuk memastikan bahwa bucket S3 mengaktifkan replikasi lintas wilayah daripada replikasi wilayah yang sama.
27 September 2023	[EKS.2] Kluster EKS harus berjalan pada versi Kubernetes yang didukung	Security Hub CSPM memperbarui versi Kubernetes tertua yang didukung yang dapat dijalankan oleh kluster Amazon EKS untuk menghasilkan temuan yang lewat. Versi tertua yang didukung saat ini adalah Kubernetes 1.24.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
20 September 2023	[CloudFront.2] CloudFront distribusi harus mengaktifkan identitas akses asal	Security Hub CSPM menghentikan kontrol ini dan menghapusnya dari semua standar. Sebaliknya, gunakan [CloudFront.13] CloudFront distribusi harus menggunakan kontrol akses asal . Kontrol akses asal adalah praktik terbaik keamanan saat ini. Kontrol ini akan dihapus dari dokumentasi dalam 90 hari.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
20 September 2023	[EC2.22] Grup EC2 keamanan Amazon yang tidak digunakan harus dihapus	Security Hub CSPM menghapus kontrol ini dari AWS Foundational Security Best Practices (FSBP) dan National Institute of Standards and Technology (NIST) SP 800-53 Rev. 5. Itu masih merupakan bagian dari Standar yang Dikelola Layanan: AWS Control Tower. Kontrol ini menghasilkan temuan yang dilewatkan jika grup keamanan dilampirkan ke EC2 instance atau ke elastic network interface. Namun, untuk kasus penggunaan tertentu, kelompok keamanan yang tidak terikat tidak menimbulkan risiko keamanan. Anda dapat menggunakan EC2 kontrol lain—seperti EC2 .2, EC2 .13, EC2 .14, EC2 .18, dan EC2 .19—untuk memantau grup keamanan Anda.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
20 September 2023	[EC2.29] EC2 instance harus diluncurkan dalam VPC	Security Hub CSPM menghentikan kontrol ini dan menghapusnya dari semua standar. Amazon EC2 telah memigrasikan instans EC2 -Classic ke VPC. Kontrol ini akan dihapus dari dokumentasi dalam 90 hari.
20 September 2023	[S3.4] Bucket S3 harus mengaktifkan enkripsi sisi server	Security Hub CSPM menghentikan kontrol ini dan menghapusnya dari semua standar. Amazon S3 sekarang menyediakan enkripsi default dengan kunci terkelola S3 (SS3-S3) pada bucket S3 baru dan yang sudah ada. Pengaturan enkripsi tidak berubah untuk bucket yang ada yang dienkripsi dengan enkripsi sisi server SS3 -S3 atau -KMS. SS3 Kontrol ini akan dihapus dari dokumentasi dalam 90 hari.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
14 September 2023	[EC2.2] Grup keamanan default VPC tidak boleh mengizinkan lalu lintas masuk atau keluar	Judul kontrol yang diubah dari Grup keamanan default VPC tidak boleh mengizinkan lalu lintas masuk dan keluar ke grup keamanan default VPC tidak boleh mengizinkan lalu lintas masuk atau keluar.
14 September 2023	[IAM.9] MFA harus diaktifkan untuk pengguna root	Judul kontrol yang diubah dari MFA Virtual harus diaktifkan untuk pengguna root ke MFA harus diaktifkan untuk pengguna root.
14 September 2023	[RDS.19] Langganan pemberitahuan acara RDS yang ada harus dikonfigurasi untuk peristiwa klaster penting	Judul kontrol yang diubah dari Langganan pemberitahuan peristiwa RDS harus dikonfigurasi untuk peristiwa klaster penting ke langganan pemberitahuan peristiwa RDS yang ada harus dikonfigurasi untuk peristiwa klaster penting.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
14 September 2023	[RDS.20] Langganan pemberitahuan acara RDS yang ada harus dikonfigurasi untuk peristiwa instance basis data penting	Judul kontrol yang diubah dari Langganan pemberitahuan peristiwa RDS harus dikonfigurasi untuk peristiwa instance database penting ke langganan pemberitahuan peristiwa RDS yang ada harus dikonfigurasi untuk peristiwa instance database penting.
14 September 2023	[WAF.2] Aturan Regional AWS WAF Klasik harus memiliki setidaknya satu syarat	Judul kontrol yang diubah dari Aturan Regional WAF harus memiliki setidaknya satu syarat untuk aturan Regional AWS WAF Klasik harus memiliki setidaknya satu syarat.
14 September 2023	[WAF.3] Kelompok aturan Regional AWS WAF Klasik harus memiliki setidaknya satu aturan	Judul kontrol yang diubah dari grup aturan WAF Regional harus memiliki setidaknya satu aturan untuk grup aturan Regional AWS WAF Klasik harus memiliki setidaknya satu aturan.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
14 September 2023	[WAF.4] Web Regional AWS WAF Klasik ACLs harus memiliki setidaknya satu aturan atau kelompok aturan	Judul kontrol yang diubah dari ACL web Regional WAF harus memiliki setidaknya a satu aturan atau grup aturan ke web Regional AWS WAF Klasik ACLs harus memiliki setidaknya satu aturan atau grup aturan.
14 September 2023	[WAF.6] Aturan global AWS WAF klasik harus memiliki setidaknya satu syarat	Judul kontrol yang diubah dari aturan global WAF harus memiliki setidaknya a satu syarat untuk aturan global AWS WAF Klasik harus memiliki setidaknya satu kondisi.
14 September 2023	[WAF.7] Kelompok aturan global AWS WAF klasik harus memiliki setidaknya satu aturan	Judul kontrol yang diubah dari grup aturan global WAF harus memiliki setidaknya satu aturan ke grup aturan global AWS WAF Klasik harus memiliki setidaknya satu aturan.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
14 September 2023	[WAF.8] Web global AWS WAF klasik ACLs harus memiliki setidaknya satu aturan atau kelompok aturan	Judul kontrol yang diubah dari ACL web global WAF harus memiliki setidaknya a satu aturan atau grup aturan ke Web global AWS WAF Klasik ACLs harus memiliki setidaknya satu aturan atau grup aturan.
14 September 2023	[WAF.10] AWS WAF web ACLs harus memiliki setidaknya satu aturan atau kelompok aturan	Judul kontrol yang diubah dari ACL WAFv2 web harus memiliki setidaknya a satu aturan atau grup aturan ke AWS WAF web ACLs harus memiliki setidaknya satu aturan atau grup aturan.
14 September 2023	[WAF.11] pencatatan ACL AWS WAF web harus diaktifkan	Judul kontrol yang diubah dari AWS WAF v2 web ACL logging harus diaktifkan ke AWS WAF web ACL logging harus diaktifkan.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
Juli 20, 2023	[S3.4] Bucket S3 harus mengaktifkan enkripsi sisi server	S3.4 memeriksa apakah bucket Amazon S3 mengaktifkan enkripsi sisi server atau kebijakan bucket S3 secara eksplisit menolak permintaan tanpa enkripsi sisi server. PutObject Security Hub CSPM memperbarui kontrol ini untuk menyertakan enkripsi sisi server dual-layer dengan kunci KMS (DSSE-KMS). Kontrol menghasilkan temuan yang dilewatkan ketika bucket S3 dienkripsi dengan SSE-S3, SSE-KMS, atau DSSE-KMS.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
Juli 17, 2023	[S3.17] Ember tujuan umum S3 harus dienkripsi i saat istirahat AWS KMS keys	S3.17 memeriksa apakah bucket Amazon S3 dienkripsi i dengan file. AWS KMS key Security Hub CSPM memperbarui kontrol ini untuk menyertakan enkripsi sisi server dual-layer dengan kunci KMS (DSSE-KMS). Kontrol menghasilkan temuan yang dilewatkan ketika bucket S3 dienkripsi dengan SSE-KMS atau DSSE-KMS.
9 Juni 2023	[EKS.2] Kluster EKS harus berjalan pada versi Kubernetes yang didukung	EKS.2 memeriksa apakah kluster Amazon EKS berjalan pada versi Kubernetes yang didukung. Versi tertua yang didukung sekarang. 1.23

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
9 Juni 2023	[Lambda.2] Fungsi Lambda harus menggunakan runtime yang didukung	Lambda.2 memeriksa apakah setelah AWS Lambda fungsi untuk runtime cocok dengan nilai yang diharapkan yang ditetapkan untuk runtime yang didukung dalam setiap bahasa. Security Hub CSPM sekarang mendukung ruby3.2 sebagai parameter.
Juni 5, 2023	[APIGateway.5] Data cache API Gateway REST API harus dienkripsi saat istirahat	APIGateway.5.memeriksa apakah semua metode dalam tahapan API Amazon API Gateway REST dienkripsi saat istirahat. Security Hub CSPM memperbaiki kontrol untuk mengevaluasi enkripsi metode tertentu hanya ketika caching diaktifkan untuk metode itu.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
18 Mei 2023	[Lambda.2] Fungsi Lambda harus menggunakan runtime yang didukung	Lambda.2 memeriksa apakah setelan AWS Lambda fungsi untuk runtime cocok dengan nilai yang diharapkan yang ditetapkan untuk runtime yang didukung dalam setiap bahasa. Security Hub CSPM sekarang mendukung java17 sebagai parameter.
18 Mei 2023	[Lambda.2] Fungsi Lambda harus menggunakan runtime yang didukung	Lambda.2 memeriksa apakah setelan AWS Lambda fungsi untuk runtime cocok dengan nilai yang diharapkan yang ditetapkan untuk runtime yang didukung dalam setiap bahasa. Security Hub CSPM tidak lagi mendukung nodejs12.x sebagai parameter.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
April 23, 2023	[ECS.10] Layanan ECS Fargate harus berjalan pada versi platform Fargate terbaru	ECS.10 memeriksa apakah layanan Amazon ECS Fargate menjalankan versi platform Fargate terbaru. Pelanggan dapat menyebarkan Amazon ECS melalui ECS secara langsung, atau dengan menggunakan CodeDeploy Security Hub CSPM memperbaiki kontrol ini untuk menghasilkan temuan Lulus saat Anda menggunakan layanan CodeDeploy ECS Fargate.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
20 April 2023	[S3.6] Kebijakan bucket tujuan umum S3 harus membatasi akses ke yang lain Akun AWS	S3.6 memeriksa apakah kebijakan bucket Amazon Simple Storage Service (Amazon S3) mencegah prinsipal dari pihak Akun AWS lain melakukan tindakan yang ditolak pada sumber daya di bucket S3. Security Hub CSPM memperbarui kontrol untuk memperhitungkan persyaratan dalam kebijakan bucket.
18 April 2023	[Lambda.2] Fungsi Lambda harus menggunakan runtime yang didukung	Lambda.2 memeriksa apakah setelan AWS Lambda fungsi untuk runtime cocok dengan nilai yang diharapkan yang ditetapkan untuk runtime yang didukung dalam setiap bahasa. Security Hub CSPM sekarang mendukung python3.10 sebagai parameter.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
18 April 2023	[Lambda.2] Fungsi Lambda harus menggunakan runtime yang didukung	Lambda.2 memeriksa apakah setelah AWS Lambda fungsi untuk runtime cocok dengan nilai yang diharapkan yang ditetapkan untuk runtime yang didukung dalam setiap bahasa. Security Hub CSPM tidak lagi mendukung dotnetcore3.1 sebagai parameter.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
17 April 2023	[RDS.11] Instans RDS harus mengaktifkan pencadangan otomatis	RDS.11 memeriksa apakah instans Amazon RDS telah mengaktifkan pencadangan otomatis, dengan periode retensi cadangan yang lebih besar dari atau sama dengan tujuh hari. Security Hub CSPM memperbarui kontrol ini untuk mengecualikan replika baca dari evaluasi, karena tidak semua mesin mendukung pencadangan otomatis pada replika baca. Selain itu, RDS tidak menyediakan opsi untuk menentukan periode retensi cadangan saat membuat replika baca. Replika baca dibuat dengan periode retensi cadangan secara default.

Kontrol Security Hub untuk Akun AWS

Kontrol Security Hub ini mengevaluasi Akun AWS.

Kontrol ini mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat [Ketersediaan kontrol berdasarkan Wilayah](#).

[Akun.1] Informasi kontak keamanan harus disediakan untuk Akun AWS

Persyaratan terkait: Nist.800-53.r5 CM-2, Nist.800-53.r5 CM-2 (2)

Kategori: Identifikasi > Konfigurasi Sumber Daya

Tingkat keparahan: Sedang

Jenis sumber daya: AWS :: Account

AWS Config aturan: [security-account-information-provided](#)

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah akun Amazon Web Services (AWS) memiliki informasi kontak keamanan. Kontrol gagal jika informasi kontak keamanan tidak disediakan untuk akun.

Kontak keamanan alternatif memungkinkan AWS untuk menghubungi orang lain tentang masalah dengan akun Anda jika Anda tidak tersedia. Pemberitahuan dapat berasal dari Dukungan, atau Layanan AWS tim lain tentang topik terkait keamanan yang terkait dengan penggunaan Anda. Akun AWS

Remediasi

Untuk menambahkan kontak alternatif sebagai kontak keamanan ke kontak Anda Akun AWS, lihat [Memperbarui kontak alternatif untuk Anda Akun AWS](#) di Panduan Referensi Manajemen AWS Akun.

[Akun.2] Akun AWS harus menjadi bagian dari organisasi AWS Organizations

Kategori: Lindungi > Manajemen akses yang aman > Kontrol akses

Persyaratan terkait: NIST.800-53.r5 CA-9 (1), Nist.800-53.R5 CM-2

Tingkat keparahan: Tinggi

Jenis sumber daya: AWS :: Account

AWS Config aturan: [account-part-of-organizations](#)

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa Akun AWS apakah suatu bagian dari organisasi yang dikelola melalui AWS Organizations. Kontrol gagal jika akun bukan bagian dari organisasi.

Organizations membantu Anda mengelola lingkungan secara terpusat saat Anda meningkatkan beban kerja. AWS Anda dapat menggunakan beberapa Akun AWS untuk mengisolasi beban kerja yang memiliki persyaratan keamanan tertentu, atau untuk mematuhi kerangka kerja seperti HIPAA atau PCI. Dengan membuat organisasi, Anda dapat mengelola beberapa akun sebagai satu unit dan mengelola akses Layanan AWS, sumber daya, dan Wilayah secara terpusat.

Remediasi

Untuk membuat organisasi baru dan Akun AWS menambahkannya secara otomatis, lihat [Membuat organisasi](#) di Panduan AWS Organizations Pengguna. Untuk menambahkan akun ke organisasi yang ada, lihat [Mengundang Akun AWS untuk bergabung dengan organisasi Anda](#) di Panduan AWS Organizations Pengguna.

Kontrol Security Hub untuk AWS Amplify

Kontrol Security Hub ini mengevaluasi AWS Amplify layanan dan sumber daya. Kontrol mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat [Ketersediaan kontrol berdasarkan Wilayah](#).

[Amplify.1] Aplikasi Amplify harus diberi tag

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: AWS::Amplify::App

AWS Config aturan: [amplify-app-tagged](#)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
<code>requiredKeyTags</code>	Daftar kunci tag non-sistem yang harus ditetapkan ke sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS .	Tidak ada nilai default

Kontrol ini memeriksa apakah AWS Amplify aplikasi memiliki kunci tag yang ditentukan oleh `requiredKeyTags` parameter. Kontrol gagal jika aplikasi tidak memiliki kunci tag, atau tidak memiliki semua kunci yang ditentukan oleh `requiredKeyTags` parameter. Jika Anda tidak menentukan nilai apa pun untuk `requiredKeyTags` parameter, kontrol hanya akan memeriksa keberadaan kunci tag dan gagal jika aplikasi tidak memiliki kunci tag. Kontrol mengabaikan tag sistem, yang diterapkan secara otomatis dan memiliki `aws:` awalan.

Tag adalah label yang Anda buat dan tetapkan ke AWS sumber daya. Setiap tanda terdiri dari kunci tanda yang diperlukan dan nilai tanda opsional. Anda dapat menggunakan tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Mereka dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Mereka juga dapat membantu Anda melacak pemilik sumber daya untuk tindakan dan pemberitahuan. Anda juga dapat menggunakan tag untuk menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi. Untuk informasi selengkapnya tentang strategi ABAC, lihat [Menentukan izin berdasarkan atribut dengan otorisasi ABAC](#) di Panduan Pengguna IAM. Untuk informasi selengkapnya tentang tag, lihat [Panduan Pengguna AWS Sumber Daya Penandaan dan Editor Tag](#).

Note

Jangan menyimpan informasi pengenalan pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses dari banyak orang Layanan AWS. Mereka tidak dimaksudkan untuk digunakan untuk data pribadi atau sensitif.

Remediasi

Untuk informasi tentang menambahkan tag ke AWS Amplify aplikasi, lihat [Dukungan penandaan sumber daya](#) di Panduan Pengguna AWS Amplify Hosting.

[Amplify.2] Amplify branch harus diberi tag

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::Amplify::Branch`

AWS Config aturan: [amplify-branch-tagged](#)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
<code>requiredKeyTags</code>	Daftar kunci tag non-sistem yang harus ditetapkan ke sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS .	Tidak ada nilai default

Kontrol ini memeriksa apakah AWS Amplify cabang memiliki kunci tag yang ditentukan oleh `requiredKeyTags` parameter. Kontrol gagal jika cabang tidak memiliki kunci tag, atau tidak memiliki semua kunci yang ditentukan oleh `requiredKeyTags` parameter. Jika Anda tidak menentukan nilai apa pun untuk `requiredKeyTags` parameter, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika cabang tidak memiliki kunci tag. Kontrol mengabaikan tag sistem, yang diterapkan secara otomatis dan memiliki `aws:` awalan.

Tag adalah label yang Anda buat dan tetapkan ke AWS sumber daya. Setiap tanda terdiri dari kunci tanda yang diperlukan dan nilai tanda opsional. Anda dapat menggunakan tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Mereka dapat membantu

Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Mereka juga dapat membantu Anda melacak pemilik sumber daya untuk tindakan dan pemberitahuan. Anda juga dapat menggunakan tag untuk menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi. Untuk informasi selengkapnya tentang strategi ABAC, lihat [Menentukan izin berdasarkan atribut dengan otorisasi ABAC](#) di Panduan Pengguna IAM. Untuk informasi selengkapnya tentang tag, lihat [Panduan Pengguna AWS Sumber Daya Penandaan dan Editor Tag](#).

Note

Jangan menyimpan informasi pengenalan pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses dari banyak orang Layanan AWS. Mereka tidak dimaksudkan untuk digunakan untuk data pribadi atau sensitif.

Remediasi

Untuk informasi tentang menambahkan tag ke AWS Amplify cabang, lihat [Dukungan penandaan sumber daya](#) di Panduan Pengguna AWS Amplify Hosting.

Kontrol Security Hub untuk Amazon API Gateway

AWS Security Hub Kontrol ini mengevaluasi layanan dan sumber daya Amazon API Gateway. Kontrol mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat [Ketersediaan kontrol berdasarkan Wilayah](#).

[APIGateway.1] API Gateway REST dan pencatatan eksekusi WebSocket API harus diaktifkan

Persyaratan terkait: NIST.800-53.r5 AC-4 (26),, NIST.800-53.r5 SC-7 (9) NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, NIST.800-53.R5 SI-7 (8)

Kategori: Identifikasi > Logging

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::ApiGateway::Stage, AWS::ApiGatewayV2::Stage

AWS Config aturan: [api-gw-execution-logging-enabled](#)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang Diizinkan	Nilai default Security Hub
loggingLevel	Tingkat pencatatan log	Enum	ERROR, INFO	No default value

Kontrol ini memeriksa apakah semua tahapan Amazon API Gateway REST atau WebSocket API telah mengaktifkan logging. Kontrol gagal jika loggingLevel tidak ERROR atau INFO untuk semua tahapan API. Kecuali Anda memberikan nilai parameter khusus untuk menunjukkan bahwa jenis log tertentu harus diaktifkan, Security Hub akan menghasilkan temuan yang diteruskan jika tingkat logging adalah salah satu ERROR atau INFO.

API Gateway REST atau WebSocket API tahapan harus mengaktifkan log yang relevan. API Gateway REST dan pencatatan eksekusi WebSocket API menyediakan catatan terperinci tentang permintaan yang dibuat ke API Gateway REST dan tahapan WebSocket API. Tahapannya meliputi respons backend integrasi API, respons otorisasi Lambda, dan titik akhir untuk integrasi. requestId AWS

Tindakan Perbaikan

Untuk mengaktifkan logging untuk operasi REST dan WebSocket API, lihat [Mengatur pencatatan CloudWatch API menggunakan konsol API Gateway](#) di Panduan Pengembang API Gateway.

[APIGateway.2] Tahapan API Gateway REST API harus dikonfigurasi untuk menggunakan sertifikat SSL untuk otentikasi backend

Persyaratan terkait: NIST.800-53.r5 AC-1 7 (2),, NIST.800-53.r5 IA-5 (1) NIST.800-53.r5 AC-4, NIST.800-53.r5 SC-1 2 (3), 3, 3, 3 (NIST.800-53.r5 SC-13), NIST.800-53.r5 SC-2 (4),, NIST.800-53.r5 SC-2 (1), NIST.800-53.r5 SC-7 (2), NIST.800-53.r5 SC-8 Nist.800-53.r5 SI-7 NIST.800-53.r5 SC-8 (6), Nist.800-171.r2 3.13.15 NIST.800-53.r5 SC-8

Kategori: Lindungi > Perlindungan Data > Enkripsi data-in-transit

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::ApiGateway::Stage

AWS Config aturan: [api-gw-ssl-enabled](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah tahapan API Amazon API Gateway REST memiliki sertifikat SSL yang dikonfigurasi. Sistem backend menggunakan sertifikat ini untuk mengautentikasi bahwa permintaan yang masuk berasal dari API Gateway.

Tahapan API Gateway REST API harus dikonfigurasi dengan sertifikat SSL untuk memungkinkan sistem backend mengautentikasi permintaan tersebut berasal dari API Gateway.

Tindakan Perbaikan

Untuk petunjuk terperinci tentang cara membuat dan mengonfigurasi sertifikat SSL API Gateway REST API, lihat [Menghasilkan dan mengonfigurasi sertifikat SSL untuk autentikasi backend di Panduan Pengembang](#) API Gateway.

[APIGateway.3] Tahapan API Gateway REST API harus mengaktifkan AWS X-Ray penelusuran

Persyaratan terkait: NIST.800-53.r5 CA-7

Kategori: Deteksi > Layanan deteksi

Tingkat keparahan: Rendah

Jenis sumber daya: AWS::ApiGateway::Stage

AWS Config aturan: [api-gw-xray-enabled](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah penelusuran AWS X-Ray aktif diaktifkan untuk tahapan API REST Amazon API Gateway Anda.

X-Ray active tracing memungkinkan respons yang lebih cepat terhadap perubahan kinerja pada infrastruktur yang mendasarinya. Perubahan kinerja dapat mengakibatkan kurangnya ketersediaan API. X-Ray active tracing menyediakan metrik real-time permintaan pengguna yang mengalir melalui operasi API API Gateway REST API dan layanan yang terhubung.

Tindakan Perbaikan

Untuk petunjuk terperinci tentang cara mengaktifkan penelusuran aktif X-Ray untuk operasi API Gateway REST API, lihat [dukungan penelusuran aktif Amazon API Gateway AWS X-Ray](#) di Panduan AWS X-Ray Pengembang.

[APIGateway.4] API Gateway harus dikaitkan dengan ACL Web WAF

Persyaratan terkait: NIST.800-53.r5 AC-4 (21)

Kategori: Lindungi > Layanan pelindung

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::ApiGateway::Stage

AWS Config aturan: [api-gw-associated-with-waf](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah API Gateway menggunakan daftar kontrol akses (ACL) AWS WAF web. Kontrol ini gagal jika ACL AWS WAF web tidak dilampirkan ke tahap REST API Gateway.

AWS WAF adalah firewall aplikasi web yang membantu melindungi aplikasi web dan APIs dari serangan. Ini memungkinkan Anda untuk mengonfigurasi ACL, yang merupakan seperangkat aturan yang memungkinkan, memblokir, atau menghitung permintaan web berdasarkan aturan dan kondisi keamanan web yang dapat disesuaikan yang Anda tentukan. Pastikan tahap API Gateway Anda dikaitkan dengan ACL AWS WAF web untuk membantu melindunginya dari serangan berbahaya.

Tindakan Perbaikan

Untuk informasi tentang cara menggunakan konsol API Gateway untuk mengaitkan ACL web AWS WAF Regional dengan tahap API Gateway API yang ada, lihat [Menggunakan AWS WAF untuk melindungi Anda APIs](#) di Panduan Pengembang API Gateway.

[APIGateway.5] Data cache API Gateway REST API harus dienkripsi saat istirahat

Persyaratan terkait: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-1 3, NIST.800-53.r5 SC-2 8, NIST.800-53.r5 SC-2 8 (1), NIST.800-53.r5 SC-7 (10), NIST.800-53.R5 SI-7 (6)

Kategori: Lindungi > Perlindungan data > Enkripsi data saat istirahat

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::ApiGateway::Stage

AWS Config aturan: `api-gw-cache-encrypted` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah semua metode dalam tahapan API Gateway REST API yang mengaktifkan cache dienkripsi. Kontrol gagal jika metode apa pun dalam tahap API Gateway REST API dikonfigurasi ke cache dan cache tidak dienkripsi. Security Hub mengevaluasi enkripsi metode tertentu hanya ketika caching diaktifkan untuk metode itu.

Mengenkripsi data saat istirahat mengurangi risiko data yang disimpan pada disk diakses oleh pengguna yang tidak diautentikasi. AWS ini menambahkan satu set kontrol akses lain untuk membatasi kemampuan pengguna yang tidak sah mengakses data. Misalnya, izin API diperlukan untuk mendekripsi data sebelum dapat dibaca.

Cache API Gateway REST API harus dienkripsi saat istirahat untuk lapisan keamanan tambahan.

Tindakan Perbaikan

Untuk mengonfigurasi cache API untuk suatu tahap, lihat [Mengaktifkan caching Amazon API Gateway di Panduan](#) Pengembang API Gateway. Di Pengaturan Cache, pilih Enkripsi data cache.

[APIGateway.8] Rute API Gateway harus menentukan jenis otorisasi

Persyaratan terkait: NIST.800-53.r5 AC-3, Nist.800-53.r5 CM-2, Nist.800-53.R5 CM-2 (2)

Kategori: Lindungi > Manajemen Akses Aman

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::ApiGatewayV2::Route

AWS Config aturan: [api-gwv2-authorization-type-configured](#)

Jenis jadwal: Periodik

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang Diizinkan	Nilai default Security Hub
authorizationType	Jenis otorisasi rute API	Enum	AWS_IAM, CUSTOM, JWT	Tidak ada nilai default

Kontrol ini memeriksa apakah rute Amazon API Gateway memiliki jenis otorisasi. Kontrol gagal jika rute API Gateway tidak memiliki jenis otorisasi apa pun. Secara opsional, Anda dapat memberikan nilai parameter khusus jika Anda ingin kontrol lulus hanya jika rute menggunakan jenis otorisasi yang ditentukan dalam parameter. `authorizationType`

API Gateway mendukung beberapa mekanisme untuk mengontrol dan mengelola akses ke API Anda. Dengan menentukan jenis otorisasi, Anda dapat membatasi akses ke API hanya untuk pengguna atau proses yang diizinkan.

Tindakan Perbaikan

Untuk menetapkan jenis otorisasi untuk HTTP APIs, lihat [Mengendalikan dan mengelola akses ke API HTTP di API Gateway di Panduan Developer API Gateway](#). Untuk menetapkan jenis otorisasi WebSocket APIs, lihat [Mengontrol dan mengelola akses ke WebSocket API di API Gateway di Panduan Pengembang API Gateway](#).

[APIGateway.9] Pencatatan akses harus dikonfigurasi untuk Tahap API Gateway V2

Persyaratan terkait: NIST.800-53.r5 AC-4 (26),, NIST.800-53.r5 SC-7 (9) NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, NIST.800-53.R5 SI-7 (8), PCI DSS v4.0.1/10.4.2

Kategori: Identifikasi > Logging

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::ApiGatewayV2::Stage

AWS Config aturan: [api-gwv2-access-logs-enabled](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah tahapan Amazon API Gateway V2 memiliki pencatatan akses yang dikonfigurasi. Kontrol ini gagal jika pengaturan log akses tidak ditentukan.

Log akses API Gateway memberikan informasi terperinci tentang siapa yang telah mengakses API Anda dan bagaimana penelepon mengakses API. Log ini berguna untuk aplikasi seperti audit keamanan dan akses dan investigasi forensik. Aktifkan log akses ini untuk menganalisis pola lalu lintas dan memecahkan masalah.

Untuk praktik terbaik lainnya, lihat [Memantau REST APIs](#) di Panduan Pengembang API Gateway.

Tindakan Perbaikan

Untuk menyiapkan pencatatan akses, lihat [Mengatur pencatatan CloudWatch API menggunakan konsol API Gateway](#) di Panduan Pengembang API Gateway.

Kontrol Security Hub untuk AWS AppConfig

Kontrol Security Hub ini mengevaluasi AWS AppConfig layanan dan sumber daya.

Kontrol ini mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat [Ketersediaan kontrol berdasarkan Wilayah](#).

[AppConfig.1] AWS AppConfig aplikasi harus diberi tag

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: AWS::AppConfig::Application

AWS Config aturan: appconfig-application-tagged

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
requiredKeyTags	Daftar kunci tag non-sistem yang harus berisi sumber daya	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi	Tidak ada nilai default

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
	yang dievaluasi. Kunci tag peka huruf besar dan kecil.		persyaratan AWS .	

Kontrol ini memeriksa apakah AWS AppConfig aplikasi memiliki tag dengan kunci tertentu yang ditentukan dalam `parameterrequiredKeyTags`. Kontrol gagal jika aplikasi tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam `parameterrequiredKeyTags`. Jika parameter `requiredKeyTags` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika aplikasi tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws :`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat [Menentukan izin berdasarkan atribut dengan otorisasi ABAC di Panduan Pengguna IAM](#).

Note

Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk mengetahui praktik terbaik penandaan lainnya, lihat [Praktik dan strategi terbaik](#) di Panduan Pengguna AWS Sumber Daya Penandaan dan Editor Tag.

Remediasi

Untuk menambahkan tag ke AWS AppConfig aplikasi, lihat [TagResource](#) di Referensi API AWS AppConfig .

[AppConfig.2] profil AWS AppConfig konfigurasi harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::AppConfig::ConfigurationProfile`

AWS Config aturan: `appconfig-configuration-profile-tagged`

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
<code>requiredKeyTags</code>	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS .	Tidak ada nilai default

Kontrol ini memeriksa apakah profil AWS AppConfig konfigurasi memiliki tag dengan kunci tertentu yang ditentukan dalam parameter `requiredKeyTags`. Kontrol gagal jika profil konfigurasi tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter `requiredKeyTags`. Jika parameter `requiredKeyTags` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika profil konfigurasi tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS

sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat [Menentukan izin berdasarkan atribut dengan otorisasi ABAC di Panduan Pengguna IAM](#).

Note

Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk mengetahui praktik terbaik penandaan lainnya, lihat [Praktik dan strategi terbaik](#) di Panduan Pengguna AWS Sumber Daya Penandaan dan Editor Tag.

Remediasi

Untuk menambahkan tag ke profil AWS AppConfig konfigurasi, lihat [TagResource](#) di Referensi API AWS AppConfig .

[AppConfig.3] AWS AppConfig lingkungan harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::AppConfig::Environment`

AWS Config aturan: `appconfig-environment-tagged`

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
<code>requiredKeyTags</code>	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi	Tidak ada nilai default

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
			persyaratan AWS	

Kontrol ini memeriksa apakah AWS AppConfig lingkungan memiliki tag dengan kunci tertentu yang ditentukan dalam `parameterrequiredKeyTags`. Kontrol gagal jika lingkungan tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam `parameterrequiredKeyTags`. Jika parameter `requiredKeyTags` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika lingkungan tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws :`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat [Menentukan izin berdasarkan atribut dengan otorisasi ABAC di Panduan Pengguna IAM](#).

Note

Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk mengetahui praktik terbaik penandaan lainnya, lihat [Praktik dan strategi terbaik](#) di Panduan Pengguna AWS Sumber Daya Penandaan dan Editor Tag.

Remediasi

Untuk menambahkan tag ke AWS AppConfig lingkungan, lihat [TagResource](#) di Referensi API AWS AppConfig.

[AppConfig.4] asosiasi AWS AppConfig ekstensi harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::AppConfig::ExtensionAssociation`

AWS Config aturan: `appconfig-extension-association-tagged`

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
<code>requiredKeyTags</code>	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS .	Tidak ada nilai default

Kontrol ini memeriksa apakah asosiasi AWS AppConfig ekstensi memiliki tag dengan kunci tertentu yang ditentukan dalam parameter `requiredKeyTags`. Kontrol gagal jika asosiasi ekstensi tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter `requiredKeyTags`. Jika parameter `requiredKeyTags` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika asosiasi ekstensi tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS

sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat [Menentukan izin berdasarkan atribut dengan otorisasi ABAC di Panduan Pengguna IAM](#).

 Note

Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk mengetahui praktik terbaik penandaan lainnya, lihat [Praktik dan strategi terbaik di Panduan Pengguna AWS Sumber Daya Penandaan dan Editor Tag](#).

Remediasi

Untuk menambahkan tag ke asosiasi AWS AppConfig ekstensi, lihat [TagResource](#) di Referensi API AWS AppConfig .

Kontrol Security Hub untuk Amazon AppFlow

Kontrol Security Hub ini mengevaluasi AppFlow layanan dan sumber daya Amazon.

Kontrol ini mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat [Ketersediaan kontrol berdasarkan Wilayah](#).

[AppFlow.1] AppFlow Aliran Amazon harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: AWS::AppFlow::Flow

AWS Config aturan: appflow-flow-tagged

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
<code>requiredKeyTags</code>	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS .	Tidak ada nilai default

Kontrol ini memeriksa apakah AppFlow aliran Amazon memiliki tag dengan kunci tertentu yang ditentukan dalam parameter `requiredKeyTags`. Kontrol gagal jika aliran tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter `requiredKeyTags`. Jika parameter `requiredKeyTags` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika alur tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws :`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat [Menentukan izin berdasarkan atribut dengan otorisasi ABAC di Panduan Pengguna IAM](#).

Note

Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk mengetahui praktik terbaik penandaan lainnya, lihat [Praktik dan strategi terbaik di Panduan Pengguna AWS Sumber Daya Penandaan dan Editor Tag](#).

Remediasi

Untuk menambahkan tag ke AppFlow alur Amazon, lihat [Membuat alur di Amazon AppFlow](#) di Panduan AppFlow Pengguna Amazon.

Kontrol Security Hub untuk AWS App Runner

AWS Security Hub Kontrol ini mengevaluasi AWS App Runner layanan dan sumber daya. Kontrol mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat [Ketersediaan kontrol berdasarkan Wilayah](#).

[AppRunner.1] Layanan App Runner harus diberi tag

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: AWS::AppRunner::Service

AWS Config aturan: [apprunner-service-tagged](#)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
requiredKeyTags	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS .	Tidak ada nilai default

Kontrol ini memeriksa apakah AWS App Runner layanan memiliki tag dengan kunci tertentu yang ditentukan dalam parameter `requiredKeyTags`. Kontrol gagal jika layanan App Runner tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter `requiredKeyTags`. Jika parameter `requiredKeyTags` tidak disediakan, kontrol hanya

memeriksa keberadaan kunci tag dan gagal jika layanan App Runner tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengkategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat [Menentukan izin berdasarkan atribut dengan otorisasi ABAC di Panduan Pengguna IAM](#).

Note

Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk mengetahui praktik terbaik penandaan lainnya, lihat [Praktik dan strategi terbaik](#) di Panduan Pengguna AWS Sumber Daya Penandaan dan Editor Tag.

Remediasi

Untuk informasi tentang menambahkan tag ke AWS App Runner layanan, lihat [TagResource](#) di Referensi API AWS App Runner .

[AppRunner.2] Konektor VPC App Runner harus diberi tag

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::AppRunner::VpcConnector`

AWS Config aturan: [apprunner-vpc-connector-tagged](#)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
<code>requiredKeyTags</code>	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS .	Tidak ada nilai default

Kontrol ini memeriksa apakah konektor AWS App Runner VPC memiliki tag dengan kunci spesifik yang ditentukan dalam parameter. `requiredKeyTags` Kontrol gagal jika konektor VPC tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter. `requiredKeyTags` Jika parameter `requiredKeyTags` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika konektor VPC tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat [Menentukan izin berdasarkan atribut dengan otorisasi ABAC di Panduan Pengguna IAM](#).

Note

Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk mengetahui praktik terbaik penandaan lainnya, lihat [Praktik dan strategi terbaik di Panduan Pengguna AWS Sumber Daya Penandaan dan Editor Tag](#).

Remediasi

Untuk informasi tentang menambahkan tag ke konektor AWS App Runner VPC, lihat [TagResource](#) di Referensi API AWS App Runner .

Kontrol Security Hub untuk AWS AppSync

Kontrol Security Hub ini mengevaluasi AWS AppSync layanan dan sumber daya.

Kontrol ini mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat [Ketersediaan kontrol berdasarkan Wilayah](#).

[AppSync.1] Cache AWS AppSync API harus dienkripsi saat istirahat

Kategori: Lindungi > Perlindungan Data > Enkripsi data-at-rest

Tingkat keparahan: Sedang

Jenis sumber daya: AWS :: AppSync :: GraphQLApi

AWS Config aturan: [appsync-cache-ct-encryption-at-rest](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah cache AWS AppSync API dienkripsi saat istirahat. Kontrol gagal jika cache API tidak dienkripsi saat istirahat.

Data saat istirahat mengacu pada data yang disimpan dalam penyimpanan persisten dan tidak mudah menguap untuk durasi berapa pun. Mengenkripsi data saat istirahat membantu Anda melindungi kerahasiaannya, yang mengurangi risiko bahwa pengguna yang tidak sah dapat mengaksesnya.

Remediasi

Anda tidak dapat mengubah pengaturan enkripsi setelah mengaktifkan caching untuk API Anda AWS AppSync . Sebagai gantinya, Anda harus menghapus cache dan membuatnya kembali dengan enkripsi diaktifkan. Untuk informasi selengkapnya, lihat [Enkripsi cache](#) di Panduan AWS AppSync Pengembang.

[AppSync.2] AWS AppSync harus mengaktifkan logging tingkat lapangan

Persyaratan terkait: PCI DSS v4.0.1/10.4.2

Kategori: Identifikasi > Logging

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::AppSync::GraphQLApi

AWS Config aturan: [appsync-logging-enabled](#)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub	
fieldLoggingLevel	Tingkat pencatatan lapangan	Enum	ERROR, ALL, INFO, DEBUG	No default value	

Kontrol ini memeriksa apakah AWS AppSync API telah mengaktifkan logging tingkat bidang. Kontrol gagal jika tingkat log penyelesaian bidang diatur ke Tidak Ada. Kecuali Anda memberikan nilai parameter khusus untuk menunjukkan bahwa jenis log tertentu harus diaktifkan, Security Hub menghasilkan temuan yang diteruskan jika tingkat log penyelesaian bidang adalah salah satu atau ERROR. ALL

Anda dapat menggunakan logging dan metrik untuk mengidentifikasi, memecahkan masalah, dan mengoptimalkan kueri GraphQL Anda. Mengaktifkan logging untuk AWS AppSync GraphQL membantu Anda mendapatkan informasi terperinci tentang permintaan dan tanggapan API, mengidentifikasi dan menanggapi masalah, dan mematuhi persyaratan peraturan.

Remediasi

Untuk mengaktifkan pencatatan AWS AppSync, lihat [Pengaturan dan konfigurasi](#) di Panduan AWS AppSync Pengembang.

[AppSync.4] AWS AppSync APIs GraphQL harus diberi tag

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::AppSync::GraphQLApi`

AWS Config aturan: `tagged-appsync-graphqlapi` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
<code>requiredTagKeys</code>	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS .	Tidak ada nilai default

Kontrol ini memeriksa apakah AWS AppSync GraphQL API memiliki tag dengan kunci spesifik yang ditentukan dalam parameter. `requiredTagKeys` Kontrol gagal jika GraphQL API tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter. `requiredTagKeys` Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika GraphQL API tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat [Untuk apa ABAC? AWS](#) di Panduan Pengguna IAM.

Note

Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat [Menandai AWS sumber daya Anda](#) di Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke AWS AppSync GraphQL API, lihat [TagResource](#) di Referensi API AWS AppSync .

[AppSync.5] AWS AppSync APIs GraphQL tidak boleh diautentikasi dengan kunci API

Persyaratan terkait: NIST.800-53.r5 AC-2 (1) NIST.800-53.r5 AC-3,, NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-6

Kategori: Lindungi > Manajemen akses aman > Otentikasi tanpa kata sandi

Tingkat keparahan: Tinggi

Jenis sumber daya: AWS::AppSync::GraphQLApi

AWS Config aturan: [appsync-authorization-check](#)

Jenis jadwal: Perubahan dipicu

Parameter:

- AllowedAuthorizationTypes: AWS_LAMBDA, AWS_IAM, OPENID_CONNECT, AMAZON_COGNITO_USER_POOLS (tidak dapat disesuaikan)

Kontrol ini memeriksa apakah aplikasi Anda menggunakan kunci API untuk berinteraksi dengan AWS AppSync GraphQL API. Kontrol gagal jika AWS AppSync GraphQL API diautentikasi dengan kunci API.

Kunci API adalah nilai hard-code dalam aplikasi Anda yang dihasilkan oleh AWS AppSync layanan saat Anda membuat titik akhir GraphQL yang tidak diautentikasi. Jika kunci API ini dikompromikan, titik akhir Anda rentan terhadap akses yang tidak diinginkan. Kecuali Anda mendukung aplikasi

atau situs web yang dapat diakses publik, kami tidak menyarankan menggunakan kunci API untuk otentikasi.

Remediasi

Untuk menetapkan opsi otorisasi untuk AWS AppSync GraphQL API Anda, [lihat Otorisasi dan otentikasi](#) di Panduan Pengembang.AWS AppSync

[AppSync.6] Cache AWS AppSync API harus dienkripsi saat transit

Kategori: Lindungi > Perlindungan Data > Enkripsi data-in-transit

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::AppSync::ApiCache

AWS Config aturan: [appsync-cache-ct-encryption-in-transit](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah cache AWS AppSync API dienkripsi saat transit. Kontrol gagal jika cache API tidak dienkripsi saat transit.

Data dalam transit mengacu pada data yang berpindah dari satu lokasi ke lokasi lain, seperti antar node di cluster Anda atau antara cluster Anda dan aplikasi Anda. Data dapat bergerak di internet atau dalam jaringan pribadi. Mengenkripsi data dalam perjalanan mengurangi risiko bahwa pengguna yang tidak sah dapat menguping lalu lintas jaringan.

Remediasi

Anda tidak dapat mengubah pengaturan enkripsi setelah mengaktifkan caching untuk API Anda AWS AppSync . Sebagai gantinya, Anda harus menghapus cache dan membuatnya kembali dengan enkripsi diaktifkan. Untuk informasi selengkapnya, lihat [Enkripsi cache](#) di Panduan AWS AppSync Pengembang.

Kontrol Security Hub untuk Amazon Athena

AWS Security Hub Kontrol ini mengevaluasi layanan dan sumber daya Amazon Athena. Kontrol mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat [Ketersediaan kontrol berdasarkan Wilayah](#).

[Athena.1] Kelompok kerja Athena harus dienkripsi saat istirahat

Important

Security Hub menghentikan kontrol ini pada April 2024. Untuk informasi selengkapnya, lihat [Ubah log untuk kontrol CSPM Security Hub](#).

Kategori: Lindungi > Perlindungan data > Enkripsi data saat istirahat

Persyaratan terkait: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-1 3, NIST.800-53.r5 SC-2 8, NIST.800-53.r5 SC-2 8 (1), NIST.800-53.r5 SC-7 (10), NIST.800-53.R5 SI-7 (6)

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::Athena::WorkGroup

AWS Config aturan: [athena-workgroup-encrypted-at-rest](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah workgroup Athena dienkripsi saat istirahat. Kontrol gagal jika workgroup Athena tidak dienkripsi saat istirahat.

Di Athena, Anda dapat membuat grup kerja untuk menjalankan kueri untuk tim, aplikasi, atau beban kerja yang berbeda. Setiap workgroup memiliki pengaturan untuk mengaktifkan enkripsi pada semua query. Anda memiliki opsi untuk menggunakan enkripsi sisi server dengan kunci terkelola Amazon Simple Storage Service (Amazon S3), enkripsi sisi server dengan kunci AWS KMS(), atau enkripsi sisi klien AWS Key Management Service dengan kunci KMS yang dikelola pelanggan. Data saat istirahat mengacu pada data apa pun yang disimpan dalam penyimpanan persisten dan tidak mudah dikuap untuk durasi berapa pun. Enkripsi membantu Anda melindungi kerahasiaan data tersebut, mengurangi risiko bahwa pengguna yang tidak sah dapat mengaksesnya.

Remediasi

Untuk mengaktifkan enkripsi saat istirahat untuk grup kerja Athena, lihat [Mengedit grup kerja di Panduan Pengguna](#) Amazon Athena. Di bagian Konfigurasi Hasil Kueri, pilih Enkripsi hasil kueri.

[Athena.2] Katalog data Athena harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: AWS::Athena::DataCatalog

AWS Config aturan: tagged-athena-datacatalog (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
<code>requiredTagKeys</code>	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS.	No default value

Kontrol ini memeriksa apakah katalog data Amazon Athena memiliki tag dengan kunci tertentu yang ditentukan dalam parameter. `requiredTagKeys` Kontrol gagal jika katalog data tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter `requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika katalog data tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke

AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat [Untuk apa ABAC? AWS](#) di Panduan Pengguna IAM.

Note

Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat [Menandai AWS sumber daya Anda](#) di Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke katalog data Athena, lihat [Menandai sumber daya Athena di Panduan Pengguna Amazon Athena](#).

[Athena.3] Kelompok kerja Athena harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: AWS::Athena::WorkGroup

AWS Config aturan: tagged-athena-workgroup (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
requiredTagKeys	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi	No default value

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
			persyaratan AWS .	

Kontrol ini memeriksa apakah workgroup Amazon Athena memiliki tag dengan kunci tertentu yang ditentukan dalam parameter. `requiredTagKeys` Kontrol gagal jika workgroup tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter `requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika workgroup tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws :`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat [Untuk apa ABAC? AWS](#) di Panduan Pengguna IAM.

Note

Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat [Menandai AWS sumber daya Anda](#) di Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke workgroup Athena, lihat [Menambahkan dan menghapus tag pada grup kerja individual di Panduan Pengguna](#) Amazon Athena.

[Athena.4] Kelompok kerja Athena seharusnya mengaktifkan logging

Kategori: Identifikasi > Logging

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::Athena::WorkGroup

AWS Config aturan: [athena-workgroup-logging-enabled](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah workgroup Amazon Athena telah mengaktifkan logging. Kontrol gagal jika workgroup tidak mengaktifkan logging.

Log audit melacak dan memantau aktivitas sistem. Mereka menyediakan catatan peristiwa yang dapat membantu Anda mendeteksi pelanggaran keamanan, menyelidiki insiden, dan mematuhi peraturan. Log audit juga meningkatkan akuntabilitas dan transparansi organisasi Anda secara keseluruhan.

Remediasi

Untuk informasi tentang mengaktifkan pencatatan untuk grup kerja Athena, [lihat CloudWatch Mengaktifkan metrik kueri di Athena di Panduan Pengguna Amazon Athena](#).

Kontrol Security Hub untuk AWS Backup

Kontrol Security Hub ini mengevaluasi AWS Backup layanan dan sumber daya.

Kontrol ini mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat [Ketersediaan kontrol berdasarkan Wilayah](#).

[Backup.1] titik AWS Backup pemulihan harus dienkripsi saat istirahat

Persyaratan terkait: NIST.800-53.R5 CP-9 (8), NIST.800-53.R5 SI-12

Kategori: Lindungi > Perlindungan Data > Enkripsi data-at-rest

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::Backup::RecoveryPoint

AWS Config aturan: [backup-recovery-point-encrypted](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah titik AWS Backup pemulihan dienkripsi saat istirahat. Kontrol gagal jika titik pemulihan tidak dienkripsi saat istirahat.

Titik AWS Backup pemulihan mengacu pada salinan atau snapshot data tertentu yang dibuat sebagai bagian dari proses pencadangan. Ini merupakan momen tertentu dalam waktu ketika data dicadangkan dan berfungsi sebagai titik pemulihan jika data asli hilang, rusak, atau tidak dapat diakses. Mengenkripsi titik pemulihan cadangan menambahkan lapisan perlindungan ekstra terhadap akses yang tidak sah. Enkripsi adalah praktik terbaik untuk melindungi kerahasiaan, integritas, dan keamanan data cadangan.

Remediasi

Untuk mengenkripsi titik AWS Backup pemulihan, lihat [Enkripsi untuk cadangan AWS Backup di Panduan Pengembang](#).AWS Backup

[Backup.2] poin AWS Backup pemulihan harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: AWS::Backup::RecoveryPoint

AWS Config aturan: tagged-backup-recoverypoint (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
requiredTagKeys	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS .	Tidak ada nilai default

Kontrol ini memeriksa apakah titik AWS Backup pemulihan memiliki tag dengan kunci spesifik yang ditentukan dalam parameter `requiredTagKeys`. Kontrol gagal jika titik pemulihan tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter `requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika titik pemulihan tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws :`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat [Untuk apa ABAC? AWS](#) di Panduan Pengguna IAM.

Note

Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat [Menandai AWS sumber daya Anda](#) di Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke titik AWS Backup pemulihan

1. Buka AWS Backup konsol di <https://console.aws.amazon.com/backup>.
2. Di panel navigasi, pilih Rencana cadangan.
3. Pilih paket cadangan dari daftar.
4. Di bagian Tag paket Backup, pilih Kelola tag.
5. Masukkan kunci dan nilai untuk tanda tersebut. Pilih Tambahkan tag baru untuk pasangan nilai kunci tambahan.

6. Setelah Anda selesai menambahkan tanda, pilih Simpan.

[Backup.3] AWS Backup brankas harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::Backup::BackupVault`

AWS Config aturan: `tagged-backup-backupvault` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
<code>requiredTagKeys</code>	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS .	Tidak ada nilai default

Kontrol ini memeriksa apakah AWS Backup vault memiliki tag dengan kunci spesifik yang ditentukan dalam parameter `requiredTagKeys`. Kontrol gagal jika titik pemulihan tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter `requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika titik pemulihan tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengkategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang

bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat [Untuk apa ABAC? AWS](#) di Panduan Pengguna IAM.

Note

Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat [Menandai AWS sumber daya Anda](#) di Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke AWS Backup brankas

1. Buka AWS Backup konsol di <https://console.aws.amazon.com/backup>.
2. Di panel navigasi, pilih Brankas cadangan.
3. Pilih brankas cadangan dari daftar.
4. Di bagian Backup vault tags, pilih Kelola tag.
5. Masukkan kunci dan nilai untuk tanda tersebut. Pilih Tambahkan tag baru untuk pasangan nilai kunci tambahan.
6. Setelah Anda selesai menambahkan tanda, pilih Simpan.

[Backup.4] rencana AWS Backup laporan harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: AWS::Backup::ReportPlan

AWS Config aturan: tagged-backup-reportplan (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
<code>requiredTagKeys</code>	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS .	Tidak ada nilai default

Kontrol ini memeriksa apakah rencana AWS Backup laporan memiliki tag dengan kunci spesifik yang ditentukan dalam parameter `requiredTagKeys`. Kontrol gagal jika rencana laporan tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter `requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika rencana laporan tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat [Untuk apa ABAC? AWS](#) di Panduan Pengguna IAM.

Note

Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS

Billing. Untuk praktik terbaik penandaan lainnya, lihat [Menandai AWS sumber daya Anda](#) di Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke rencana AWS Backup laporan

1. Buka AWS Backup konsol di <https://console.aws.amazon.com/backup>.
2. Di panel navigasi, pilih Brankas cadangan.
3. Pilih brankas cadangan dari daftar.
4. Di bagian Backup vault tags, pilih Kelola tag.
5. Pilih Tambahkan tag baru. Masukkan kunci dan nilai untuk tanda tersebut. Ulangi untuk pasangan nilai kunci tambahan.
6. Setelah Anda selesai menambahkan tanda, pilih Simpan.

[Backup.5] rencana AWS Backup cadangan harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: AWS::Backup::BackupPlan

AWS Config aturan: tagged-backup-backupplan (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
requiredTagKeys	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi	Tidak ada nilai default

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub

[persyaratan AWS](#).

Kontrol ini memeriksa apakah rencana AWS Backup cadangan memiliki tag dengan kunci spesifik yang ditentukan dalam `parameterrequiredTagKeys`. Kontrol gagal jika paket cadangan tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam `parameterrequiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika paket cadangan tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengkategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat [Untuk apa ABAC? AWS](#) di Panduan Pengguna IAM.

Note

Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat [Menandai AWS sumber daya Anda](#) di Referensi Umum AWS.

Remediasi

Untuk menambahkan tag ke rencana AWS Backup cadangan

1. Buka AWS Backup konsol di <https://console.aws.amazon.com/backup>.
2. Di panel navigasi, pilih Brankas cadangan.
3. Pilih brankas cadangan dari daftar.
4. Di bagian Backup vault tags, pilih Kelola tag.
5. Pilih Tambahkan tag baru. Masukkan kunci dan nilai untuk tanda tersebut. Ulangi untuk pasangan nilai kunci tambahan.
6. Setelah Anda selesai menambahkan tanda, pilih Simpan.

Kontrol Security Hub untuk AWS Batch

Kontrol Security Hub ini mengevaluasi AWS Batch layanan dan sumber daya. Kontrol mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat [Ketersediaan kontrol berdasarkan Wilayah](#).

[Batch.1] Antrian pekerjaan batch harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: AWS::Batch::JobQueue

AWS Config aturan: [batch-job-queue-tagged](#)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
<code>requiredKeyTags</code>	Daftar kunci tag non-sistem yang harus berisi sumber daya	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi	Tidak ada nilai default

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
	yang dievaluasi. Kunci tag peka huruf besar dan kecil.		persyaratan AWS .	

Kontrol ini memeriksa apakah antrian AWS Batch pekerjaan memiliki tag dengan kunci tertentu yang ditentukan dalam parameter `requiredKeyTags`. Kontrol gagal jika antrian pekerjaan tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter `requiredKeyTags`. Jika parameter `requiredKeyTags` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika antrian pekerjaan tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws :`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat [Menentukan izin berdasarkan atribut dengan otorisasi ABAC di Panduan Pengguna IAM](#).

Note

Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk mengetahui praktik terbaik penandaan lainnya, lihat [Praktik dan strategi terbaik](#) di Panduan Pengguna AWS Sumber Daya Penandaan dan Editor Tag.

Remediasi

Untuk menambahkan tag ke antrian pekerjaan Batch, lihat [Menandai sumber daya Anda](#) di Panduan AWS Batch Pengguna.

[Batch.2] Kebijakan penjadwalan batch harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::Batch::SchedulingPolicy`

AWS Config aturan: [batch-scheduling-policy-tagged](#)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
<code>requiredKeyTags</code>	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS .	Tidak ada nilai default

Kontrol ini memeriksa apakah kebijakan AWS Batch penjadwalan memiliki tag dengan kunci spesifik yang ditentukan dalam parameter `requiredKeyTags`. Kontrol gagal jika kebijakan penjadwalan tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter `requiredKeyTags`. Jika parameter `requiredKeyTags` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika kebijakan penjadwalan tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS

sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat [Menentukan izin berdasarkan atribut dengan otorisasi ABAC di Panduan Pengguna IAM](#).

Note

Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk mengetahui praktik terbaik penandaan lainnya, lihat [Praktik dan strategi terbaik di Panduan Pengguna AWS Sumber Daya Penandaan dan Editor Tag](#).

Remediasi

Untuk menambahkan tag ke kebijakan penjadwalan Batch, lihat [Menandai sumber daya Anda](#) di Panduan AWS Batch Pengguna.

[Batch.3] Lingkungan komputasi Batch harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::Batch::ComputeEnvironment`

AWS Config aturan: [batch-compute-environment-tagged](#)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
<code>requiredKeyTags</code>	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi	Tidak ada nilai default

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub

[persyaratan AWS](#).

Kontrol ini memeriksa apakah lingkungan AWS Batch komputasi memiliki tag dengan kunci tertentu yang ditentukan dalam `parameterrequiredKeyTags`. Kontrol gagal jika lingkungan komputasi tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam `parameterrequiredKeyTags`. Jika parameter `requiredKeyTags` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika lingkungan komputasi tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat [Menentukan izin berdasarkan atribut dengan otorisasi ABAC di Panduan Pengguna IAM](#).

Note

Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk mengetahui praktik terbaik penandaan lainnya, lihat [Praktik dan strategi terbaik](#) di Panduan Pengguna AWS Sumber Daya Penandaan dan Editor Tag.

Remediasi

Untuk menambahkan tag ke lingkungan komputasi Batch, lihat [Menandai sumber daya Anda](#) di Panduan AWS Batch Pengguna.

[Batch.4] Properti sumber daya komputasi di lingkungan komputasi Batch terkelola harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::Batch::ComputeEnvironment`

AWS Config aturan: [batch-managed-compute-env-compute-resources-tagged](#)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
<code>requiredKeyTags</code>	Daftar kunci tag non-sistem yang harus ditetapkan ke sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS	Tidak ada nilai default

Kontrol ini memeriksa apakah properti sumber daya komputasi di lingkungan AWS Batch komputasi terkelola memiliki kunci tag yang ditentukan oleh parameter. `requiredKeyTags` Kontrol gagal jika properti sumber daya komputasi tidak memiliki kunci tag, atau tidak memiliki semua kunci yang ditentukan oleh `requiredKeyTags` parameter. Jika Anda tidak menentukan nilai apa pun untuk `requiredKeyTags` parameter, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika properti sumber daya komputasi tidak memiliki kunci tag. Kontrol mengabaikan tag sistem, yang diterapkan secara otomatis dan memiliki `aws:` awalan. Kontrol ini tidak mengevaluasi lingkungan komputasi yang tidak dikelola, atau lingkungan terkelola yang menggunakan AWS Fargate sumber daya.

Tag adalah label yang Anda buat dan tetapkan ke AWS sumber daya. Setiap tanda terdiri dari kunci tanda yang diperlukan dan nilai tanda opsional. Anda dapat menggunakan tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Mereka dapat membantu

Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Mereka juga dapat membantu Anda melacak pemilik sumber daya untuk tindakan dan pemberitahuan. Anda juga dapat menggunakan tag untuk menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi. Untuk informasi selengkapnya tentang strategi ABAC, lihat [Menentukan izin berdasarkan atribut dengan otorisasi ABAC](#) di Panduan Pengguna IAM. Untuk informasi selengkapnya tentang tag, lihat [Panduan Pengguna AWS Sumber Daya Penandaan dan Editor Tag](#).

Note

Jangan menyimpan informasi pengenalan pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses dari banyak orang Layanan AWS. Mereka tidak dimaksudkan untuk digunakan untuk data pribadi atau sensitif.

Remediasi

Untuk informasi tentang menambahkan tag untuk menghitung sumber daya di lingkungan AWS Batch komputasi terkelola, lihat [Menandai sumber daya Anda](#) di AWS Batch Panduan Pengguna.

Kontrol Security Hub untuk AWS Certificate Manager

AWS Security Hub Kontrol ini mengevaluasi layanan dan sumber daya AWS Certificate Manager (ACM). Kontrol mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat [Ketersediaan kontrol berdasarkan Wilayah](#).

[ACM.1] Sertifikat yang diimpor dan diterbitkan ACM harus diperbarui setelah jangka waktu tertentu

Persyaratan terkait: NIST.800-53.r5 SC-2 8 (3), NIST.800-53.r5 SC-7 (16), Nist.800-171.r2 3.13.15, PCI DSS v4.0.1/4.2.1

Kategori: Lindungi > Perlindungan Data > Enkripsi data-in-transit

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::ACM::Certificate

AWS Config aturan: [acm-certificate-expiration-check](#)

Jenis jadwal: Perubahan yang dipicu dan berkala

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang Diizinkan	Nilai default Security Hub
daysToExpiration	Jumlah hari di mana sertifikat ACM harus diperpanjang	Bilangan Bulat	14 untuk 365	30

Kontrol ini memeriksa apakah sertifikat AWS Certificate Manager (ACM) diperbarui dalam jangka waktu yang ditentukan. Ini memeriksa sertifikat impor dan sertifikat yang disediakan oleh ACM. Kontrol gagal jika sertifikat tidak diperbarui dalam jangka waktu yang ditentukan. Kecuali Anda memberikan nilai parameter khusus untuk periode perpanjangan, Security Hub menggunakan nilai default 30 hari.

ACM dapat secara otomatis memperbarui sertifikat yang menggunakan validasi DNS. Untuk sertifikat yang menggunakan validasi email, Anda harus menanggapi email validasi domain. ACM tidak secara otomatis memperbarui sertifikat yang Anda impor. Anda harus memperbarui sertifikat yang diimpor secara manual.

Remediasi

ACM menyediakan pembaruan terkelola untuk sertifikat SSL/TLS Anda yang diterbitkan oleh Amazon. Ini berarti bahwa ACM memperbarui sertifikat Anda secara otomatis (jika Anda menggunakan validasi DNS), atau mengirim Anda pemberitahuan email ketika kedaluwarsa sertifikat mendekati. Layanan ini disediakan untuk sertifikat ACM publik dan swasta.

Untuk domain yang divalidasi melalui email

Ketika sertifikat 45 hari dari kedaluwarsa, ACM mengirimkan email kepada pemilik domain untuk setiap nama domain. Untuk memvalidasi domain dan menyelesaikan pembaruan, Anda harus menanggapi pemberitahuan email.

Untuk informasi selengkapnya, lihat [Perpanjangan domain yang divalidasi melalui email di Panduan Pengguna AWS Certificate Manager](#)

Untuk domain yang divalidasi oleh DNS

ACM secara otomatis memperbarui sertifikat yang menggunakan validasi DNS. 60 hari sebelum kedaluwarsa, ACM memverifikasi bahwa sertifikat dapat diperpanjang.

Jika tidak dapat memvalidasi nama domain, maka ACM mengirimkan pemberitahuan bahwa validasi manual diperlukan. Ini mengirimkan pemberitahuan ini 45 hari, 30 hari, 7 hari, dan 1 hari sebelum kedaluwarsa.

Untuk informasi selengkapnya, lihat [Perpanjangan domain yang divalidasi oleh DNS](#) di Panduan Pengguna.AWS Certificate Manager

[ACM.2] Sertifikat RSA yang dikelola oleh ACM harus menggunakan panjang kunci minimal 2.048 bit

Persyaratan terkait: PCI DSS v4.0.1/4.2.1

Kategori: Identifikasi > Persediaan > Layanan inventaris

Tingkat keparahan: Tinggi

Jenis sumber daya: AWS::ACM::Certificate

AWS Config aturan: [acm-certificate-rsa-check](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah sertifikat RSA dikelola dengan AWS Certificate Manager menggunakan panjang kunci minimal 2.048 bit. Kontrol gagal jika panjang kunci lebih kecil dari 2.048 bit.

Kekuatan enkripsi berkorelasi langsung dengan ukuran kunci. Kami merekomendasikan panjang kunci setidaknya 2.048 bit untuk melindungi AWS sumber daya Anda karena daya komputasi menjadi lebih murah dan server menjadi lebih maju.

Remediasi

Panjang kunci minimum untuk sertifikat RSA yang dikeluarkan oleh ACM sudah 2.048 bit. Untuk petunjuk tentang menerbitkan sertifikat RSA baru dengan ACM, lihat [Menerbitkan dan mengelola sertifikat](#) di Panduan Pengguna.AWS Certificate Manager

Meskipun ACM memungkinkan Anda untuk mengimpor sertifikat dengan panjang kunci yang lebih pendek, Anda harus menggunakan kunci minimal 2.048 bit untuk melewati kontrol ini. Anda

tidak dapat mengubah panjang kunci setelah mengimpor sertifikat. Sebagai gantinya, Anda harus menghapus sertifikat dengan panjang kunci lebih kecil dari 2.048 bit. Untuk informasi selengkapnya tentang mengimpor sertifikat ke ACM, lihat [Prasyarat untuk mengimpor](#) sertifikat ke Panduan Pengguna.AWS Certificate Manager

[ACM.3] Sertifikat ACM harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: AWS::ACM::Certificate

AWS Config aturan: tagged-acm-certificate (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang Diizinkan	Nilai default Security Hub
requiredTagKeys	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS .	Tidak ada nilai default

Kontrol ini memeriksa apakah sertifikat AWS Certificate Manager (ACM) memiliki tag dengan kunci spesifik yang ditentukan dalam parameter `requiredTagKeys`. Kontrol gagal jika sertifikat tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter `requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika sertifikat tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws:`, diabaikan.

Tag adalah sebuah label yang Anda tetapkan ke sebuah AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengkategorikan sumber daya berdasarkan tujuan,

pemilik, lingkungan, atau kriteria lainnya. Tag membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat Anda menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang mendefinisikan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk penanggung jawab IAM Anda. Anda dapat merancang kebijakan ABAC ini untuk mengizinkan operasi ketika tag penanggung jawab cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat Untuk [apa ABAC untuk? AWS](#) di Panduan Pengguna IAM.

Note

Jangan menambahkan informasi pengenalan pribadi (PII) atau informasi rahasia atau sensitif lainnya di tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat [Menandai AWS sumber daya Anda](#) di Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke sertifikat ACM, lihat [Menandai AWS Certificate Manager sertifikat](#) di AWS Certificate Manager Panduan Pengguna.

Kontrol Security Hub untuk AWS CloudFormation

Kontrol Security Hub ini mengevaluasi AWS CloudFormation layanan dan sumber daya.

Kontrol ini mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat [Ketersediaan kontrol berdasarkan Wilayah](#).

[CloudFormation.1] CloudFormation tumpukan harus diintegrasikan dengan Simple Notification Service (SNS)

Important

Security Hub menghentikan kontrol ini pada April 2024. Untuk informasi selengkapnya, lihat [Ubah log untuk kontrol CSPM Security Hub](#).

Persyaratan terkait: NIST.800-53.R5 SI-4 (12), NIST.800-53.R5 SI-4 (5)

Kategori: Deteksi > Layanan deteksi > Pemantauan aplikasi

Tingkat keparahan: Rendah

Jenis sumber daya: AWS::CloudFormation::Stack

AWS Config aturan: [cloudformation-stack-notification-check](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah pemberitahuan Amazon Simple Notification Service terintegrasi dengan AWS CloudFormation tumpukan. Kontrol gagal untuk CloudFormation tumpukan jika tidak ada pemberitahuan SNS yang terkait dengannya.

Mengonfigurasi notifikasi SNS dengan CloudFormation tumpukan Anda membantu segera memberi tahu pemangku kepentingan tentang peristiwa atau perubahan apa pun yang terjadi dengan tumpukan.

Remediasi

Untuk mengintegrasikan CloudFormation tumpukan dan topik SNS, lihat [Memperbarui tumpukan secara langsung](#) di AWS CloudFormation Panduan Pengguna.

[CloudFormation.2] CloudFormation tumpukan harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: AWS::CloudFormation::Stack

AWS Config aturan: tagged-cloudformation-stack (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
<code>requiredTagKeys</code>	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS .	Tidak ada nilai default

Kontrol ini memeriksa apakah AWS CloudFormation tumpukan memiliki tag dengan kunci tertentu yang ditentukan dalam parameter `requiredTagKeys`. Kontrol gagal jika tumpukan tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter `requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika tumpukan tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat [Untuk apa ABAC? AWS](#) di Panduan Pengguna IAM.

Note

Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat [Menandai AWS sumber daya Anda](#) di Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke CloudFormation tumpukan, lihat [CreateStack](#) di Referensi AWS CloudFormation API.

Kontrol Security Hub untuk Amazon CloudFront

AWS Security Hub Kontrol ini mengevaluasi CloudFront layanan dan sumber daya Amazon. Kontrol mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat [Ketersediaan kontrol berdasarkan Wilayah](#).

[CloudFront.1] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi

Persyaratan terkait: NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), PCI DSS v4.0.1/2.2.6

Kategori: Lindungi > Manajemen akses aman > Sumber daya tidak dapat diakses publik

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::CloudFront::Distribution`

AWS Config aturan: [cloudfront-default-root-object-configured](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah CloudFront distribusi Amazon dikonfigurasi untuk mengembalikan objek tertentu yang merupakan objek root default. Kontrol gagal jika CloudFront distribusi tidak memiliki objek root default yang dikonfigurasi.

Pengguna terkadang meminta URL root distribusi alih-alih objek dalam distribusi. Ketika ini terjadi, menentukan objek akar default dapat membantu Anda menghindari pemaparan konten distribusi web Anda.

Tindakan Perbaikan

Untuk mengonfigurasi objek root default untuk CloudFront distribusi, lihat [Cara menentukan objek root default](#) di Panduan CloudFront Pengembang Amazon.

[CloudFront.3] CloudFront distribusi harus memerlukan enkripsi dalam perjalanan

Persyaratan terkait: NIST.800-53.r5 AC-1 7 (2),, NIST.800-53.r5 IA-5 (1) NIST.800-53.r5 AC-4, NIST.800-53.r5 SC-1 2 (3), 3, 3, NIST.800-53.r5 SC-1 3 (3), NIST.800-53.r5 SC-2 (4),, NIST.800-53.r5 SC-2 (1), NIST.800-53.r5 SC-7 (2) NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 Nist.800-53.r5 SI-7 NIST.800-53.r5 SC-8 (6), PCI DSS v4.0.1/4.2.1

Kategori: Lindungi > Perlindungan Data > Enkripsi data-in-transit

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::CloudFront::Distribution

AWS Config aturan: [cloudfront-viewer-policy-https](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah CloudFront distribusi Amazon mengharuskan pemirsa untuk menggunakan HTTPS secara langsung atau menggunakan pengalihan. Kontrol gagal jika ViewerProtocolPolicy disetel ke allow-all untuk defaultCacheBehavior atau untuk cacheBehaviors.

HTTPS (TLS) dapat digunakan untuk membantu mencegah penyerang potensial dari menggunakan person-in-the-middle atau serangan serupa untuk menguping atau memanipulasi lalu lintas jaringan. Hanya koneksi terenkripsi melalui HTTPS (TLS) yang diizinkan. Mengenkripsi data dalam perjalanan dapat memengaruhi kinerja. Anda harus menguji aplikasi Anda dengan fitur ini untuk memahami profil kinerja dan dampak TLS.

Tindakan Perbaikan

Untuk mengenkripsi CloudFront distribusi saat transit, lihat [Memerlukan HTTPS untuk komunikasi antara pemirsa dan CloudFront](#) di Panduan CloudFront Pengembang Amazon.

[CloudFront.4] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi

Persyaratan terkait: NIST.800-53.r5 CP-10, NIST.800-53.r5 SC-3 6, NIST.800-53.r5 SC-5 (2), NIST.800-53.R5 SI-13 (5)

Kategori: Pulihkan > Ketahanan > Ketersediaan tinggi

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::CloudFront::Distribution`

AWS Config aturan: [cloudfront-origin-failover-enabled](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah CloudFront distribusi Amazon dikonfigurasi dengan grup asal yang memiliki dua atau lebih asal.

CloudFront origin failover dapat meningkatkan ketersediaan. Tindakan Perbaikan asal secara otomatis mengalihkan lalu lintas ke asal sekunder jika asal utama tidak tersedia atau jika mengembalikan kode status respons HTTP tertentu.

Tindakan Perbaikan

Untuk mengonfigurasi failover asal untuk CloudFront distribusi, lihat [Membuat grup asal](#) di Panduan CloudFront Pengembang Amazon.

[CloudFront.5] CloudFront distribusi seharusnya mengaktifkan logging

Persyaratan terkait: NIST.800-53.r5 AC-2 (4), (26), NIST.800-53.r5 AC-4 (9),, NIST.800-53.r5 AC-6 (9), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7 Nist.800-53.R5 SI-3 NIST.800-53.r5 SC-7 (8), Nist.800-53.R5 SI-4 (20), Nist.800-53.R5 SI-7 (8), PCI DSS v4.0.1/10.4.2

Kategori: Identifikasi > Logging

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::CloudFront::Distribution`

AWS Config aturan: [cloudfront-accesslogs-enabled](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah pencatatan akses server diaktifkan pada CloudFront distribusi. Kontrol gagal jika pencatatan akses tidak diaktifkan untuk distribusi. Kontrol ini hanya mengevaluasi apakah pencatatan standar (lama) diaktifkan untuk distribusi.

CloudFront Access log memberikan informasi rinci tentang setiap permintaan pengguna yang CloudFront diterima. Setiap log berisi informasi seperti tanggal dan waktu permintaan diterima, alamat IP penampil yang membuat permintaan, sumber permintaan, dan nomor port permintaan dari penampil. Log ini berguna untuk aplikasi seperti audit keamanan dan akses dan investigasi forensik. Untuk informasi selengkapnya tentang menganalisis log akses, lihat [Kueri CloudFront log Amazon](#) di Panduan Pengguna Amazon Athena.

Tindakan Perbaikan

Untuk mengonfigurasi pencatatan standar (lama) untuk CloudFront distribusi, lihat [Mengonfigurasi pencatatan standar \(lama\)](#) di Panduan CloudFront Pengembang Amazon.

[CloudFront.6] CloudFront distribusi harus mengaktifkan WAF

Persyaratan terkait: NIST.800-53.r5 AC-4 (21), PCI DSS v4.0.1/6.4.2

Kategori: Lindungi > Layanan pelindung

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::CloudFront::Distribution`

AWS Config aturan: [cloudfront-associated-with-waf](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah CloudFront distribusi terkait dengan AWS WAF Classic atau AWS WAF web ACLs. Kontrol gagal jika distribusi tidak terkait dengan ACL web.

AWS WAF adalah firewall aplikasi web yang membantu melindungi aplikasi web dan APIs dari serangan. Ini memungkinkan Anda untuk mengonfigurasi seperangkat aturan, yang disebut daftar kontrol akses web (web ACL), yang memungkinkan, memblokir, atau menghitung permintaan web berdasarkan aturan dan kondisi keamanan web yang dapat disesuaikan yang Anda tentukan. Pastikan CloudFront distribusi Anda dikaitkan dengan ACL AWS WAF web untuk membantu melindunginya dari serangan berbahaya.

Tindakan Perbaikan

Untuk mengaitkan ACL AWS WAF web dengan CloudFront distribusi, lihat [Menggunakan AWS WAF untuk mengontrol akses ke konten Anda](#) di Panduan CloudFront Pengembang Amazon.

[CloudFront.7] CloudFront distribusi harus menggunakan sertifikat SSL/TLS khusus

Persyaratan terkait: NIST.800-53.r5 AC-1 7 (2),, NIST.800-53.r5 IA-5 (1) NIST.800-53.r5 AC-4, NIST.800-53.r5 SC-1 2 (3), 3, 3, 3 (NIST.800-53.r5 SC-13), NIST.800-53.r5 SC-2 (4),, NIST.800-53.r5 SC-2 (1), NIST.800-53.r5 SC-7 (2), NIST.800-53.r5 SC-8 Nist.800-53.r5 SI-7 NIST.800-53.r5 SC-8 (6), Nist.800-171.r2 3.13.15 NIST.800-53.r5 SC-8

Kategori: Lindungi > Perlindungan Data > Enkripsi data-in-transit

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::CloudFront::Distribution

AWS Config aturan: [cloudfront-custom-ssl-certificate](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah CloudFront distribusi menggunakan SSL/TLS certificate CloudFront provides. This control passes if the CloudFront distribution uses a custom SSL/TLS certificate. This control fails if the CloudFront distribution uses the default SSL/TLS sertifikat default.

SSL/TLS khusus memungkinkan pengguna Anda mengakses konten dengan menggunakan nama domain alternatif. Anda dapat menyimpan sertifikat khusus di AWS Certificate Manager (disarankan), atau di IAM.

Tindakan Perbaikan

Untuk menambahkan nama domain alternatif untuk CloudFront distribusi menggunakan sertifikat SSL/TLS kustom, lihat [Menambahkan nama domain alternatif di](#) Panduan Pengembang Amazon. CloudFront

[CloudFront.8] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS

Persyaratan terkait: NIST.800-53.r5 CA-9 (1), Nist.800-53.R5 CM-2

Kategori: Lindungi > Konfigurasi jaringan aman

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::CloudFront::Distribution`

AWS Config aturan: [cloudfront-sni-enabled](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah CloudFront distribusi Amazon menggunakan metode SSL/TLS certificate and are configured to use SNI to serve HTTPS requests. This control fails if a custom SSL/TLS certificate is associated but the SSL/TLS dukungan khusus adalah alamat IP khusus.

Indikasi Nama Server (Ser Server Name Indication atau SNI) adalah ekstensi untuk protokol TLS yang didukung oleh browser dan klien yang dirilis setelah tahun 2010. Jika Anda mengonfigurasi CloudFront untuk melayani permintaan HTTPS menggunakan SNI, CloudFront mengaitkan nama domain alternatif Anda dengan alamat IP untuk setiap lokasi edge. Saat penampil mengirimkan permintaan HTTPS untuk konten Anda, DNS mengirimkan permintaan ke alamat IP untuk lokasi tepi yang benar. Alamat IP untuk nama domain Anda ditentukan selama negosiasi jabat tangan SSL/TLS; alamat IP tidak dikhususkan untuk distribusi Anda.

Tindakan Perbaikan

Untuk mengonfigurasi CloudFront distribusi agar menggunakan SNI untuk melayani permintaan HTTPS, lihat [Menggunakan SNI untuk Melayani Permintaan HTTPS \(berfungsi untuk Sebagian Besar Klien\)](#) di Panduan CloudFront Pengembang. Untuk informasi tentang sertifikat SSL kustom, lihat [Persyaratan untuk menggunakan sertifikat SSL/TLS](#) dengan. CloudFront

[CloudFront.9] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus

Persyaratan terkait: NIST.800-53.r5 AC-1 7 (2),, NIST.800-53.r5 IA-5 (1) NIST.800-53.r5 AC-4, NIST.800-53.r5 SC-1 2 (3), 3, 3, NIST.800-53.r5 SC-1 3 (3), NIST.800-53.r5 SC-2 (4),, NIST.800-53.r5 SC-2 (1), NIST.800-53.r5 SC-7 (2) NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 Nist.800-53.r5 SI-7 NIST.800-53.r5 SC-8 (6), PCI DSS v4.0.1/4.2.1

Kategori: Lindungi > Perlindungan Data > Enkripsi data-in-transit

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::CloudFront::Distribution`

AWS Config aturan: [cloudfront-traffic-to-origin-encrypted](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah CloudFront distribusi Amazon mengenkripsi lalu lintas ke asal kustom. Kontrol ini gagal untuk CloudFront distribusi yang kebijakan protokol asalnya memungkinkan 'hanya http'. Kontrol ini juga gagal jika kebijakan protokol asal distribusi adalah 'penampil pencocokan' sedangkan kebijakan protokol penampil adalah 'izinkan semua'.

HTTPS (TLS) dapat digunakan untuk membantu mencegah penyadapan atau manipulasi lalu lintas jaringan. Hanya koneksi terenkripsi melalui HTTPS (TLS) yang diizinkan.

Tindakan Perbaikan

Untuk memperbarui Kebijakan Protokol Asal agar memerlukan enkripsi untuk CloudFront sambungan, lihat [Memerlukan HTTPS untuk komunikasi antara CloudFront dan asal kustom Anda](#) di Panduan CloudFront Pengembang Amazon.

[CloudFront.10] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal kustom

Persyaratan terkait: NIST.800-53.r5 AC-1 7 (2), (1) NIST.800-53.r5 AC-4, 2 NIST.800-53.r5 IA-5 (3), 3, 3, (4), NIST.800-53.r5 SC-1 (1), NIST.800-53.r5 SC-2 NIST.800-53.r5 SC-7 (NIST.800-53.r5 SC-12) NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 Nist.800-53.r5 SI-7 NIST.800-53.r5 SC-8 (6), Nist.800-171.r2 3.13.15, PCI DSS v4.0.1/4.2.1

Kategori: Lindungi > Perlindungan Data > Enkripsi data-in-transit

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::CloudFront::Distribution

AWS Config aturan: [cloudfront-no-deprecated-ssl-protocols](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah CloudFront distribusi Amazon menggunakan protokol SSL yang tidak digunakan lagi untuk komunikasi HTTPS antara CloudFront lokasi tepi dan asal kustom Anda. Kontrol ini gagal jika CloudFront distribusi memiliki CustomOriginConfig where OriginSslProtocols includeSSLv3.

Pada tahun 2015, Internet Engineering Task Force (IETF) secara resmi mengumumkan bahwa SSL 3.0 harus dihentikan karena protokol tidak cukup aman. Disarankan agar Anda menggunakan TLSv1.2 atau yang lebih baru untuk komunikasi HTTPS ke asal kustom Anda.

Tindakan Perbaikan

Untuk memperbarui Protokol SSL Asal untuk CloudFront distribusi, lihat [Memerlukan HTTPS untuk komunikasi antara CloudFront dan asal kustom Anda di Panduan Pengembang](#) Amazon CloudFront.

[CloudFront.12] CloudFront distribusi seharusnya tidak menunjukkan asal S3 yang tidak ada

Persyaratan terkait: NIST.800-53.R5 CM-2, NIST.800-53.R5 CM-2 (2), PCI DSS v4.0.1/2.2.6

Kategori: Identifikasi > Konfigurasi sumber daya

Tingkat keparahan: Tinggi

Jenis sumber daya: AWS::CloudFront::Distribution

AWS Config aturan: [cloudfront-s3-origin-non-existent-bucket](#)

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah CloudFront distribusi Amazon menunjuk ke asal Amazon S3 yang tidak ada. Kontrol gagal untuk CloudFront distribusi jika asal dikonfigurasi untuk menunjuk ke bucket yang tidak ada. Kontrol ini hanya berlaku untuk CloudFront distribusi di mana bucket S3 tanpa hosting situs web statis adalah asal S3.

Ketika CloudFront distribusi di akun Anda dikonfigurasi untuk menunjuk ke bucket yang tidak ada, pihak ketiga yang berbahaya dapat membuat bucket yang direferensikan dan menyajikan konten mereka sendiri melalui distribusi Anda. Sebaiknya periksa semua asal terlepas dari perilaku perutean untuk memastikan bahwa distribusi Anda mengarah ke asal yang sesuai.

Tindakan Perbaikan

Untuk mengubah CloudFront distribusi agar mengarah ke asal baru, lihat [Memperbarui distribusi](#) di Panduan CloudFront Pengembang Amazon.

[CloudFront.13] CloudFront distribusi harus menggunakan kontrol akses asal

Kategori: Lindungi > Manajemen akses aman > Sumber daya tidak dapat diakses publik

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::CloudFront::Distribution`

AWS Config aturan: [cloudfront-s3-origin-access-control-enabled](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah CloudFront distribusi Amazon dengan asal Amazon S3 memiliki kontrol akses asal (OAC) yang dikonfigurasi. Kontrol gagal jika OAC tidak dikonfigurasi untuk CloudFront distribusi.

Saat menggunakan bucket S3 sebagai asal CloudFront distribusi Anda, Anda dapat mengaktifkan OAC. Ini memungkinkan akses ke konten dalam bucket hanya melalui CloudFront distribusi yang ditentukan, dan melarang akses langsung dari bucket atau distribusi lain. Meskipun CloudFront mendukung Origin Access Identity (OAI), OAC menawarkan fungsionalitas tambahan, dan distribusi menggunakan OAI dapat bermigrasi ke OAC. Meskipun OAI menyediakan cara aman untuk mengakses asal S3, ia memiliki keterbatasan, seperti kurangnya dukungan untuk konfigurasi kebijakan granular dan untuk permintaan HTTP/HTTPS yang menggunakan metode POST Wilayah AWS yang memerlukan AWS Signature Version 4 (SigV4). OAI juga tidak mendukung enkripsi dengan AWS Key Management Service. OAC didasarkan pada praktik AWS terbaik menggunakan prinsip layanan IAM untuk mengautentikasi dengan asal-usul S3.

Tindakan Perbaikan

Untuk mengonfigurasi OAC untuk CloudFront distribusi dengan asal S3, lihat [Membatasi akses ke asal Amazon S3 di](#) Panduan Pengembang Amazon. CloudFront

[CloudFront.14] CloudFront distribusi harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::CloudFront::Distribution`

AWS Config aturan: `tagged-cloudfront-distribution` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
<code>requiredTagKeys</code>	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS .	Tidak ada nilai default

Kontrol ini memeriksa apakah CloudFront distribusi Amazon memiliki tag dengan kunci tertentu yang ditentukan dalam parameter `requiredTagKeys`. Kontrol gagal jika distribusi tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter `requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika distribusi tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws:`, diabaikan.

Tag adalah sebuah label yang Anda tetapkan ke sebuah AWS sumber daya, dan itu terdiri dari sebuah kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag membantu Anda mengidentifikasi, mengatur, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat Anda menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau set kebijakan terpisah untuk penanggung jawab IAM Anda. Anda dapat merancang kebijakan ABAC ini untuk mengizinkan operasi ketika tag penanggung jawab cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat [Untuk apa ABAC untuk? AWS](#) di Panduan Pengguna IAM.

Note

Jangan menambahkan informasi pengenalan pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS

Billing. Untuk praktik terbaik penandaan lainnya, lihat [Menandai AWS sumber daya Anda](#) di Referensi Umum AWS

Tindakan Perbaikan

Untuk menambahkan tag ke CloudFront distribusi, lihat [Menandai CloudFront distribusi Amazon di Panduan CloudFront](#) Pengembang Amazon.

Kontrol Security Hub untuk AWS CloudTrail

AWS Security Hub Kontrol ini mengevaluasi AWS CloudTrail layanan dan sumber daya. Kontrol mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat [Ketersediaan kontrol berdasarkan Wilayah](#).

[CloudTrail.1] CloudTrail harus diaktifkan dan dikonfigurasi dengan setidaknya satu jejak Multi-wilayah yang mencakup acara manajemen baca dan tulis

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v1.2.0/2.1, Tolok Ukur AWS Yayasan CIS v1.4.0/3.1, Tolok Ukur AWS Yayasan CIS v3.0.0/3.1, NIST.800-53.r5 AC-2 (4), (26), (9), (9), NIST.800-53.r5 AC-4 (22) NIST.800-53.r5 AC-6 NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 AU-14(1), NIST.800-53.r5 CA-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SI-3(8), NIST.800-53.r5 SI-4(20), NIST.800-53.r5 SI-7(8), NIST.800-53.r5 SA-8

Kategori: Identifikasi > Logging

Tingkat keparahan: Tinggi

Jenis sumber daya: AWS :: : Account

AWS Config aturan: [multi-region-cloudtrail-enabled](#)

Jenis jadwal: Periodik

Parameter:

- `readWriteType`: ALL (tidak dapat disesuaikan)
- `includeManagementEvents`: true (tidak dapat disesuaikan)

Kontrol ini memeriksa apakah ada setidaknya satu AWS CloudTrail jejak Multi-wilayah yang menangkap peristiwa manajemen baca dan tulis. Kontrol gagal jika CloudTrail dinonaktifkan atau jika tidak ada setidaknya satu CloudTrail jejak yang menangkap peristiwa manajemen baca dan tulis.

AWS CloudTrail merekam panggilan AWS API untuk akun Anda dan memberikan file log untuk Anda. Informasi yang direkam mencakup informasi berikut:

- Identitas pemanggil API
- Waktu panggilan API
- Alamat IP sumber pemanggil API
- Permintaan parameter
- elemen respon dikembalikan oleh Layanan AWS

CloudTrail menyediakan riwayat panggilan AWS API untuk akun, termasuk panggilan API yang dibuat dari AWS Management Console, AWS SDKs, alat baris perintah. Riwayat ini juga mencakup panggilan API dari tingkat yang lebih tinggi Layanan AWS seperti. AWS CloudFormation

Riwayat panggilan AWS API yang dihasilkan CloudTrail memungkinkan analisis keamanan, pelacakan perubahan sumber daya, dan audit kepatuhan. Jalur Multi-Region juga memberikan manfaat berikut.

- Jejak multi-wilayah membantu mendeteksi aktivitas tak terduga yang terjadi di Wilayah yang tidak digunakan.
- Jejak multi-wilayah memastikan bahwa pencatatan peristiwa layanan global diaktifkan untuk jejak secara default. Pencatatan peristiwa layanan global mencatat peristiwa yang dihasilkan oleh layanan AWS global.
- Untuk jejak Multi-wilayah, acara manajemen untuk semua operasi baca dan tulis memastikan bahwa operasi manajemen CloudTrail catatan pada semua sumber daya dalam file Akun AWS.

Secara default, CloudTrail jalur yang dibuat menggunakan jalur Multi-wilayah. AWS Management Console

Tindakan Perbaikan

Untuk membuat jejak Multi-wilayah baru CloudTrail, lihat [Membuat jejak](#) di Panduan AWS CloudTrail Pengguna. Gunakan nilai berikut:

Bidang	Nilai
Pengaturan tambahan, validasi file log	Diaktifkan
Pilih peristiwa log, Acara manajemen, aktivitas API	Baca dan Tulis. Kosongkan kotak centang untuk pengecualian.

Untuk memperbarui jejak yang ada, lihat [Memperbarui jejak](#) di Panduan AWS CloudTrail Pengguna. Di acara Manajemen, untuk aktivitas API, pilih Baca dan Tulis.

[CloudTrail.2] CloudTrail harus mengaktifkan enkripsi saat istirahat

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v1.2.0/2.7, Tolok Ukur Yayasan CIS v1.4.0/3.7, Tolok Ukur AWS Yayasan CIS v3.0.0/3.5, (1), 3, 8, 8 NIST.800-53.r5 AU-9, NIST.800-53.r5 CA-9 (1), (10), AWS NIST.800-53.R5 SI-7 (6), NIST.800-171.R2 NIST.800-53.r5 SC-2 3.3.8, PCI DSS NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-1 v3.2.1/3.4, NIST.800-53.r5 SC-2 PCI DSS v4.0.1/10.3.2 NIST.800-53.r5 SC-7

Kategori: Lindungi > Perlindungan Data > Enkripsi data-at-rest

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::CloudTrail::Trail

AWS Config aturan: [cloud-trail-encryption-enabled](#)

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah CloudTrail dikonfigurasi untuk menggunakan enkripsi sisi server (SSE). AWS KMS key Kontrol gagal jika KmsKeyId tidak ditentukan.

Untuk lapisan keamanan tambahan untuk file CloudTrail log sensitif Anda, Anda harus menggunakan [enkripsi sisi server dengan AWS KMS keys \(SSE-KMS\)](#) untuk file CloudTrail log Anda untuk enkripsi saat istirahat. Perhatikan bahwa secara default, berkas log yang dikirim CloudTrail ke bucket Anda dienkripsi oleh enkripsi [sisi server Amazon dengan kunci enkripsi yang dikelola Amazon S3 \(SSE-S3\)](#).

Tindakan Perbaikan

Untuk mengaktifkan enkripsi SSE-KMS untuk file CloudTrail log, lihat [Memperbarui jejak untuk menggunakan kunci KMS](#) di Panduan Pengguna.AWS CloudTrail

[CloudTrail.3] Setidaknya satu CloudTrail jejak harus diaktifkan

Persyaratan terkait: Nist.800-171.r2 3.3.1, Nist.800-171.r2 3.14.6, Nist.800-171.r2 3.14.7, PCI DSS v3.2.1/10.1, PCI DSS v3.2.1/10.2.1, PCI DSS v3.2.1/10.2.2, PCI DSS v3.2.1/10.2.3, PCI DSS v3.2.1/10.2.3 2.4, PCI DSS v3.2.1/10.2.5, PCI DSS v3.2.1/10.2.6, PCI DSS v3.2.1/10.2.7, PCI DSS v3.2.1/10.3.1, PCI DSS v3.2.1/10.3.2, PCI DSS v3.2.1/10.3.3, PCI DSS v3.2.1/10.3.4, PCI DSS v3.2.1/10.3.5, DSS v3.2.1/10.3.6, PCI DSS v4.0.1/10.2.1

Kategori: Identifikasi > Logging

Tingkat keparahan: Tinggi

Jenis sumber daya: AWS : : : Account

AWS Config aturan: [cloudtrail-enabled](#)

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah AWS CloudTrail jejak diaktifkan di Anda Akun AWS. Kontrol gagal jika akun Anda tidak memiliki setidaknya satu CloudTrail jejak yang diaktifkan.

Namun, beberapa AWS layanan tidak mengaktifkan pencatatan semua APIs dan acara. Anda harus menerapkan jejak audit tambahan selain CloudTrail dan meninjau dokumentasi untuk setiap layanan di [Layanan dan Integrasi yang CloudTrail Didukung](#).

Tindakan Perbaikan

Untuk memulai CloudTrail dan membuat jejak, lihat [AWS CloudTrail tutorial Memulai dengan](#) di Panduan AWS CloudTrail Pengguna.

[CloudTrail.4] validasi file CloudTrail log harus diaktifkan

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v1.2.0/2.2, Tolok Ukur Yayasan CIS v1.4.0/3.2, Tolok Ukur AWS Yayasan CIS v3.0.0/3.2, NIST.800-53.R5 AU-9, NIST.800-53.R5

SI-4, NIST.800-53.R5 SI-7 (3), NIST.800-53.R5 3.R5 SI-7 (7), NIST.800-171.R2 3.3.8, PCI DSS v3.2.1/10.5.2, PCI DSS v3.2.1/10.5.5, PCI DSS v4.0.1/10.3.2 AWS

Kategori: Perlindungan data > Integritas data

Tingkat keparahan: Rendah

Jenis sumber daya: AWS::CloudTrail::Trail

AWS Config aturan: [cloud-trail-log-file-validation-enabled](#)

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah validasi integritas file log diaktifkan pada CloudTrail jejak.

CloudTrail validasi file log membuat file digest yang ditandatangani secara digital yang berisi hash dari setiap log yang menulis ke CloudTrail Amazon S3. Anda dapat menggunakan file intisari ini untuk menentukan apakah file log diubah, dihapus, atau tidak diubah setelah CloudTrail mengirimkan log.

Security Hub merekomendasikan agar Anda mengaktifkan validasi file di semua jalur. Validasi file log memberikan pemeriksaan integritas tambahan CloudTrail log.

Tindakan Perbaikan

Untuk mengaktifkan validasi file CloudTrail log, lihat [Mengaktifkan validasi integritas file log CloudTrail di Panduan](#) Pengguna.AWS CloudTrail

[CloudTrail.5] CloudTrail jalur harus diintegrasikan dengan Amazon Logs CloudWatch

Persyaratan terkait: PCI DSS v3.2.1/10.5.3, Tolok Ukur Yayasan CIS v1.2.0/2.4, Tolok Ukur AWS Yayasan CIS v1.4.0/3.4, (4), (26), (9), (9), NIST.800-53.R5 SI-20, NIST.800-53.R5 SI-3 NIST.800-53.r5 AC-2 (8), NIST.800-53.R5 SI-4 NIST.800-53.r5 AC-4 NIST.800-53.r5 AC-6 (20) NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(1), NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 AU-6(5), NIST.800-53.r5 AU-7(1), NIST.800-53.r5 CA-7, NIST.800-53.R5 SI-4 NIST.800-53.r5 SC-7 (5), NIST.800-53.R5 SI-7 (8) AWS

Kategori: Identifikasi > Logging

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::CloudTrail::Trail`

AWS Config aturan: [cloud-trail-cloud-watch-logs-enabled](#)

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah CloudTrail jejak dikonfigurasi untuk mengirim log ke CloudWatch Log. Kontrol gagal jika `CloudWatchLogsLogGroupArn` properti jejak kosong.

CloudTrail merekam panggilan AWS API yang dibuat di akun tertentu. Informasi yang direkam mencakup hal berikut:

- Identitas pemanggil API
- Waktu panggilan API
- Alamat IP sumber dari pemanggil API
- Parameter permintaan
- Elemen respons yang dikembalikan oleh Layanan AWS

CloudTrail menggunakan Amazon S3 untuk penyimpanan dan pengiriman file log. Anda dapat menangkap CloudTrail log dalam bucket S3 tertentu untuk analisis jangka panjang. Untuk melakukan analisis real-time, Anda dapat mengonfigurasi CloudTrail untuk mengirim log ke CloudWatch Log.

Untuk jejak yang diaktifkan di semua Wilayah dalam akun, CloudTrail kirimkan file log dari semua Wilayah tersebut ke grup CloudWatch log Log.

Security Hub merekomendasikan agar Anda mengirim CloudTrail log ke CloudWatch Log. Perhatikan bahwa rekomendasi ini dimaksudkan untuk memastikan bahwa aktivitas akun ditangkap, dipantau, dan diwaspadai dengan tepat. Anda dapat menggunakan CloudWatch Log untuk mengatur ini dengan Anda Layanan AWS. Rekomendasi ini tidak menghalangi penggunaan solusi yang berbeda.

Mengirim CloudTrail CloudWatch log ke Log memfasilitasi pencatatan aktivitas real-time dan historis berdasarkan pengguna, API, sumber daya, dan alamat IP. Anda dapat menggunakan pendekatan ini untuk membuat alarm dan pemberitahuan untuk aktivitas akun anomali atau sensitivitas.

Tindakan Perbaikan

Untuk mengintegrasikan CloudTrail dengan CloudWatch Log, lihat [Mengirim peristiwa ke CloudWatch Log](#) di Panduan AWS CloudTrail Pengguna.

[CloudTrail.6] Pastikan bucket S3 yang digunakan untuk menyimpan CloudTrail log tidak dapat diakses publik

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v1.2.0/2.3, Tolok Ukur Yayasan CIS v1.4.0/3.3, PCI DSS AWS v4.0.1/1.4.4

Kategori: Identifikasi > Logging

Tingkat keparahan: Kritis

Jenis sumber daya: AWS :: S3 :: Bucket

AWS Config aturan: Tidak ada (aturan Security Hub khusus)

Jenis jadwal: Berkala dan perubahan dipicu

Parameter: Tidak ada

CloudTrail mencatat catatan setiap panggilan API yang dilakukan di akun Anda. File log ini disimpan di bucket S3. CIS merekomendasikan agar kebijakan bucket S3, atau daftar kontrol akses (ACL), diterapkan pada bucket S3 yang CloudTrail mencatat untuk mencegah akses publik ke log. CloudTrail Mengizinkan akses publik ke konten CloudTrail log dapat membantu musuh dalam mengidentifikasi kelemahan dalam penggunaan atau konfigurasi akun yang terpengaruh.

Untuk menjalankan pemeriksaan ini, Security Hub pertama-tama menggunakan logika kustom untuk mencari bucket S3 tempat CloudTrail log Anda disimpan. Kemudian menggunakan aturan AWS Config terkelola untuk memeriksa apakah bucket dapat diakses publik.

Jika Anda menggabungkan log Anda ke dalam satu bucket S3 terpusat, maka Security Hub hanya menjalankan pemeriksaan terhadap akun dan Wilayah tempat bucket S3 terpusat berada. Untuk akun dan Wilayah lain, status kontrolnya adalah Tidak ada data.

Jika bucket dapat diakses publik, cek akan menghasilkan temuan yang gagal.

Tindakan Perbaikan

Untuk memblokir akses publik ke bucket CloudTrail S3 Anda, lihat [Mengonfigurasi blok akses publik untuk bucket S3 Anda di](#) Panduan Pengguna Amazon Simple Storage Service. Pilih keempat Amazon S3 Block Public Access Settings.

[CloudTrail.7] Pastikan pencatatan akses bucket S3 diaktifkan pada bucket CloudTrail S3

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v1.2.0/2.6, Tolok Ukur Yayasan CIS v1.4.0/3.6, Tolok Ukur AWS Yayasan CIS v3.0.0/3.4, PCI DSS v4.0.1/10.2.1 AWS

Kategori: Identifikasi > Logging

Tingkat keparahan: Rendah

Jenis sumber daya: AWS :: S3 :: Bucket

AWS Config aturan: Tidak ada (aturan Security Hub khusus)

Jenis jadwal: Periodik

Parameter: Tidak ada

Pencatatan akses bucket S3 menghasilkan log yang berisi catatan akses untuk setiap permintaan yang dibuat ke bucket S3 Anda. Catatan akses berisi detail tentang permintaan, seperti jenis permintaan, sumber daya yang ditentukan dalam permintaan berfungsi, dan waktu serta tanggal pemrosesan permintaan.

CIS menyarankan agar Anda mengaktifkan pencatatan akses bucket pada bucket CloudTrail S3.

Dengan mengaktifkan pencatatan bucket S3 pada bucket S3 target, Anda dapat menangkap semua peristiwa yang mungkin memengaruhi objek dalam bucket target. Mengkonfigurasi log untuk ditempatkan di bucket terpisah memungkinkan akses ke informasi log, yang dapat berguna dalam alur kerja keamanan dan respons insiden.

Untuk menjalankan pemeriksaan ini, Security Hub pertama-tama menggunakan logika kustom untuk mencari bucket tempat CloudTrail log Anda disimpan dan kemudian menggunakan aturan AWS Config terkelola untuk memeriksa apakah logging diaktifkan.

Jika CloudTrail mengirimkan file log dari beberapa Akun AWS ke dalam satu bucket Amazon S3 tujuan, Security Hub mengevaluasi kontrol ini hanya terhadap bucket tujuan di Wilayah tempatnya berada. Ini merampingkan temuan Anda. Namun, Anda harus mengaktifkan CloudTrail semua akun yang mengirimkan log ke bucket tujuan. Untuk semua akun kecuali akun yang menyimpan bucket tujuan, status kontrolnya adalah Tidak ada data.

Tindakan Perbaikan

Untuk mengaktifkan pencatatan akses server untuk bucket CloudTrail S3 Anda, lihat [Mengaktifkan log akses server Amazon S3 di Panduan](#) Pengguna Layanan Penyimpanan Sederhana Amazon.

[CloudTrail.9] CloudTrail jejak harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::CloudTrail::Trail`

AWS Config aturan: `tagged-cloudtrail-trail` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
<code>requiredTagKeys</code>	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS .	No default value

Kontrol ini memeriksa apakah AWS CloudTrail jejak memiliki tag dengan kunci spesifik yang ditentukan dalam parameter `requiredTagKeys`. Kontrol gagal jika jejak tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter `requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika jejak tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws:`, diabaikan.

Tag adalah sebuah label yang Anda tetapkan ke sebuah AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag membantu Anda mengidentifikasi, mengatur, mencari,

dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat Anda menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang mendefinisikan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk penanggung jawab IAM Anda. Anda dapat merancang kebijakan ABAC ini untuk memungkinkan operasi ketika tag penanggung jawab cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat Untuk [apa ABAC untuk? AWS](#) di Panduan Pengguna IAM.

Note

Jangan menambahkan informasi pengenalan pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat [Menandai AWS sumber daya Anda](#) di Referensi Umum AWS

Tindakan Perbaikan

Untuk menambahkan tag ke CloudTrail jejak, lihat [AddTags](#) di Referensi AWS CloudTrail API.

[CloudTrail.10] Penyimpanan data acara CloudTrail danau harus dienkripsi dengan pelanggan yang dikelola AWS KMS keys

Persyaratan terkait: NIST.800-53.r5 AU-9, NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SC-1 2 (2), NIST.800-53.r5 SC-1 3, 8, NIST.800-53.r5 SC-2 NIST.800-53.r5 SC-2 8 (1), Nist.800-53.R5 SI-7 (6)

Kategori: Lindungi > Perlindungan Data > Enkripsi data-at-rest

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::CloudTrail::EventDataStore`

AWS Config aturan: [event-data-store-cmk-encryption-enabled](#)

Jenis jadwal: Periodik

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
kmsKeyArns	Daftar Nama Sumber Daya Amazon (ARNs) AWS KMS keys untuk disertakan dalam evaluasi. Kontrol menghasilkan FAILED temuan jika penyimpanan data peristiwa tidak dienkripsi dengan kunci KMS dalam daftar.	StringList (maksimal 3 item)	1—3 kunci ARNs KMS yang ada. Sebagai contoh: arn:aws:kms:us-west-2:11112223333:key/1234abcd-12ab-34cd-56ef-1234567890ab .	Tidak ada nilai default

Kontrol ini memeriksa apakah penyimpanan data acara AWS CloudTrail Lake dienkripsi saat istirahat dengan pelanggan yang dikelola. AWS KMS key Kontrol gagal jika penyimpanan data peristiwa tidak dienkripsi dengan kunci KMS yang dikelola pelanggan. Anda dapat secara opsional menentukan daftar kunci KMS untuk kontrol untuk disertakan dalam evaluasi.

Secara default, AWS CloudTrail Lake mengenkripsi penyimpanan data peristiwa dengan kunci terkelola Amazon S3 (SSE-S3), menggunakan algoritma AES-256. Untuk kontrol tambahan, Anda dapat mengonfigurasi CloudTrail Lake untuk mengenkripsi penyimpanan data peristiwa dengan pelanggan yang dikelola AWS KMS key (SSE-KMS) sebagai gantinya. Kunci KMS yang dikelola pelanggan adalah kunci AWS KMS key yang Anda buat, miliki, dan kelola di Akun AWS. Anda memiliki kontrol penuh atas kunci KMS jenis ini. Ini termasuk mendefinisikan dan memelihara kebijakan kunci, mengelola hibah, memutar materi kriptografi, menetapkan tag, membuat alias, dan mengaktifkan dan menonaktifkan kunci. Anda dapat menggunakan kunci KMS yang dikelola pelanggan dalam operasi kriptografi untuk CloudTrail data Anda dan penggunaan audit dengan CloudTrail log.

Tindakan Perbaikan

Untuk informasi tentang mengenkripsi penyimpanan data peristiwa AWS CloudTrail Lake dengan AWS KMS key yang Anda tentukan, lihat [Memperbarui penyimpanan data peristiwa](#) di AWS CloudTrail Panduan Pengguna. Setelah Anda mengaitkan penyimpanan data peristiwa dengan kunci KMS, kunci KMS tidak dapat dihapus atau diubah.

Kontrol Security Hub untuk Amazon CloudWatch

AWS Security Hub Kontrol ini mengevaluasi CloudWatch layanan dan sumber daya Amazon. Kontrol mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat [Ketersediaan kontrol berdasarkan Wilayah](#).

[CloudWatch.1] Filter metrik log dan alarm harus ada untuk penggunaan pengguna “root”

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v1.2.0/1.1, Tolok Ukur Yayasan CIS v1.2.0/3.3, Tolok Ukur Yayasan CIS v1.4.0/1.7, Tolok Ukur AWS Yayasan CIS v1.4.0/4.3, Nist.800-171.r2 3.14.6, AWS NIST.800-171.r2 3.14.7, PCI DSS v3.2.1/7.2.1 AWS

Kategori: Deteksi > Layanan deteksi

Tingkat keparahan: Rendah

Jenis sumber

daya:AWS::Logs::MetricFilter,AWS::CloudWatch::Alarm,AWS::CloudTrail::Trail,AWS::SNS::Topic

AWS Config aturan: Tidak ada (aturan Security Hub khusus)

Jenis jadwal: Periodik

Parameter: Tidak ada

Pengguna root memiliki akses tak terbatas ke semua layanan dan sumber daya dalam file Akun AWS. Kami sangat menyarankan Anda menghindari penggunaan pengguna root untuk tugas sehari-hari. Minimalkan penggunaan pengguna root dan mengadopsi prinsip hak istimewa paling sedikit untuk manajemen akses mengurangi risiko perubahan yang tidak disengaja dan pengungkapan kredensial yang sangat istimewa yang tidak diinginkan.

Sebagai praktik terbaik, gunakan kredensi pengguna akar Anda hanya jika diperlukan untuk [melakukan tugas manajemen akun dan layanan](#). Terapkan kebijakan AWS Identity and Access Management (IAM) secara langsung ke grup dan peran tetapi bukan pengguna. Untuk tutorial tentang cara menyiapkan administrator untuk penggunaan sehari-hari, lihat [Membuat pengguna dan grup admin IAM pertama Anda di Panduan Pengguna IAM](#)

Untuk menjalankan pemeriksaan ini, Security Hub menggunakan logika kustom untuk melakukan langkah-langkah audit yang tepat yang ditentukan untuk kontrol 1.7 di [CIS AWS Foundations Benchmark v1.4.0](#). Kontrol ini gagal jika filter metrik yang tepat yang ditentukan oleh CIS tidak digunakan. Bidang atau istilah tambahan tidak dapat ditambahkan ke filter metrik.

Note

Ketika Security Hub melakukan pemeriksaan untuk kontrol ini, ia mencari CloudTrail jejak yang digunakan akun saat ini. Jalur ini mungkin merupakan jalur organisasi yang dimiliki oleh akun lain. Jalur Multi-Wilayah juga mungkin berbasis di Wilayah yang berbeda. Hasil pemeriksaan dalam FAILED temuan dalam kasus-kasus berikut:

- Tidak ada jejak yang dikonfigurasi.
- Jalur yang tersedia yang berada di Wilayah saat ini dan yang dimiliki oleh rekening giro tidak memenuhi persyaratan kontrol.

Hasil pemeriksaan dalam status kontrol NO_DATA dalam kasus berikut:

- Jejak multi-wilayah berbasis di Wilayah yang berbeda. Security Hub hanya dapat menghasilkan temuan di Wilayah tempat jejak itu berada.
- Jejak multi-wilayah milik akun yang berbeda. Security Hub hanya dapat menghasilkan temuan untuk akun yang memiliki jejak.

Kami merekomendasikan jejak organisasi untuk mencatat peristiwa dari banyak akun dalam suatu organisasi. Jejak organisasi adalah jalur Multi-wilayah secara default dan hanya dapat dikelola oleh akun AWS Organizations manajemen atau akun administrator yang CloudTrail didelegasikan. Menggunakan jejak organisasi menghasilkan status kontrol NO_DATA untuk kontrol yang dievaluasi dalam akun anggota organisasi. Di akun anggota, Security Hub hanya menghasilkan temuan untuk sumber daya milik anggota. Temuan yang berkaitan dengan jejak organisasi dihasilkan di akun pemilik sumber daya. Anda dapat melihat temuan ini di akun administrator yang didelegasikan Security Hub menggunakan agregasi lintas wilayah.

Untuk alarm, akun saat ini harus memiliki topik Amazon SNS yang direferensikan, atau harus mendapatkan akses ke topik Amazon SNS dengan menelepon. `ListSubscriptionsByTopic` Jika tidak, Security Hub menghasilkan WARNING temuan untuk kontrol.

Perbaikan

Untuk melewati kontrol ini, ikuti langkah-langkah berikut untuk membuat topik Amazon SNS, AWS CloudTrail jejak, filter metrik, dan alarm untuk filter metrik.

1. Buat topik Amazon SNS. Untuk instruksi, lihat [Memulai dengan Amazon SNS di Panduan Pengembang Amazon SNS](#) di Panduan Developer Amazon SNS. Buat topik yang menerima semua alarm CIS, dan buat setidaknya satu langganan ke topik tersebut.
2. Buat CloudTrail jejak yang berlaku untuk semua Wilayah AWS. Untuk petunjuk, lihat [Membuat jejak](#) di Panduan AWS CloudTrail Pengguna.

Catat nama grup CloudWatch log Log yang Anda kaitkan dengan CloudTrail jejak. Anda membuat filter metrik untuk grup log pada langkah berikutnya.

3. Membuat sebuah filter metrik. Untuk petunjuknya, lihat [Membuat filter metrik untuk grup log](#) di Panduan CloudWatch Pengguna Amazon. Gunakan nilai berikut:

Bidang	Nilai
Tentukan pola, Pola filter	<code>{\$.userIdentity.type="Root" && \$.userIdentity.invokedBy NOT EXISTS && \$.eventType != "AwsServiceEvent"}</code>
namespace metrik	LogMetrics
Nilai metrik	1
Nilai default	0

4. Buat alarm berdasarkan pada filter. Untuk petunjuknya, lihat [Membuat CloudWatch alarm berdasarkan filter metrik grup log](#) di CloudWatch Panduan Pengguna Amazon. Gunakan nilai berikut:

Bidang	Nilai
Kondisi, tipe Ambang	Statis
<i>your-metric-name</i> Kapanpun...	lebih besar/sama
dari...	1

[CloudWatch.2] Pastikan filter metrik log dan alarm ada untuk panggilan API yang tidak sah

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v1.2.0/3.1, Nist.800-171.r2 3.13.1, Nist.800-171.r2 3.14.6, Nist.800-171.r2 3.14.7

Kategori: Deteksi > Layanan deteksi

Tingkat keparahan: Rendah

Jenis sumber

daya:AWS::Logs::MetricFilter,AWS::CloudWatch::Alarm,AWS::CloudTrail::Trail,AWS::SNS::Topic

AWS Config aturan: Tidak ada (aturan Security Hub khusus)

Jenis jadwal: Periodik

Parameter: Tidak ada

Anda dapat melakukan pemantauan real-time panggilan API dengan mengarahkan CloudTrail CloudWatch log ke Log dan membuat filter dan alarm metrik yang sesuai.

CIS menyarankan agar Anda membuat filter metrik dan alarm untuk panggilan API yang tidak sah. Memantau panggilan API yang tidak sah membantu mengungkapkan kesalahan aplikasi dan dapat mengurangi waktu untuk mendeteksi aktivitas berbahaya.

Untuk menjalankan pemeriksaan ini, Security Hub menggunakan logika khusus untuk melakukan langkah-langkah audit yang tepat yang ditentukan untuk kontrol 3.1 di [CIS AWS Foundations](#)

Benchmark v1.2. Kontrol ini gagal jika filter metrik yang tepat yang ditentukan oleh CIS tidak digunakan. Bidang atau istilah tambahan tidak dapat ditambahkan ke filter metrik.

 Note

Ketika Security Hub melakukan pemeriksaan untuk kontrol ini, ia mencari CloudTrail jejak yang digunakan akun saat ini. Jalur ini mungkin merupakan jalur organisasi yang dimiliki oleh akun lain. Jalur Multi-Wilayah juga mungkin berbasis di Wilayah yang berbeda.

Hasil pemeriksaan dalam FAILED temuan dalam kasus-kasus berikut:

- Tidak ada jejak yang dikonfigurasi.
- Jalur yang tersedia yang berada di Wilayah saat ini dan yang dimiliki oleh rekening giro tidak memenuhi persyaratan kontrol.

Hasil pemeriksaan dalam status kontrol NO_DATA dalam kasus berikut:

- Jejak multi-wilayah berbasis di Wilayah yang berbeda. Security Hub hanya dapat menghasilkan temuan di Wilayah tempat jejak itu berada.
- Jejak multi-wilayah milik akun yang berbeda. Security Hub hanya dapat menghasilkan temuan untuk akun yang memiliki jejak.

Kami merekomendasikan jejak organisasi untuk mencatat peristiwa dari banyak akun dalam suatu organisasi. Jejak organisasi adalah jalur Multi-wilayah secara default dan hanya dapat dikelola oleh akun AWS Organizations manajemen atau akun administrator yang CloudTrail didelegasikan. Menggunakan jejak organisasi menghasilkan status kontrol NO_DATA untuk kontrol yang dievaluasi dalam akun anggota organisasi. Di akun anggota, Security Hub hanya menghasilkan temuan untuk sumber daya milik anggota. Temuan yang berkaitan dengan jejak organisasi dihasilkan di akun pemilik sumber daya. Anda dapat melihat temuan ini di akun administrator yang didelegasikan Security Hub menggunakan agregasi lintas wilayah.

Untuk alarm, akun saat ini harus memiliki topik Amazon SNS yang direferensikan, atau harus mendapatkan akses ke topik Amazon SNS dengan menelepon.

`ListSubscriptionsByTopic` Jika tidak, Security Hub menghasilkan WARNING temuan untuk kontrol.

Perbaikan

Untuk melewati kontrol ini, ikuti langkah-langkah berikut untuk membuat topik Amazon SNS, AWS CloudTrail jejak, filter metrik, dan alarm untuk filter metrik.

1. Buat topik Amazon SNS. Untuk instruksi, lihat [Memulai dengan Amazon SNS di Panduan Pengembang Amazon SNS](#) di Panduan Developer Amazon SNS. Buat topik yang menerima semua alarm CIS, dan buat setidaknya satu langganan ke topik tersebut.
2. Buat CloudTrail jejak yang berlaku untuk semua Wilayah AWS. Untuk petunjuk, lihat [Membuat jejak](#) di Panduan AWS CloudTrail Pengguna.

Catat nama grup CloudWatch log Log yang Anda kaitkan dengan CloudTrail jejak. Anda membuat filter metrik untuk grup log pada langkah berikutnya.

3. Membuat sebuah filter metrik. Untuk petunjuknya, lihat [Membuat filter metrik untuk grup log](#) di Panduan CloudWatch Pengguna Amazon. Gunakan nilai berikut:

Bidang	Nilai
Tentukan pola, Pola filter	<code>{{\$.errorCode="*UnauthorizedOperation"}} {{\$.errorCode="AccessDenied*"}}}</code>
namespace metrik	LogMetrics
Nilai metrik	1
Nilai default	0

4. Buat alarm didasarkan pada filter. Untuk petunjuknya, lihat [Membuat CloudWatch alarm berdasarkan filter metrik grup log](#) di CloudWatch Panduan Pengguna Amazon. Gunakan nilai berikut:

Bidang	Nilai
Kondisi, tipe Ambang	Statis
<i>your-metric-name</i> Kapanpun...	lebih besar/sama
dari...	1

[CloudWatch.3] Pastikan filter metrik log dan alarm ada untuk login Konsol Manajemen tanpa MFA

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v1.2.0/3.2

Kategori: Deteksi > Layanan deteksi

Tingkat keparahan: Rendah

Jenis sumber

daya:AWS::Logs::MetricFilter,AWS::CloudWatch::Alarm,AWS::CloudTrail::Trail,AWS::SNS::Topic

AWS Config aturan: Tidak ada (aturan Security Hub khusus)

Jenis jadwal: Periodik

Parameter: Tidak ada

Anda dapat melakukan pemantauan real-time panggilan API dengan mengarahkan CloudTrail CloudWatch log ke Log dan membuat filter dan alarm metrik yang sesuai.

CIS merekomendasikan agar Anda membuat filter metrik dan login konsol alarm yang tidak dilindungi oleh MFA. Pemantauan untuk login konsol faktor tunggal meningkatkan visibilitas ke akun yang tidak dilindungi oleh MFA.

Untuk menjalankan pemeriksaan ini, Security Hub menggunakan logika khusus untuk melakukan langkah-langkah audit yang tepat yang ditentukan untuk kontrol 3.2 di [CIS AWS Foundations Benchmark](#) v1.2. Kontrol ini gagal jika filter metrik yang tepat yang ditentukan oleh CIS tidak digunakan. Bidang atau istilah tambahan tidak dapat ditambahkan ke filter metrik.

Note

Ketika Security Hub melakukan pemeriksaan untuk kontrol ini, ia mencari CloudTrail jejak yang digunakan akun saat ini. Jalur ini mungkin merupakan jalur organisasi yang dimiliki oleh akun lain. Jalur Multi-Wilayah juga mungkin berbasis di Wilayah yang berbeda.

Hasil pemeriksaan dalam FAILED temuan dalam kasus-kasus berikut:

- Tidak ada jejak yang dikonfigurasi.
- Jalur yang tersedia yang berada di Wilayah saat ini dan yang dimiliki oleh rekening giro tidak memenuhi persyaratan kontrol.

Hasil pemeriksaan dalam status kontrol NO_DATA dalam kasus berikut:

- Jejak multi-wilayah berbasis di Wilayah yang berbeda. Security Hub hanya dapat menghasilkan temuan di Wilayah tempat jejak itu berada.
- Jejak multi-wilayah milik akun yang berbeda. Security Hub hanya dapat menghasilkan temuan untuk akun yang memiliki jejak.

Kami merekomendasikan jejak organisasi untuk mencatat peristiwa dari banyak akun dalam suatu organisasi. Jejak organisasi adalah jalur Multi-wilayah secara default dan hanya dapat dikelola oleh akun AWS Organizations manajemen atau akun administrator yang CloudTrail didelegasikan. Menggunakan jejak organisasi menghasilkan status kontrol NO_DATA untuk kontrol yang dievaluasi dalam akun anggota organisasi. Di akun anggota, Security Hub hanya menghasilkan temuan untuk sumber daya milik anggota. Temuan yang berkaitan dengan jejak organisasi dihasilkan di akun pemilik sumber daya. Anda dapat melihat temuan ini di akun administrator yang didelegasikan Security Hub menggunakan agregasi lintas wilayah.

Untuk alarm, akun saat ini harus memiliki topik Amazon SNS yang direferensikan, atau harus mendapatkan akses ke topik Amazon SNS dengan menelepon. `ListSubscriptionsByTopic` Jika tidak, Security Hub menghasilkan WARNING temuan untuk kontrol.

Perbaikan

Untuk melewati kontrol ini, ikuti langkah-langkah berikut untuk membuat topik Amazon SNS, AWS CloudTrail jejak, filter metrik, dan alarm untuk filter metrik.

1. Buat topik Amazon SNS. Untuk instruksi, lihat [Memulai dengan Amazon SNS di Panduan Pengembang Amazon SNS](#) di Panduan Developer Amazon SNS. Buat topik yang menerima semua alarm CIS, dan buat setidaknya satu langganan ke topik tersebut.
2. Buat CloudTrail jejak yang berlaku untuk semua Wilayah AWS. Untuk petunjuk, lihat [Membuat jejak](#) di Panduan AWS CloudTrail Pengguna.

Catat nama grup CloudWatch log Log yang Anda kaitkan dengan CloudTrail jejak. Anda membuat filter metrik untuk grup log pada langkah berikutnya.

3. Membuat sebuah filter metrik. Untuk petunjuknya, lihat [Membuat filter metrik untuk grup log](#) di Panduan CloudWatch Pengguna Amazon. Gunakan nilai berikut:

Bidang	Nilai
Tentukan pola, Pola filter	<pre>{ (\$.eventName = "ConsoleLogin") && (\$.additionalEventData.MFAUsed != "Yes") && (\$.userIdentity.type = "IAMUser") && (\$.responseElements.ConsoleLogin = "Success") }</pre>
namespace metrik	LogMetrics
Nilai metrik	1
Nilai default	0

4. Buat alarm didasarkan pada filter. Untuk petunjuknya, lihat [Membuat CloudWatch alarm berdasarkan filter metrik grup log](#) di CloudWatch Panduan Pengguna Amazon. Gunakan nilai berikut:

Bidang	Nilai
Kondisi, tipe Ambang	Statis
<i>your-metric-name</i> Kapanpun...	lebih besar/sama
dari...	1

[CloudWatch.4] Pastikan filter metrik log dan alarm ada untuk perubahan kebijakan IAM

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v1.2.0/3.4, Tolok Ukur Yayasan CIS v1.4.0/4.4, Nist.800-171.r2 3.14.6, AWS Nist.800-171.r2 3.14.7

Kategori: Deteksi > Layanan deteksi

Tingkat keparahan: Rendah

Jenis sumber

daya:AWS::Logs::MetricFilter,AWS::CloudWatch::Alarm,AWS::CloudTrail::Trail,AWS::SNS::Topic

AWS Config aturan: Tidak ada (aturan Security Hub khusus)

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah Anda memantau panggilan API secara real time dengan mengarahkan CloudTrail CloudWatch log ke Log dan membuat filter dan alarm metrik yang sesuai.

CIS menyarankan agar Anda membuat filter metrik dan alarm untuk perubahan yang dibuat pada kebijakan IAM. Memantau perubahan ini membantu memastikan bahwa kontrol otentikasi dan otorisasi tetap utuh.

Note

Ketika Security Hub melakukan pemeriksaan untuk kontrol ini, ia mencari CloudTrail jejak yang digunakan akun saat ini. Jalur ini mungkin merupakan jalur organisasi yang dimiliki oleh akun lain. Jalur Multi-Wilayah juga mungkin berbasis di Wilayah yang berbeda.

Hasil pemeriksaan dalam FAILED temuan dalam kasus-kasus berikut:

- Tidak ada jejak yang dikonfigurasi.
- Jalur yang tersedia yang berada di Wilayah saat ini dan yang dimiliki oleh rekening giro tidak memenuhi persyaratan kontrol.

Hasil pemeriksaan dalam status kontrol NO_DATA dalam kasus berikut:

- Jejak multi-wilayah berbasis di Wilayah yang berbeda. Security Hub hanya dapat menghasilkan temuan di Wilayah tempat jejak itu berada.
- Jejak multi-wilayah milik akun yang berbeda. Security Hub hanya dapat menghasilkan temuan untuk akun yang memiliki jejak.

Kami merekomendasikan jejak organisasi untuk mencatat peristiwa dari banyak akun dalam suatu organisasi. Jejak organisasi adalah jalur Multi-wilayah secara default dan

hanya dapat dikelola oleh akun AWS Organizations manajemen atau akun administrator yang CloudTrail didelegasikan. Menggunakan jejak organisasi menghasilkan status kontrol NO_DATA untuk kontrol yang dievaluasi dalam akun anggota organisasi. Di akun anggota, Security Hub hanya menghasilkan temuan untuk sumber daya milik anggota. Temuan yang berkaitan dengan jejak organisasi dihasilkan di akun pemilik sumber daya. Anda dapat melihat temuan ini di akun administrator yang didelegasikan Security Hub menggunakan agregasi lintas wilayah.

Untuk alarm, akun saat ini harus memiliki topik Amazon SNS yang direferensikan, atau harus mendapatkan akses ke topik Amazon SNS dengan menelepon.

ListSubscriptionsByTopic Jika tidak, Security Hub menghasilkan WARNING temuan untuk kontrol.

Perbaikan

Note

Pola filter yang kami rekomendasikan dalam langkah-langkah remediasi ini berbeda dari pola filter dalam panduan CIS. Filter yang kami rekomendasikan hanya menargetkan peristiwa yang berasal dari panggilan API IAM.

Untuk melewati kontrol ini, ikuti langkah-langkah berikut untuk membuat topik Amazon SNS, AWS CloudTrail jejak, filter metrik, dan alarm untuk filter metrik.

1. Buat topik Amazon SNS. Untuk instruksi, lihat [Memulai dengan Amazon SNS di Panduan Pengembang Amazon SNS](#) di Panduan Developer Amazon SNS. Buat topik yang menerima semua alarm CIS, dan buat setidaknya satu langganan ke topik tersebut.
2. Buat CloudTrail jejak yang berlaku untuk semua Wilayah AWS. Untuk petunjuk, lihat [Membuat jejak](#) di Panduan AWS CloudTrail Pengguna.

Catat nama grup CloudWatch log Log yang Anda kaitkan dengan CloudTrail jejak. Anda membuat filter metrik untuk grup log pada langkah berikutnya.

3. Membuat sebuah filter metrik. Untuk petunjuknya, lihat [Membuat filter metrik untuk grup log](#) di Panduan CloudWatch Pengguna Amazon. Gunakan nilai berikut:

Bidang	Nilai
Tentukan pola, Pola filter	<pre>{(\$.eventSource=iam.amazonaws.com) && ((\$.eventName=DeleteGroupPolicy) (\$.eventName=DeleteRolePolicy) (\$.eventName=DeleteUserPolicy) (\$.eventName=PutGroupPolicy) (\$.eventName=PutRolePolicy) (\$.eventName=PutUserPolicy) (\$.eventName=CreatePolicy) (\$.eventName=DeletePolicy) (\$.eventName=CreatePolicyVersion) (\$.eventName=DeletePolicyVersion) (\$.eventName=AttachRolePolicy) (\$.eventName=DetachRolePolicy) (\$.eventName=AttachUserPolicy) (\$.eventName=DetachUserPolicy) (\$.eventName=AttachGroupPolicy) (\$.eventName=DetachGroupPolicy)))}</pre>
namespace metrik	LogMetrics
Nilai metrik	1
Nilai default	0

4. Buat alarm didasarkan pada filter. Untuk petunjuknya, lihat [Membuat CloudWatch alarm berdasarkan filter metrik grup log](#) di CloudWatch Panduan Pengguna Amazon. Gunakan nilai berikut:

Bidang	Nilai
Kondisi, tipe Ambang	Statis
<i>your-metric-name</i> Kapanpun...	lebih besar/sama
dari...	1

[CloudWatch.5] Pastikan filter metrik log dan alarm ada untuk perubahan CloudTrail konfigurasi

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v1.2.0/3.5, Tolok Ukur Yayasan CIS v1.4.0/4.5, Nist.800-171.r2 3.3.8, AWS Nist.800-171.r2 3.14.6, Nist.800-171.r2 3.14.7

Kategori: Deteksi > Layanan deteksi

Tingkat keparahan: Rendah

Jenis sumber

daya:AWS::Logs::MetricFilter,AWS::CloudWatch::Alarm,AWS::CloudTrail::Trail,AWS::SNS::Topic

AWS Config aturan: Tidak ada (aturan Security Hub khusus)

Jenis jadwal: Periodik

Parameter: Tidak ada

Anda dapat melakukan pemantauan real-time panggilan API dengan mengarahkan CloudTrail CloudWatch log ke Log dan membuat filter dan alarm metrik yang sesuai.

CIS merekomendasikan agar Anda membuat filter metrik dan alarm untuk perubahan pengaturan CloudTrail konfigurasi. Memantau perubahan ini membantu memastikan visibilitas berkelanjutan terhadap aktivitas di akun.

Untuk menjalankan pemeriksaan ini, Security Hub menggunakan logika kustom untuk melakukan langkah-langkah audit yang tepat yang ditentukan untuk kontrol 4.5 di [CIS AWS Foundations Benchmark](#) v1.4.0. Kontrol ini gagal jika filter metrik yang tepat yang ditentukan oleh CIS tidak digunakan. Bidang atau istilah tambahan tidak dapat ditambahkan ke filter metrik.

 Note

Ketika Security Hub melakukan pemeriksaan untuk kontrol ini, ia mencari CloudTrail jejak yang digunakan akun saat ini. Jalur ini mungkin merupakan jalur organisasi yang dimiliki oleh akun lain. Jalur Multi-Wilayah juga mungkin berbasis di Wilayah yang berbeda.

Hasil pemeriksaan dalam FAILED temuan dalam kasus-kasus berikut:

- Tidak ada jejak yang dikonfigurasi.
- Jalur yang tersedia yang berada di Wilayah saat ini dan yang dimiliki oleh rekening giro tidak memenuhi persyaratan kontrol.

Hasil pemeriksaan dalam status kontrol NO_DATA dalam kasus berikut:

- Jejak multi-wilayah berbasis di Wilayah yang berbeda. Security Hub hanya dapat menghasilkan temuan di Wilayah tempat jejak itu berada.
- Jejak multi-wilayah milik akun yang berbeda. Security Hub hanya dapat menghasilkan temuan untuk akun yang memiliki jejak.

Kami merekomendasikan jejak organisasi untuk mencatat peristiwa dari banyak akun dalam suatu organisasi. Jejak organisasi adalah jalur Multi-wilayah secara default dan hanya dapat dikelola oleh akun AWS Organizations manajemen atau akun administrator yang CloudTrail didelegasikan. Menggunakan jejak organisasi menghasilkan status kontrol NO_DATA untuk kontrol yang dievaluasi dalam akun anggota organisasi. Di akun anggota, Security Hub hanya menghasilkan temuan untuk sumber daya milik anggota. Temuan yang berkaitan dengan jejak organisasi dihasilkan di akun pemilik sumber daya. Anda dapat melihat temuan ini di akun administrator yang didelegasikan Security Hub menggunakan agregasi lintas wilayah.

Untuk alarm, akun saat ini harus memiliki topik Amazon SNS yang direferensikan, atau harus mendapatkan akses ke topik Amazon SNS dengan menelepon.

ListSubscriptionsByTopic Jika tidak, Security Hub menghasilkan WARNING temuan untuk kontrol.

Perbaikan

Untuk melewati kontrol ini, ikuti langkah-langkah berikut untuk membuat topik Amazon SNS, AWS CloudTrail jejak, filter metrik, dan alarm untuk filter metrik.

1. Buat topik Amazon SNS. Untuk instruksi, lihat [Memulai dengan Amazon SNS di Panduan Pengembang Amazon SNS](#) di Panduan Developer Amazon SNS. Buat topik yang menerima semua alarm CIS, dan buat setidaknya satu langganan ke topik tersebut.
2. Buat CloudTrail jejak yang berlaku untuk semua Wilayah AWS. Untuk petunjuk, lihat [Membuat jejak](#) di Panduan AWS CloudTrail Pengguna.

Catat nama grup CloudWatch log Log yang Anda kaitkan dengan CloudTrail jejak. Anda membuat filter metrik untuk grup log pada langkah berikutnya.

3. Membuat sebuah filter metrik. Untuk petunjuknya, lihat [Membuat filter metrik untuk grup log](#) di Panduan CloudWatch Pengguna Amazon. Gunakan nilai berikut:

Bidang	Nilai
Tentukan pola, Pola filter	<code>{{\$.eventName=CreateTrail}} {{\$.eventName=UpdateTrail}} {{\$.eventName=DeleteTrail}} {{\$.eventName=StartLogging}} {{\$.eventName=StopLogging}}</code>
namespace metrik	LogMetrics
Nilai metrik	1
Nilai default	0

4. Buat alarm didasarkan pada filter. Untuk petunjuknya, lihat [Membuat CloudWatch alarm berdasarkan filter metrik grup log](#) di CloudWatch Panduan Pengguna Amazon. Gunakan nilai berikut:

Bidang	Nilai
Kondisi, tipe Ambang	Statis

Bidang	Nilai
<i>your-metric-name</i> Kapanpun...	lebih besar/sama
dari...	1

[CloudWatch.6] Pastikan filter metrik log dan alarm ada untuk kegagalan AWS Management Console otentikasi

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v1.2.0/3.6, Tolok Ukur Yayasan CIS v1.4.0/4.6, Nist.800-171.r2 3.14.6, AWS Nist.800-171.r2 3.14.7

Kategori: Deteksi > Layanan deteksi

Tingkat keparahan: Rendah

Jenis sumber

daya:AWS::Logs::MetricFilter,AWS::CloudWatch::Alarm,AWS::CloudTrail::Trail,AWS::SNS::Topic

AWS Config aturan: Tidak ada (aturan Security Hub khusus)

Jenis jadwal: Periodik

Parameter: Tidak ada

Anda dapat melakukan pemantauan real-time panggilan API dengan mengarahkan CloudTrail CloudWatch log ke Log dan membuat filter dan alarm metrik yang sesuai.

CIS menyarankan agar Anda membuat filter metrik dan alarm untuk upaya otentikasi konsol yang gagal. Memantau login konsol yang gagal dapat mengurangi waktu tunggu untuk mendeteksi upaya untuk memaksa kredensi, yang mungkin memberikan indikator, seperti IP sumber, yang dapat Anda gunakan dalam korelasi peristiwa lain.

Untuk menjalankan pemeriksaan ini, Security Hub menggunakan logika kustom untuk melakukan langkah-langkah audit yang tepat yang ditentukan untuk kontrol 4.6 di [CIS AWS Foundations Benchmark v1.4.0](#). Kontrol ini gagal jika filter metrik yang tepat yang ditentukan oleh CIS tidak digunakan. Bidang atau istilah tambahan tidak dapat ditambahkan ke filter metrik.

 Note

Ketika Security Hub melakukan pemeriksaan untuk kontrol ini, ia mencari CloudTrail jejak yang digunakan akun saat ini. Jalur ini mungkin merupakan jalur organisasi yang dimiliki oleh akun lain. Jalur Multi-Wilayah juga mungkin berbasis di Wilayah yang berbeda.

Hasil pemeriksaan dalam FAILED temuan dalam kasus-kasus berikut:

- Tidak ada jejak yang dikonfigurasi.
- Jalur yang tersedia yang berada di Wilayah saat ini dan yang dimiliki oleh rekening giro tidak memenuhi persyaratan kontrol.

Hasil pemeriksaan dalam status kontrol NO_DATA dalam kasus berikut:

- Jejak multi-wilayah berbasis di Wilayah yang berbeda. Security Hub hanya dapat menghasilkan temuan di Wilayah tempat jejak itu berada.
- Jejak multi-wilayah milik akun yang berbeda. Security Hub hanya dapat menghasilkan temuan untuk akun yang memiliki jejak.

Kami merekomendasikan jejak organisasi untuk mencatat peristiwa dari banyak akun dalam suatu organisasi. Jejak organisasi adalah jalur Multi-wilayah secara default dan hanya dapat dikelola oleh akun AWS Organizations manajemen atau akun administrator yang CloudTrail didelegasikan. Menggunakan jejak organisasi menghasilkan status kontrol NO_DATA untuk kontrol yang dievaluasi dalam akun anggota organisasi. Di akun anggota, Security Hub hanya menghasilkan temuan untuk sumber daya milik anggota. Temuan yang berkaitan dengan jejak organisasi dihasilkan di akun pemilik sumber daya. Anda dapat melihat temuan ini di akun administrator yang didelegasikan Security Hub menggunakan agregasi lintas wilayah.

Untuk alarm, akun saat ini harus memiliki topik Amazon SNS yang direferensikan, atau harus mendapatkan akses ke topik Amazon SNS dengan menelepon.

ListSubscriptionsByTopic Jika tidak, Security Hub menghasilkan WARNING temuan untuk kontrol.

Perbaikan

Untuk melewati kontrol ini, ikuti langkah-langkah berikut untuk membuat topik Amazon SNS, AWS CloudTrail jejak, filter metrik, dan alarm untuk filter metrik.

1. Buat topik Amazon SNS. Untuk instruksi, lihat [Memulai dengan Amazon SNS di Panduan Pengembang Amazon SNS](#) di Panduan Developer Amazon SNS. Buat topik yang menerima semua alarm CIS, dan buat setidaknya satu langganan ke topik tersebut.
2. Buat CloudTrail jejak yang berlaku untuk semua Wilayah AWS. Untuk petunjuk, lihat [Membuat jejak](#) di Panduan AWS CloudTrail Pengguna.

Catat nama grup CloudWatch log Log yang Anda kaitkan dengan CloudTrail jejak. Anda membuat filter metrik untuk grup log pada langkah berikutnya.

3. Membuat sebuah filter metrik. Untuk petunjuknya, lihat [Membuat filter metrik untuk grup log](#) di Panduan CloudWatch Pengguna Amazon. Gunakan nilai berikut:

Bidang	Nilai
Tentukan pola, Pola filter	<code>{{\$.eventName=ConsoleLogin}&& (\$.errorMessage="Failed authentication")}</code>
namespace metrik	LogMetrics
Nilai metrik	1
Nilai default	0

4. Buat alarm didasarkan pada filter. Untuk petunjuknya, lihat [Membuat CloudWatch alarm berdasarkan filter metrik grup log](#) di CloudWatch Panduan Pengguna Amazon. Gunakan nilai berikut:

Bidang	Nilai
Kondisi, tipe Ambang	Statis
<i>your-metric-name</i> Kapanpun...	lebih besar/sama
dari...	1

[CloudWatch.7] Pastikan filter metrik log dan alarm ada untuk menonaktifkan atau menjadwalkan penghapusan kunci yang dikelola pelanggan

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v1.2.0/3.7, Tolok Ukur Yayasan CIS v1.4.0/4.7, Nist.800-171.r2 3.13.10, Nist.800-171.r2 3.13.16, AWS Nist.800-171.r2 3.14.6, Nist.800-171.r2 3.14.7

Kategori: Deteksi > Layanan deteksi

Tingkat keparahan: Rendah

Jenis sumber

daya:AWS::Logs::MetricFilter,AWS::CloudWatch::Alarm,AWS::CloudTrail::Trail,AWS::SNS::Topic

AWS Config aturan: Tidak ada (aturan Security Hub khusus)

Jenis jadwal: Periodik

Parameter: Tidak ada

Anda dapat melakukan pemantauan real-time panggilan API dengan mengarahkan CloudTrail CloudWatch log ke Log dan membuat filter dan alarm metrik yang sesuai.

CIS merekomendasikan agar Anda membuat filter metrik dan alarm untuk kunci terkelola pelanggan yang telah mengubah status menjadi penghapusan dinonaktifkan atau terjadwal. Data yang dienkripsi dengan kunci yang dinonaktifkan atau dihapus tidak lagi dapat diakses.

Untuk menjalankan pemeriksaan ini, Security Hub menggunakan logika kustom untuk melakukan langkah-langkah audit yang tepat yang ditentukan untuk kontrol 4.7 di [CIS AWS Foundations Benchmark v1.4.0](#). Kontrol ini gagal jika filter metrik yang tepat yang ditentukan oleh CIS tidak digunakan. Bidang atau istilah tambahan tidak dapat ditambahkan ke filter metrik. Kontrol juga gagal jika `ExcludeManagementEventSources` berisikan `amazonaws.com`.

Note

Ketika Security Hub melakukan pemeriksaan untuk kontrol ini, ia mencari CloudTrail jejak yang digunakan akun saat ini. Jalur ini mungkin merupakan jalur organisasi yang dimiliki oleh akun lain. Jalur Multi-Wilayah juga mungkin berbasis di Wilayah yang berbeda.

Hasil pemeriksaan dalam FAILED temuan dalam kasus-kasus berikut:

- Tidak ada jejak yang dikonfigurasi.

- Jalur yang tersedia yang berada di Wilayah saat ini dan yang dimiliki oleh rekening giro tidak memenuhi persyaratan kontrol.

Hasil pemeriksaan dalam status kontrol NO_DATA dalam kasus berikut:

- Jejak multi-wilayah berbasis di Wilayah yang berbeda. Security Hub hanya dapat menghasilkan temuan di Wilayah tempat jejak itu berada.
- Jejak multi-wilayah milik akun yang berbeda. Security Hub hanya dapat menghasilkan temuan untuk akun yang memiliki jejak.

Kami merekomendasikan jejak organisasi untuk mencatat peristiwa dari banyak akun dalam suatu organisasi. Jejak organisasi adalah jalur Multi-wilayah secara default dan hanya dapat dikelola oleh akun AWS Organizations manajemen atau akun administrator yang CloudTrail didelegasikan. Menggunakan jejak organisasi menghasilkan status kontrol NO_DATA untuk kontrol yang dievaluasi dalam akun anggota organisasi. Di akun anggota, Security Hub hanya menghasilkan temuan untuk sumber daya milik anggota. Temuan yang berkaitan dengan jejak organisasi dihasilkan di akun pemilik sumber daya. Anda dapat melihat temuan ini di akun administrator yang didelegasikan Security Hub menggunakan agregasi lintas wilayah.

Untuk alarm, akun saat ini harus memiliki topik Amazon SNS yang direferensikan, atau harus mendapatkan akses ke topik Amazon SNS dengan menelepon.

ListSubscriptionsByTopic Jika tidak, Security Hub menghasilkan WARNING temuan untuk kontrol.

Perbaikan

Untuk melewati kontrol ini, ikuti langkah-langkah berikut untuk membuat topik Amazon SNS, AWS CloudTrail jejak, filter metrik, dan alarm untuk filter metrik.

1. Buat topik Amazon SNS. Untuk instruksi, lihat [Memulai dengan Amazon SNS di Panduan Pengembang Amazon SNS](#) di Panduan Developer Amazon SNS. Buat topik yang menerima semua alarm CIS, dan buat setidaknya satu langganan ke topik tersebut.
2. Buat CloudTrail jejak yang berlaku untuk semua Wilayah AWS. Untuk petunjuk, lihat [Membuat jejak](#) di Panduan AWS CloudTrail Pengguna.

Catat nama grup CloudWatch log Log yang Anda kaitkan dengan CloudTrail jejak. Anda membuat filter metrik untuk grup log pada langkah berikutnya.

3. Membuat sebuah filter metrik. Untuk petunjuknya, lihat [Membuat filter metrik untuk grup log](#) di Panduan CloudWatch Pengguna Amazon. Gunakan nilai berikut:

Bidang	Nilai
Tentukan pola, Pola filter	<code>{(\$.eventSource=kms.amazonaws.com) && ((\$.eventName=DisableKey) (\$.eventName=ScheduleKeyDeletion))}</code>
namespace metrik	LogMetrics
Nilai metrik	1
Nilai default	0

4. Buat alarm didasarkan pada filter. Untuk petunjuknya, lihat [Membuat CloudWatch alarm berdasarkan filter metrik grup log](#) di CloudWatch Panduan Pengguna Amazon. Gunakan nilai berikut:

Bidang	Nilai
Kondisi, tipe Ambang	Statis
<i>your-metric-name</i> Kapanpun...	lebih besar/sama
dari...	1

[CloudWatch.8] Pastikan filter metrik log dan alarm ada untuk perubahan kebijakan bucket S3

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v1.2.0/3.8, Tolok Ukur Yayasan CIS v1.4.0/4.8, Nist.800-171.r2 3.14.6, AWS Nist.800-171.r2 3.14.7

Kategori: Deteksi > Layanan deteksi

Tingkat keparahan: Rendah

Jenis sumber

daya:AWS::Logs::MetricFilter,AWS::CloudWatch::Alarm,AWS::CloudTrail::Trail,
AWS::SNS::Topic

AWS Config aturan: Tidak ada (aturan Security Hub khusus)

Jenis jadwal: Periodik

Parameter: Tidak ada

Anda dapat melakukan pemantauan real-time panggilan API dengan mengarahkan CloudTrail CloudWatch log ke Log dan membuat filter dan alarm metrik yang sesuai.

CIS menyarankan Anda membuat filter metrik dan alarm untuk perubahan kebijakan bucket S3. Memantau perubahan ini dapat mengurangi waktu untuk mendeteksi dan memperbaiki kebijakan permisif pada bucket S3 yang sensitif.

Untuk menjalankan pemeriksaan ini, Security Hub menggunakan logika kustom untuk melakukan langkah-langkah audit yang tepat yang ditentukan untuk kontrol 4.8 di [CIS AWS Foundations Benchmark v1.4.0](#). Kontrol ini gagal jika filter metrik yang tepat yang ditentukan oleh CIS tidak digunakan. Bidang atau istilah tambahan tidak dapat ditambahkan ke filter metrik.

Note

Ketika Security Hub melakukan pemeriksaan untuk kontrol ini, ia mencari CloudTrail jejak yang digunakan akun saat ini. Jalur ini mungkin merupakan jalur organisasi yang dimiliki oleh akun lain. Jalur Multi-Wilayah juga mungkin berbasis di Wilayah yang berbeda.

Hasil pemeriksaan dalam FAILED temuan dalam kasus-kasus berikut:

- Tidak ada jejak yang dikonfigurasi.
- Jalur yang tersedia yang berada di Wilayah saat ini dan yang dimiliki oleh rekening giro tidak memenuhi persyaratan kontrol.

Hasil pemeriksaan dalam status kontrol NO_DATA dalam kasus berikut:

- Jejak multi-wilayah berbasis di Wilayah yang berbeda. Security Hub hanya dapat menghasilkan temuan di Wilayah tempat jejak itu berada.

- Jejak multi-wilayah milik akun yang berbeda. Security Hub hanya dapat menghasilkan temuan untuk akun yang memiliki jejak.

Kami merekomendasikan jejak organisasi untuk mencatat peristiwa dari banyak akun dalam suatu organisasi. Jejak organisasi adalah jalur Multi-wilayah secara default dan hanya dapat dikelola oleh akun AWS Organizations manajemen atau akun administrator yang CloudTrail didelegasikan. Menggunakan jejak organisasi menghasilkan status kontrol NO_DATA untuk kontrol yang dievaluasi dalam akun anggota organisasi. Di akun anggota, Security Hub hanya menghasilkan temuan untuk sumber daya milik anggota. Temuan yang berkaitan dengan jejak organisasi dihasilkan di akun pemilik sumber daya. Anda dapat melihat temuan ini di akun administrator yang didelegasikan Security Hub menggunakan agregasi lintas wilayah.

Untuk alarm, akun saat ini harus memiliki topik Amazon SNS yang direferensikan, atau harus mendapatkan akses ke topik Amazon SNS dengan menelepon. `ListSubscriptionsByTopic` Jika tidak, Security Hub menghasilkan WARNING temuan untuk kontrol.

Perbaikan

Untuk melewati kontrol ini, ikuti langkah-langkah berikut untuk membuat topik Amazon SNS, AWS CloudTrail jejak, filter metrik, dan alarm untuk filter metrik.

1. Buat topik Amazon SNS. Untuk instruksi, lihat [Memulai dengan Amazon SNS di Panduan Pengembang Amazon SNS](#) di Panduan Developer Amazon SNS. Buat topik yang menerima semua alarm CIS, dan buat setidaknya satu langganan ke topik tersebut.
2. Buat CloudTrail jejak yang berlaku untuk semua Wilayah AWS. Untuk petunjuk, lihat [Membuat jejak](#) di Panduan AWS CloudTrail Pengguna.

Catat nama grup CloudWatch log Log yang Anda kaitkan dengan CloudTrail jejak. Anda membuat filter metrik untuk grup log pada langkah berikutnya.

3. Membuat sebuah filter metrik. Untuk petunjuknya, lihat [Membuat filter metrik untuk grup log](#) di Panduan CloudWatch Pengguna Amazon. Gunakan nilai berikut:

Bidang	Nilai
Tentukan pola, Pola filter	<code>{ (\$.eventSource=s3.amazonaws.com) && ((\$.eventName=PutBucketAcl) (\$.eventName=PutBucketPolicy) (\$.eventName=PutBucketCors) (\$.eventName=PutBucketLifecycle) (\$.eventName=PutBucketReplication) (\$.eventName=DeleteBucketPolicy) (\$.eventName=DeleteBucketCors) (\$.eventName=DeleteBucketLifecycle) (\$.eventName=DeleteBucketReplication)) }</code>
namespace metrik	LogMetrics
Nilai metrik	1
Nilai default	0

4. Buat alarm didasarkan pada filter. Untuk petunjuknya, lihat [Membuat CloudWatch alarm berdasarkan filter metrik grup log](#) di CloudWatch Panduan Pengguna Amazon. Gunakan nilai berikut:

Bidang	Nilai
Kondisi, tipe Ambang	Statis
<i>your-metric-name</i> Kapanpun...	lebih besar/sama
dari...	1

[CloudWatch.9] Pastikan filter metrik log dan alarm ada untuk perubahan AWS Config konfigurasi

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v1.2.0/3.9, Tolok Ukur Yayasan CIS v1.4.0/4.9, Nist.800-171.r2 3.3.8, Nist.800-171.r2 AWS 3.14.6, Nist.800-171.r2 3.14.7

Kategori: Deteksi > Layanan deteksi

Tingkat keparahan: Rendah

Jenis sumber

daya:AWS::Logs::MetricFilter,AWS::CloudWatch::Alarm,AWS::CloudTrail::Trail,AWS::SNS::Topic

AWS Config aturan: Tidak ada (aturan Security Hub khusus)

Jenis jadwal: Periodik

Parameter: Tidak ada

Anda dapat melakukan pemantauan real-time panggilan API dengan mengarahkan CloudTrail CloudWatch log ke Log dan membuat filter dan alarm metrik yang sesuai.

CIS merekomendasikan agar Anda membuat filter metrik dan alarm untuk perubahan pengaturan AWS Config konfigurasi. Memantau perubahan ini membantu memastikan visibilitas item konfigurasi yang berkelanjutan di akun.

Untuk menjalankan pemeriksaan ini, Security Hub menggunakan logika kustom untuk melakukan langkah-langkah audit yang tepat yang ditentukan untuk kontrol 4.9 di [CIS AWS Foundations Benchmark v1.4.0](#). Kontrol ini gagal jika filter metrik yang tepat yang ditentukan oleh CIS tidak digunakan. Bidang atau istilah tambahan tidak dapat ditambahkan ke filter metrik.

Note

Ketika Security Hub melakukan pemeriksaan untuk kontrol ini, ia mencari CloudTrail jejak yang digunakan akun saat ini. Jalur ini mungkin merupakan jalur organisasi yang dimiliki oleh akun lain. Jalur Multi-Wilayah juga mungkin berbasis di Wilayah yang berbeda.

Hasil pemeriksaan dalam FAILED temuan dalam kasus-kasus berikut:

- Tidak ada jejak yang dikonfigurasi.

- Jalur yang tersedia yang berada di Wilayah saat ini dan yang dimiliki oleh rekening giro tidak memenuhi persyaratan kontrol.

Hasil pemeriksaan dalam status kontrol NO_DATA dalam kasus berikut:

- Jejak multi-wilayah berbasis di Wilayah yang berbeda. Security Hub hanya dapat menghasilkan temuan di Wilayah tempat jejak itu berada.
- Jejak multi-wilayah milik akun yang berbeda. Security Hub hanya dapat menghasilkan temuan untuk akun yang memiliki jejak.

Kami merekomendasikan jejak organisasi untuk mencatat peristiwa dari banyak akun dalam suatu organisasi. Jejak organisasi adalah jalur Multi-wilayah secara default dan hanya dapat dikelola oleh akun AWS Organizations manajemen atau akun administrator yang CloudTrail didelegasikan. Menggunakan jejak organisasi menghasilkan status kontrol NO_DATA untuk kontrol yang dievaluasi dalam akun anggota organisasi. Di akun anggota, Security Hub hanya menghasilkan temuan untuk sumber daya milik anggota. Temuan yang berkaitan dengan jejak organisasi dihasilkan di akun pemilik sumber daya. Anda dapat melihat temuan ini di akun administrator yang didelegasikan Security Hub menggunakan agregasi lintas wilayah.

Untuk alarm, akun saat ini harus memiliki topik Amazon SNS yang direferensikan, atau harus mendapatkan akses ke topik Amazon SNS dengan menelepon.

ListSubscriptionsByTopic Jika tidak, Security Hub menghasilkan WARNING temuan untuk kontrol.

Perbaikan

Untuk melewati kontrol ini, ikuti langkah-langkah berikut untuk membuat topik Amazon SNS, AWS CloudTrail jejak, filter metrik, dan alarm untuk filter metrik.

1. Buat topik Amazon SNS. Untuk instruksi, lihat [Memulai dengan Amazon SNS di Panduan Pengembang Amazon SNS](#) di Panduan Developer Amazon SNS. Buat topik yang menerima semua alarm CIS, dan buat setidaknya satu langganan ke topik tersebut.
2. Buat CloudTrail jejak yang berlaku untuk semua Wilayah AWS. Untuk petunjuk, lihat [Membuat jejak](#) di Panduan AWS CloudTrail Pengguna.

Catat nama grup CloudWatch log Log yang Anda kaitkan dengan CloudTrail jejak. Anda membuat filter metrik untuk grup log pada langkah berikutnya.

3. Membuat sebuah filter metrik. Untuk petunjuknya, lihat [Membuat filter metrik untuk grup log](#) di Panduan CloudWatch Pengguna Amazon. Gunakan nilai berikut:

Bidang	Nilai
Tentukan pola, Pola filter	<code>{(\$.eventSource=config.amazonaws.com) && (\$.eventName=StopConfigurationRecorder) (\$.eventName=DeleteDeliveryChannel) (\$.eventName=PutDeliveryChannel) (\$.eventName=PutConfigurationRecorder))}</code>
namespace metrik	LogMetrics
Nilai metrik	1
Nilai default	0

4. Buat alarm didasarkan pada filter. Untuk petunjuknya, lihat [Membuat CloudWatch alarm berdasarkan filter metrik grup log](#) di CloudWatch Panduan Pengguna Amazon. Gunakan nilai berikut:

Bidang	Nilai
Kondisi, tipe Ambang	Statis
<i>your-metric-name</i> Kapanpun...	lebih besar/sama
dari...	1

[CloudWatch.10] Pastikan filter metrik log dan alarm ada untuk perubahan grup keamanan

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v1.2.0/3.10, Tolok Ukur Yayasan CIS v1.4.0/4.10, Nist.800-171.r2 3.14.6, AWS Nist.800-171.r2 3.14.7

Kategori: Deteksi > Layanan deteksi

Tingkat keparahan: Rendah

Jenis sumber

daya:AWS::Logs::MetricFilter,AWS::CloudWatch::Alarm,AWS::CloudTrail::Trail,AWS::SNS::Topic

AWS Config aturan: Tidak ada (aturan Security Hub khusus)

Jenis jadwal: Periodik

Parameter: Tidak ada

Anda dapat melakukan pemantauan real-time panggilan API dengan mengarahkan CloudTrail CloudWatch log ke Log dan membuat filter dan alarm metrik yang sesuai. Grup keamanan adalah filter paket stateful yang mengontrol lalu lintas masuk dan keluar di VPC.

CIS merekomendasikan agar Anda membuat filter metrik dan alarm untuk perubahan pada grup keamanan. Memantau perubahan ini membantu memastikan bahwa sumber daya dan layanan tidak terekspos secara tidak sengaja.

Untuk menjalankan pemeriksaan ini, Security Hub menggunakan logika kustom untuk melakukan langkah-langkah audit yang tepat yang ditentukan untuk kontrol 4.10 di [CIS AWS Foundations Benchmark v1.4.0](#). Kontrol ini gagal jika filter metrik yang tepat yang ditentukan oleh CIS tidak digunakan. Bidang atau istilah tambahan tidak dapat ditambahkan ke filter metrik.

Note

Ketika Security Hub melakukan pemeriksaan untuk kontrol ini, ia mencari CloudTrail jejak yang digunakan akun saat ini. Jalur ini mungkin merupakan jalur organisasi yang dimiliki oleh akun lain. Jalur Multi-Wilayah juga mungkin berbasis di Wilayah yang berbeda.

Hasil pemeriksaan dalam FAILED temuan dalam kasus-kasus berikut:

- Tidak ada jejak yang dikonfigurasi.

- Jalur yang tersedia yang berada di Wilayah saat ini dan yang dimiliki oleh rekening giro tidak memenuhi persyaratan kontrol.

Hasil pemeriksaan dalam status kontrol NO_DATA dalam kasus berikut:

- Jejak multi-wilayah berbasis di Wilayah yang berbeda. Security Hub hanya dapat menghasilkan temuan di Wilayah tempat jejak itu berada.
- Jejak multi-wilayah milik akun yang berbeda. Security Hub hanya dapat menghasilkan temuan untuk akun yang memiliki jejak.

Kami merekomendasikan jejak organisasi untuk mencatat peristiwa dari banyak akun dalam suatu organisasi. Jejak organisasi adalah jalur Multi-wilayah secara default dan hanya dapat dikelola oleh akun AWS Organizations manajemen atau akun administrator yang CloudTrail didelegasikan. Menggunakan jejak organisasi menghasilkan status kontrol NO_DATA untuk kontrol yang dievaluasi dalam akun anggota organisasi. Di akun anggota, Security Hub hanya menghasilkan temuan untuk sumber daya milik anggota. Temuan yang berkaitan dengan jejak organisasi dihasilkan di akun pemilik sumber daya. Anda dapat melihat temuan ini di akun administrator yang didelegasikan Security Hub menggunakan agregasi lintas wilayah.

Untuk alarm, akun saat ini harus memiliki topik Amazon SNS yang direferensikan, atau harus mendapatkan akses ke topik Amazon SNS dengan menelepon.

ListSubscriptionsByTopic Jika tidak, Security Hub menghasilkan WARNING temuan untuk kontrol.

Perbaikan

Untuk melewati kontrol ini, ikuti langkah-langkah berikut untuk membuat topik Amazon SNS, AWS CloudTrail jejak, filter metrik, dan alarm untuk filter metrik.

1. Buat topik Amazon SNS. Untuk instruksi, lihat [Memulai dengan Amazon SNS di Panduan Pengembang Amazon SNS](#) di Panduan Developer Amazon SNS. Buat topik yang menerima semua alarm CIS, dan buat setidaknya satu langganan ke topik tersebut.
2. Buat CloudTrail jejak yang berlaku untuk semua Wilayah AWS. Untuk petunjuk, lihat [Membuat jejak](#) di Panduan AWS CloudTrail Pengguna.

Catat nama grup CloudWatch log Log yang Anda kaitkan dengan CloudTrail jejak. Anda membuat filter metrik untuk grup log pada langkah berikutnya.

3. Membuat sebuah filter metrik. Untuk petunjuknya, lihat [Membuat filter metrik untuk grup log](#) di Panduan CloudWatch Pengguna Amazon. Gunakan nilai berikut:

Bidang	Nilai
Tentukan pola, Pola filter	<code>{(\$.eventName=AuthorizeSecurityGroupIngress) (\$.eventName=AuthorizeSecurityGroupEgress) (\$.eventName=RevokeSecurityGroupIngress) (\$.eventName=RevokeSecurityGroupEgress) (\$.eventName=CreateSecurityGroup) (\$.eventName>DeleteSecurityGroup)}</code>
namespace metrik	LogMetrics
Nilai metrik	1
Nilai default	0

4. Buat alarm didasarkan pada filter. Untuk petunjuknya, lihat [Membuat CloudWatch alarm berdasarkan filter metrik grup log](#) di CloudWatch Panduan Pengguna Amazon. Gunakan nilai berikut:

Bidang	Nilai
Kondisi, tipe Ambang	Statis
<i>your-metric-name</i> Kapanpun...	lebih besar/sama
dari...	1

[CloudWatch.11] Pastikan filter metrik log dan alarm ada untuk perubahan pada Daftar Kontrol Akses Jaringan (NACL)

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v1.2.0/3.11, Tolok Ukur Yayasan CIS v1.4.0/4.11, Nist.800-171.r2 3.14.6, AWS Nist.800-171.r2 3.14.7

Kategori: Deteksi > Layanan deteksi

Tingkat keparahan: Rendah

Jenis sumber

daya:AWS::Logs::MetricFilter,AWS::CloudWatch::Alarm,AWS::CloudTrail::Trail,AWS::SNS::Topic

AWS Config aturan: Tidak ada (aturan Security Hub khusus)

Jenis jadwal: Periodik

Parameter: Tidak ada

Anda dapat melakukan pemantauan real-time panggilan API dengan mengarahkan CloudTrail CloudWatch log ke Log dan membuat filter dan alarm metrik yang sesuai. NACLs digunakan sebagai filter paket stateless untuk mengontrol masuknya dan keluar lalu lintas untuk subnet dalam VPC.

CIS merekomendasikan agar Anda membuat filter metrik dan alarm untuk NACLs perubahan. Memantau perubahan ini membantu memastikan bahwa AWS sumber daya dan layanan tidak terekspos secara tidak sengaja.

Untuk menjalankan pemeriksaan ini, Security Hub menggunakan logika kustom untuk melakukan langkah-langkah audit yang tepat yang ditentukan untuk kontrol 4.11 di [CIS AWS Foundations Benchmark v1.4.0](#). Kontrol ini gagal jika filter metrik yang tepat yang ditentukan oleh CIS tidak digunakan. Bidang atau istilah tambahan tidak dapat ditambahkan ke filter metrik.

Note

Ketika Security Hub melakukan pemeriksaan untuk kontrol ini, ia mencari CloudTrail jejak yang digunakan akun saat ini. Jalur ini mungkin merupakan jalur organisasi yang dimiliki oleh akun lain. Jalur Multi-Wilayah juga mungkin berbasis di Wilayah yang berbeda.

Hasil pemeriksaan dalam FAILED temuan dalam kasus-kasus berikut:

- Tidak ada jejak yang dikonfigurasi.

- Jalur yang tersedia yang berada di Wilayah saat ini dan yang dimiliki oleh rekening giro tidak memenuhi persyaratan kontrol.

Hasil pemeriksaan dalam status kontrol NO_DATA dalam kasus berikut:

- Jejak multi-wilayah berbasis di Wilayah yang berbeda. Security Hub hanya dapat menghasilkan temuan di Wilayah tempat jejak itu berada.
- Jejak multi-wilayah milik akun yang berbeda. Security Hub hanya dapat menghasilkan temuan untuk akun yang memiliki jejak.

Kami merekomendasikan jejak organisasi untuk mencatat peristiwa dari banyak akun dalam suatu organisasi. Jejak organisasi adalah jalur Multi-wilayah secara default dan hanya dapat dikelola oleh akun AWS Organizations manajemen atau akun administrator yang CloudTrail didelegasikan. Menggunakan jejak organisasi menghasilkan status kontrol NO_DATA untuk kontrol yang dievaluasi dalam akun anggota organisasi. Di akun anggota, Security Hub hanya menghasilkan temuan untuk sumber daya milik anggota. Temuan yang berkaitan dengan jejak organisasi dihasilkan di akun pemilik sumber daya. Anda dapat melihat temuan ini di akun administrator yang didelegasikan Security Hub menggunakan agregasi lintas wilayah.

Untuk alarm, akun saat ini harus memiliki topik Amazon SNS yang direferensikan, atau harus mendapatkan akses ke topik Amazon SNS dengan menelepon.

ListSubscriptionsByTopic Jika tidak, Security Hub menghasilkan WARNING temuan untuk kontrol.

Perbaikan

Untuk melewati kontrol ini, ikuti langkah-langkah berikut untuk membuat topik Amazon SNS, AWS CloudTrail jejak, filter metrik, dan alarm untuk filter metrik.

1. Buat topik Amazon SNS. Untuk instruksi, lihat [Memulai dengan Amazon SNS di Panduan Pengembang Amazon SNS](#) di Panduan Developer Amazon SNS. Buat topik yang menerima semua alarm CIS, dan buat setidaknya satu langganan ke topik tersebut.
2. Buat CloudTrail jejak yang berlaku untuk semua Wilayah AWS. Untuk petunjuk, lihat [Membuat jejak](#) di Panduan AWS CloudTrail Pengguna.

Catat nama grup CloudWatch log Log yang Anda kaitkan dengan CloudTrail jejak. Anda membuat filter metrik untuk grup log pada langkah berikutnya.

3. Membuat sebuah filter metrik. Untuk petunjuknya, lihat [Membuat filter metrik untuk grup log](#) di Panduan CloudWatch Pengguna Amazon. Gunakan nilai berikut:

Bidang	Nilai
Tentukan pola, Pola filter	<code>{(\$.eventName=CreateNetworkAcl) (\$.eventName=CreateNetworkAclEntry) (\$.eventName>DeleteNetworkAcl) (\$.eventName>DeleteNetworkAclEntry) (\$.eventName=ReplaceNetworkAclEntry) (\$.eventName=ReplaceNetworkAclAssociation)}</code>
namespace metrik	LogMetrics
Nilai metrik	1
Nilai default	0

4. Buat alarm didasarkan pada filter. Untuk petunjuknya, lihat [Membuat CloudWatch alarm berdasarkan filter metrik grup log](#) di CloudWatch Panduan Pengguna Amazon. Gunakan nilai berikut:

Bidang	Nilai
Kondisi, tipe Ambang	Statis
<i>your-metric-name</i> Kapanpun...	lebih besar/sama
dari...	1

[CloudWatch.12] Pastikan filter metrik log dan alarm ada untuk perubahan pada gateway jaringan

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v1.2.0/3.12, Tolok Ukur Yayasan CIS v1.4.0/4.12, Nist.800-171.r2 3.3.1, AWS Nist.800-171.r2 3.13.1

Kategori: Deteksi > Layanan deteksi

Tingkat keparahan: Rendah

Jenis sumber

daya:AWS::Logs::MetricFilter,AWS::CloudWatch::Alarm,AWS::CloudTrail::Trail,AWS::SNS::Topic

AWS Config aturan: Tidak ada (aturan Security Hub khusus)

Jenis jadwal: Periodik

Parameter: Tidak ada

Anda dapat melakukan pemantauan real-time panggilan API dengan mengarahkan CloudTrail CloudWatch log ke Log dan membuat filter dan alarm metrik yang sesuai. Gateway jaringan diperlukan untuk mengirim dan menerima lalu lintas ke tujuan di luar VPC.

CIS merekomendasikan agar Anda membuat filter metrik dan alarm untuk perubahan gateway jaringan. Memantau perubahan ini membantu memastikan bahwa semua lalu lintas masuk dan keluar melintasi perbatasan VPC melalui jalur yang terkendali.

Untuk menjalankan pemeriksaan ini, Security Hub menggunakan logika khusus untuk melakukan langkah-langkah audit yang tepat yang ditentukan untuk kontrol 4.12 di [CIS AWS Foundations Benchmark](#) v1.2. Kontrol ini gagal jika filter metrik yang tepat yang ditentukan oleh CIS tidak digunakan. Bidang atau istilah tambahan tidak dapat ditambahkan ke filter metrik.

Note

Ketika Security Hub melakukan pemeriksaan untuk kontrol ini, ia mencari CloudTrail jejak yang digunakan akun saat ini. Jalur ini mungkin merupakan jalur organisasi yang dimiliki oleh akun lain. Jalur Multi-Wilayah juga mungkin berbasis di Wilayah yang berbeda.

Hasil pemeriksaan dalam FAILED temuan dalam kasus-kasus berikut:

- Tidak ada jejak yang dikonfigurasi.

- Jalur yang tersedia yang berada di Wilayah saat ini dan yang dimiliki oleh rekening giro tidak memenuhi persyaratan kontrol.

Hasil pemeriksaan dalam status kontrol NO_DATA dalam kasus berikut:

- Jejak multi-wilayah berbasis di Wilayah yang berbeda. Security Hub hanya dapat menghasilkan temuan di Wilayah tempat jejak itu berada.
- Jejak multi-wilayah milik akun yang berbeda. Security Hub hanya dapat menghasilkan temuan untuk akun yang memiliki jejak.

Kami merekomendasikan jejak organisasi untuk mencatat peristiwa dari banyak akun dalam suatu organisasi. Jejak organisasi adalah jalur Multi-wilayah secara default dan hanya dapat dikelola oleh akun AWS Organizations manajemen atau akun administrator yang CloudTrail didelegasikan. Menggunakan jejak organisasi menghasilkan status kontrol NO_DATA untuk kontrol yang dievaluasi dalam akun anggota organisasi. Di akun anggota, Security Hub hanya menghasilkan temuan untuk sumber daya milik anggota. Temuan yang berkaitan dengan jejak organisasi dihasilkan di akun pemilik sumber daya. Anda dapat melihat temuan ini di akun administrator yang didelegasikan Security Hub menggunakan agregasi lintas wilayah.

Untuk alarm, akun saat ini harus memiliki topik Amazon SNS yang direferensikan, atau harus mendapatkan akses ke topik Amazon SNS dengan menelepon.

ListSubscriptionsByTopic Jika tidak, Security Hub menghasilkan WARNING temuan untuk kontrol.

Perbaikan

Untuk melewati kontrol ini, ikuti langkah-langkah berikut untuk membuat topik Amazon SNS, AWS CloudTrail jejak, filter metrik, dan alarm untuk filter metrik.

1. Buat topik Amazon SNS. Untuk instruksi, lihat [Memulai dengan Amazon SNS di Panduan Pengembang Amazon SNS](#) di Panduan Developer Amazon SNS. Buat topik yang menerima semua alarm CIS, dan buat setidaknya satu langganan ke topik tersebut.
2. Buat CloudTrail jejak yang berlaku untuk semua Wilayah AWS. Untuk petunjuk, lihat [Membuat jejak](#) di Panduan AWS CloudTrail Pengguna.

Catat nama grup CloudWatch log Log yang Anda kaitkan dengan CloudTrail jejak. Anda membuat filter metrik untuk grup log pada langkah berikutnya.

3. Membuat sebuah filter metrik. Untuk petunjuknya, lihat [Membuat filter metrik untuk grup log](#) di Panduan CloudWatch Pengguna Amazon. Gunakan nilai berikut:

Bidang	Nilai
Tentukan pola, Pola filter	<code>{(\$.eventName=CreateCustomerGateway) (\$.eventName>DeleteCustomerGateway) (\$.eventName=AttachInternetGateway) (\$.eventName=CreateInternetGateway) (\$.eventName>DeleteInternetGateway) (\$.eventName=DetachInternetGateway)}</code>
namespace metrik	LogMetrics
Nilai metrik	1
Nilai default	0

4. Buat alarm didasarkan pada filter. Untuk petunjuknya, lihat [Membuat CloudWatch alarm berdasarkan filter metrik grup log](#) di CloudWatch Panduan Pengguna Amazon. Gunakan nilai berikut:

Bidang	Nilai
Kondisi, tipe Ambang	Statis
<i>your-metric-name</i> Kapanpun...	lebih besar/sama
dari...	1

[CloudWatch.13] Pastikan filter metrik log dan alarm ada untuk perubahan tabel rute

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v1.2.0/3.13, Tolok Ukur Yayasan CIS v1.4.0/4.13, Nist.800-171.r2 3.3.1, Nist.800-171.r2 3.13.1, AWS Nist.800-171.r2 3.14.6, Nist.800-171.r2 3.14.7

Kategori: Deteksi > Layanan deteksi

Tingkat keparahan: Rendah

Jenis sumber

daya:AWS::Logs::MetricFilter,AWS::CloudWatch::Alarm,AWS::CloudTrail::Trail,AWS::SNS::Topic

AWS Config aturan: Tidak ada (aturan Security Hub khusus)

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah Anda memantau panggilan API secara real time dengan mengarahkan CloudTrail CloudWatch log ke Log dan membuat filter dan alarm metrik yang sesuai. Tabel routing merutekan lalu lintas jaringan antara subnet dan ke gateway jaringan.

CIS merekomendasikan agar Anda membuat filter metrik dan alarm untuk perubahan pada tabel rute. Memantau perubahan ini membantu memastikan bahwa semua lalu lintas VPC mengalir melalui jalur yang diharapkan.

Note

Ketika Security Hub melakukan pemeriksaan untuk kontrol ini, ia mencari CloudTrail jejak yang digunakan akun saat ini. Jalur ini mungkin merupakan jalur organisasi yang dimiliki oleh akun lain. Jalur Multi-Wilayah juga mungkin berbasis di Wilayah yang berbeda.

Hasil pemeriksaan dalam FAILED temuan dalam kasus-kasus berikut:

- Tidak ada jejak yang dikonfigurasi.
- Jalur yang tersedia yang berada di Wilayah saat ini dan yang dimiliki oleh rekening giro tidak memenuhi persyaratan kontrol.

Hasil pemeriksaan dalam status kontrol NO_DATA dalam kasus berikut:

- Jejak multi-wilayah berbasis di Wilayah yang berbeda. Security Hub hanya dapat menghasilkan temuan di Wilayah tempat jejak itu berada.
- Jejak multi-wilayah milik akun yang berbeda. Security Hub hanya dapat menghasilkan temuan untuk akun yang memiliki jejak.

Kami merekomendasikan jejak organisasi untuk mencatat peristiwa dari banyak akun dalam suatu organisasi. Jejak organisasi adalah jalur Multi-wilayah secara default dan hanya dapat dikelola oleh akun AWS Organizations manajemen atau akun administrator yang CloudTrail didelegasikan. Menggunakan jejak organisasi menghasilkan status kontrol NO_DATA untuk kontrol yang dievaluasi dalam akun anggota organisasi. Di akun anggota, Security Hub hanya menghasilkan temuan untuk sumber daya milik anggota. Temuan yang berkaitan dengan jejak organisasi dihasilkan di akun pemilik sumber daya. Anda dapat melihat temuan ini di akun administrator yang didelegasikan Security Hub menggunakan agregasi lintas wilayah.

Untuk alarm, akun saat ini harus memiliki topik Amazon SNS yang direferensikan, atau harus mendapatkan akses ke topik Amazon SNS dengan menelepon. `ListSubscriptionsByTopic` Jika tidak, Security Hub menghasilkan WARNING temuan untuk kontrol.

Perbaikan

Note

Pola filter yang kami rekomendasikan dalam langkah-langkah remediasi ini berbeda dari pola filter dalam panduan CIS. Filter yang kami rekomendasikan hanya menargetkan peristiwa yang berasal dari panggilan API Amazon Elastic Compute Cloud (EC2).

Untuk melewati kontrol ini, ikuti langkah-langkah berikut untuk membuat topik Amazon SNS, AWS CloudTrail jejak, filter metrik, dan alarm untuk filter metrik.

1. Buat topik Amazon SNS. Untuk instruksi, lihat [Memulai dengan Amazon SNS di Panduan Pengembang Amazon SNS](#) di Panduan Developer Amazon SNS. Buat topik yang menerima semua alarm CIS, dan buat setidaknya satu langganan ke topik tersebut.

2. Buat CloudTrail jejak yang berlaku untuk semua Wilayah AWS. Untuk petunjuk, lihat [Membuat jejak](#) di Panduan AWS CloudTrail Pengguna.

Catat nama grup CloudWatch log Log yang Anda kaitkan dengan CloudTrail jejak. Anda membuat filter metrik untuk grup log pada langkah berikutnya.

3. Membuat sebuah filter metrik. Untuk petunjuknya, lihat [Membuat filter metrik untuk grup log](#) di Panduan CloudWatch Pengguna Amazon. Gunakan nilai berikut:

Bidang	Nilai
Tentukan pola, Pola filter	<code>{ (\$.eventSource=ec2.amazonaws.com) && ((\$.eventName=CreateRoute) (\$.eventName=CreateRouteTable) (\$.eventName=ReplaceRoute) (\$.eventName=ReplaceRouteTableAssociation) (\$.eventName=DeleteRouteTable) (\$.eventName=DeleteRoute) (\$.eventName=DisassociateRouteTable)) }</code>
namespace metrik	LogMetrics
Nilai metrik	1
Nilai default	0

4. Buat alarm didasarkan pada filter. Untuk petunjuknya, lihat [Membuat CloudWatch alarm berdasarkan filter metrik grup log](#) di CloudWatch Panduan Pengguna Amazon. Gunakan nilai berikut:

Bidang	Nilai
Kondisi, tipe Ambang	Statis
<i>your-metric-name</i> Kapanpun...	lebih besar/sama
dari...	1

[CloudWatch.14] Pastikan filter metrik log dan alarm ada untuk perubahan VPC

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v1.2.0/3.14, Tolok Ukur Yayasan CIS v1.4.0/4.14, Nist.800-171.r2 3.3.1, Nist.800-171.r2 3.13.1, AWS Nist.800-171.r2 3.14.6, Nist.800-171.r2 3.14.7

Kategori: Deteksi > Layanan deteksi

Tingkat keparahan: Rendah

Jenis sumber

daya:AWS::Logs::MetricFilter,AWS::CloudWatch::Alarm,AWS::CloudTrail::Trail,AWS::SNS::Topic

AWS Config aturan: Tidak ada (aturan Security Hub khusus)

Jenis jadwal: Periodik

Parameter: Tidak ada

Anda dapat melakukan pemantauan real-time panggilan API dengan mengarahkan CloudTrail CloudWatch log ke Log dan membuat filter dan alarm metrik yang sesuai. Anda dapat memiliki lebih dari satu VPC di akun, dan Anda dapat membuat koneksi peer antara dua VPCs, memungkinkan lalu lintas jaringan untuk rute antara VPCs

CIS merekomendasikan agar Anda membuat filter metrik dan alarm untuk VPCs perubahan. Memantau perubahan ini membantu memastikan bahwa kontrol otentikasi dan otorisasi tetap utuh.

Untuk menjalankan pemeriksaan ini, Security Hub menggunakan logika kustom untuk melakukan langkah-langkah audit yang tepat yang ditentukan untuk kontrol 4.14 di [CIS AWS Foundations Benchmark v1.4.0](#). Kontrol ini gagal jika filter metrik yang tepat yang ditentukan oleh CIS tidak digunakan. Bidang atau istilah tambahan tidak dapat ditambahkan ke filter metrik.

Note

Ketika Security Hub melakukan pemeriksaan untuk kontrol ini, ia mencari CloudTrail jejak yang digunakan akun saat ini. Jalur ini mungkin merupakan jalur organisasi yang dimiliki oleh akun lain. Jalur Multi-Wilayah juga mungkin berbasis di Wilayah yang berbeda.

Hasil pemeriksaan dalam FAILED temuan dalam kasus-kasus berikut:

- Tidak ada jejak yang dikonfigurasi.
- Jalur yang tersedia yang berada di Wilayah saat ini dan yang dimiliki oleh rekening giro tidak memenuhi persyaratan kontrol.

Hasil pemeriksaan dalam status kontrol NO_DATA dalam kasus berikut:

- Jejak multi-wilayah berbasis di Wilayah yang berbeda. Security Hub hanya dapat menghasilkan temuan di Wilayah tempat jejak itu berada.
- Jejak multi-wilayah milik akun yang berbeda. Security Hub hanya dapat menghasilkan temuan untuk akun yang memiliki jejak.

Kami merekomendasikan jejak organisasi untuk mencatat peristiwa dari banyak akun dalam suatu organisasi. Jejak organisasi adalah jalur Multi-wilayah secara default dan hanya dapat dikelola oleh akun AWS Organizations manajemen atau akun administrator yang CloudTrail didelegasikan. Menggunakan jejak organisasi menghasilkan status kontrol NO_DATA untuk kontrol yang dievaluasi dalam akun anggota organisasi. Di akun anggota, Security Hub hanya menghasilkan temuan untuk sumber daya milik anggota. Temuan yang berkaitan dengan jejak organisasi dihasilkan di akun pemilik sumber daya. Anda dapat melihat temuan ini di akun administrator yang didelegasikan Security Hub menggunakan agregasi lintas wilayah.

Untuk alarm, akun saat ini harus memiliki topik Amazon SNS yang direferensikan, atau harus mendapatkan akses ke topik Amazon SNS dengan menelepon. `ListSubscriptionsByTopic` Jika tidak, Security Hub menghasilkan WARNING temuan untuk kontrol.

Perbaikan

Untuk melewati kontrol ini, ikuti langkah-langkah berikut untuk membuat topik Amazon SNS, AWS CloudTrail jejak, filter metrik, dan alarm untuk filter metrik.

1. Buat topik Amazon SNS. Untuk instruksi, lihat [Memulai dengan Amazon SNS di Panduan Pengembang Amazon SNS](#) di Panduan Developer Amazon SNS. Buat topik yang menerima semua alarm CIS, dan buat setidaknya satu langganan ke topik tersebut.
2. Buat CloudTrail jejak yang berlaku untuk semua Wilayah AWS. Untuk petunjuk, lihat [Membuat jejak](#) di Panduan AWS CloudTrail Pengguna.

Catat nama grup CloudWatch log Log yang Anda kaitkan dengan CloudTrail jejak. Anda membuat filter metrik untuk grup log pada langkah berikutnya.

3. Membuat sebuah filter metrik. Untuk petunjuknya, lihat [Membuat filter metrik untuk grup log](#) di Panduan CloudWatch Pengguna Amazon. Gunakan nilai berikut:

Bidang	Nilai
Tentukan pola, Pola filter	<code>{(\$.eventName=CreateVpc) (\$.eventName>DeleteVpc) (\$.eventName=ModifyVpcAttribute) (\$.eventName=AcceptVpcPeeringConnection) (\$.eventName=CreateVpcPeeringConnection) (\$.eventName>DeleteVpcPeeringConnection) (\$.eventName=RejectVpcPeeringConnection) (\$.eventName=AttachClassicLinkVpc) (\$.eventName=DetachClassicLinkVpc) (\$.eventName=DisableVpcClassicLink) (\$.eventName=EnableVpcClassicLink)}</code>
namespace metrik	LogMetrics
Nilai metrik	1
Nilai default	0

4. Buat alarm didasarkan pada filter. Untuk petunjuknya, lihat [Membuat CloudWatch alarm berdasarkan filter metrik grup log](#) di CloudWatch Panduan Pengguna Amazon. Gunakan nilai berikut:

Bidang	Nilai
Kondisi, tipe Ambang	Statis
<i>your-metric-name</i> Kapanpun...	lebih besar/sama

Bidang	Nilai
dari...	1

[CloudWatch.15] CloudWatch alarm harus memiliki tindakan tertentu yang dikonfigurasi

Persyaratan terkait: NIST.800-53.r5 AU-6(1), NIST.800-53.r5 AU-6(5), NIST.800-53.r5 CA-7, Nist.800-53.R5 IR-4 (1), Nist.800-53.R5 IR-4 (5), Nist.800-53.R5 SI-2, Nist.800-53.r5 SI-20, Nist.800-53.R5 SI-4 (12), Nist.800-53.r5 SI-4 (5), Nist.800-53.r5 SI-4 (5), Nist.800-53.r5 00-171.r2 3.3.4, Nist.800-171.r2 3.14.6

Kategori: Deteksi > Layanan deteksi

Tingkat keparahan: Tinggi

Jenis sumber daya: AWS::CloudWatch::Alarm

AWS Config aturan: [cloudwatch-alarm-action-check](#)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
alarmActionRequired	Kontrol menghasilkan PASSED temuan jika parameter disetel ke <code>true</code> dan alarm memiliki tindakan ketika status alarm berubah menjadi ALARM.	Boolean	Tidak dapat disesuaikan	<code>true</code>
insufficientDataActionRequired	Kontrol menghasilkan PASSED temuan jika parameter disetel ke <code>true</code> dan alarm memiliki tindakan ketika status alarm	Boolean	<code>true</code> atau <code>false</code>	<code>false</code>

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
	berubah menjadi INSUFFICIENT_DATA .			
okActionRequired	Kontrol menghasilkan PASSED temuan jika parameter disetel ke true dan alarm memiliki tindakan ketika status alarm berubah menjadi OK.	Boolean	true atau false	false

Kontrol ini memeriksa apakah CloudWatch alarm Amazon memiliki setidaknya satu tindakan yang dikonfigurasi untuk ALARM status. Kontrol gagal jika alarm tidak memiliki tindakan yang dikonfigurasi untuk ALARM status. Secara opsional, Anda dapat menyertakan nilai parameter khusus untuk juga memerlukan tindakan alarm untuk OK status INSUFFICIENT_DATA atau.

Note

Security Hub mengevaluasi kontrol ini berdasarkan alarm CloudWatch metrik. Alarm metrik dapat menjadi bagian dari alarm komposit yang memiliki tindakan yang ditentukan dikonfigurasi. Kontrol menghasilkan FAILED temuan dalam kasus-kasus berikut:

- Tindakan yang ditentukan tidak dikonfigurasi untuk alarm metrik.
- Alarm metrik adalah bagian dari alarm komposit yang memiliki tindakan yang ditentukan dikonfigurasi.

Kontrol ini berfokus pada apakah CloudWatch alarm memiliki tindakan alarm yang dikonfigurasi, sedangkan [CloudWatch.17](#) berfokus pada status aktivasi tindakan CloudWatch alarm.

Kami merekomendasikan tindakan CloudWatch alarm untuk secara otomatis mengingatkan Anda ketika metrik yang dipantau berada di luar ambang batas yang ditentukan. Memantau alarm membantu Anda mengidentifikasi aktivitas yang tidak biasa dan dengan cepat menanggapi masalah keamanan dan operasional ketika alarm masuk ke keadaan tertentu. Jenis tindakan alarm yang paling umum adalah memberi tahu satu atau lebih pengguna dengan mengirim pesan ke topik Amazon SNS (Amazon SNS).

Perbaikan

Untuk informasi tentang tindakan yang didukung oleh CloudWatch alarm, lihat [Tindakan alarm](#) di Panduan CloudWatch Pengguna Amazon.

[CloudWatch.16] grup CloudWatch log harus dipertahankan untuk jangka waktu tertentu

Kategori: Identifikasi > Logging

Persyaratan terkait: NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-11, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, NIST.800-53.R5 SI-12

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::Logs::LogGroup

AWS Config aturan: [cw-loggroup-retention-period-check](#)

Jenis jadwal: Periodik

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub	
minRetentionTime	Periode retensi minimum dalam beberapa hari untuk grup CloudWatch log	Enum	365, 400, 545, 731, 1827, 3653	365	

Kontrol ini memeriksa apakah grup CloudWatch log Amazon memiliki periode retensi setidaknya dalam jumlah hari yang ditentukan. Kontrol gagal jika periode retensi kurang dari jumlah yang ditentukan. Kecuali Anda memberikan nilai parameter khusus untuk periode retensi, Security Hub menggunakan nilai default 365 hari.

CloudWatch Logs memusatkan log dari semua sistem, aplikasi, dan Layanan AWS dalam satu layanan yang sangat dapat diskalakan. Anda dapat menggunakan CloudWatch Logs untuk memantau, menyimpan, dan mengakses berkas log dari instans Amazon Elastic Compute Cloud (EC2), AWS CloudTrail Amazon Route 53, dan sumber lain. Mempertahankan log Anda setidaknya selama 1 tahun dapat membantu Anda mematuhi standar penyimpanan log.

Perbaikan

Untuk mengonfigurasi setelan penyimpanan [log](#), lihat [Mengubah penyimpanan data CloudWatch log di Log](#) di Panduan CloudWatch Pengguna Amazon.

[CloudWatch.17] tindakan CloudWatch alarm harus diaktifkan

Kategori: Deteksi > Layanan deteksi

Persyaratan terkait: NIST.800-53.r5 AU-6(1), NIST.800-53.r5 AU-6(5), NIST.800-53.r5 CA-7, NIST.800-53.R5 SI-2, NIST.800-53.R5 SI-4 (12)

Tingkat keparahan: Tinggi

Jenis sumber daya: AWS::CloudWatch::Alarm

AWS Config aturan: [cloudwatch-alarm-action-enabled-check](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah tindakan CloudWatch alarm diaktifkan (ActionEnabled harus disetel ke true). Kontrol gagal jika tindakan alarm untuk CloudWatch alarm dinonaktifkan.

Note

Security Hub mengevaluasi kontrol ini berdasarkan alarm CloudWatch metrik. Alarm metrik dapat menjadi bagian dari alarm komposit yang mengaktifkan tindakan alarm. Kontrol menghasilkan FAILED temuan dalam kasus-kasus berikut:

- Tindakan yang ditentukan tidak dikonfigurasi untuk alarm metrik.
- Alarm metrik adalah bagian dari alarm komposit yang mengaktifkan tindakan alarm.

Kontrol ini berfokus pada status aktivasi tindakan CloudWatch alarm, sedangkan [CloudWatch.15](#) berfokus pada apakah ALARM tindakan apa pun dikonfigurasi dalam CloudWatch alarm.

Tindakan alarm secara otomatis mengingatkan Anda ketika metrik yang dipantau berada di luar ambang batas yang ditentukan. Jika tindakan alarm dinonaktifkan, tidak ada tindakan yang dijalankan saat alarm berubah status, dan Anda tidak akan diberitahu tentang perubahan dalam metrik yang dipantau. Sebaiknya aktifkan tindakan CloudWatch alarm untuk membantu Anda merespons masalah keamanan dan operasional dengan cepat.

Perbaikan

Untuk mengaktifkan aksi CloudWatch alarm (konsol)

1. Buka CloudWatch konsol di <https://console.aws.amazon.com/cloudwatch/>.
2. Di panel navigasi, di bawah Alarm, pilih Semua alarm.
3. Pilih alarm yang ingin Anda aktifkan tindakan.
4. Untuk Tindakan, pilih Tindakan alarm — baru, lalu pilih Aktifkan.

Untuk informasi selengkapnya tentang mengaktifkan tindakan CloudWatch alarm, lihat [Tindakan alarm](#) di Panduan CloudWatch Pengguna Amazon.

Kontrol Security Hub untuk CodeArtifact

Kontrol Security Hub ini mengevaluasi AWS CodeArtifact layanan dan sumber daya.

Kontrol ini mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat [Ketersediaan kontrol berdasarkan Wilayah](#).

[CodeArtifact.1] CodeArtifact repositori harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::CodeArtifact::Repository`

AWS Config aturan: `tagged-codeartifact-repository` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
<code>requiredTagKeys</code>	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS .	Tidak ada nilai default

Kontrol ini memeriksa apakah AWS CodeArtifact repositori memiliki tag dengan kunci tertentu yang ditentukan dalam parameter. `requiredTagKeys` Kontrol gagal jika repositori tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter. `requiredTagKeys` Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika repositori tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat [Untuk apa ABAC? AWS](#) di Panduan Pengguna IAM.

Note

Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat [Menandai AWS sumber daya Anda](#) di Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke CodeArtifact repositori, lihat [Tag repositori CodeArtifact di Panduan Pengguna](#).AWS CodeArtifact

Kontrol Security Hub untuk CodeBuild

Kontrol Security Hub ini mengevaluasi AWS CodeBuild layanan dan sumber daya.

Kontrol ini mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat [Ketersediaan kontrol berdasarkan Wilayah](#).

[CodeBuild.1] Repositori sumber CodeBuild Bitbucket tidak URLs boleh berisi kredensial sensitif

Persyaratan terkait: NIST.800-53.r5 SA-3, PCI DSS v3.2.1/8.2.1, PCI DSS v4.0.1/8.3.2

Kategori: Lindungi > Pengembangan aman

Tingkat keparahan: Kritis

Jenis sumber daya: `AWS::CodeBuild::Project`

AWS Config aturan: [codebuild-project-source-repo-url-check](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah URL repositori sumber Bitbucket AWS CodeBuild proyek berisi token akses pribadi atau nama pengguna dan kata sandi. Kontrol gagal jika URL repositori sumber Bitbucket berisi token akses pribadi atau nama pengguna dan kata sandi.

Note

Kontrol ini mengevaluasi sumber primer dan sumber sekunder dari proyek CodeBuild pembangunan. Untuk informasi selengkapnya tentang sumber proyek, lihat [Beberapa sumber input dan sampel artefak keluaran](#) di Panduan AWS CodeBuild Pengguna.

Kredensi login tidak boleh disimpan atau ditransmisikan dalam teks yang jelas atau muncul di URL repositori sumber. Alih-alih token akses pribadi atau kredensial masuk, Anda harus mengakses

penyedia sumber Anda CodeBuild, dan mengubah URL repositori sumber Anda agar hanya berisi jalur ke lokasi repositori Bitbucket. Menggunakan token akses pribadi atau kredensi masuk dapat mengakibatkan paparan data yang tidak diinginkan atau akses yang tidak sah.

Remediasi

Anda dapat memperbarui CodeBuild proyek Anda untuk digunakan OAuth.

Untuk menghapus otentikasi dasar/(GitHub) Token Akses Pribadi dari sumber CodeBuild proyek

1. Buka CodeBuild konsol di <https://console.aws.amazon.com/codebuild/>.
2. Pilih proyek build yang berisi token akses pribadi atau nama pengguna dan kata sandi.
3. Dari Edit, pilih Sumber.
4. Pilih Putuskan sambungan GitHub dari/Bitbucket.
5. Pilih Connect menggunakan OAuth, lalu pilih Connect to GitHub/Bitbucket.
6. Saat diminta, pilih otorisasi yang sesuai.
7. Konfigurasi ulang URL repositori Anda dan pengaturan konfigurasi tambahan, sesuai kebutuhan.
8. Pilih Perbarui sumber.

Untuk informasi selengkapnya, lihat [CodeBuild menggunakan sampel berbasis kasus](#) di AWS CodeBuild Panduan Pengguna.

[CodeBuild.2] variabel lingkungan CodeBuild proyek tidak boleh berisi kredensial teks yang jelas

Persyaratan terkait: NIST.800-53.r5 IA-5 (7),, PCI DSS v3.2.1/8.2.1 NIST.800-53.r5 SA-3, PCI DSS v4.0.1/8.3.2

Kategori: Lindungi > Pengembangan aman

Tingkat keparahan: Kritis

Jenis sumber daya: AWS::CodeBuild::Project

AWS Config aturan: [codebuild-project-envvar-awscred-check](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah proyek berisi variabel lingkungan `AWS_ACCESS_KEY_ID` dan `AWS_SECRET_ACCESS_KEY`.

Kredensi otentikasi `AWS_ACCESS_KEY_ID` dan tidak `AWS_SECRET_ACCESS_KEY` boleh disimpan dalam teks yang jelas, karena ini dapat menyebabkan paparan data yang tidak diinginkan dan akses yang tidak sah.

Remediasi

Untuk menghapus variabel lingkungan dari CodeBuild proyek, lihat [Mengubah setelan proyek build AWS CodeBuild di Panduan AWS CodeBuild Pengguna](#). Pastikan tidak ada yang dipilih untuk variabel Lingkungan.

Anda dapat menyimpan variabel lingkungan dengan nilai sensitif di AWS Systems Manager Parameter Store atau AWS Secrets Manager kemudian mengambilnya dari spesifikasi build. Untuk petunjuk, lihat kotak berlabel Penting di [bagian Lingkungan](#) di Panduan AWS CodeBuild Pengguna.

[CodeBuild.3] Log CodeBuild S3 harus dienkrpsi

Persyaratan terkait: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-1 3, 8, NIST.800-53.r5 SC-2 8 (1), NIST.800-53.R5 NIST.800-53.r5 SC-2 SI-7 (6), PCI DSS v4.0.1/10.3.2

Kategori: Lindungi > Perlindungan Data > Enkripsi data-at-rest

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::CodeBuild::Project`

AWS Config aturan: [codebuild-project-s3-logs-encrypted](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah log Amazon S3 untuk AWS CodeBuild proyek dienkrpsi. Kontrol gagal jika enkripsi dinonaktifkan untuk log S3 untuk sebuah CodeBuild proyek.

Enkripsi data saat istirahat adalah praktik terbaik yang disarankan untuk menambahkan lapisan manajemen akses di sekitar data Anda. Mengenkripsi log saat istirahat mengurangi risiko bahwa pengguna yang tidak diautentikasi oleh AWS akan mengakses data yang disimpan pada disk. Ini

menambahkan satu set kontrol akses untuk membatasi kemampuan pengguna yang tidak sah untuk mengakses data.

Remediasi

Untuk mengubah setelan enkripsi log S3 CodeBuild proyek, lihat [Mengubah setelan proyek build AWS CodeBuild di](#) Panduan AWS CodeBuild Pengguna.

[CodeBuild.4] lingkungan CodeBuild proyek harus memiliki urasi logging AWS Config

Persyaratan terkait: NIST.800-53.r5 AC-2 (12), (4), NIST.800-53.r5 AC-2 (26), (9),, NIST.800-53.r5 AC-4 (9), NIST.800-53.r5 AC-6 Nist.800-53.R5 SI-3 NIST.800-53.r5 SC-7 (8) NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 AU-9(7), NIST.800-53.r5 CA-7, Nist.800-53.R5 SI-4, Nist.800-53.R5 SI-4 (20), NIST.800-53.R5 SI-7 (8)

Kategori: Identifikasi > Logging

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::CodeBuild::Project

AWS Config aturan: [codebuild-project-logging-enabled](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah lingkungan CodeBuild proyek memiliki setidaknya satu opsi log, baik untuk S3 atau CloudWatch log diaktifkan. Kontrol ini gagal jika lingkungan CodeBuild proyek tidak memiliki setidaknya satu opsi log diaktifkan.

Dari perspektif keamanan, logging adalah fitur penting untuk memungkinkan upaya forensik masa depan dalam kasus insiden keamanan apa pun. Mengkorelasikan anomali dalam CodeBuild proyek dengan deteksi ancaman dapat meningkatkan kepercayaan pada keakuratan deteksi ancaman tersebut.

Remediasi

Untuk informasi selengkapnya tentang cara mengonfigurasi setelan log CodeBuild proyek, lihat [Membuat proyek build \(konsol\)](#) di Panduan CodeBuild Pengguna.

[CodeBuild.5] lingkungan CodeBuild proyek seharusnya tidak mengaktifkan mode istimewa

⚠ Important

Security Hub menghentikan kontrol ini pada April 2024. Untuk informasi selengkapnya, lihat [Ubah log untuk kontrol CSPM Security Hub](#).

Persyaratan terkait: NIST.800-53.r5 AC-2 (1) NIST.800-53.r5 AC-3,, NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-5, NIST.800-53.r5 AC-6, NIST.800-53.r5 AC-6 (10), NIST.800-53.r5 AC-6 (2)

Kategori: Lindungi > Manajemen Akses Aman

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::CodeBuild::Project`

AWS Config aturan: [codebuild-project-environment-privileged-check](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah lingkungan AWS CodeBuild proyek memiliki mode istimewa yang diaktifkan atau dinonaktifkan. Kontrol gagal jika lingkungan CodeBuild proyek memiliki mode istimewa diaktifkan.

Secara default, kontainer Docker tidak mengizinkan akses ke perangkat apa pun. Mode istimewa memberikan akses container Docker proyek build ke semua perangkat. Pengaturan `privilegedMode` dengan nilai `true` memungkinkan daemon Docker berjalan di dalam wadah Docker. Daemon Docker mendengarkan permintaan API Docker dan mengelola objek Docker seperti gambar, wadah, jaringan, dan volume. Parameter ini hanya boleh disetel ke `true` jika proyek build digunakan untuk membangun image Docker. Jika tidak, pengaturan ini harus dinonaktifkan untuk mencegah akses yang tidak diinginkan ke Docker APIs serta perangkat keras yang mendasarinya. Pengaturan `privilegedMode` untuk `false` membantu melindungi sumber daya penting dari gangguan dan penghapusan.

Remediasi

Untuk mengonfigurasi pengaturan lingkungan CodeBuild proyek, lihat [Membuat proyek build \(konsol\)](#) di Panduan CodeBuild Pengguna. Di bagian Lingkungan, jangan pilih pengaturan Privileged.

[CodeBuild.7] ekspor kelompok CodeBuild laporan harus dienkripsi saat istirahat

Kategori: Lindungi > Perlindungan Data > Enkripsi data-at-rest

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::CodeBuild::ReportGroup`

AWS Config aturan: [codebuild-report-group-encrypted-at-rest](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah hasil pengujian grup AWS CodeBuild laporan yang diekspor ke bucket Amazon Simple Storage Service (Amazon S3) dienkripsi saat istirahat. Kontrol gagal jika ekspor grup laporan tidak dienkripsi saat istirahat.

Data saat istirahat mengacu pada data yang disimpan dalam penyimpanan persisten dan tidak mudah menguap untuk durasi berapa pun. Mengenkripsi data saat istirahat membantu Anda melindungi kerahasiaannya, yang mengurangi risiko bahwa pengguna yang tidak sah dapat mengaksesnya.

Remediasi

Untuk mengenkripsi ekspor grup laporan ke S3, lihat [Memperbarui grup laporan](#) di AWS CodeBuild Panduan Pengguna.

Kontrol Security Hub untuk Amazon CodeGuru Profiler

Kontrol Security Hub ini mengevaluasi layanan dan sumber daya Amazon CodeGuru Profiler.

Kontrol ini mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat [Ketersediaan kontrol berdasarkan Wilayah](#).

[CodeGuruProfiler.1] Grup CodeGuru profil profiler harus diberi tag

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::CodeGuruProfiler::ProfilingGroup`

AWS Config aturan: `codeguruprofiler-profiling-group-tagged`

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
<code>requiredKeyTags</code>	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS .	Tidak ada nilai default

Kontrol ini memeriksa apakah grup CodeGuru profil Amazon Profiler memiliki tag dengan kunci tertentu yang ditentukan dalam parameter `requiredKeyTags`. Kontrol gagal jika grup profil tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter `requiredKeyTags`. Jika parameter `requiredKeyTags` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika grup profil tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat [Menentukan izin berdasarkan atribut dengan otorisasi ABAC di Panduan Pengguna IAM](#).

Note

Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk mengetahui praktik terbaik penandaan lainnya, lihat [Praktik dan strategi terbaik](#) di Panduan Pengguna AWS Sumber Daya Penandaan dan Editor Tag.

Remediasi

Untuk menambahkan tag ke grup CodeGuru profil Profiler, lihat [Menandai grup profil di](#) Panduan Pengguna Amazon CodeGuru Profiler.

Kontrol Security Hub untuk Amazon CodeGuru Reviewer

Kontrol Security Hub ini mengevaluasi layanan dan sumber daya Amazon CodeGuru Reviewer.

Kontrol ini mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat [Ketersediaan kontrol berdasarkan Wilayah](#).

[CodeGuruReviewer.1] Asosiasi CodeGuru repositori peninjau harus diberi tag

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::CodeGuruReviewer::RepositoryAssociation`

AWS Config aturan: `codegurureviewer-repository-association-tagged`

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
<code>requiredKeyTags</code>	Daftar kunci tag non-sistem yang harus berisi sumber daya	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi	Tidak ada nilai default

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
	yang dievaluasi. Kunci tag peka huruf besar dan kecil.		persyaratan AWS .	

Kontrol ini memeriksa apakah asosiasi CodeGuru repositori Amazon Reviewer memiliki tag dengan kunci tertentu yang ditentukan dalam parameter. `requiredKeyTags` Kontrol gagal jika asosiasi repositori tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter. `requiredKeyTags` Jika parameter `requiredKeyTags` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika asosiasi repositori tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat [Menentukan izin berdasarkan atribut dengan otorisasi ABAC di Panduan Pengguna IAM](#).

Note

Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk mengetahui praktik terbaik penandaan lainnya, lihat [Praktik dan strategi terbaik di Panduan Pengguna AWS Sumber Daya Penandaan dan Editor Tag](#).

Remediasi

Untuk menambahkan tag ke asosiasi CodeGuru repositori Reviewer, lihat [Menandai asosiasi repositori di Panduan Pengguna Amazon Reviewer](#). CodeGuru

Kontrol Security Hub untuk Amazon Cognito

AWS Security Hub Kontrol ini mengevaluasi layanan dan sumber daya Amazon Cognito. Kontrol mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat [Ketersediaan kontrol berdasarkan Wilayah](#).

[Cognito.1] Kumpulan pengguna Cognito harus mengaktifkan perlindungan ancaman dengan mode penegakan fungsi penuh untuk otentikasi standar

Kategori: Lindungi > Manajemen akses yang aman

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::Cognito::UserPool

AWS Config aturan: [cognito-user-pool-advanced-security-enabled](#)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
SecurityMode	Mode penegakan perlindungan ancaman yang diperiksa oleh kontrol.	String	AUDIT, ENFORCED	ENFORCED

Kontrol ini memeriksa apakah kumpulan pengguna Amazon Cognito memiliki perlindungan ancaman yang diaktifkan dengan mode penegakan yang disetel ke fungsi penuh untuk otentikasi standar. Kontrol gagal jika kumpulan pengguna menonaktifkan perlindungan ancaman atau jika mode penegakan tidak disetel ke fungsi penuh untuk otentikasi standar. Kecuali Anda memberikan nilai parameter khusus, Security Hub menggunakan nilai default ENFORCED untuk mode penegakan yang disetel ke fungsi penuh untuk otentikasi standar.

Setelah membuat kumpulan pengguna Amazon Cognito, Anda dapat mengaktifkan perlindungan ancaman dan menyesuaikan tindakan yang diambil sebagai respons terhadap berbagai risiko. Atau, Anda dapat menggunakan mode audit untuk mengumpulkan metrik risiko yang terdeteksi tanpa

menerapkan mitigasi keamanan apa pun. Dalam mode audit, perlindungan ancaman menerbitkan metrik ke Amazon. CloudWatch Anda dapat melihat metrik setelah Amazon Cognito menghasilkan acara pertamanya.

Remediasi

Untuk informasi tentang mengaktifkan perlindungan ancaman untuk kumpulan pengguna Amazon Cognito, [lihat Keamanan lanjutan dengan perlindungan ancaman](#) di Panduan Pengembang Amazon Cognito.

Kontrol Security Hub untuk AWS Config

Kontrol Security Hub ini mengevaluasi AWS Config layanan dan sumber daya.

Kontrol ini mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat [Ketersediaan kontrol berdasarkan Wilayah](#).

[Config.1] AWS Config harus diaktifkan dan menggunakan peran terkait layanan untuk perekaman sumber daya

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v1.2.0/2.5, Tolok Ukur Yayasan CIS v1.4.0/3.5, Tolok Ukur AWS Yayasan CIS v3.0.0/3.3, NIST.800-53.R5 CM-3, NIST.800-53.r5 AWS CM-6 (1), NIST.800-53.R5 CM-8 (2), PCI DSS v3.2.1/10.5.2, PCI DSS v3.2.1/11.5

Kategori: Identifikasi > Inventaris

Tingkat keparahan: Kritis

Jenis sumber daya: AWS :: : Account

AWS Config aturan: Tidak ada (aturan Security Hub khusus)

Jenis jadwal: Periodik

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
includeConfigService	Kontrol tidak mengevaluasi apakah AWS Config	Boolean	true atau false	true

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
ceLinkedRoleCheck	menggunakan peran terkait layanan jika parameter disetel ke. false			

Kontrol ini memeriksa apakah AWS Config diaktifkan di akun Anda saat ini Wilayah AWS, mencatat semua sumber daya yang sesuai dengan kontrol yang diaktifkan di Wilayah saat ini, dan menggunakan peran [terkait layanan AWS Config](#). Nama peran terkait layanan adalah. AWSServiceRoleForConfig Jika Anda tidak menggunakan peran terkait layanan dan tidak menyetel `includeConfigServiceLinkedRoleCheck` parameternya `false`, kontrol gagal karena peran lain mungkin tidak memiliki izin yang diperlukan AWS Config untuk merekam sumber daya Anda secara akurat.

AWS Config Layanan ini melakukan manajemen konfigurasi AWS sumber daya yang didukung di akun Anda dan mengirimkan file log kepada Anda. Informasi yang direkam mencakup item konfigurasi (AWS sumber daya), hubungan antara item konfigurasi, dan perubahan konfigurasi apa pun dalam sumber daya. Sumber daya global adalah sumber daya yang tersedia di Wilayah mana pun.

Kontrol dievaluasi sebagai berikut:

- Jika Wilayah saat ini ditetapkan sebagai [Wilayah agregasi](#) Anda, kontrol menghasilkan PASSED temuan hanya jika sumber daya global AWS Identity and Access Management (IAM) direkam (jika Anda telah mengaktifkan kontrol yang memerlukannya).
- Jika Wilayah saat ini ditetapkan sebagai Wilayah tertaut, kontrol tidak mengevaluasi apakah sumber daya global IAM dicatat.
- Jika Wilayah saat ini tidak ada dalam agregator Anda, atau jika agregasi lintas wilayah tidak diatur di akun Anda, kontrol akan menghasilkan PASSED temuan hanya jika sumber daya global IAM direkam (jika Anda telah mengaktifkan kontrol yang memerlukannya).

Hasil kontrol tidak terpengaruh oleh apakah Anda memilih pencatatan harian atau terus menerus dari perubahan status sumber daya di AWS Config. Namun, hasil kontrol ini dapat berubah ketika kontrol baru dirilis jika Anda telah mengonfigurasi pengaktifan otomatis kontrol baru atau memiliki kebijakan konfigurasi pusat yang secara otomatis mengaktifkan kontrol baru. Dalam kasus ini, jika Anda tidak

merekam semua sumber daya, Anda harus mengonfigurasi rekaman untuk sumber daya yang terkait dengan kontrol baru untuk menerima PASSED temuan.

Pemeriksaan keamanan Security Hub berfungsi sebagaimana dimaksud hanya jika Anda mengaktifkan AWS Config di semua Wilayah dan mengonfigurasi perekaman sumber daya untuk kontrol yang memerlukannya.

Note

Config.1 mengharuskan itu AWS Config diaktifkan di semua Wilayah tempat Anda menggunakan Security Hub.

Karena Security Hub adalah layanan Regional, pemeriksaan yang dilakukan untuk kontrol ini hanya mengevaluasi Wilayah saat ini untuk akun tersebut.

Untuk mengizinkan pemeriksaan keamanan terhadap sumber daya global IAM di suatu Wilayah, Anda harus mencatat sumber daya global IAM di Wilayah tersebut. Wilayah yang tidak memiliki sumber daya global IAM yang direkam akan menerima PASSED temuan default untuk kontrol yang memeriksa sumber daya global IAM. Karena sumber daya global IAM identik Wilayah AWS, kami sarankan Anda merekam sumber daya global IAM hanya di Wilayah asal (jika agregasi lintas wilayah diaktifkan di akun Anda). Sumber daya IAM hanya akan direkam di Wilayah di mana perekaman sumber daya global dihidupkan.

Jenis sumber daya yang direkam secara global IAM yang AWS Config mendukung adalah pengguna IAM, grup, peran, dan kebijakan yang dikelola pelanggan. Anda dapat mempertimbangkan untuk menonaktifkan kontrol Security Hub yang memeriksa jenis sumber daya ini di Wilayah tempat perekaman sumber daya global dinonaktifkan. Untuk informasi selengkapnya, lihat [Kontrol yang disarankan untuk dinonaktifkan di CSPM Security Hub](#).

Remediasi

Di Wilayah dan Wilayah asal yang bukan merupakan bagian dari agregator, catat semua sumber daya yang diperlukan untuk kontrol yang diaktifkan di Wilayah saat ini, termasuk sumber daya global IAM jika Anda telah mengaktifkan kontrol yang memerlukan sumber daya global IAM.

Di Wilayah tertaut, Anda dapat menggunakan mode AWS Config perekaman apa pun, selama Anda merekam semua sumber daya yang sesuai dengan kontrol yang diaktifkan di Wilayah saat ini. Di Wilayah tertaut, jika Anda telah mengaktifkan kontrol yang memerlukan perekaman sumber daya global IAM, Anda tidak akan menerima FAILED temuan (rekaman sumber daya lainnya sudah cukup).

StatusReasonsBidang dalam Compliance objek temuan Anda dapat membantu Anda menentukan mengapa Anda memiliki temuan yang gagal untuk kontrol ini. Untuk informasi selengkapnya, lihat [Detail kepatuhan untuk temuan kontrol](#).

Untuk daftar sumber daya mana yang harus direkam untuk setiap kontrol, lihat [AWS Config Sumber daya yang diperlukan untuk temuan kontrol](#). Untuk informasi umum tentang mengaktifkan AWS Config dan mengonfigurasi perekaman sumber daya, lihat [Mengaktifkan dan mengonfigurasi AWS Config untuk Security Hub CSPM](#).

Kontrol Security Hub untuk Amazon Connect

Kontrol Security Hub ini mengevaluasi layanan dan sumber daya Amazon Connect.

Kontrol ini mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat [Ketersediaan kontrol berdasarkan Wilayah](#).

[Connect.1] Jenis objek Amazon Connect Customer Profiles harus diberi tag

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::CustomerProfiles::ObjectType`

AWS Config aturan: `customerprofiles-object-type-tagged`

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
<code>requiredKeyTags</code>	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS .	Tidak ada nilai default

Kontrol ini memeriksa apakah jenis objek Amazon Connect Customer Profiles memiliki tag dengan kunci spesifik yang ditentukan dalam parameter `requiredKeyTags`. Kontrol gagal jika jenis objek tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter `requiredKeyTags`. Jika parameter `requiredKeyTags` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika jenis objek tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws :`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat [Menentukan izin berdasarkan atribut dengan otorisasi ABAC di Panduan Pengguna IAM](#).

Note

Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk mengetahui praktik terbaik penandaan lainnya, lihat [Praktik dan strategi terbaik di Panduan Pengguna AWS Sumber Daya Penandaan dan Editor Tag](#).

Remediasi

Untuk menambahkan tag ke jenis objek Profil Pelanggan, lihat [Menambahkan tag ke sumber daya di Amazon Connect](#) di Panduan Administrator Amazon Connect.

[Connect.2] Instans Amazon Connect seharusnya mengaktifkan logging CloudWatch

Kategori: Identifikasi > Logging

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::Connect::Instance`

AWS Config aturan: [connect-instance-logging-enabled](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah instans Amazon Connect dikonfigurasi untuk membuat dan menyimpan log aliran dalam grup CloudWatch log Amazon. Kontrol gagal jika instans Amazon Connect tidak dikonfigurasi untuk membuat dan menyimpan log aliran dalam grup CloudWatch log.

Log alur Amazon Connect memberikan detail real-time tentang peristiwa di alur Amazon Connect. Alur mendefinisikan pengalaman pelanggan dengan pusat kontak Amazon Connect dari awal hingga akhir. Secara default, saat Anda membuat instans Amazon Connect baru, grup CloudWatch log Amazon dibuat secara otomatis untuk menyimpan log alur untuk instance tersebut. Log aliran dapat membantu Anda menganalisis alur, menemukan kesalahan, dan memantau metrik operasional. Anda juga dapat mengatur peringatan untuk peristiwa tertentu yang dapat terjadi dalam alur.

Remediasi

Untuk informasi tentang mengaktifkan log alur untuk instans Amazon Connect, lihat [Mengaktifkan log aliran Amazon Connect di grup CloudWatch log Amazon](#) di Panduan Administrator Amazon Connect.

Kontrol Security Hub untuk Amazon Data Firehose

Kontrol Security Hub ini mengevaluasi layanan dan sumber daya Amazon Data Firehose.

Kontrol ini mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat [Ketersediaan kontrol berdasarkan Wilayah](#).

[DataFirehose.1] Aliran pengiriman Firehose harus dienkrpsi saat istirahat

Persyaratan terkait: NIST.800-53.r5 AC-3, NIST.800-53.r5 AU-3, NIST.800-53.r5 SC-1 2, NIST.800-53.r5 SC-1 3, NIST.800-53.r5 SC-2 8

Kategori: Lindungi > Perlindungan Data > Enkripsi data-at-rest

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::KinesisFirehose::DeliveryStream

AWS Config aturan: [kinesis-firehose-delivery-stream-encrypted](#)

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah aliran pengiriman Amazon Data Firehose dienkripsi saat istirahat dengan enkripsi sisi server. Kontrol ini gagal jika aliran pengiriman Firehose tidak dienkripsi saat istirahat dengan enkripsi sisi server.

Enkripsi sisi server adalah fitur dalam aliran pengiriman Amazon Data Firehose yang secara otomatis mengenkripsi data sebelum diam dengan menggunakan kunci yang dibuat di (). AWS Key Management Service AWS KMS Data dienkripsi sebelum ditulis ke lapisan penyimpanan aliran Firehose Data, dan didekripsi setelah diambil dari penyimpanan. Ini memungkinkan Anda untuk mematuhi persyaratan peraturan dan meningkatkan keamanan data Anda.

Remediasi

Untuk mengaktifkan enkripsi sisi server pada aliran pengiriman Firehose, lihat Perlindungan Data di Amazon Data Firehose [di Panduan Pengembang Amazon Data Firehose](#).

Kontrol Security Hub untuk AWS DataSync

Kontrol Security Hub ini mengevaluasi AWS DataSync layanan dan sumber daya. Kontrol mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat [Ketersediaan kontrol berdasarkan Wilayah](#).

[DataSync.1] DataSync tugas harus mengaktifkan logging

Kategori: Identifikasi > Logging

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::DataSync::Task

AWS Config aturan: [datasync-task-logging-enabled](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah AWS DataSync tugas telah mengaktifkan pencatatan. Kontrol gagal jika tugas tidak mengaktifkan logging.

Log audit melacak dan memantau aktivitas sistem. Mereka menyediakan catatan peristiwa yang dapat membantu Anda mendeteksi pelanggaran keamanan, menyelidiki insiden, dan mematuhi peraturan. Log audit juga meningkatkan akuntabilitas dan transparansi organisasi Anda secara keseluruhan.

Remediasi

Untuk informasi tentang mengonfigurasi pencatatan AWS DataSync tugas, lihat [Memantau transfer data dengan CloudWatch Log Amazon](#) di Panduan AWS DataSync Pengguna.

[DataSync.2] DataSync tugas harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: AWS::DataSync::Task

AWS Config aturan: [datasync-task-tagged](#)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
<code>requiredKeyTags</code>	Daftar kunci tag non-sistem yang harus ditetapkan ke sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS	Tidak ada nilai default

Kontrol ini memeriksa apakah AWS DataSync tugas memiliki kunci tag yang ditentukan oleh `requiredKeyTags` parameter. Kontrol gagal jika tugas tidak memiliki kunci tag, atau tidak memiliki semua kunci yang ditentukan oleh `requiredKeyTags` parameter. Jika Anda tidak menentukan nilai apa pun untuk `requiredKeyTags` parameter, kontrol hanya memeriksa keberadaan kunci tag dan

gagal jika tugas tidak memiliki kunci tag. Kontrol mengabaikan tag sistem, yang diterapkan secara otomatis dan memiliki aws : awalan.

Tag adalah label yang Anda buat dan tetapkan ke AWS sumber daya. Setiap tanda terdiri dari kunci tanda yang diperlukan dan nilai tanda opsional. Anda dapat menggunakan tag untuk mengkategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Mereka dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Mereka juga dapat membantu Anda melacak pemilik sumber daya untuk tindakan dan pemberitahuan. Anda juga dapat menggunakan tag untuk menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi. Untuk informasi selengkapnya tentang strategi ABAC, lihat [Menentukan izin berdasarkan atribut dengan otorisasi ABAC](#) di Panduan Pengguna IAM. Untuk informasi selengkapnya tentang tag, lihat [Panduan Pengguna AWS Sumber Daya Penandaan dan Editor Tag](#).

Note

Jangan menyimpan informasi pengenalan pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses dari banyak orang Layanan AWS. Mereka tidak dimaksudkan untuk digunakan untuk data pribadi atau sensitif.

Remediasi

Untuk informasi tentang menambahkan tag ke AWS DataSync tugas, lihat [Menandai AWS DataSync tugas Anda](#) di Panduan AWS DataSync Pengguna.

Kontrol Security Hub untuk Amazon Detective

AWS Security Hub Kontrol ini mengevaluasi layanan dan sumber daya Detektif Amazon. Kontrol mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat [Ketersediaan kontrol berdasarkan Wilayah](#).

[Detective.1] Grafik perilaku detektif harus diberi tag

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: AWS::Detective::Graph

AWS Config aturan: tagged-detective-graph (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
<code>requiredTagKeys</code>	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS.	No default value

Kontrol ini memeriksa apakah grafik perilaku Detektif Amazon memiliki tag dengan kunci tertentu yang ditentukan dalam parameter. `requiredTagKeys` Kontrol gagal jika grafik perilaku tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter `requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika grafik perilaku tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat [Untuk apa ABAC? AWS](#) di Panduan Pengguna IAM.

Note

Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS

Billing. Untuk praktik terbaik penandaan lainnya, lihat [Menandai AWS sumber daya Anda](#) di Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke grafik perilaku Detektif, lihat [Menambahkan tag ke grafik perilaku](#) di Panduan Administrasi Detektif Amazon.

Kontrol Security Hub untuk AWS DMS

Kontrol Security Hub ini mengevaluasi AWS Database Migration Service (AWS DMS) layanan dan sumber daya.

Kontrol ini mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat [Ketersediaan kontrol berdasarkan Wilayah](#).

[DMS.1] Instans replikasi Layanan Migrasi Database tidak boleh bersifat publik

Persyaratan terkait: NIST.800-53.r5 AC-2 1,, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-3,, (21),, NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (11), (16) NIST.800-53.r5 AC-6, (20) NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), (4), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SC-7 PCI DSS v3.2.1/1.2.1, NIST.800-53.r5 SC-7 PCI DSS v3.2.1/1.3.1, PCI DSS v3.2.1/1.3.4, PCI DSS v3.2.1/1.3.2, PCI DSS v3.2.1/1.3.6, PCI DSS v4.0.1/1.4.4 NIST.800-53.r5 SC-7

Kategori: Lindungi > Konfigurasi jaringan aman

Tingkat keparahan: Kritis

Jenis sumber daya: AWS::DMS::ReplicationInstance

AWS Config aturan: [dms-replication-not-public](#)

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah instance AWS DMS replikasi bersifat publik. Untuk melakukan ini, ia memeriksa nilai PubliclyAccessible bidang.

Instance replikasi pribadi memiliki alamat IP pribadi yang tidak dapat Anda akses di luar jaringan replikasi. Sebuah contoh replikasi harus memiliki alamat IP pribadi ketika database sumber dan target berada dalam jaringan yang sama. Jaringan juga harus terhubung ke VPC instance replikasi menggunakan VPN AWS Direct Connect, atau VPC peering. Untuk mempelajari lebih lanjut tentang instans replikasi publik dan pribadi, lihat Instans [replikasi publik dan pribadi di Panduan Pengguna](#).AWS Database Migration Service

Anda juga harus memastikan bahwa akses ke konfigurasi AWS DMS instans terbatas hanya untuk pengguna yang berwenang. Untuk melakukan ini, batasi izin IAM pengguna untuk mengubah AWS DMS pengaturan dan sumber daya.

Remediasi

Anda tidak dapat mengubah pengaturan akses publik untuk instance replikasi DMS setelah membuatnya. Untuk mengubah setelan akses publik, [hapus instans Anda saat ini](#), lalu [buat ulang](#). Jangan pilih opsi yang dapat diakses publik.

[DMS.2] Sertifikat DMS harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: AWS::DMS::Certificate

AWS Config aturan: tagged-dms-certificate (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
requiredTagKeys	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi	No default value

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
			persyaratan AWS	

Kontrol ini memeriksa apakah AWS DMS sertifikat memiliki tag dengan kunci spesifik yang ditentukan dalam `parameterrequiredTagKeys`. Kontrol gagal jika sertifikat tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam `parameterrequiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika sertifikat tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws :`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat [Untuk apa ABAC? AWS](#) di Panduan Pengguna IAM.

Note

Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat [Menandai AWS sumber daya Anda](#) di Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke sertifikat DMS, lihat [Menandai sumber daya AWS Database Migration Service di AWS Database Migration Service](#) Panduan Pengguna.

[DMS.3] Langganan acara DMS harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: AWS::DMS::EventSubscription

AWS Config aturan: tagged-dms-eventsubscription (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
<code>requiredTagKeys</code>	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS .	No default value

Kontrol ini memeriksa apakah langganan AWS DMS acara memiliki tag dengan kunci tertentu yang ditentukan dalam parameter `requiredTagKeys`. Kontrol gagal jika langganan acara tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter `requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika langganan acara tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke

AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat [Untuk apa ABAC? AWS](#) di Panduan Pengguna IAM.

Note

Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat [Menandai AWS sumber daya Anda](#) di Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke langganan acara DMS, lihat [Menandai sumber daya AWS Database Migration Service](#) di [AWS Database Migration Service](#) Panduan Pengguna.

[DMS.4] Contoh replikasi DMS harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::DMS::ReplicationInstance`

AWS Config aturan: `tagged-dms-replicationinstance` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
<code>requiredTagKeys</code>	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi	No default value

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
			persyaratan AWS	

Kontrol ini memeriksa apakah instance AWS DMS replikasi memiliki tag dengan kunci spesifik yang ditentukan dalam parameter `requiredTagKeys`. Kontrol gagal jika instance replikasi tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter `requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika instance replikasi tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws :`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat [Untuk apa ABAC? AWS](#) di Panduan Pengguna IAM.

Note

Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat [Menandai AWS sumber daya Anda](#) di Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke instance replikasi DMS, lihat [Menandai sumber daya AWS Database Migration Service di Panduan Pengguna](#). AWS Database Migration Service

[DMS.5] Grup subnet replikasi DMS harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: AWS::DMS::ReplicationSubnetGroup

AWS Config aturan: tagged-dms-replicationsubnetgroup (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
<code>requiredTagKeys</code>	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS .	No default value

Kontrol ini memeriksa apakah grup subnet AWS DMS replikasi memiliki tag dengan kunci tertentu yang ditentukan dalam parameter. `requiredTagKeys` Kontrol gagal jika grup subnet replikasi tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter. `requiredTagKeys` Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika grup subnet replikasi tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke

AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat [Untuk apa ABAC? AWS](#) di Panduan Pengguna IAM.

 Note

Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat [Menandai AWS sumber daya Anda](#) di Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke grup subnet replikasi DMS, lihat [Menandai sumber daya AWS Database Migration Service di Panduan Pengguna](#).AWS Database Migration Service

[DMS.6] Instans replikasi DMS harus mengaktifkan peningkatan versi minor otomatis

Persyaratan terkait: NIST.800-53.R5 SI-2, NIST.800-53.R5 SI-2 (2), NIST.800-53.R5 SI-2 (4), Nist.800-53.R5 SI-2 (5), PCI DSS v4.0.1/6.3.3

Kategori: Identifikasi > Kerentanan, tambalan, dan manajemen versi

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::DMS::ReplicationInstance

AWS Config aturan: [dms-auto-minor-version-upgrade-check](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah upgrade versi minor otomatis diaktifkan untuk instance AWS DMS replikasi. Kontrol gagal jika upgrade versi minor otomatis tidak diaktifkan untuk instance replikasi DMS.

DMS menyediakan upgrade versi minor otomatis ke setiap mesin replikasi yang didukung sehingga Anda dapat menyimpan instance replikasi Anda. up-to-date Versi minor dapat memperkenalkan

fitur perangkat lunak baru, perbaikan bug, patch keamanan, dan peningkatan kinerja. Dengan mengaktifkan pemutakhiran versi minor otomatis pada instance replikasi DMS, peningkatan kecil diterapkan secara otomatis selama jendela pemeliharaan atau segera jika opsi Terapkan segera berubah dipilih.

Remediasi

Untuk mengaktifkan pemutakhiran versi minor otomatis pada instance replikasi DMS, lihat [Memodifikasi instance replikasi](#) di Panduan Pengguna AWS Database Migration Service

[DMS.7] Tugas replikasi DMS untuk database target seharusnya mengaktifkan logging

Persyaratan terkait: NIST.800-53.r5 AC-2 (4), (26), NIST.800-53.r5 AC-4 (9),, NIST.800-53.r5 AC-6 (9), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7 Nist.800-53.R5 SI-3 NIST.800-53.r5 SC-7 (8), Nist.800-53.R5 SI-4 (20), Nist.800-53.R5 SI-7 (8), PCI DSS v4.0.1/10.4.2

Kategori: Identifikasi > Logging

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::DMS::ReplicationTask

AWS Config aturan: [dms-replication-task-targetdb-logging](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah logging diaktifkan dengan tingkat keparahan minimum `LOGGER_SEVERITY_DEFAULT` untuk tugas `TARGET_APPLY` replikasi DMS dan `TARGET_LOAD`. Kontrol gagal jika logging tidak diaktifkan untuk tugas-tugas ini atau jika tingkat keparahan minimum kurang dari `LOGGER_SEVERITY_DEFAULT`.

DMS menggunakan Amazon CloudWatch untuk mencatat informasi selama proses migrasi. Menggunakan pengaturan tugas logging, Anda dapat menentukan aktivitas komponen mana yang dicatat dan berapa banyak informasi yang dicatat. Anda harus menentukan logging untuk tugas-tugas berikut:

- `TARGET_APPLY`— Pernyataan bahasa definisi data dan data (DDL) diterapkan ke database target.

- **TARGET_LOAD**— Data dimuat ke database target.

Logging memainkan peran penting dalam tugas replikasi DMS dengan memungkinkan pemantauan, pemecahan masalah, audit, analisis kinerja, deteksi kesalahan, dan pemulihan, serta analisis historis dan pelaporan. Ini membantu memastikan keberhasilan replikasi data antar database sambil menjaga integritas data dan kepatuhan terhadap persyaratan peraturan. Level logging selain DEFAULT jarang diperlukan untuk komponen ini selama pemecahan masalah. Kami merekomendasikan untuk menjaga tingkat logging seperti DEFAULT untuk komponen ini kecuali secara khusus diminta untuk mengubahnya Dukungan. Tingkat logging minimal DEFAULT memastikan bahwa pesan informasi, peringatan, dan pesan kesalahan ditulis ke log. Kontrol ini memeriksa apakah tingkat logging setidaknya salah satu dari yang berikut untuk tugas replikasi sebelumnya: `LOGGER_SEVERITY_DEFAULT`, `LOGGER_SEVERITY_DEBUG` atau `LOGGER_SEVERITY_DETAILED_DEBUG`

Remediasi

Untuk mengaktifkan pencatatan tugas replikasi DMS basis data target, lihat [Melihat dan mengelola log AWS DMS tugas](#) di AWS Database Migration Service Panduan Pengguna.

[DMS.8] Tugas replikasi DMS untuk database sumber seharusnya mengaktifkan logging

Persyaratan terkait: NIST.800-53.r5 AC-2 (4), (26), NIST.800-53.r5 AC-4 (9),, NIST.800-53.r5 AC-6 (9), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7 Nist.800-53.R5 SI-3 NIST.800-53.r5 SC-7 (8), Nist.800-53.R5 SI-4 (20), Nist.800-53.R5 SI-7 (8), PCI DSS v4.0.1/10.4.2

Kategori: Identifikasi > Logging

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::DMS::ReplicationTask`

AWS Config aturan: [dms-replication-task-sourcedb-logging](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah logging diaktifkan dengan tingkat keparahan minimum `LOGGER_SEVERITY_DEFAULT` untuk tugas `SOURCE_CAPTURE` replikasi DMS dan `SOURCE_UNLOAD`

Kontrol gagal jika logging tidak diaktifkan untuk tugas-tugas ini atau jika tingkat keparahan minimum kurang dari `LOGGER_SEVERITY_DEFAULT`.

DMS menggunakan Amazon CloudWatch untuk mencatat informasi selama proses migrasi.

Menggunakan pengaturan tugas logging, Anda dapat menentukan aktivitas komponen mana yang dicatat dan berapa banyak informasi yang dicatat. Anda harus menentukan logging untuk tugas-tugas berikut:

- `SOURCE_CAPTURE` Data replikasi atau perubahan data capture (CDC) yang sedang berlangsung diambil dari database sumber atau layanan, dan diteruskan ke komponen `SORTER` layanan.
- `SOURCE_UNLOAD`— Data diturunkan dari database sumber atau layanan selama pemuatan penuh.

Logging memainkan peran penting dalam tugas replikasi DMS dengan memungkinkan pemantauan, pemecahan masalah, audit, analisis kinerja, deteksi kesalahan, dan pemulihan, serta analisis historis dan pelaporan. Ini membantu memastikan keberhasilan replikasi data antar database sambil menjaga integritas data dan kepatuhan terhadap persyaratan peraturan. Level logging selain `DEFAULT` jarang diperlukan untuk komponen ini selama pemecahan masalah. Kami merekomendasikan untuk menjaga tingkat logging seperti `DEFAULT` untuk komponen ini kecuali secara khusus diminta untuk mengubahnya Dukungan. Tingkat logging minimal `DEFAULT` memastikan bahwa pesan informasi, peringatan, dan pesan kesalahan ditulis ke log. Kontrol ini memeriksa apakah tingkat logging setidaknya salah satu dari yang berikut untuk tugas replikasi sebelumnya: `LOGGER_SEVERITY_DEFAULT`, `LOGGER_SEVERITY_DEBUG` atau `LOGGER_SEVERITY_DETAILED_DEBUG`.

Remediasi

Untuk mengaktifkan pencatatan tugas replikasi DMS basis data sumber, lihat [Melihat dan mengelola log AWS DMS tugas](#) di AWS Database Migration Service Panduan Pengguna.

[DMS.9] Titik akhir DMS harus menggunakan SSL

Persyaratan terkait: NIST.800-53.r5 AC-4, NIST.800-53.r5 SC-1 3, NIST.800-53.r5 SC-2 3, 3 (NIST.800-53.r5 SC-23), (4),, NIST.800-53.r5 SC-7 (1) NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 NIST.800-53.r5 SC-8 (2), PCI DSS v4.0.1/4.2.1

Kategori: Lindungi > Perlindungan Data > Enkripsi data-in-transit

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::DMS::Endpoint

AWS Config aturan: [dms-endpoint-ssl-configured](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah AWS DMS titik akhir menggunakan koneksi SSL. Kontrol gagal jika titik akhir tidak menggunakan SSL.

Koneksi SSL/TLS menyediakan lapisan keamanan dengan mengenkripsi koneksi antara instance replikasi DMS dan database Anda. Menggunakan sertifikat memberikan lapisan keamanan tambahan dengan memvalidasi bahwa koneksi sedang dibuat ke database yang diharapkan. Ia melakukannya dengan memeriksa sertifikat server yang secara otomatis diinstal pada semua instance database yang Anda berikan. Dengan mengaktifkan koneksi SSL pada titik akhir DMS Anda, Anda melindungi kerahasiaan data selama migrasi.

Remediasi

Untuk menambahkan koneksi SSL ke titik akhir DMS baru atau yang sudah ada, lihat [Menggunakan SSL dengan AWS Database Migration Service](#) di Panduan Pengguna AWS Database Migration Service

[DMS.10] Titik akhir DMS untuk database Neptune harus mengaktifkan otorisasi IAM

Persyaratan terkait: NIST.800-53.r5 AC-2,,, NIST.800-53.r5 AC-1 7 NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-6,, NIST.800-53.r5 IA-2 NIST.800-53.r5 IA-5, PCI DSS v4.0.1/7.3.1

Kategori: Lindungi > Manajemen akses aman > Otentikasi tanpa kata sandi

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::DMS::Endpoint

AWS Config aturan: [dms-neptune-iam-authorization-enabled](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah AWS DMS titik akhir untuk database Amazon Neptune dikonfigurasi dengan otorisasi IAM. Kontrol gagal jika titik akhir DMS tidak mengaktifkan otorisasi IAM.

AWS Identity and Access Management (IAM) menyediakan kontrol akses berbutir halus di seluruh. AWS Dengan IAM, Anda dapat menentukan siapa yang dapat mengakses layanan dan sumber daya mana, dan dalam kondisi apa. Dengan kebijakan IAM, Anda mengelola izin untuk tenaga kerja dan sistem Anda untuk memastikan izin hak istimewa paling sedikit. Dengan mengaktifkan otorisasi IAM pada AWS DMS titik akhir untuk database Neptune, Anda dapat memberikan hak otorisasi kepada pengguna IAM dengan menggunakan peran layanan yang ditentukan oleh parameter. `ServiceAccessRoleARN`

Remediasi

Untuk mengaktifkan otorisasi IAM pada titik akhir DMS untuk database Neptune, lihat [Menggunakan Amazon Neptune sebagai target dalam Panduan Pengguna](#). AWS Database Migration Service AWS Database Migration Service

[DMS.11] Titik akhir DMS untuk MongoDB harus mengaktifkan mekanisme otentikasi

Persyaratan terkait: NIST.800-53.r5 AC-3,,, NIST.800-53.r5 AC-6 NIST.800-53.r5 IA-2 NIST.800-53.r5 IA-5, PCI DSS v4.0.1/7.3.1

Kategori: Lindungi > Manajemen akses aman > Otentikasi tanpa kata sandi

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::DMS::Endpoint`

AWS Config aturan: [dms-mongo-db-authentication-enabled](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah AWS DMS titik akhir untuk MongoDB dikonfigurasi dengan mekanisme otentikasi. Kontrol gagal jika jenis otentikasi tidak disetel untuk titik akhir.

AWS Database Migration Service mendukung dua metode otentikasi untuk MongoDB- MONGODB-CR untuk MongoDB versi 2.x, dan SCRAM-SHA-1 untuk MongoDB versi 3.x atau yang lebih baru. Metode otentikasi ini digunakan untuk mengautentikasi dan mengenkripsi kata sandi MongoDB

jika pengguna ingin menggunakan kata sandi untuk mengakses database. Otentikasi pada AWS DMS titik akhir memastikan bahwa hanya pengguna yang berwenang yang dapat mengakses dan memodifikasi data yang sedang dimigrasi antar database. Tanpa autentikasi yang tepat, pengguna yang tidak sah dapat memperoleh akses ke data sensitif selama proses migrasi. Hal ini dapat mengakibatkan pelanggaran data, kehilangan data, atau insiden keamanan lainnya.

Remediasi

Untuk mengaktifkan mekanisme otentikasi pada titik akhir DMS untuk MongoDB, lihat [Menggunakan MongoDB sebagai sumber di Panduan Pengguna](#). AWS DMS

[DMS.12] Titik akhir DMS untuk Redis OSS seharusnya mengaktifkan TLS

Persyaratan terkait: NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-1 3, PCI DSS v4.0.1/4.2.1

Kategori: Lindungi > Perlindungan Data > Enkripsi data-in-transit

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::DMS::Endpoint

AWS Config aturan: [dms-redis-tls-enabled](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah AWS DMS titik akhir untuk Redis OSS dikonfigurasi dengan koneksi TLS. Kontrol gagal jika titik akhir tidak mengaktifkan TLS.

TLS memberikan end-to-end keamanan ketika data dikirim antara aplikasi atau database melalui internet. Saat Anda mengonfigurasi enkripsi SSL untuk titik akhir DMS Anda, ini memungkinkan komunikasi terenkripsi antara basis data sumber dan target selama proses migrasi. Ini membantu mencegah penyadapan dan intersepsi data sensitif oleh aktor jahat. Tanpa enkripsi SSL, data sensitif dapat diakses, mengakibatkan pelanggaran data, kehilangan data, atau insiden keamanan lainnya.

Remediasi

Untuk mengaktifkan koneksi TLS pada titik akhir DMS untuk Redis, lihat [Menggunakan Redis sebagai target dalam Panduan Pengguna](#). AWS Database Migration Service

Kontrol Security Hub untuk Amazon DocumentDB

AWS Security Hub Kontrol ini mengevaluasi layanan dan sumber daya Amazon DocumentDB (dengan kompatibilitas MongoDB). Kontrol mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat [Ketersediaan kontrol berdasarkan Wilayah](#).

[DocumentDB.1] Cluster Amazon DocumentDB harus dienkrpsi saat istirahat

Persyaratan terkait: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-1 3, NIST.800-53.r5 SC-2 8, NIST.800-53.r5 SC-2 8 (1), NIST.800-53.r5 SC-7 (10), NIST.800-53.R5 SI-7 (6)

Kategori: Lindungi > Perlindungan Data > Enkripsi data-at-rest

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::RDS::DBCluster

AWS Config aturan: [docdb-cluster-encrypted](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah cluster Amazon DocumentDB dienkrpsi saat istirahat. Kontrol gagal jika cluster Amazon DocumentDB tidak dienkrpsi saat istirahat.

Data saat istirahat mengacu pada data apa pun yang disimpan dalam penyimpanan persisten dan tidak mudah menguap untuk durasi berapa pun. Enkripsi membantu Anda melindungi kerahasiaan data tersebut, mengurangi risiko bahwa pengguna yang tidak sah mendapatkan akses ke sana. Data di cluster Amazon DocumentDB harus dienkrpsi saat istirahat untuk lapisan keamanan tambahan. Amazon DocumentDB menggunakan Advanced Encryption Standard 256-bit (AES-256) untuk mengenkripsi data Anda menggunakan kunci enkripsi yang disimpan dalam AWS Key Management Service (AWS KMS).

Remediasi

Anda dapat mengaktifkan enkripsi saat istirahat saat membuat klaster Amazon DocumentDB. Anda tidak dapat mengubah pengaturan enkripsi setelah membuat cluster. Untuk informasi selengkapnya, lihat [Mengaktifkan enkripsi saat istirahat untuk klaster Amazon DocumentDB di Panduan Pengembang Amazon DocumentDB](#).

[DocumentDB.2] Cluster Amazon DocumentDB harus memiliki periode retensi cadangan yang memadai

Persyaratan terkait: NIST.800-53.R5 SI-12, PCI DSS v4.0.1/3.2.1

Kategori: Pulih> Ketahanan > Cadangan diaktifkan

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::RDS::DBCluster

AWS Config aturan: [docdb-cluster-backup-retention-check](#)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub	
minimumBackupRetentionPeriod	Periode retensi cadangan minimum dalam beberapa hari	Bilangan Bulat	7 untuk 35	7	

Kontrol ini memeriksa apakah klaster Amazon DocumentDB memiliki periode retensi cadangan yang lebih besar dari atau sama dengan kerangka waktu yang ditentukan. Kontrol gagal jika periode retensi cadangan kurang dari kerangka waktu yang ditentukan. Kecuali Anda memberikan nilai parameter khusus untuk periode penyimpanan cadangan, Security Hub menggunakan nilai default 7 hari.

Pencadangan membantu Anda pulih lebih cepat dari insiden keamanan dan memperkuat ketahanan sistem Anda. Dengan mengotomatiskan backup untuk cluster Amazon DocumentDB Anda, Anda akan dapat memulihkan sistem Anda ke titik waktu tertentu dan meminimalkan waktu henti dan kehilangan data. Di Amazon DocumentDB, cluster memiliki periode retensi cadangan default 1 hari. Ini harus ditingkatkan menjadi nilai antara 7 dan 35 hari untuk melewati kontrol ini.

Remediasi

Untuk mengubah periode retensi cadangan untuk kluster Amazon DocumentDB Anda, lihat [Memodifikasi kluster Amazon DocumentDB di Panduan Pengembang Amazon DocumentDB](#). Untuk Backup, pilih periode retensi cadangan.

[DocumentDB.3] Cuplikan cluster manual Amazon DocumentDB seharusnya tidak bersifat publik

Persyaratan terkait: NIST.800-53.r5 AC-2 1, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21),, NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (9), PCI DSS v4.0.1/1.4.4

Kategori: Lindungi > Konfigurasi jaringan aman

Tingkat keparahan: Kritis

Jenis sumber daya: AWS : : RDS : : DBClusterSnapshot

AWS Config aturan: [docdb-cluster-snapshot-public-prohibited](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah snapshot kluster manual Amazon DocumentDB bersifat publik. Kontrol gagal jika snapshot cluster manual bersifat publik.

Snapshot kluster manual Amazon DocumentDB tidak boleh bersifat publik kecuali dimaksudkan. Jika Anda membagikan snapshot manual yang tidak terenkripsi sebagai publik, snapshot tersedia untuk semua. Akun AWS Cuplikan publik dapat mengakibatkan eksposur data yang tidak diinginkan.

Note

Kontrol ini mengevaluasi snapshot cluster manual. Anda tidak dapat membagikan snapshot kluster otomatis Amazon DocumentDB. Namun, Anda dapat membuat snapshot manual dengan menyalin snapshot otomatis, lalu membagikan salinannya.

Remediasi

Untuk menghapus akses publik untuk snapshot kluster manual Amazon DocumentDB, [lihat Berbagi snapshot](#) di Panduan Pengembang Amazon DocumentDB. Secara terprogram, Anda dapat menggunakan operasi Amazon DocumentDB. `modify-db-snapshot-attribute` Tetapkan `attribute-name` sebagai `restore` dan `values-to-remove` sebagai `all`.

[DocumentDB.4] Cluster Amazon DocumentDB harus mempublikasikan log audit ke Log CloudWatch

Persyaratan terkait: NIST.800-53.r5 AC-2 (4), (26), NIST.800-53.r5 AC-4 (9),, NIST.800-53.r5 AC-6 (9), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7 Nist.800-53.R5 SI-3 NIST.800-53.r5 SC-7 (8), Nist.800-53.R5 SI-4 (20), Nist.800-53.R5 SI-7 (8), PCI DSS v4.0.1/10.3.3

Kategori: Identifikasi > Logging

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::RDS::DBCluster

AWS Config aturan: [docdb-cluster-audit-logging-enabled](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah klaster Amazon DocumentDB menerbitkan log audit ke Amazon Logs. CloudWatch Kontrol gagal jika klaster tidak mempublikasikan log audit ke CloudWatch Log.

Amazon DocumentDB (dengan kompatibilitas MongoDB) memungkinkan Anda mengaudit peristiwa yang dilakukan di cluster Anda. Contoh log acara termasuk upaya autentikasi yang berhasil dan gagal, membuang koleksi dalam basis data, atau membuat indeks. Secara default, audit dinonaktifkan di Amazon DocumentDB dan mengharuskan Anda mengambil tindakan untuk mengaktifkannya.

Remediasi

Untuk mempublikasikan log audit Amazon DocumentDB CloudWatch ke Log, [lihat Mengaktifkan](#) audit di Panduan Pengembang Amazon DocumentDB.

[DocumentDB.5] Cluster Amazon DocumentDB harus mengaktifkan perlindungan penghapusan

Persyaratan terkait: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2(2), NIST.800-53.r5 CM-3, NIST.800-53.r5 SC-5 (2)

Kategori: Lindungi > Perlindungan data > Perlindungan penghapusan data

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::RDS::DBCluster

AWS Config aturan: [docdb-cluster-deletion-protection-enabled](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah klaster Amazon DocumentDB memiliki perlindungan penghapusan yang diaktifkan. Kontrol gagal jika cluster tidak mengaktifkan perlindungan penghapusan.

Mengaktifkan perlindungan penghapusan klaster menawarkan lapisan perlindungan tambahan terhadap penghapusan atau penghapusan database yang tidak disengaja oleh pengguna yang tidak sah. Cluster Amazon DocumentDB tidak dapat dihapus saat perlindungan penghapusan diaktifkan. Anda harus menonaktifkan perlindungan penghapusan terlebih dahulu sebelum permintaan penghapusan berhasil. Perlindungan penghapusan diaktifkan secara default saat Anda membuat klaster di konsol Amazon DocumentDB.

Remediasi

Untuk mengaktifkan perlindungan penghapusan klaster Amazon DocumentDB yang ada, lihat Memodifikasi klaster Amazon DocumentDB di Panduan [Pengembang Amazon DocumentDB](#). Di bagian Modify Cluster, pilih Enable for Deletion protection.

[DocumentDB.6] Cluster Amazon DocumentDB harus dienkripsi saat transit

Kategori: Lindungi > Perlindungan Data > Enkripsi data-in-transit

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::RDS::DBCluster

AWS Config aturan: [docdb-cluster-encrypted-in-transit](#)

Jenis jadwal: Periodik

Parameter: `excludeTlsParameters:disabled, enabled` (tidak dapat disesuaikan)

Kontrol ini memeriksa apakah klaster Amazon DocumentDB memerlukan TLS untuk koneksi ke cluster. Kontrol gagal jika grup parameter cluster yang terkait dengan cluster tidak sinkron, atau parameter cluster TLS diatur ke `disabled` atau `enabled`.

Anda dapat menggunakan TLS untuk mengenkripsi koneksi antara aplikasi dan cluster Amazon DocumentDB. Penggunaan TLS dapat membantu melindungi data agar tidak dicegat saat data sedang transit antara aplikasi dan cluster Amazon DocumentDB. Enkripsi dalam perjalanan untuk klaster Amazon DocumentDB dikelola menggunakan parameter TLS di grup parameter cluster yang terkait dengan cluster. Ketika enkripsi dalam transit diaktifkan, koneksi aman menggunakan TLS diperlukan untuk terhubung ke klaster. Sebaiknya gunakan parameter TLS berikut: `tls1.2+`, `tls1.3+`, dan `fips-140-3`.

Remediasi

Untuk informasi tentang mengubah setelan TLS untuk klaster Amazon DocumentDB, [lihat *Mengenkripsi data saat transit*](#) di Panduan Pengembang Amazon DocumentDB.

Kontrol Security Hub untuk DynamoDB

AWS Security Hub Kontrol ini mengevaluasi layanan dan sumber daya Amazon DynamoDB. Kontrol mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat [Ketersediaan kontrol berdasarkan Wilayah](#).

[DynamoDB.1] Tabel DynamoDB harus secara otomatis menskalakan kapasitas sesuai permintaan

Persyaratan terkait: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-2(2), NIST.800-53.r5 CP-6(2), NIST.800-53.r5 SC-3 6, NIST.800-53.r5 SC-5 (2), NIST.800-53.R5 SI-13 (5)

Kategori: Pulihkan > Ketahanan > Ketersediaan tinggi

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::DynamoDB::Table`

AWS Config aturan: [dynamodb-autoscaling-enabled](#)

Jenis jadwal: Periodik

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang valid	Nilai default Security Hub
minProvisionedReadCapacity	Jumlah minimum unit kapasitas baca yang disediakan untuk penskalaan otomatis DynamoDB	Bilangan Bulat	1 untuk 40000	Tidak ada nilai default
targetReadUtilization	Target persentase pemanfaatan untuk kapasitas baca	Bilangan Bulat	20 untuk 90	Tidak ada nilai default
minProvisionedWriteCapacity	Jumlah minimum unit kapasitas tulis yang disediakan untuk penskalaan otomatis DynamoDB	Bilangan Bulat	1 untuk 40000	Tidak ada nilai default
targetWriteUtilization	Target persentase pemanfaatan untuk kapasitas tulis	Bilangan Bulat	20 untuk 90	Tidak ada nilai default

Kontrol ini memeriksa apakah tabel Amazon DynamoDB dapat menskalakan kapasitas baca dan tulisnya sesuai kebutuhan. Kontrol gagal jika tabel tidak menggunakan mode kapasitas sesuai permintaan atau mode yang disediakan dengan penskalaan otomatis yang dikonfigurasi. Secara default, kontrol ini hanya mengharuskan salah satu mode ini dikonfigurasi, tanpa memperhatikan tingkat kapasitas baca atau tulis tertentu. Secara opsional, Anda dapat memberikan nilai parameter khusus untuk memerlukan tingkat kapasitas baca dan tulis tertentu atau pemanfaatan target.

Kapasitas penskalaan dengan permintaan menghindari pengecualian pembatasan, yang membantu menjaga ketersediaan aplikasi Anda. Tabel DynamoDB yang menggunakan mode kapasitas sesuai permintaan hanya dibatasi oleh kuota tabel default throughput DynamoDB. Untuk menaikkan kuota ini, Anda dapat mengajukan tiket dukungan dengan Dukungan. Tabel DynamoDB yang

menggunakan mode yang disediakan dengan penskalaan otomatis menyesuaikan kapasitas throughput yang disediakan secara dinamis sebagai respons terhadap pola lalu lintas. Untuk informasi selengkapnya tentang pembatasan permintaan DynamoDB, [lihat Meminta pelambatan dan kapasitas burst di Panduan Pengembang Amazon](#) DynamoDB.

Remediasi

Untuk mengaktifkan penskalaan otomatis DynamoDB pada tabel yang ada dalam mode kapasitas, lihat Mengaktifkan penskalaan otomatis [DynamoDB pada tabel yang ada di Panduan Pengembang Amazon DynamoDB](#).

[DynamoDB.2] Tabel DynamoDB harus mengaktifkan pemulihan point-in-time

Persyaratan terkait: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6(2), NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5 (2), NIST.800-53.R5 SI-12, NIST.800-53.R5 SI-13 (5)

Kategori: Pulih> Ketahanan > Cadangan diaktifkan

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::DynamoDB::Table

AWS Config aturan: [dynamodb-pitr-enabled](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah point-in-time pemulihan (PITR) diaktifkan untuk tabel Amazon DynamoDB.

Cadangan membantu Anda pulih lebih cepat dari insiden keamanan. Mereka juga memperkuat ketahanan sistem Anda. DynamoDB recovery point-in-time mengotomatiskan backup untuk tabel DynamoDB. Ini mengurangi waktu untuk memulihkan dari menghapus atau menulis operasi yang tidak disengaja. Tabel DynamoDB yang mengaktifkan PITR dapat dikembalikan ke titik waktu mana pun dalam 35 hari terakhir.

Remediasi

Untuk mengembalikan tabel DynamoDB ke titik waktu, lihat [Memulihkan tabel DynamoDB ke titik waktu dalam Panduan Pengembang Amazon DynamoDB](#).

[DynamoDB.3] Cluster DynamoDB Accelerator (DAX) harus dienkripsi saat istirahat

Persyaratan terkait: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-1 3, NIST.800-53.r5 SC-2 8, NIST.800-53.r5 SC-2 8 (1), NIST.800-53.r5 SC-7 (10), NIST.800-53.R5 SI-7 (6)

Kategori: Lindungi > Perlindungan Data > Enkripsi data-at-rest

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::DAX::Cluster

AWS Config aturan: [dax-encryption-enabled](#)

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah klaster Amazon DynamoDB Accelerator (DAX) dienkripsi saat istirahat. Kontrol gagal jika cluster DAX tidak dienkripsi saat istirahat.

Mengenkripsi data saat istirahat mengurangi risiko data yang disimpan pada disk yang diakses oleh pengguna yang tidak diautentikasi. AWS Enkripsi menambahkan satu set kontrol akses lain untuk membatasi kemampuan pengguna yang tidak sah untuk mengakses data. Misalnya, izin API diperlukan untuk mendekripsi data sebelum dapat dibaca.

Remediasi

Anda tidak dapat mengaktifkan atau menonaktifkan enkripsi saat istirahat setelah cluster dibuat. Anda harus membuat ulang cluster untuk mengaktifkan enkripsi saat istirahat. Untuk petunjuk terperinci tentang cara membuat klaster DAX dengan enkripsi saat istirahat diaktifkan, lihat [Mengaktifkan enkripsi saat istirahat menggunakan Panduan Pengembang Amazon DynamoDB AWS Management Console di Amazon DynamoDB](#).

[DynamoDB.4] Tabel DynamoDB harus ada dalam rencana cadangan

Persyaratan terkait: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6, NIST.800-53.r5 CP-6(1), NIST.800-53.r5 CP-6(2), NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5 (2), NIST.800-53.R5 SI-12, NIST.800-53.R5 SI-13 (5)

Kategori: Pulih > Ketahanan > Cadangan diaktifkan

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::DynamoDB::Table

AWS Config aturan: [dynamodb-resources-protected-by-backup-plan](#)

Jenis jadwal: Periodik

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
backupVaultLockCheck	Kontrol menghasilkan PASSED temuan jika parameter disetel ke <code>true</code> dan sumber daya menggunakan AWS Backup Vault Lock.	Boolean	<code>true</code> atau <code>false</code>	Tidak ada nilai default

Kontrol ini mengevaluasi apakah ACTIVE tabel Amazon DynamoDB dalam status dicakup oleh rencana cadangan. Kontrol gagal jika tabel DynamoDB tidak dicakup oleh rencana cadangan. Jika Anda menyetel `backupVaultLockCheck` parameter sama dengan `true`, kontrol hanya akan diteruskan jika tabel DynamoDB dicadangkan di AWS Backup vault terkunci.

AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya yang membantu Anda memusatkan dan mengotomatiskan pencadangan data di seluruh. Layanan AWS Dengan AWS Backup, Anda dapat membuat rencana cadangan yang menentukan persyaratan pencadangan Anda, seperti seberapa sering mencadangkan data Anda dan berapa lama untuk menyimpan cadangan tersebut. Menyertakan tabel DynamoDB dalam paket cadangan membantu Anda melindungi data dari kehilangan atau penghapusan yang tidak diinginkan.

Remediasi

Untuk menambahkan tabel DynamoDB ke AWS Backup paket cadangan, [lihat Menetapkan sumber daya ke paket cadangan di Panduan Pengembang](#). AWS Backup

[DynamoDB.5] Tabel DynamoDB harus diberi tag

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: AWS::DynamoDB::Table

AWS Config aturan: tagged-dynamodb-table (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
<code>requiredTagKeys</code>	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS.	No default value

Kontrol ini memeriksa apakah tabel Amazon DynamoDB memiliki tag dengan kunci tertentu yang ditentukan dalam parameter. `requiredTagKeys` Kontrol gagal jika tabel tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter `requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika tabel tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat [Untuk apa ABAC? AWS](#) di Panduan Pengguna IAM.

 Note

Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat [Menandai AWS sumber daya Anda](#) di Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke tabel DynamoDB, [lihat Menandai sumber daya di DynamoDB di Panduan Pengembang Amazon](#) DynamoDB.

[DynamoDB.6] Tabel DynamoDB harus mengaktifkan perlindungan penghapusan

Persyaratan terkait: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2(2), NIST.800-53.r5 CM-3, NIST.800-53.r5 SC-5 (2)

Kategori: Lindungi > Perlindungan data > Perlindungan penghapusan data

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::DynamoDB::Table

AWS Config aturan: [dynamodb-table-deletion-protection-enabled](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah tabel Amazon DynamoDB memiliki perlindungan penghapusan yang diaktifkan. Kontrol gagal jika tabel DynamoDB tidak mengaktifkan proteksi penghapusan.

Anda dapat melindungi tabel DynamoDB dari penghapusan yang tidak disengaja dengan properti perlindungan penghapusan. Mengaktifkan properti ini untuk tabel membantu memastikan bahwa tabel tidak terhapus secara tidak sengaja selama operasi manajemen tabel reguler oleh administrator Anda. Ini membantu mencegah gangguan pada operasi bisnis normal Anda.

Remediasi

Untuk mengaktifkan perlindungan penghapusan untuk tabel DynamoDB, lihat [Menggunakan perlindungan penghapusan](#) di Panduan Pengembang Amazon DynamoDB.

[DynamoDB.7] Cluster DynamoDB Accelerator harus dienkripsi saat transit

Persyaratan terkait: NIST.800-53.r5 AC-1 7,, NIST.800-53.r5 SC-1 3 NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-2 3, PCI DSS v4.0.1/4.2.1

Kategori: Lindungi > Perlindungan Data > Enkripsi data-in-transit

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::DAX::Cluster`

AWS Config aturan: [dax-tls-endpoint-encryption](#)

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah kluster Amazon DynamoDB Accelerator (DAX) dienkripsi saat transit, dengan jenis enkripsi endpoint disetel ke TLS. Kontrol gagal jika kluster DAX tidak dienkripsi saat transit.

HTTPS (TLS) dapat digunakan untuk membantu mencegah penyerang potensial menggunakan person-in-the-middle atau serangan serupa untuk menguping atau memanipulasi lalu lintas jaringan. Anda hanya boleh mengizinkan koneksi terenkripsi melalui TLS untuk mengakses kluster DAX. Namun, mengenkripsi data dalam perjalanan dapat memengaruhi kinerja. Anda harus menguji aplikasi Anda dengan enkripsi diaktifkan untuk memahami profil kinerja dan dampak TLS.

Remediasi

Anda tidak dapat mengubah setelan enkripsi TLS setelah membuat cluster DAX. Untuk mengenkripsi kluster DAX yang ada, buat kluster baru dengan enkripsi saat transit diaktifkan, geser lalu lintas aplikasi Anda ke kluster tersebut, lalu hapus kluster lama. Untuk informasi selengkapnya, lihat [Menggunakan perlindungan penghapusan](#) di Panduan Pengembang Amazon DynamoDB.

Kontrol Security Hub untuk Amazon EC2

AWS Security Hub Kontrol ini mengevaluasi layanan dan sumber daya Amazon Elastic Compute Cloud (Amazon EC2). Kontrol mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat [Ketersediaan kontrol berdasarkan Wilayah](#).

[EC2.1] Cuplikan Amazon EBS tidak boleh dipulihkan secara publik

Persyaratan terkait: PCI DSS v3.2.1/1.2.1, PCI DSS v3.2.1/1.3.1, PCI DSS v3.2.1/1.3.4, PCI DSS v3.2.1/7.2.1, NIST.800-53.r5 AC-2 1,, NIST.800-53.r5 AC-3 (7),, (21),,, (11), (16), (20) NIST.800-53.r5 AC-3, (21), (3) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (4), NIST.800-53.r5 AC-6 (9) NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7

Kategori: Lindungi > Konfigurasi jaringan aman

Tingkat keparahan: Kritis

Jenis sumber daya: AWS : : : Account

AWS Config aturan: [ebs-snapshot-public-restorable-check](#)

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah snapshot Amazon Elastic Block Store tidak bersifat publik. Kontrol gagal jika snapshot Amazon EBS dapat dipulihkan oleh siapa pun.

Snapshot EBS digunakan untuk mencadangkan data pada volume EBS Anda ke Amazon S3 pada titik waktu tertentu. Anda dapat menggunakan snapshot untuk memulihkan status volume EBS sebelumnya. Jarang dapat diterima untuk berbagi snapshot dengan publik. Biasanya keputusan untuk membagikan snapshot secara publik dibuat karena kesalahan atau tanpa pemahaman lengkap tentang implikasinya. Pemeriksaan ini membantu memastikan bahwa semua pembagian tersebut sepenuhnya direncanakan dan disengaja.

IP Perbaikan

Untuk menjadikan snapshot EBS publik menjadi pribadi, lihat [Bagikan snapshot di Panduan Pengguna Amazon EC2](#) . Untuk Tindakan, Ubah izin, pilih Pribadi.

[EC2.2] Grup keamanan default VPC tidak boleh mengizinkan lalu lintas masuk atau keluar

Persyaratan terkait: PCI DSS v3.2.1/1.2.1, PCI DSS v3.2.1/1.3.4, PCI DSS v3.2.1/2.1, Tolok Ukur Yayasan CIS v1.2.0/4.3, Tolok Ukur Yayasan CIS v1.4.0/5.3, Tolok Ukur AWS Yayasan CIS v3.0.0/5.4,, (21),, (11), (16), (21), (21), (21), (21), (21) AWS), (21), (21), (21)) AWS NIST.800-53.r5

AC-4 NIST.800-53.r5 AC-4 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7
NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7

Kategori: Lindungi > Konfigurasi jaringan aman

Tingkat keparahan: Tinggi

Jenis sumber daya: AWS::EC2::SecurityGroup

AWS Config aturan: [vpc-default-security-group-closed](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah grup keamanan default VPC memungkinkan lalu lintas masuk atau keluar. Kontrol gagal jika grup keamanan memungkinkan lalu lintas masuk atau keluar.

Aturan untuk [grup keamanan default](#) mengizinkan semua lalu lintas keluar dan masuk dari antarmuka jaringan (dan instans terkait mereka) yang ditetapkan ke grup keamanan yang sama. Kami merekomendasikan agar Anda tidak menggunakan grup keamanan default. Karena grup keamanan default tidak dapat dihapus, Anda harus mengubah pengaturan aturan grup keamanan default untuk membatasi lalu lintas masuk dan keluar. Ini mencegah lalu lintas yang tidak diinginkan jika grup keamanan default secara tidak sengaja dikonfigurasi untuk sumber daya seperti EC2 instance.

IP Perbaikan

Untuk mengatasi masalah ini, mulailah dengan membuat grup keamanan paling tidak memiliki hak istimewa baru. Untuk petunjuknya, lihat [Membuat grup keamanan](#) di Panduan Pengguna Amazon VPC. Kemudian, tetapkan grup keamanan baru ke EC2 instans Anda. Untuk petunjuknya, lihat [Mengubah grup keamanan instans](#) di Panduan EC2 Pengguna Amazon.

Setelah Anda menetapkan grup keamanan baru ke sumber daya Anda, hapus semua aturan masuk dan keluar dari grup keamanan default. Untuk petunjuknya, lihat [Mengonfigurasi aturan grup keamanan](#) di Panduan Pengguna Amazon VPC.

[EC2.3] Volume Amazon EBS yang terlampir harus dienkripsi saat istirahat

Persyaratan terkait: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-1 3, NIST.800-53.r5 SC-2 8, NIST.800-53.r5 SC-2 8 (1), NIST.800-53.r5 SC-7 (10), NIST.800-53.R5 SI-7 (6)

Kategori: Lindungi > Perlindungan Data > Enkripsi data-at-rest

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::EC2::Volume

AWS Config aturan: [encrypted-volumes](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah volume EBS yang berada dalam keadaan terlampir dienkripsi. Untuk lulus pemeriksaan ini, volume EBS harus digunakan dan dienkripsi. Jika volume EBS tidak terpasang, maka tidak tunduk pada pemeriksaan ini.

Untuk lapisan keamanan tambahan data sensitif Anda dalam volume EBS, Anda harus mengaktifkan enkripsi EBS saat istirahat. Enkripsi EBS Amazon menawarkan solusi enkripsi langsung untuk sumber daya EBS Anda yang tidak mengharuskan Anda membangun, memelihara, dan mengamankan infrastruktur manajemen kunci Anda sendiri. Ini menggunakan kunci KMS saat membuat volume dan snapshot terenkripsi.

Untuk mempelajari lebih lanjut tentang enkripsi Amazon EBS, lihat [enkripsi Amazon EBS](#) di EC2 Panduan Pengguna Amazon.

IP Perbaikan

Tidak ada cara langsung untuk mengenkripsi volume atau snapshot yang tidak terenkripsi yang ada. Anda hanya dapat mengenkripsi volume atau snapshot baru saat Anda membuatnya.

Jika Anda mengaktifkan enkripsi secara default, Amazon EBS mengenkripsi volume atau snapshot baru yang dihasilkan menggunakan kunci default untuk enkripsi Amazon EBS. Meskipun Anda belum mengaktifkan enkripsi secara default, Anda dapat mengaktifkan enkripsi saat Anda membuat volume atau snapshot individu. Dalam kedua kasus tersebut, Anda dapat mengganti kunci default untuk enkripsi Amazon EBS dan memilih kunci terkelola pelanggan simetris.

Untuk informasi selengkapnya, lihat [Membuat volume Amazon EBS](#) dan [Menyalin snapshot Amazon EBS di Panduan Pengguna](#) Amazon. EC2

[EC2.4] EC2 Instans yang dihentikan harus dihapus setelah periode waktu tertentu

Persyaratan terkait: NIST.800-53.r5 CA-9 (1), Nist.800-53.R5 CM-2, Nist.800-53.R5 CM-2 (2)

Kategori: Identifikasi > Inventaris

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::EC2::Instance

AWS Config aturan: [ec2-stopped-instance](#)

Jenis jadwal: Periodik

Parameter:

Parameter	Deskripsi	Tipe	Nilai yang Diizinkan	Nilai yang Diizinkan
AllowedDays	Jumlah hari EC2 instance diizinkan berada dalam keadaan berhenti sebelum menghasilkan temuan yang gagal.	Bilangan Bulat	1 untuk 365	30

Kontrol ini memeriksa apakah EC2 instans Amazon telah dihentikan lebih lama dari jumlah hari yang diizinkan. Kontrol gagal jika EC2 instance dihentikan lebih lama dari periode waktu maksimum yang diizinkan. Kecuali Anda memberikan nilai parameter khusus untuk jangka waktu maksimum yang diizinkan, Security Hub menggunakan nilai default 30 hari.

Ketika sebuah EC2 instance tidak berjalan untuk jangka waktu yang signifikan, itu menciptakan risiko keamanan karena instance tidak dipelihara secara aktif (dianalisis, ditambah, diperbarui). Jika kemudian diluncurkan, kurangnya perawatan yang tepat dapat mengakibatkan masalah tak terduga di AWS lingkungan Anda. Untuk mempertahankan EC2 instance dengan aman dari waktu ke waktu dalam keadaan tidak aktif, mulailah secara berkala untuk pemeliharaan dan kemudian hentikan setelah pemeliharaan. Idealnya, ini harus menjadi proses otomatis.

IP Perbaikan

Untuk menghentikan EC2 instance yang tidak aktif, lihat [Mengakhiri instance di Panduan Pengguna Amazon EC2](#).

[EC2.6] Pencatatan aliran VPC harus diaktifkan di semua VPCs

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v1.2.0/2.9, Tolok Ukur Yayasan CIS v1.4.0/3.9, Tolok Ukur AWS Yayasan CIS v3.0.0/3.7, NIST.800-53.r5 AC-4 (26), Nist.800-53.r5 SI-7 (8),

NIST.800-171.r2 3.1.20, Nist.800-171.r2 3.3.1, NIST.800-171.R2 3.13.1, PCI DSS v3.2.1/10.3.3
NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3),
NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, PCI DSS v3.2.1/10.3.4, PCI DSS v3.2.1/10.3.5, PCI
DSS v3.2.1/10.3.6 AWS

Kategori: Identifikasi > Logging

Tingkat keparahan: Sedang

Jenis sumber daya: AWS : : EC2 : : VPC

AWS Config aturan: [vpc-flow-logs-enabled](#)

Jenis jadwal: Periodik

Parameter:

- `trafficType`: REJECT (tidak dapat disesuaikan)

Kontrol ini memeriksa apakah Amazon VPC Flow Logs ditemukan dan diaktifkan. VPCs Jenis lalu lintas diatur keReject. Kontrol gagal jika Log Aliran VPC tidak diaktifkan VPCs di akun Anda.

 Note

Kontrol ini tidak memeriksa apakah Amazon VPC Flow Logs diaktifkan melalui Amazon Security Lake untuk file. Akun AWS

Dengan fitur VPC Flow Logs, Anda dapat menangkap informasi tentang lalu lintas alamat IP yang pergi ke dan dari antarmuka jaringan di VPC Anda. Setelah Anda membuat log alur, Anda dapat melihat dan mengambil datanya di CloudWatch Log. Untuk mengurangi biaya, Anda juga dapat mengirim log alur ke Amazon S3.

Security Hub merekomendasikan agar Anda mengaktifkan flow logging untuk penolakan paket. VPCs Flow log memberikan visibilitas ke lalu lintas jaringan yang melintasi VPC dan dapat mendeteksi lalu lintas anomali atau memberikan wawasan selama alur kerja keamanan.

Secara default, catatan mencakup nilai-nilai untuk berbagai komponen alur alamat IP, termasuk sumber, tujuan, dan protokol. Untuk informasi selengkapnya dan deskripsi bidang log, lihat Log [Aliran VPC](#) di Panduan Pengguna Amazon VPC.

IP Perbaikan

Untuk membuat Log Aliran VPC, lihat [Membuat Log Aliran](#) di Panduan Pengguna Amazon VPC. Setelah Anda membuka konsol VPC Amazon, pilih Your VPCs Untuk Filter, pilih Tolak atau Semua.

[EC2.7] Enkripsi default EBS harus diaktifkan

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v1.4.0/2.2.1, Tolok Ukur AWS Yayasan CIS v3.0.0/2.2.1, (1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-1 3, 8, NIST.800-53.r5 SC-2 8 NIST.800-53.r5 CA-9 (1), (10), NIST.800-53.R5 SI-7 (NIST.800-53.r5 SC-26) NIST.800-53.r5 SC-7

Kategori: Lindungi > Perlindungan Data > Enkripsi data-at-rest

Tingkat keparahan: Sedang

Jenis sumber daya: AWS :: Account

AWS Config aturan: [ec2-ebs-encryption-by-default](#)

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah enkripsi tingkat akun diaktifkan secara default untuk volume Amazon Elastic Block Store (Amazon EBS). Kontrol gagal jika enkripsi tingkat akun tidak diaktifkan untuk volume EBS.

Saat enkripsi diaktifkan untuk akun Anda, volume Amazon EBS dan salinan snapshot dienkripsi saat istirahat. Ini menambahkan lapisan perlindungan tambahan untuk data Anda. Untuk informasi selengkapnya, lihat [Enkripsi secara default](#) di Panduan EC2 Pengguna Amazon.

IP Perbaikan

Untuk mengonfigurasi enkripsi default untuk volume Amazon EBS, lihat [Enkripsi secara default](#) di Panduan EC2 Pengguna Amazon.

[EC2.8] EC2 instans harus menggunakan Instance Metadata Service Versi 2 () IMDSv2

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v3.0.0/5.6., NIST.800-53.r5 AC-3 (15), (7), NIST.800-53.r5 AC-3, PCI DSS v4.0.1/2.2.6 NIST.800-53.r5 AC-3 NIST.800-53.r5 AC-6

Kategori: Lindungi > Keamanan Jaringan

Tingkat keparahan: Tinggi

Jenis sumber daya: AWS::EC2::Instance

AWS Config aturan: [ec2-imdsv2-check](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah versi metadata EC2 instans Anda dikonfigurasi dengan Instance Metadata Service Version 2 (). IMDSv2 Kontrol lolos jika `HttpTokens` diatur ke `required` for IMDSv2. Kontrol gagal jika `HttpTokens` disetel ke `optional`.

Anda menggunakan metadata instans untuk mengonfigurasi atau mengelola instans yang sedang berjalan. IMDS menyediakan akses ke kredensial sementara yang sering diputar. Kredensial ini menghapus kebutuhan untuk kode keras atau mendistribusikan kredensial sensitif ke instance secara manual atau terprogram. IMDS dilampirkan secara lokal ke setiap EC2 instance. Ini berjalan pada alamat IP "link lokal" khusus 169.254.169.254. Alamat IP ini hanya dapat diakses oleh perangkat lunak yang berjalan pada instance.

Versi 2 IMDS menambahkan perlindungan baru untuk jenis kerentanan berikut. Kerentanan ini dapat digunakan untuk mencoba mengakses IMDS.

- Buka firewall aplikasi situs web
- Membuka reverse proxy
- Kerentanan pemalsuan permintaan sisi server (SSRF)
- Buka Layer 3 Firewall dan penerjemahan alamat jaringan (NAT)

Security Hub menyarankan agar Anda mengonfigurasi EC2 instans dengan IMDSv2.

IP Perbaikan

Untuk mengonfigurasi EC2 instans dengan IMDSv2, lihat [Jalur yang disarankan untuk membutuhkan IMDSv2](#) di Panduan EC2 Pengguna Amazon.

[EC2.9] EC2 Instans Amazon seharusnya tidak memiliki alamat publik IPv4

Persyaratan terkait: NIST.800-53.r5 AC-2 1 NIST.800-53.r5 AC-3,, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-4,, NIST.800-53.r5 AC-4 (21) NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7,,

NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9)

Kategori: Lindungi > Konfigurasi jaringan aman > Sumber daya tidak dapat diakses publik

Tingkat keparahan: Tinggi

Jenis sumber daya: AWS::EC2::Instance

AWS Config aturan: [ec2-instance-no-public-ip](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah EC2 instans memiliki alamat IP publik. Kontrol gagal jika `publicIp` bidang hadir dalam item konfigurasi EC2 instance. Kontrol ini hanya berlaku untuk IPv4 alamat.

IPv4 Alamat publik adalah alamat IP yang dapat dijangkau dari internet. Jika Anda meluncurkan instans Anda dengan alamat IP publik, maka EC2 instans Anda dapat dijangkau dari internet. IPv4 Alamat pribadi adalah alamat IP yang tidak dapat dijangkau dari Internet. Anda dapat menggunakan IPv4 alamat pribadi untuk komunikasi antar EC2 instans di VPC yang sama atau di jaringan pribadi Anda yang terhubung.

IPv6 Alamat bersifat unik secara global, jadi dapat diakses dari Internet. Namun, secara default, semua subnet memiliki atribut IPv6 pengalamatan diatur ke false. Untuk informasi selengkapnya IPv6, lihat [Pengalamatan IP di VPC Anda di](#) Panduan Pengguna Amazon VPC.

Jika Anda memiliki kasus penggunaan yang sah untuk mempertahankan EC2 instance dengan alamat IP publik, maka Anda dapat menekan temuan dari kontrol ini. Untuk informasi selengkapnya tentang opsi arsitektur front-end, lihat [Blog AWS Arsitektur](#) atau [seri AWS video seri This Is My Architecture](#).

IP Perbaikan

Gunakan VPC non-default sehingga instans Anda tidak diberi alamat IP publik secara default.

Saat Anda meluncurkan sebuah EC2 instans ke dalam VPC default, itu akan diberi alamat IP publik. Saat Anda meluncurkan EC2 instance ke VPC non-default, konfigurasi subnet menentukan apakah ia menerima alamat IP publik. Subnet memiliki atribut untuk menentukan apakah EC2 instans baru di subnet menerima alamat IP publik dari kumpulan alamat publik IPv4 .

Anda dapat memisahkan alamat IP publik yang ditetapkan secara otomatis dari instans Anda. EC2 Untuk informasi selengkapnya, lihat [IPv4 Alamat publik dan nama host DNS eksternal](#) di EC2 Panduan Pengguna Amazon.

[EC2.10] Amazon EC2 harus dikonfigurasi untuk menggunakan titik akhir VPC yang dibuat untuk layanan Amazon EC2

Persyaratan terkait: NIST.800-53.r5 AC-2 1, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7),, (21) NIST.800-53.r5 AC-4,,, NIST.800-53.r5 AC-4 (11) NIST.800-53.r5 AC-6, (16) NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 Nist.800-171.r2 3.1.3, Nist.800-171.r2 3.13.1 NIST.800-53.r5 SC-7

Kategori: Lindungi > Konfigurasi jaringan aman > Akses pribadi API

Tingkat keparahan: Sedang

Jenis sumber daya: AWS : : EC2 : : VPC

AWS Config aturan: [service-vpc-endpoint-enabled](#)

Jenis jadwal: Periodik

Parameter:

- `serviceName: ec2` (tidak dapat disesuaikan)

Kontrol ini memeriksa apakah titik akhir layanan untuk Amazon EC2 dibuat untuk setiap VPC. Kontrol gagal jika VPC tidak memiliki titik akhir VPC yang dibuat untuk layanan Amazon. EC2

Kontrol ini mengevaluasi sumber daya dalam satu akun. Itu tidak dapat menggambarkan sumber daya yang berada di luar akun. Karena AWS Config Security Hub tidak melakukan pemeriksaan lintas akun, Anda akan melihat FAILED temuan VPCs yang dibagikan di seluruh akun. Security Hub merekomendasikan agar Anda menekan FAILED temuan ini.

Untuk meningkatkan postur keamanan VPC Anda, Anda dapat mengonfigurasi Amazon EC2 untuk menggunakan titik akhir VPC antarmuka. Endpoint antarmuka didukung oleh AWS PrivateLink teknologi yang memungkinkan Anda mengakses operasi Amazon EC2 API secara privat. Hal ini membatasi semua lalu lintas jaringan antara VPC Anda dan Amazon EC2 ke jaringan Amazon. Karena titik akhir hanya didukung dalam Wilayah yang sama, Anda tidak dapat membuat titik akhir

antara VPC dan layanan di Wilayah yang berbeda. Ini mencegah panggilan Amazon EC2 API yang tidak diinginkan ke Wilayah lain.

Untuk mempelajari selengkapnya tentang membuat titik akhir VPC untuk Amazon, EC2 lihat [Amazon dan titik akhir VPC EC2 antarmuka](#) di Panduan Pengguna Amazon. EC2

IP Perbaikan

Untuk membuat titik akhir antarmuka ke Amazon EC2 dari konsol VPC Amazon, [lihat Membuat titik akhir VPC](#) di Panduan.AWS PrivateLink Untuk nama Layanan, pilih com.amazonaws. **region**.ec2.

Anda juga dapat membuat dan melampirkan kebijakan endpoint VPC Anda untuk mengontrol akses ke Amazon API. EC2 Untuk petunjuk cara membuat kebijakan titik akhir VPC, lihat [Membuat kebijakan titik akhir di Panduan Pengguna](#) Amazon. EC2

[EC2.12] Amazon yang tidak terpakai EC2 EIPs harus dihapus

Persyaratan terkait: PCI DSS v3.2.1/2.4, Nist.800-53.r5 CM-8 (1)

Kategori: Lindungi > Konfigurasi jaringan aman

Tingkat keparahan: Rendah

Jenis sumber daya: AWS : : EC2 : : EIP

AWS Config aturan: [eip-attached](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah alamat Elastic IP (EIP) yang dialokasikan ke VPC dilampirkan ke EC2 instance atau antarmuka jaringan elastis yang sedang digunakan (). ENIs

Temuan yang gagal menunjukkan Anda mungkin tidak digunakan EC2 EIPs.

Ini akan membantu Anda mempertahankan inventaris aset yang akurat EIPs di lingkungan data pemegang kartu (CDE) Anda.

IP Perbaikan

Untuk merilis EIP yang tidak digunakan, lihat [Melepaskan alamat IP Elastis](#) di EC2 Panduan Pengguna Amazon.

[EC2.13] Grup keamanan seharusnya tidak mengizinkan masuknya dari 0.0.0.0/0 atau: :/0 ke port 22

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v1.2.0/4.1,, (21),, (11), (16) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), (4), NIST.800-53.r5 SC-7 (5) NIST.800-53.r5 CM-7, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 Nist.800-171.r2 3.1.3, NIST.800-53.r5 SC-7 Nist.800-171.r2 3.13.1, PCI NIST.800-53.r5 SC-7 DSS v3.2.1/1.2.1, PCI DSS v3.2.1/1.3.1, PCI DSS v3.2.1/1.3.1, PCI DSS v3.2.1/1.3.1 2.2.2, PCI DSS v4.0.1/1.3.1 NIST.800-53.r5 SC-7

Kategori: Lindungi > Konfigurasi jaringan aman

Tingkat keparahan: Tinggi

Jenis sumber daya: AWS::EC2::SecurityGroup

AWS Config aturan: [restricted-ssh](#)

Jenis jadwal: Perubahan yang dipicu dan berkala

Parameter: Tidak ada

Kontrol ini memeriksa apakah grup EC2 keamanan Amazon mengizinkan masuknya dari 0.0.0.0/0 atau: :/0 ke port 22. Kontrol gagal jika grup keamanan mengizinkan masuknya dari 0.0.0.0/0 atau: :/0 ke port 22.

Grup keamanan menyediakan penyaringan stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Kami menyarankan agar tidak ada grup keamanan yang mengizinkan akses masuk tanpa batas ke port 22. Menghapus konektivitas tanpa batas ke layanan konsol jarak jauh, seperti SSH, mengurangi eksposur server terhadap risiko.

IP Perbaikan

Untuk melarang masuknya ke port 22, hapus aturan yang memungkinkan akses tersebut untuk setiap grup keamanan yang terkait dengan VPC. Untuk petunjuknya, lihat [Memperbarui aturan grup keamanan](#) di Panduan EC2 Pengguna Amazon. Setelah memilih grup keamanan di EC2 konsol Amazon, pilih Tindakan, Edit aturan masuk. Hapus aturan yang memungkinkan akses ke port 22.

[EC2.14] Grup keamanan seharusnya tidak mengizinkan masuknya dari 0.0.0.0/0 atau: :/0 ke port 3389

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v1.2.0/4.2, PCI DSS v4.0.1/1.3.1

Kategori: Lindungi > Konfigurasi jaringan aman

Tingkat keparahan: Tinggi

Jenis sumber daya: AWS::EC2::SecurityGroup

AWS Config aturan: [restricted-common-ports](#) (aturan yang dibuat adalah `restricted-rdp`)

Jenis jadwal: Perubahan yang dipicu dan berkala

Parameter: Tidak ada

Kontrol ini memeriksa apakah grup EC2 keamanan Amazon mengizinkan masuknya dari 0.0.0.0/0 atau ::/0 ke port 3389. Kontrol gagal jika grup keamanan mengizinkan masuknya dari 0.0.0.0/0 atau ::/0 ke port 3389.

Grup keamanan menyediakan penyaringan stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Kami menyarankan agar tidak ada grup keamanan yang mengizinkan akses masuk tanpa batas ke port 3389. Menghapus konektivitas tanpa batas ke layanan konsol jarak jauh, seperti RDP, mengurangi eksposur server terhadap risiko.

IP Perbaikan

Untuk melarang masuknya ke port 3389, hapus aturan yang memungkinkan akses tersebut untuk setiap grup keamanan yang terkait dengan VPC. Untuk petunjuknya, lihat [Memperbarui aturan grup keamanan](#) di Panduan Pengguna Amazon VPC. Setelah memilih grup keamanan di Konsol VPC Amazon, pilih Tindakan, Edit aturan masuk. Hapus aturan yang memungkinkan akses ke port 3389.

[EC2.15] EC2 Subnet Amazon seharusnya tidak secara otomatis menetapkan alamat IP publik

Persyaratan terkait: NIST.800-53.r5 AC-2 1, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21),, NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (9), PCI DSS v4.0.1/1.4.4

Kategori: Lindungi > Keamanan Jaringan

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::EC2::Subnet

AWS Config aturan: [subnet-auto-assign-public-ip-disabled](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah penugasan publik IPs di subnet MapPublicIpOnLaunch Amazon Virtual Private Cloud (Amazon VPC) telah disetel ke FALSE. Kontrol lolos jika bendera disetel ke FALSE.

Semua subnet memiliki atribut yang menentukan apakah antarmuka jaringan yang dibuat di subnet secara otomatis menerima alamat publik IPv4. Instance yang diluncurkan ke subnet yang memiliki atribut ini diaktifkan memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utama mereka.

IP Perbaikan

Untuk mengonfigurasi subnet agar tidak menetapkan alamat IP publik, lihat [Memodifikasi atribut IPv4 pengalaman publik untuk subnet Anda di Panduan Pengguna](#) Amazon VPC. Kosongkan kotak centang untuk Aktifkan alamat publik IPv4 penetapan otomatis.

[EC2.16] Daftar Kontrol Akses Jaringan yang Tidak Digunakan harus dihapus

Persyaratan terkait: Nist.800-53.r5 CM-8 (1), Nist.800-171.R2 3.4.7, PCI DSS v4.0.1/1.2.7

Kategori: Lindungi > Keamanan Jaringan

Tingkat keparahan: Rendah

Jenis sumber daya: AWS::EC2::NetworkACL

AWS Config aturan: [vpc-network-acl-unused-check](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah ada daftar kontrol akses jaringan (jaringan ACLs) yang tidak digunakan di cloud pribadi virtual (VPC) Anda. Kontrol gagal jika ACL jaringan tidak terkait dengan subnet. Kontrol tidak menghasilkan temuan untuk ACL jaringan default yang tidak digunakan.

Kontrol memeriksa konfigurasi item sumber daya AWS::EC2::NetworkACL dan menentukan hubungan ACL jaringan.

Jika satu-satunya hubungan adalah VPC jaringan ACL, kontrol gagal.

Jika hubungan lain terdaftar, maka kontrol berlalu.

IP Perbaikan

Untuk petunjuk cara menghapus ACL jaringan yang tidak digunakan, lihat [Menghapus ACL jaringan](#) di Panduan Pengguna Amazon VPC. Anda tidak dapat menghapus ACL jaringan default atau ACL jaringan default.

[EC2.17] EC2 Instans Amazon seharusnya tidak menggunakan banyak ENIs

Persyaratan terkait: NIST.800-53.r5 AC-4 (21)

Kategori: Lindungi > Keamanan Jaringan

Tingkat keparahan: Rendah

Jenis sumber daya: AWS::EC2::Instance

AWS Config aturan: [ec2-instance-multiple-eni-check](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah sebuah EC2 instance menggunakan beberapa Elastic Network Interfaces (ENIs) atau Elastic Fabric Adapters (EFAs). Kontrol ini lolos jika adaptor jaringan tunggal digunakan. Kontrol mencakup daftar parameter opsional untuk mengidentifikasi yang diizinkan ENIs. Kontrol ini juga gagal jika EC2 instance milik kluster Amazon EKS menggunakan lebih dari satu ENI. Jika EC2 instans Anda perlu memiliki beberapa ENIs sebagai bagian dari kluster Amazon EKS, Anda dapat menekan temuan kontrol tersebut.

Beberapa ENIs dapat menyebabkan instance dual-homed, yang berarti instance yang memiliki beberapa subnet. Ini dapat menambah kompleksitas keamanan jaringan dan memperkenalkan jalur dan akses jaringan yang tidak diinginkan.

IP Perbaikan

Untuk melepaskan antarmuka jaringan dari EC2 instance, lihat [Melepaskan antarmuka jaringan dari instance](#) di EC2 Panduan Pengguna Amazon.

[EC2.18] Grup keamanan seharusnya hanya mengizinkan lalu lintas masuk yang tidak terbatas untuk port resmi

Persyaratan terkait: NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), (11), (16) NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (5), NIST.800-53.r5 SC-7 Nist.800-171.r2 3.1.3, Nist.800-171.r2 3.1.20, Nist.800-171.r2 3.13.1 NIST.800-53.r5 SC-7

Kategori: Lindungi > Konfigurasi jaringan aman > Konfigurasi grup keamanan

Tingkat keparahan: Tinggi

Jenis sumber daya: AWS::EC2::SecurityGroup

AWS Config aturan: [vpc-sg-open-only-to-authorized-ports](#)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai yang Diizinkan	Nilai yang Diizinkan
<code>authorizeTcpPorts</code>	Daftar port TCP resmi	IntegerList (minimal 1 item dan maksimal 32 item)	1 untuk 65535	[80, 443]
<code>authorizeUdpPorts</code>	Daftar port UDP resmi	IntegerList (minimal 1 item dan maksimal 32 item)	1 untuk 65535	Tidak ada nilai default

Kontrol ini memeriksa apakah grup EC2 keamanan Amazon mengizinkan lalu lintas masuk yang tidak dibatasi dari port yang tidak sah. Status kontrol ditentukan sebagai berikut:

- Jika Anda menggunakan nilai default untuk `authorizedTcpPorts`, kontrol gagal jika grup keamanan mengizinkan lalu lintas masuk yang tidak dibatasi dari port selain port 80 dan 443.

- Jika Anda memberikan nilai khusus untuk `authorizedTcpPorts` atau `authorizedUdpPorts`, kontrol gagal jika grup keamanan mengizinkan lalu lintas masuk yang tidak dibatasi dari port yang tidak terdaftar.

Grup keamanan menyediakan penyaringan stateful dari lalu lintas jaringan masuk dan keluar ke. AWS Aturan grup keamanan harus mengikuti prinsip akses yang paling tidak memiliki hak istimewa. Akses tidak terbatas (alamat IP dengan akhiran /0) meningkatkan peluang aktivitas berbahaya seperti peretasan, denial-of-service serangan, dan kehilangan data. Kecuali port diizinkan secara khusus, port harus menolak akses tidak terbatas.

IP Perbaikan

Untuk mengubah grup keamanan, lihat [Bekerja dengan grup keamanan](#) di Panduan Pengguna Amazon VPC.

[EC2.19] Kelompok keamanan tidak boleh mengizinkan akses tidak terbatas ke port dengan risiko tinggi

Persyaratan terkait: NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), (1),, NIST.800-53.r5 CA-9 (11), (16) NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2(2), NIST.800-53.r5 CM-7, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (21), (4), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (5), NIST.800-53.r5 SC-7 Nist.800-171.r2 3.1.3, NIST.800-53.r5 SC-7 Nist.800-171.r2 3.1.20, Nist.800-171.r2 3.13.1

Kategori: Lindungi > Akses jaringan terbatas

Tingkat keparahan: Kritis

Jenis sumber daya: AWS::EC2::SecurityGroup

AWS Config aturan: [restricted-common-ports](#)(aturan yang dibuat adalah `vpc-sg-restricted-common-ports`)

Jenis jadwal: Perubahan yang dipicu dan berkala

Parameter: "blockedPorts":

"20,21,22,23,25,110,135,143,445,1433,1434,3000,3306,3389,4333,5000,5432,5500,5600"
(tidak dapat disesuaikan)

Kontrol ini memeriksa apakah lalu lintas masuk yang tidak dibatasi untuk grup EC2 keamanan Amazon dapat diakses ke port tertentu yang dianggap berisiko tinggi. Kontrol ini gagal jika salah

satu aturan dalam grup keamanan mengizinkan lalu lintas masuk dari '0.0.0.0/0' atau ':::/0' ke port tersebut.

Grup keamanan menyediakan penyaringan stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Akses tak terbatas (0.0.0.0/0) meningkatkan peluang aktivitas jahat, seperti peretasan, denial-of-service serangan, dan hilangnya data. Tidak ada grup keamanan yang mengizinkan akses masuk tanpa batas ke port berikut:

- 20, 21 (FTP)
- 22 (SSH)
- 23 (Telnet)
- 25 (SMTP)
- 110 (POP3)
- 135 (RPC)
- 143 (IMAP)
- 445 (CIFS)
- 1433, 1434 (MSSQL)
- 3000 (kerangka kerja pengembangan web Go, Node.js, dan Ruby)
- 3306 (MySQL)
- 3389 (RDP)
- 4333 (ahsp)
- 5000 (Kerangka pengembangan web Python)
- 5432 (PostgreSQL)
- 5500 (fcp-addr-srvr1)
- 5601 (Dasbor) OpenSearch
- 8080 (proxy)
- 8088 (port HTTP lama)
- 8888 (port HTTP alternatif)
- 9200 atau 9300 () OpenSearch

IP Perbaikan

Untuk menghapus aturan dari grup keamanan, lihat [Menghapus aturan dari grup keamanan](#) di Panduan EC2 Pengguna Amazon.

[EC2.20] Kedua terowongan VPN untuk koneksi AWS Site-to-Site VPN harus siap

Persyaratan terkait: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6(2), NIST.800-53.r5 SC-3 6, NIST.800-53.r5 SC-5 (2), Nist.800-53.R5 SI-13 (5), Nist.800-171.R2 3.1.13, Nist.800-171.R2 3.1.20

Kategori: Pulihkan > Ketahanan > Ketersediaan tinggi

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::EC2::VPNConnection

AWS Config aturan: [vpc-vpn-2-tunnels-up](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Terowongan VPN adalah tautan terenkripsi tempat data dapat lewat dari jaringan pelanggan ke atau dari AWS koneksi AWS Site-to-Site VPN. Setiap koneksi VPN mencakup dua terowongan VPN yang dapat Anda gunakan secara bersamaan untuk ketersediaan tinggi. Memastikan bahwa kedua terowongan VPN siap untuk koneksi VPN penting untuk mengonfirmasi koneksi yang aman dan sangat tersedia antara AWS VPC dan jaringan jarak jauh Anda.

Kontrol ini memeriksa apakah kedua terowongan VPN yang disediakan oleh AWS Site-to-Site VPN berada dalam status UP. Kontrol gagal jika salah satu atau kedua terowongan berada dalam status DOWN.

IP Perbaikan

Untuk mengubah opsi terowongan VPN, lihat [Memodifikasi opsi terowongan Site-to-Site AWS Site-to-Site VPN](#) di Panduan Pengguna VPN.

[EC2.21] Jaringan ACLs seharusnya tidak mengizinkan masuknya dari 0.0.0.0/0 ke port 22 atau port 3389.

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v1.4.0/5.1, Tolok Ukur AWS Yayasan CIS v3.0.0/5.1, (21), (1),, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 SC-7 (5), Nist.800-171.r2 3.1.3,

NIST.800-53.r5 CA-9 Nist.800-171.r2 3.1.20 NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2(2), NIST.800-53.r5 CM-7, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 Nist.800-171.r2 3.13.1, PCI DSS v4.0.1/1.3.1

Kategori: Lindungi > Konfigurasi Jaringan Aman

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::EC2::NetworkACL

AWS Config aturan: [nacl-no-unrestricted-ssh-rdp](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah daftar kontrol akses jaringan (ACL jaringan) memungkinkan akses tidak terbatas ke port TCP default untuk lalu lintas masuk SSH/RDP. Kontrol gagal jika entri masuk ACL jaringan memungkinkan blok CIDR sumber '0.0.0.0/0' atau '::/0' untuk port TCP 22 atau 3389. Kontrol tidak menghasilkan temuan untuk ACL jaringan default.

Akses ke port administrasi server jarak jauh, seperti port 22 (SSH) dan port 3389 (RDP), tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke sumber daya dalam VPC Anda.

IP Perbaikan

Untuk mengedit aturan lalu lintas ACL jaringan, lihat [Bekerja dengan jaringan ACLs](#) di Panduan Pengguna Amazon VPC.

[EC2.22] Grup EC2 keamanan Amazon yang tidak digunakan harus dihapus

Kategori: Identifikasi > Inventaris

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::EC2::NetworkInterface, AWS::EC2::SecurityGroup

AWS Config aturan: [ec2-security-group-attached-to-eni-periodic](#)

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah grup keamanan dilampirkan ke instans Amazon Elastic Compute Cloud (Amazon EC2) atau ke antarmuka elastic network. Kontrol gagal jika grup keamanan tidak terkait dengan EC2 instans Amazon atau elastic network interface.

 Important

Pada tanggal 20 September 2023, Security Hub menghapus kontrol ini dari standar Praktik Terbaik Keamanan AWS Dasar dan NIST SP 800-53 Revisi 5. Kontrol ini terus menjadi bagian dari standar yang AWS Control Tower dikelola layanan. Kontrol ini menghasilkan temuan yang dilewatkan jika grup keamanan dilampirkan ke EC2 instance atau elastic network interface. Namun, untuk kasus penggunaan tertentu, kelompok keamanan yang tidak terikat tidak menimbulkan risiko keamanan. Anda dapat menggunakan EC2 kontrol lain—seperti EC2 .2, EC2 .13, EC2 .14, EC2 .18, dan EC2 .19—untuk memantau grup keamanan Anda.

IP Perbaikan

Untuk membuat, menetapkan, dan menghapus grup keamanan, lihat [Grup keamanan untuk EC2 instans Anda](#) di EC2 Panduan Pengguna Amazon.

[EC2.23] Amazon EC2 Transit Gateways seharusnya tidak secara otomatis menerima permintaan lampiran VPC

Persyaratan terkait: NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 CA-9 (1), Nist.800-53.r5 CM-2

Kategori: Lindungi > Konfigurasi jaringan aman

Tingkat keparahan: Tinggi

Jenis sumber daya: AWS::EC2::TransitGateway

AWS Config aturan: [ec2-transit-gateway-auto-vpc-attach-disabled](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah gateway EC2 transit secara otomatis menerima lampiran VPC bersama. Kontrol ini gagal untuk gateway transit yang secara otomatis menerima permintaan lampiran VPC bersama.

Menghidupkan `AutoAcceptSharedAttachments` mengonfigurasi gateway transit untuk secara otomatis menerima permintaan lampiran VPC lintas akun apa pun tanpa memverifikasi permintaan atau akun tempat lampiran berasal. Untuk mengikuti praktik otorisasi dan otentikasi terbaik, kami sarankan untuk mematikan fitur ini untuk memastikan bahwa hanya permintaan lampiran VPC resmi yang diterima.

IP Perbaikan

Untuk mengubah gateway transit, lihat [Memodifikasi gateway transit](#) di Panduan Pengembang Amazon VPC.

[EC2.24] Jenis instance EC2 paravirtual Amazon tidak boleh digunakan

Persyaratan terkait: Nist.800-53.r5 CM-2, Nist.800-53.r5 CM-2 (2)

Kategori: Identifikasi > Kerentanan, tambalan, dan manajemen versi

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::EC2::Instance

AWS Config aturan: [ec2-paravirtual-instance-check](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah jenis virtualisasi EC2 instance adalah paravirtual. Kontrol gagal jika EC2 instance diatur keparavirtual. `virtualizationType`

Linux Amazon Machine Images (AMIs) menggunakan salah satu dari dua jenis virtualisasi: paravirtual (PV) atau mesin virtual perangkat keras (HVM). Perbedaan utama antara PV dan HVM AMIs adalah caranya melakukan booting dan apakah keduanya dapat memanfaatkan ekstensi perangkat keras khusus (CPU, jaringan, dan penyimpanan) untuk kinerja yang lebih baik.

Secara historis, tamu PV memiliki kinerja yang lebih baik dibandingkan tamu HVM dalam banyak kasus, tetapi karena peningkatan virtualisasi HVM dan ketersediaan driver IT untuk HVM AMIs, ini tidak lagi benar. Untuk informasi selengkapnya, lihat [Jenis virtualisasi Linux AMI](#) dalam Panduan EC2 Pengguna Amazon.

IP Perbaikan

Untuk memperbarui EC2 instance ke jenis instans baru, lihat [Mengubah jenis instans](#) di Panduan EC2 Pengguna Amazon.

[EC2.25] Templat EC2 peluncuran Amazon tidak boleh menetapkan publik IPs ke antarmuka jaringan

Persyaratan terkait: NIST.800-53.r5 AC-2 1, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21),, NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (9), PCI DSS v4.0.1/1.4.4

Kategori: Lindungi > Konfigurasi jaringan aman > Sumber daya tidak dapat diakses publik

Tingkat keparahan: Tinggi

Jenis sumber daya: AWS::EC2::LaunchTemplate

AWS Config aturan: [ec2-launch-template-public-ip-disabled](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah templat EC2 peluncuran Amazon dikonfigurasi untuk menetapkan alamat IP publik ke antarmuka jaringan saat diluncurkan. Kontrol gagal jika template EC2 peluncuran dikonfigurasi untuk menetapkan alamat IP publik ke antarmuka jaringan atau jika ada setidaknya satu antarmuka jaringan yang memiliki alamat IP publik.

Alamat IP publik adalah alamat yang dapat dijangkau dari internet. Jika Anda mengonfigurasi antarmuka jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan antarmuka jaringan tersebut dapat dijangkau dari internet. EC2 sumber daya tidak boleh diakses publik karena ini memungkinkan akses yang tidak diinginkan ke beban kerja Anda.

IP Perbaikan

Untuk memperbarui template EC2 peluncuran, lihat [Mengubah setelan antarmuka jaringan default](#) di Panduan Pengguna Amazon EC2 Auto Scaling.

[EC2.28] Volume EBS harus dicakup oleh rencana cadangan

Kategori: Pulih> Ketahanan > Cadangan diaktifkan

Persyaratan terkait: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6, NIST.800-53.r5 CP-6(1), NIST.800-53.r5 CP-6(2), NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5 (2), NIST.800-53.R5 SI-12, NIST.800-53.R5 SI-13 (5)

Tingkat keparahan: Rendah

Jenis sumber daya: AWS::EC2::Volume

AWS Config aturan: [ebs-resources-protected-by-backup-plan](#)

Jenis jadwal: Periodik

Parameter:

Parameter	Deskripsi	Tipe	Nilai yang Diizinkan	Nilai yang Diizinkan
backupVaultLockCheck	Kontrol menghasilkan PASSED temuan jika parameter disetel ke true dan sumber daya menggunakan AWS Backup Vault Lock.	Boolean	true atau false	Tidak ada nilai default

Kontrol ini mengevaluasi jika volume Amazon EBS dalam in-use status tercakup oleh paket cadangan. Kontrol gagal jika volume EBS tidak tercakup oleh paket cadangan. Jika Anda menyetel backupVaultLockCheck parameter sama dengan true, kontrol hanya akan diteruskan jika volume EBS dicadangkan di brankas yang AWS Backup terkunci.

Cadangan membantu Anda pulih lebih cepat dari insiden keamanan. Mereka juga memperkuat ketahanan sistem Anda. Menyertakan volume Amazon EBS dalam paket cadangan membantu Anda melindungi data dari kehilangan atau penghapusan yang tidak diinginkan.

IP Perbaikan

Untuk menambahkan volume Amazon EBS ke paket AWS Backup cadangan, lihat [Menetapkan sumber daya ke paket cadangan di Panduan AWS Backup](#) Pengembang.

[EC2.33] lampiran gateway EC2 transit harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::EC2::TransitGatewayAttachment`

AWS Config aturan: `tagged-ec2-transitgatewayattachment` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai yang Diizinkan	Nilai yang Diizinkan
<code>requiredTagKeys</code>	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS .	Tidak ada nilai default

Kontrol ini memeriksa apakah lampiran gateway EC2 transit Amazon memiliki tag dengan kunci tertentu yang ditentukan dalam parameter `requiredTagKeys`. Kontrol gagal jika lampiran gateway transit tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter `requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika lampiran gateway transit tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws:`, diabaikan.

Tanda adalah sebuah label yang Anda tetapkan ke sebuah AWS sumber daya, dan terdiri dari sebuah kunci dan nilai opsional. Anda dapat membuat tag untuk mengkategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat Anda menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal

atau serangkaian kebijakan terpisah untuk penanggung jawab IAM Anda. Anda dapat merancang kebijakan ABAC ini untuk mengizinkan operasi ketika tag penanggung jawab cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat [Untuk apa ABAC untuk? AWS](#) di Panduan Pengguna IAM.

Note

Jangan menambahkan informasi pengenalan pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat [Menandai AWS sumber daya Anda](#) di Referensi Umum AWS

IP Perbaikan

Untuk menambahkan tag ke lampiran gateway EC2 transit, lihat [Menandai EC2 sumber daya Amazon Anda](#) di Panduan EC2 Pengguna Amazon.

[EC2.34] tabel rute gateway EC2 transit harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::EC2::TransitGatewayRouteTable`

AWS Config aturan: `tagged-ec2-transitgatewayroutetable` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai yang Diizinkan	Nilai yang Diizinkan
<code>requiredTagKeys</code>	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi	Tidak ada nilai default

Parameter	Deskripsi	Tipe	Nilai yang Diizinkan	Nilai yang Diizinkan
			persyaratan AWS .	

Kontrol ini memeriksa apakah tabel rute gateway EC2 transit Amazon memiliki tag dengan kunci tertentu yang ditentukan dalam parameter `requiredTagKeys`. Kontrol gagal jika tabel rute gateway transit tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter `requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika tabel rute gateway transit tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws:`, diabaikan.

Tanda adalah sebuah label yang Anda tetapkan ke sebuah AWS sumber daya, dan terdiri dari sebuah kunci dan nilai opsional. Anda dapat membuat tag untuk mengkategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat Anda menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk penanggung jawab IAM Anda. Anda dapat merancang kebijakan ABAC ini untuk mengizinkan operasi ketika tag penanggung jawab cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat [Untuk apa ABAC untuk? AWS](#) di Panduan Pengguna IAM.

Note

Jangan menambahkan informasi pengenalan pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat [Menandai AWS sumber daya Anda](#) di Referensi Umum AWS

IP Perbaikan

Untuk menambahkan tag ke tabel rute gateway EC2 transit, lihat [Menandai EC2 sumber daya Amazon Anda](#) di Panduan EC2 Pengguna Amazon.

[EC2.35] antarmuka EC2 jaringan harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::EC2::NetworkInterface`

AWS Config aturan: `tagged-ec2-networkinterface` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai yang Diizinkan	Nilai yang Diizinkan
<code>requiredTagKeys</code>	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS .	Tidak ada nilai default

Kontrol ini memeriksa apakah antarmuka EC2 jaringan Amazon memiliki tag dengan kunci tertentu yang ditentukan dalam parameter `requiredTagKeys`. Kontrol gagal jika antarmuka jaringan tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter `requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika antarmuka jaringan tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws:`, diabaikan.

Tanda adalah sebuah label yang Anda tetapkan ke sebuah AWS sumber daya, dan terdiri dari sebuah kunci dan nilai opsional. Anda dapat membuat tag untuk mengkategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat Anda menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal

atau serangkaian kebijakan terpisah untuk penanggung jawab IAM Anda. Anda dapat merancang kebijakan ABAC ini untuk mengizinkan operasi ketika tag penanggung jawab cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat [Untuk apa ABAC untuk? AWS](#) di Panduan Pengguna IAM.

Note

Jangan menambahkan informasi pengenalan pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat [Menandai AWS sumber daya Anda](#) di Referensi Umum AWS

IP Perbaikan

Untuk menambahkan tag ke antarmuka EC2 jaringan, lihat [Menandai EC2 sumber daya Amazon Anda](#) di Panduan EC2 Pengguna Amazon.

[EC2.36] gateway EC2 pelanggan harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: AWS::EC2::CustomerGateway

AWS Config aturan: tagged-ec2-customergateway (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai yang Diizinkan	Nilai yang Diizinkan
requiredTagKeys	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi	Tidak ada nilai default

Parameter	Deskripsi	Tipe	Nilai yang Diizinkan	Nilai yang Diizinkan
			persyaratan AWS .	

Kontrol ini memeriksa apakah gateway EC2 pelanggan Amazon memiliki tag dengan kunci spesifik yang ditentukan dalam parameter `requiredTagKeys`. Kontrol gagal jika gateway pelanggan tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter `requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika gateway pelanggan tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws:`, diabaikan.

Tanda adalah sebuah label yang Anda tetapkan ke sebuah AWS sumber daya, dan terdiri dari sebuah kunci dan nilai opsional. Anda dapat membuat tag untuk mengkategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat Anda menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk penanggung jawab IAM Anda. Anda dapat merancang kebijakan ABAC ini untuk memungkinkan operasi ketika tag penanggung jawab cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat [Untuk apa ABAC untuk? AWS](#) di Panduan Pengguna IAM.

Note

Jangan menambahkan informasi pengenalan pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat [Menandai AWS sumber daya Anda](#) di Referensi Umum AWS.

IP Perbaikan

Untuk menambahkan tag ke gateway EC2 pelanggan, lihat [Menandai EC2 sumber daya Amazon Anda](#) di Panduan EC2 Pengguna Amazon.

[EC2.37] Alamat IP EC2 elastis harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: AWS :: EC2 :: EIP

AWS Config aturan: tagged-ec2-eip (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai yang Diizinkan	Nilai yang Diizinkan
<code>requiredTagKeys</code>	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS .	Tidak ada nilai default

Kontrol ini memeriksa apakah alamat IP Amazon EC2 Elastic memiliki tag dengan kunci spesifik yang ditentukan dalam parameter `requiredTagKeys`. Kontrol gagal jika alamat IP Elastis tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter `requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika alamat IP Elastis tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws :`, diabaikan.

Tanda adalah sebuah label yang Anda tetapkan ke sebuah AWS sumber daya, dan terdiri dari sebuah kunci dan nilai opsional. Anda dapat membuat tag untuk mengkategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat Anda menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal

atau serangkaian kebijakan terpisah untuk penanggung jawab IAM Anda. Anda dapat merancang kebijakan ABAC ini untuk memungkinkan operasi ketika tag penanggung jawab cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat [Untuk apa ABAC untuk? AWS](#) di Panduan Pengguna IAM.

Note

Jangan menambahkan informasi pengenalan pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat [Menandai AWS sumber daya Anda](#) di Referensi Umum AWS

IP Perbaikan

Untuk menambahkan tag ke alamat IP EC2 Elastis, lihat [Menandai EC2 sumber daya Amazon Anda](#) di Panduan EC2 Pengguna Amazon.

[EC2.38] EC2 instance harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: AWS::EC2::Instance

AWS Config aturan: tagged-ec2-instance (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai yang Diizinkan	Nilai yang Diizinkan
requiredTagKeys	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi	Tidak ada nilai default

Parameter	Deskripsi	Tipe	Nilai yang Diizinkan	Nilai yang Diizinkan
			persyaratan AWS .	

Kontrol ini memeriksa apakah EC2 instance Amazon memiliki tag dengan kunci tertentu yang ditentukan dalam parameter `requiredTagKeys`. Kontrol gagal jika instance tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter `requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika instance tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws :`, diabaikan.

Tanda adalah sebuah label yang Anda tetapkan ke sebuah AWS sumber daya, dan terdiri dari sebuah kunci dan nilai opsional. Anda dapat membuat tag untuk mengkategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat Anda menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk penanggung jawab IAM Anda. Anda dapat merancang kebijakan ABAC ini untuk memungkinkan operasi ketika tag penanggung jawab cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat [Untuk apa ABAC untuk? AWS](#) di Panduan Pengguna IAM.

Note

Jangan menambahkan informasi pengenalan pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat [Menandai AWS sumber daya Anda](#) di Referensi Umum AWS

IP Perbaikan

Untuk menambahkan tag ke EC2 instans, lihat [Menandai EC2 sumber daya Amazon Anda](#) di Panduan EC2 Pengguna Amazon.

[EC2.39] gateway EC2 internet harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: AWS::EC2::InternetGateway

AWS Config aturan: tagged-ec2-internetgateway (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai yang Diizinkan	Nilai yang Diizinkan
<code>requiredTagKeys</code>	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS .	Tidak ada nilai default

Kontrol ini memeriksa apakah gateway EC2 internet Amazon memiliki tag dengan kunci tertentu yang ditentukan dalam parameter `requiredTagKeys`. Kontrol gagal jika gateway internet tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter `requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika gateway internet tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws:`, diabaikan.

Tanda adalah sebuah label yang Anda tetapkan ke sebuah AWS sumber daya, dan terdiri dari sebuah kunci dan nilai opsional. Anda dapat membuat tag untuk mengkategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat Anda menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal

atau serangkaian kebijakan terpisah untuk penanggung jawab IAM Anda. Anda dapat merancang kebijakan ABAC ini untuk memungkinkan operasi ketika tag penanggung jawab cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat [Untuk apa ABAC untuk? AWS](#) di Panduan Pengguna IAM.

Note

Jangan menambahkan informasi pengenalan pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat [Menandai AWS sumber daya Anda](#) di Referensi Umum AWS

IP Perbaikan

Untuk menambahkan tag ke gateway EC2 internet, lihat [Menandai EC2 sumber daya Amazon Anda](#) di Panduan EC2 Pengguna Amazon.

[EC2.40] Gateway EC2 NAT harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: AWS::EC2::NatGateway

AWS Config aturan: tagged-ec2-natgateway (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai yang Diizinkan	Nilai yang Diizinkan
requiredTagKeys	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi	Tidak ada nilai default

Parameter	Deskripsi	Tipe	Nilai yang Diizinkan	Nilai yang Diizinkan
			persyaratan AWS .	

Kontrol ini memeriksa apakah gateway terjemahan alamat EC2 jaringan Amazon (NAT) memiliki tag dengan kunci tertentu yang ditentukan dalam parameter `requiredTagKeys`. Kontrol gagal jika gateway NAT tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter `requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika gateway NAT tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws:`, diabaikan.

Tanda adalah sebuah label yang Anda tetapkan ke sebuah AWS sumber daya, dan terdiri dari sebuah kunci dan nilai opsional. Anda dapat membuat tag untuk mengkategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat Anda menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk penanggung jawab IAM Anda. Anda dapat merancang kebijakan ABAC ini untuk memungkinkan operasi ketika tag penanggung jawab cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat [Untuk apa ABAC untuk? AWS](#) di Panduan Pengguna IAM.

Note

Jangan menambahkan informasi pengenalan pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat [Menandai AWS sumber daya Anda](#) di Referensi Umum AWS

IP Perbaikan

Untuk menambahkan tag ke gateway EC2 NAT, lihat [Menandai EC2 sumber daya Amazon Anda](#) di Panduan EC2 Pengguna Amazon.

[EC2.41] EC2 jaringan ACLs harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::EC2::NetworkACL`

AWS Config aturan: `tagged-ec2-networkacl` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai yang Diizinkan	Nilai yang Diizinkan
<code>requiredTagKeys</code>	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS .	Tidak ada nilai default

Kontrol ini memeriksa apakah daftar kontrol akses EC2 jaringan Amazon (ACL jaringan) memiliki tag dengan kunci tertentu yang ditentukan dalam parameter `requiredTagKeys`. Kontrol gagal jika ACL jaringan tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter `requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika ACL jaringan tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws:`, diabaikan.

Tanda adalah sebuah label yang Anda tetapkan ke sebuah AWS sumber daya, dan terdiri dari sebuah kunci dan nilai opsional. Anda dapat membuat tag untuk mengkategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat Anda menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal

atau serangkaian kebijakan terpisah untuk penanggung jawab IAM Anda. Anda dapat merancang kebijakan ABAC ini untuk memungkinkan operasi ketika tag penanggung jawab cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat [Untuk apa ABAC untuk? AWS](#) di Panduan Pengguna IAM.

Note

Jangan menambahkan informasi pengenalan pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat [Menandai AWS sumber daya Anda](#) di Referensi Umum AWS

IP Perbaikan

Untuk menambahkan tag ke ACL EC2 jaringan, lihat [Menandai EC2 sumber daya Amazon Anda](#) di Panduan EC2 Pengguna Amazon.

[EC2.42] tabel EC2 rute harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: AWS::EC2::RouteTable

AWS Config aturan: tagged-ec2-routetable (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai yang Diizinkan	Nilai yang Diizinkan
requiredTagKeys	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi	Tidak ada nilai default

Parameter	Deskripsi	Tipe	Nilai yang Diizinkan	Nilai yang Diizinkan
			persyaratan AWS .	

Kontrol ini memeriksa apakah tabel EC2 rute Amazon memiliki tag dengan kunci tertentu yang ditentukan dalam parameter `requiredTagKeys`. Kontrol gagal jika tabel rute tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter `requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika tabel rute tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws :`, diabaikan.

Tanda adalah sebuah label yang Anda tetapkan ke sebuah AWS sumber daya, dan terdiri dari sebuah kunci dan nilai opsional. Anda dapat membuat tag untuk mengkategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat Anda menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk penanggung jawab IAM Anda. Anda dapat merancang kebijakan ABAC ini untuk memungkinkan operasi ketika tag penanggung jawab cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat [Untuk apa ABAC untuk? AWS](#) di Panduan Pengguna IAM.

Note

Jangan menambahkan informasi pengenalan pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat [Menandai AWS sumber daya Anda](#) di Referensi Umum AWS

IP Perbaikan

Untuk menambahkan tag ke tabel EC2 rute, lihat [Menandai EC2 sumber daya Amazon Anda](#) di Panduan EC2 Pengguna Amazon.

[EC2.43] grup EC2 keamanan harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::EC2::SecurityGroup`

AWS Config aturan: `tagged-ec2-securitygroup` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai yang Diizinkan	Nilai yang Diizinkan
<code>requiredTagKeys</code>	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS .	Tidak ada nilai default

Kontrol ini memeriksa apakah grup EC2 keamanan Amazon memiliki tag dengan kunci tertentu yang ditentukan dalam parameter `requiredTagKeys`. Kontrol gagal jika grup keamanan tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter `requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika grup keamanan tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws :`, diabaikan.

Tanda adalah sebuah label yang Anda tetapkan ke sebuah AWS sumber daya, dan terdiri dari sebuah kunci dan nilai opsional. Anda dapat membuat tag untuk mengkategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat Anda menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal

atau serangkaian kebijakan terpisah untuk penanggung jawab IAM Anda. Anda dapat merancang kebijakan ABAC ini untuk memungkinkan operasi ketika tag penanggung jawab cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat [Untuk apa ABAC untuk? AWS](#) di Panduan Pengguna IAM.

Note

Jangan menambahkan informasi pengenalan pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat [Menandai AWS sumber daya Anda](#) di Referensi Umum AWS

IP Perbaikan

Untuk menambahkan tag ke grup EC2 keamanan, lihat [Menandai EC2 sumber daya Amazon Anda](#) di Panduan EC2 Pengguna Amazon.

[EC2.44] EC2 subnet harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: AWS :: EC2 :: Subnet

AWS Config aturan: tagged-ec2-subnet (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai yang Diizinkan	Nilai yang Diizinkan
requiredTagKeys	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi	Tidak ada nilai default

Parameter	Deskripsi	Tipe	Nilai yang Diizinkan	Nilai yang Diizinkan
			persyaratan AWS .	

Kontrol ini memeriksa apakah EC2 subnet Amazon memiliki tag dengan kunci tertentu yang ditentukan dalam parameter `requiredTagKeys`. Kontrol gagal jika subnet tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter `requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika subnet tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws :`, diabaikan.

Tanda adalah sebuah label yang Anda tetapkan ke sebuah AWS sumber daya, dan terdiri dari sebuah kunci dan nilai opsional. Anda dapat membuat tag untuk mengkategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat Anda menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk penanggung jawab IAM Anda. Anda dapat merancang kebijakan ABAC ini untuk memungkinkan operasi ketika tag penanggung jawab cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat [Untuk apa ABAC untuk? AWS](#) di Panduan Pengguna IAM.

Note

Jangan menambahkan informasi pengenalan pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat [Menandai AWS sumber daya Anda](#) di Referensi Umum AWS

IP Perbaikan

Untuk menambahkan tag ke EC2 subnet, lihat [Menandai EC2 sumber daya Amazon Anda](#) di Panduan EC2 Pengguna Amazon.

[EC2.45] EC2 volume harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: AWS :: EC2 :: Volume

AWS Config aturan: tagged-ec2-volume (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai yang Diizinkan	Nilai yang Diizinkan
<code>requiredTagKeys</code>	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS .	Tidak ada nilai default

Kontrol ini memeriksa apakah EC2 volume Amazon memiliki tag dengan kunci tertentu yang ditentukan dalam parameter `requiredTagKeys`. Kontrol gagal jika volume tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter `requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika volume tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws:`, diabaikan.

Tanda adalah sebuah label yang Anda tetapkan ke sebuah AWS sumber daya, dan terdiri dari sebuah kunci dan nilai opsional. Anda dapat membuat tag untuk mengkategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat Anda menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal

atau serangkaian kebijakan terpisah untuk penanggung jawab IAM Anda. Anda dapat merancang kebijakan ABAC ini untuk memungkinkan operasi ketika tag penanggung jawab cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat [Untuk apa ABAC untuk? AWS](#) di Panduan Pengguna IAM.

Note

Jangan menambahkan informasi pengenalan pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat [Menandai AWS sumber daya Anda](#) di Referensi Umum AWS

IP Perbaikan

Untuk menambahkan tag ke EC2 volume, lihat [Menandai EC2 sumber daya Amazon Anda](#) di Panduan EC2 Pengguna Amazon.

[EC2.46] Amazon VPCs harus diberi tag

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: AWS :: EC2 :: VPC

AWS Config aturan: tagged-ec2-vpc (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai yang Diizinkan	Nilai yang Diizinkan
requiredTagKeys	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi	Tidak ada nilai default

Parameter	Deskripsi	Tipe	Nilai yang Diizinkan	Nilai yang Diizinkan
			persyaratan AWS .	

Kontrol ini memeriksa apakah Amazon Virtual Private Cloud (Amazon VPC) memiliki tag dengan kunci spesifik yang ditentukan dalam parameter. `requiredTagKeys` Kontrol gagal jika VPC Amazon tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter. `requiredTagKeys` Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika VPC Amazon tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws:`, diabaikan.

Tanda adalah sebuah label yang Anda tetapkan ke sebuah AWS sumber daya, dan terdiri dari sebuah kunci dan nilai opsional. Anda dapat membuat tag untuk mengkategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat Anda menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk penanggung jawab IAM Anda. Anda dapat merancang kebijakan ABAC ini untuk memungkinkan operasi ketika tag penanggung jawab cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat [Untuk apa ABAC untuk? AWS](#) di Panduan Pengguna IAM.

Note

Jangan menambahkan informasi pengenalan pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat [Menandai AWS sumber daya Anda](#) di Referensi Umum AWS

IP Perbaikan

Untuk menambahkan tag ke VPC, lihat [Menandai EC2 sumber daya Amazon](#) Anda di EC2 Panduan Pengguna Amazon.

[EC2.47] Layanan titik akhir Amazon VPC harus diberi tag

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: AWS::EC2::VPCEndpointService

AWS Config aturan: tagged-ec2-vpcendpointservice (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai yang Diizinkan	Nilai yang Diizinkan
<code>requiredTagKeys</code>	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS .	Tidak ada nilai default

Kontrol ini memeriksa apakah layanan titik akhir VPC Amazon memiliki tag dengan kunci spesifik yang ditentukan dalam parameter. `requiredTagKeys` Kontrol gagal jika layanan endpoint tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter `requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika layanan titik akhir tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws:`, diabaikan.

Tanda adalah sebuah label yang Anda tetapkan ke sebuah AWS sumber daya, dan terdiri dari sebuah kunci dan nilai opsional. Anda dapat membuat tag untuk mengkategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat Anda menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal

atau serangkaian kebijakan terpisah untuk penanggung jawab IAM Anda. Anda dapat merancang kebijakan ABAC ini untuk memungkinkan operasi ketika tag penanggung jawab cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat [Untuk apa ABAC untuk? AWS](#) di Panduan Pengguna IAM.

Note

Jangan menambahkan informasi pengenalan pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat [Menandai AWS sumber daya Anda](#) di Referensi Umum AWS

IP Perbaikan

Untuk menambahkan tag ke layanan titik akhir Amazon VPC, lihat [Mengelola Tag](#) di bagian [Mengonfigurasi layanan titik akhir](#) dari Panduan.AWS PrivateLink

[EC2.48] Log aliran VPC Amazon harus diberi tag

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: AWS::EC2::FlowLog

AWS Config aturan: tagged-ec2-flowlog (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai yang Diizinkan	Nilai yang Diizinkan
requiredTagKeys	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi	Tidak ada nilai default

Parameter	Deskripsi	Tipe	Nilai yang Diizinkan	Nilai yang Diizinkan
			persyaratan AWS .	

Kontrol ini memeriksa apakah log aliran VPC Amazon memiliki tag dengan kunci tertentu yang ditentukan dalam parameter. `requiredTagKeys` Kontrol gagal jika log aliran tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter `requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika log aliran tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws :`, diabaikan.

Tanda adalah sebuah label yang Anda tetapkan ke sebuah AWS sumber daya, dan terdiri dari sebuah kunci dan nilai opsional. Anda dapat membuat tag untuk mengkategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat Anda menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk penanggung jawab IAM Anda. Anda dapat merancang kebijakan ABAC ini untuk memungkinkan operasi ketika tag penanggung jawab cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat [Untuk apa ABAC untuk? AWS](#) di Panduan Pengguna IAM.

Note

Jangan menambahkan informasi pengenalan pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat [Menandai AWS sumber daya Anda](#) di Referensi Umum AWS

IP Perbaikan

Untuk menambahkan tag ke log aliran VPC Amazon, lihat [Menandai log alur di Panduan Pengguna Amazon VPC](#).

[EC2.49] Koneksi peering VPC Amazon harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::EC2::VPCPeeringConnection`

AWS Config aturan: `tagged-ec2-vpcpeeringconnection` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai yang Diizinkan	Nilai yang Diizinkan
<code>requiredTagKeys</code>	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS .	Tidak ada nilai default

Kontrol ini memeriksa apakah koneksi peering VPC Amazon memiliki tag dengan kunci spesifik yang ditentukan dalam parameter. `requiredTagKeys` Kontrol gagal jika koneksi peering tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter `requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika koneksi peering tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws:`, diabaikan.

Tanda adalah sebuah label yang Anda tetapkan ke sebuah AWS sumber daya, dan terdiri dari sebuah kunci dan nilai opsional. Anda dapat membuat tag untuk mengkategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat Anda menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal

atau serangkaian kebijakan terpisah untuk penanggung jawab IAM Anda. Anda dapat merancang kebijakan ABAC ini untuk memungkinkan operasi ketika tag penanggung jawab cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat [Untuk apa ABAC untuk? AWS](#) di Panduan Pengguna IAM.

Note

Jangan menambahkan informasi pengenalan pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat [Menandai AWS sumber daya Anda](#) di Referensi Umum AWS

IP Perbaikan

Untuk menambahkan tag ke koneksi peering VPC Amazon, lihat Menandai [EC2 sumber daya Amazon Anda di Panduan](#) Pengguna Amazon EC2 .

[EC2.50] Gateway EC2 VPN harus diberi tag

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: AWS :: EC2 :: VPNGateway

AWS Config aturan: tagged-ec2-vpngateway (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai yang Diizinkan	Nilai yang Diizinkan
requiredTagKeys	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi	Tidak ada nilai default

Parameter	Deskripsi	Tipe	Nilai yang Diizinkan	Nilai yang Diizinkan
			persyaratan AWS .	

Kontrol ini memeriksa apakah gateway Amazon EC2 VPN memiliki tag dengan kunci spesifik yang ditentukan dalam parameter `requiredTagKeys`. Kontrol gagal jika gateway VPN tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter `requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika gateway VPN tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws:`, diabaikan.

Tanda adalah sebuah label yang Anda tetapkan ke sebuah AWS sumber daya, dan terdiri dari sebuah kunci dan nilai opsional. Anda dapat membuat tag untuk mengkategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat Anda menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk penanggung jawab IAM Anda. Anda dapat merancang kebijakan ABAC ini untuk memungkinkan operasi ketika tag penanggung jawab cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat [Untuk apa ABAC untuk? AWS](#) di Panduan Pengguna IAM.

Note

Jangan menambahkan informasi pengenalan pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat [Menandai AWS sumber daya Anda](#) di Referensi Umum AWS

IP Perbaikan

Untuk menambahkan tag ke gateway EC2 VPN, lihat [Menandai EC2 sumber daya Amazon Anda](#) di Panduan EC2 Pengguna Amazon.

[EC2.51] Titik akhir EC2 Client VPN harus mengaktifkan pencatatan koneksi klien

Persyaratan terkait: NIST.800-53.r5 AC-2 (12), (4), (26), NIST.800-53.r5 AC-2 (9),, NIST.800-53.r5 AC-4 (9), Nist.800-53.R5 SI-3 NIST.800-53.r5 AC-6 (8) NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 AU-9(7), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 Nist.800-53.r5 SI-4, Nist.800-53.R5 SI-4 (20), Nist.800-53.R5 SI-7 (8), Nist.800-171.R2 3.1.12, Nist.800-171.r2 3.1.20, PCI DSS v4.0.1/10.2.1

Kategori: Identifikasi > Logging

Tingkat keparahan: Rendah

Jenis sumber daya: AWS::EC2::ClientVpnEndpoint

AWS Config aturan: [ec2-client-vpn-connection-log-enabled](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah AWS Client VPN titik akhir memiliki pencatatan koneksi klien yang diaktifkan. Kontrol gagal jika titik akhir tidak mengaktifkan pencatatan koneksi klien.

Titik akhir Client VPN memungkinkan klien jarak jauh untuk terhubung dengan aman ke sumber daya di Virtual Private Cloud (VPC) di. AWS Log koneksi memungkinkan Anda melacak aktivitas pengguna di titik akhir VPN dan memberikan visibilitas. Bila Anda mengaktifkan logging koneksi, Anda dapat menentukan nama pengaliran log dalam grup log. Jika Anda tidak menentukan aliran log, layanan Client VPN akan membuatnya untuk Anda.

IP Perbaikan

Untuk mengaktifkan logging koneksi, lihat [Mengaktifkan logging koneksi untuk titik akhir Client VPN yang ada](#) di Panduan AWS Client VPN Administrator.

[EC2.52] gateway EC2 transit harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: AWS::EC2::TransitGateway

AWS Config aturan: tagged-ec2-transitgateway (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai yang Diizinkan	Nilai yang Diizinkan
<code>requiredTagKeys</code>	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS .	No default value

Kontrol ini memeriksa apakah gateway EC2 transit Amazon memiliki tag dengan kunci tertentu yang ditentukan dalam parameter `requiredTagKeys`. Kontrol gagal jika gateway transit tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter `requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika gateway transit tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws:`, diabaikan.

Tanda adalah sebuah label yang Anda tetapkan ke sebuah AWS sumber daya, dan terdiri dari sebuah kunci dan nilai opsional. Anda dapat membuat tag untuk mengkategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat Anda menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk penanggung jawab IAM Anda. Anda dapat merancang kebijakan ABAC ini untuk memungkinkan operasi ketika tag penanggung jawab cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat [Untuk apa ABAC untuk? AWS](#) di Panduan Pengguna IAM.

Note

Jangan menambahkan informasi pengenalan pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS

Billing. Untuk praktik terbaik penandaan lainnya, lihat [Menandai AWS sumber daya Anda](#) di Referensi Umum AWS

IP Perbaikan

Untuk menambahkan tag ke gateway EC2 transit, lihat [Menandai EC2 sumber daya Amazon Anda](#) di Panduan EC2 Pengguna Amazon.

[EC2.53] grup EC2 keamanan seharusnya tidak mengizinkan masuknya dari 0.0.0.0/0 ke port administrasi server jarak jauh

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v3.0.0/5.2, PCI DSS v4.0.1/1.3.1

Kategori: Lindungi > Konfigurasi jaringan aman > Konfigurasi grup keamanan

Tingkat keparahan: Tinggi

Jenis sumber daya: AWS::EC2::SecurityGroup

AWS Config aturan: [vpc-sg-port-restriction-check](#)

Jenis jadwal: Periodik

Parameter:

Parameter	Deskripsi	Tipe	Nilai yang Diizinkan	Nilai yang Diizinkan
ipType	Versi IP	String	Tidak dapat disesuaikan	IPv4
restrictPorts	Daftar port yang harus menolak lalu lintas masuk	IntegerList	Tidak dapat disesuaikan	22, 3389

Kontrol ini memeriksa apakah grup EC2 keamanan Amazon memungkinkan masuknya dari 0.0.0.0/0 ke port administrasi server jarak jauh (port 22 dan 3389). Kontrol gagal jika grup keamanan mengizinkan masuknya dari 0.0.0.0/0 ke port 22 atau 3389.

Grup keamanan menyediakan penyaringan stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Kami menyarankan agar tidak ada grup keamanan yang mengizinkan akses

masuk tanpa batas ke port administrasi server jarak jauh, seperti SSH ke port 22 dan RDP ke port 3389, menggunakan protokol TDP (6), UDP (17), atau ALL (-1). Memungkinkan akses publik ke port ini meningkatkan permukaan serangan sumber daya dan risiko kompromi sumber daya.

IP Perbaikan

Untuk memperbarui aturan grup EC2 keamanan untuk melarang lalu lintas masuk ke port yang ditentukan, lihat [Memperbarui aturan grup keamanan](#) di EC2 Panduan Pengguna Amazon. Setelah memilih grup keamanan di EC2 konsol Amazon, pilih Tindakan, Edit aturan masuk. Hapus aturan yang memungkinkan akses ke port 22 atau port 3389.

[EC2.54] grup EC2 keamanan tidak boleh mengizinkan masuknya dari: :/0 ke port administrasi server jarak jauh

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v3.0.0/5.3, PCI DSS v4.0.1/1.3.1

Kategori: Lindungi > Konfigurasi jaringan aman > Konfigurasi grup keamanan

Tingkat keparahan: Tinggi

Jenis sumber daya: AWS::EC2::SecurityGroup

AWS Config aturan: [vpc-sg-port-restriction-check](#)

Jenis jadwal: Periodik

Parameter:

Parameter	Deskripsi	Tipe	Nilai yang Diizinkan	Nilai yang Diizinkan
ipType	Versi IP	String	Tidak dapat disesuaikan	IPv6
restrictPorts	Daftar port yang harus menolak lalu lintas masuk	IntegerList	Tidak dapat disesuaikan	22, 3389

Kontrol ini memeriksa apakah grup EC2 keamanan Amazon mengizinkan masuknya dari: :/0 ke port administrasi server jarak jauh (port 22 dan 3389). Kontrol gagal jika grup keamanan mengizinkan masuknya dari: :/0 ke port 22 atau 3389.

Grup keamanan menyediakan penyaringan stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Kami menyarankan agar tidak ada grup keamanan yang mengizinkan akses masuk tanpa batas ke port administrasi server jarak jauh, seperti SSH ke port 22 dan RDP ke port 3389, menggunakan protokol TDP (6), UDP (17), atau ALL (-1). Memungkinkan akses publik ke port ini meningkatkan permukaan serangan sumber daya dan risiko kompromi sumber daya.

IP Perbaikan

Untuk memperbarui aturan grup EC2 keamanan untuk melarang lalu lintas masuk ke port yang ditentukan, lihat [Memperbarui aturan grup keamanan](#) di EC2 Panduan Pengguna Amazon. Setelah memilih grup keamanan di EC2 konsol Amazon, pilih Tindakan, Edit aturan masuk. Hapus aturan yang memungkinkan akses ke port 22 atau port 3389.

[EC2.55] VPCs harus dikonfigurasi dengan titik akhir antarmuka untuk ECR API

Persyaratan terkait: NIST.800-53.r5 AC-2 1 NIST.800-53.r5 AC-3,, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-4,, NIST.800-53.r5 AC-4 (21) NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7,, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4)

Kategori: Lindungi > Manajemen akses yang aman > Kontrol akses

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::EC2::VPC, AWS::EC2::VPCEndpoint

AWS Config aturan: [vpc-endpoint-enabled](#)

Jenis jadwal: Periodik

Parameter:

Parameter	Wajib	Deskripsi	Tipe	Nilai yang Diizinkan	Nilai yang Diizinkan
serviceName	Wajib	Nama layanan yang dievaluasi	String	Tidak dapat disesuaikan	ecr.api

Parameter	Wajib	Deskripsi	Tipe	Nilai yang Diizinkan	Nilai yang Diizinkan
i oleh kontrol					
vpcIds	Opsional	Daftar Amazon VPC untuk VPC VPC IDs yang dipisahkan koma. Jika disediakan, kontrol gagal jika layanan yang ditentukan dalam serviceName parameter tidak memiliki salah satu titik akhir VPC ini.	StringList	Sesuaikan dengan satu atau lebih VPC IDs	Tidak ada nilai default

Kontrol ini memeriksa apakah virtual private cloud (VPC) yang Anda kelola memiliki endpoint VPC antarmuka untuk Amazon ECR API. Kontrol gagal jika VPC tidak memiliki titik akhir VPC antarmuka untuk ECR API. Kontrol ini mengevaluasi sumber daya dalam satu akun.

AWS PrivateLink memungkinkan pelanggan untuk mengakses layanan yang di-host dengan AWS cara yang sangat tersedia dan terukur, sambil menjaga semua lalu lintas jaringan dalam AWS jaringan. Pengguna layanan dapat secara pribadi mengakses layanan yang didukung oleh

PrivateLink dari VPC atau lokal mereka, tanpa menggunakan IPs publik, dan tanpa memerlukan lalu lintas untuk melintasi internet.

IP Perbaikan

Untuk mengonfigurasi titik akhir VPC, lihat [Mengakses titik akhir VPC antarmuka Layanan AWS menggunakan antarmuka](#) di Panduan.AWS PrivateLink

[EC2.56] VPCs harus dikonfigurasi dengan titik akhir antarmuka untuk Docker Registry

Persyaratan terkait: NIST.800-53.r5 AC-2 1 NIST.800-53.r5 AC-3,, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-4,, NIST.800-53.r5 AC-4 (21) NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7,, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4)

Kategori: Lindungi > Manajemen akses yang aman > Kontrol akses

Tingkat keparahan: Sedang

Jenis sumber daya:AWS::EC2::VPC, AWS::EC2::VPCEndpoint

AWS Config aturan: [vpc-endpoint-enabled](#)

Jenis jadwal: Periodik

Parameter:

Parameter	Wajib	Deskripsi	Tipe	Nilai yang Diizinkan	Nilai yang Diizinkan
serviceNames	Wajib	Nama layanan yang dievaluasi oleh kontrol	String	Tidak dapat disesuaikan	ecr.dkr
vpcIds	Opsional	Daftar Amazon VPC untuk	StringList	Sesuaikan dengan satu atau	Tidak ada nilai default

Parameter	Wajib	Deskripsi	Tipe	Nilai yang Diizinkan	Nilai yang Diizinkan
		VPC VPC IDs yang dipisahkan koma. Jika disediakan, kontrol gagal jika layanan yang ditentukan dalam serviceName parameter tidak memiliki salah satu titik akhir VPC ini.		lebih VPC IDs	

Kontrol ini memeriksa apakah virtual private cloud (VPC) yang Anda kelola memiliki VPC endpoint antarmuka untuk Docker Registry. Kontrol gagal jika VPC tidak memiliki titik akhir VPC antarmuka untuk Docker Registry. Kontrol ini mengevaluasi sumber daya dalam satu akun.

AWS PrivateLink memungkinkan pelanggan untuk mengakses layanan yang di-host dengan AWS cara yang sangat tersedia dan terukur, sambil menjaga semua lalu lintas jaringan dalam AWS jaringan. Pengguna layanan dapat secara pribadi mengakses layanan yang didukung oleh PrivateLink dari VPC atau lokal mereka, tanpa menggunakan IPs publik, dan tanpa memerlukan lalu lintas untuk melintasi internet.

IP Perbaikan

Untuk mengonfigurasi titik akhir VPC, lihat [Mengakses titik akhir VPC antarmuka Layanan AWS menggunakan antarmuka](#) di Panduan.AWS PrivateLink

[EC2.57] VPCs harus dikonfigurasi dengan titik akhir antarmuka untuk Systems Manager

Persyaratan terkait: NIST.800-53.r5 AC-2 1 NIST.800-53.r5 AC-3,, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-4,, NIST.800-53.r5 AC-4 (21) NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7,, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4)

Kategori: Lindungi > Manajemen akses yang aman > Kontrol akses

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::EC2::VPC, AWS::EC2::VPCEndpoint

AWS Config aturan: [vpc-endpoint-enabled](#)

Jenis jadwal: Periodik

Parameter:

Parameter	Wajib	Deskripsi	Tipe	Nilai yang Diizinkan	Security Hub
serviceNames	Wajib	Nama layanan yang dievaluasi oleh kontrol	String	Tidak dapat disesuaikan	ssm
vpcIds	Opsional	Daftar Amazon VPC untuk VPC VPC IDs yang dipisahkan koma. Jika disediakan, kontrol gagal jika	StringList	Sesuaikan dengan satu atau lebih VPC IDs	Tidak ada nilai default

Parameter	Wajib	Deskripsi	Tipe	Nilai yang Diizinkan	Security Hub
		layanan yang ditentukan dalam serviceName parameter tidak memiliki salah satu titik akhir VPC ini.			

Kontrol ini memeriksa apakah virtual private cloud (VPC) yang Anda kelola memiliki titik akhir VPC antarmuka. AWS Systems Manager Kontrol gagal jika VPC tidak memiliki titik akhir VPC antarmuka untuk Systems Manager. Kontrol ini mengevaluasi sumber daya dalam satu akun.

AWS PrivateLink memungkinkan pelanggan untuk mengakses layanan yang di-host dengan AWS cara yang sangat tersedia dan terukur, sambil menjaga semua lalu lintas jaringan dalam AWS jaringan. Pengguna layanan dapat secara pribadi mengakses layanan yang didukung oleh PrivateLink dari VPC atau lokal mereka, tanpa menggunakan IPs publik, dan tanpa memerlukan lalu lintas untuk melintasi internet.

IP Perbaikan

Untuk mengonfigurasi titik akhir VPC, lihat [Mengakses titik akhir VPC antarmuka Layanan AWS menggunakan antarmuka](#) di Panduan.AWS PrivateLink

[EC2.58] VPCs harus dikonfigurasi dengan titik akhir antarmuka untuk Kontak Manajer Insiden Systems Manager

Persyaratan terkait: NIST.800-53.r5 AC-2 1 NIST.800-53.r5 AC-3,, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-4,, NIST.800-53.r5 AC-4 (21) NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7,, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4)

Kategori: Lindungi > Manajemen akses yang aman > Kontrol akses

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::EC2::VPC, AWS::EC2::VPCEndpoint

AWS Config aturan: [vpc-endpoint-enabled](#)

Jenis jadwal: Periodik

Parameter:

Parameter	Wajib	Deskripsi	Tipe	Nilai yang Diizinkan	Security Hub
serviceName	Wajib	Nama layanan yang dievaluasi oleh kontrol	String	Tidak dapat disesuaikan	ssm-contacts
vpcIds	Opsional	Daftar Amazon VPC untuk VPC VPC IDs yang dipisahkan koma. Jika disediakan, kontrol gagal jika layanan yang ditentukan dalam serviceName parameter	StringList	Sesuaikan dengan satu atau lebih VPC IDs	Tidak ada nilai default

Parameter	Wajib	Deskripsi	Tipe	Nilai yang Diizinkan	Security Hub
		tidak memiliki salah satu titik akhir VPC ini.			

Kontrol ini memeriksa apakah virtual private cloud (VPC) yang Anda kelola memiliki titik akhir VPC antarmuka untuk Kontak Manajer Insiden. AWS Systems Manager Kontrol gagal jika VPC tidak memiliki titik akhir VPC antarmuka untuk Kontak Manajer Insiden Manajer Systems Manager. Kontrol ini mengevaluasi sumber daya dalam satu akun.

AWS PrivateLink memungkinkan pelanggan untuk mengakses layanan yang di-host dengan AWS cara yang sangat tersedia dan terukur, sambil menjaga semua lalu lintas jaringan dalam AWS jaringan. Pengguna layanan dapat secara pribadi mengakses layanan yang didukung oleh PrivateLink dari VPC atau lokal mereka, tanpa menggunakan IPs publik, dan tanpa memerlukan lalu lintas untuk melintasi internet.

IP Perbaikan

Untuk mengonfigurasi titik akhir VPC, lihat [Mengakses titik akhir VPC antarmuka Layanan AWS menggunakan antarmuka](#) di Panduan.AWS PrivateLink

[EC2.60] VPCs harus dikonfigurasi dengan titik akhir antarmuka untuk Systems Manager Incident Manager

Persyaratan terkait: NIST.800-53.r5 AC-2 1 NIST.800-53.r5 AC-3,, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-4,, NIST.800-53.r5 AC-4 (21) NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7,, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4)

Kategori: Lindungi > Manajemen akses yang aman > Kontrol akses

Tingkat keparahan: Sedang

Jenis sumber daya:AWS::EC2::VPC, AWS::EC2::VPCEndpoint

AWS Config aturan: [vpc-endpoint-enabled](#)

Jenis jadwal: Periodik

Parameter:

Parameter	Wajib	Deskripsi	Tipe	Nilai yang Diizinkan	Security Hub
serviceName	Wajib	Nama layanan yang dievaluasi oleh kontrol	String	Tidak dapat disesuaikan	ssm-incidents
vpcIds	Opsional	Daftar Amazon VPC untuk VPC VPC IDs yang dipisahkan koma. Jika disediakan, kontrol gagal jika layanan yang ditentukan dalam serviceName parameter tidak memiliki salah satu titik akhir VPC ini.	StringList	Sesuaikan dengan satu atau lebih VPC IDs	Tidak ada nilai default

Kontrol ini memeriksa apakah virtual private cloud (VPC) yang Anda kelola memiliki endpoint VPC antarmuka untuk Manajer Insiden. AWS Systems Manager Kontrol gagal jika VPC tidak memiliki titik akhir VPC antarmuka untuk Systems Manager Incident Manager. Kontrol ini mengevaluasi sumber daya dalam satu akun.

AWS PrivateLink memungkinkan pelanggan untuk mengakses layanan yang di-host dengan AWS cara yang sangat tersedia dan terukur, sambil menjaga semua lalu lintas jaringan dalam AWS jaringan. Pengguna layanan dapat secara pribadi mengakses layanan yang didukung oleh PrivateLink dari VPC atau lokal mereka, tanpa menggunakan IPs publik, dan tanpa memerlukan lalu lintas untuk melintasi internet.

IP Perbaikan

Untuk mengonfigurasi titik akhir VPC, lihat [Mengakses titik akhir VPC antarmuka Layanan AWS menggunakan antarmuka](#) di Panduan.AWS PrivateLink

[EC2.170] templat EC2 peluncuran harus menggunakan Layanan Metadata Instance Versi 2 () IMDSv2

Persyaratan terkait: PCI DSS v4.0.1/2.2.6

Kategori: Lindungi > Keamanan Jaringan

Tingkat keparahan: Rendah

Jenis sumber daya: AWS::EC2::LaunchTemplate

AWS Config aturan: [ec2-launch-template-imdsv2-check](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah template EC2 peluncuran Amazon dikonfigurasi dengan Layanan Metadata Instans Versi 2 ()IMDSv2. Kontrol gagal jika HttpTokens disetel keoptional.

Menjalankan sumber daya pada versi perangkat lunak yang didukung memastikan kinerja, keamanan, dan akses optimal ke fitur-fitur terbaru. Pembaruan rutin melindungi terhadap kerentanan, yang membantu memastikan pengalaman pengguna yang stabil dan efisien.

IP Perbaikan

Untuk mewajibkan IMDSv2 pada template EC2 peluncuran, lihat [Mengonfigurasi opsi Layanan Metadata Instans](#) di EC2 Panduan Pengguna Amazon.

[EC2.171] Koneksi EC2 VPN seharusnya mengaktifkan logging

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v3.0.0/5.3, PCI DSS v4.0.1/10.4.2

Kategori: Identifikasi > Logging

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::EC2::VPNConnection

AWS Config aturan: [ec2-vpn-connection-logging-enabled](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah koneksi AWS Site-to-Site VPN mengaktifkan Amazon CloudWatch Logs untuk kedua terowongan. Kontrol gagal jika koneksi Site-to-Site VPN tidak mengaktifkan CloudWatch Log untuk kedua terowongan.

AWS Site-to-Site Log VPN memberi Anda visibilitas yang lebih dalam ke penerapan Site-to-Site VPN Anda. Dengan fitur ini, Anda memiliki akses ke log koneksi Site-to-Site VPN yang memberikan rincian tentang pembentukan terowongan IP Security (IPsec), negosiasi Internet Key Exchange (IKE), dan pesan protokol deteksi rekan mati (DPD). Site-to-Site Log VPN dapat dipublikasikan ke CloudWatch Log. Fitur ini memberi pelanggan satu cara konsisten untuk mengakses dan menganalisis log terperinci untuk semua koneksi Site-to-Site VPN mereka.

IP Perbaikan

Untuk mengaktifkan pencatatan terowongan pada koneksi EC2 VPN, lihat [log AWS Site-to-Site VPN](#) di Panduan Pengguna AWS Site-to-Site VPN.

[EC2.172] Pengaturan Akses Publik Blok EC2 VPC harus memblokir lalu lintas gateway internet

Kategori: Lindungi > Konfigurasi jaringan aman > Sumber daya tidak dapat diakses publik

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::EC2::VPCElasticNetworkOptions`

AWS Config aturan: `ec2-vpc-bpa-internet-gateway-blocked` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai yang Diizinkan	Security Hub
<code>vpcBpaInternetGatewayBlockMode</code>	Nilai string dari mode opsi VPC BPA.	Enum	<code>block-bidirectional</code> , <code>block-ingress</code>	Tidak ada nilai default

Kontrol ini memeriksa apakah pengaturan Amazon EC2 VPC Block Public Access (BPA) dikonfigurasi untuk memblokir lalu lintas gateway internet untuk semua Amazon VPCs di Akun AWS. Kontrol gagal jika pengaturan VPC BPA tidak dikonfigurasi untuk memblokir lalu lintas gateway internet. Agar kontrol lolos, BPA VPC `InternetGatewayBlockMode` harus disetel ke `block-bidirectional` atau `block-ingress`. Jika parameter `vpcBpaInternetGatewayBlockMode` disediakan, kontrol hanya lewat jika nilai VPC BPA `InternetGatewayBlockMode` cocok dengan parameter.

Mengkonfigurasi pengaturan BPA VPC untuk akun Anda di Wilayah AWS sebuah memungkinkan Anda memblokir sumber daya dan subnet yang Anda miliki VPCs di Wilayah itu agar tidak menjangkau atau dijangkau dari internet melalui gateway internet dan gateway internet khusus egress. Jika Anda memerlukan subnet VPCs dan spesifik untuk dapat menjangkau atau dapat dijangkau dari internet, Anda dapat mengecualikannya dengan mengonfigurasi pengecualian VPC BPA. Untuk petunjuk cara membuat dan menghapus pengecualian, lihat [Membuat dan menghapus pengecualian](#) di Panduan Pengguna Amazon VPC.

IP Perbaikan

Untuk mengaktifkan BPA dua arah di tingkat akun, lihat [Mengaktifkan mode dua arah BPA untuk akun Anda di](#) Panduan Pengguna Amazon VPC. Untuk mengaktifkan BPA khusus masuk, lihat Mengubah mode BPA [VPC](#) menjadi hanya masuk. Untuk mengaktifkan BPA VPC di tingkat Organisasi, lihat Mengaktifkan [BPA VPC](#) di tingkat Organisasi.

[EC2.173] Permintaan Armada EC2 Spot harus mengaktifkan enkripsi untuk volume EBS terlampir

Kategori: Lindungi > Perlindungan Data > Enkripsi data-at-rest

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::EC2::SpotFleet

AWS Config aturan: [ec2-spot-fleet-request-ct-encryption-at-rest](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah permintaan Amazon EC2 Spot Fleet mengaktifkan enkripsi untuk semua volume Amazon Elastic Block Store (Amazon EBS) yang terpasang ke instans. EC2 Kontrol gagal jika permintaan Armada Spot tidak mengaktifkan enkripsi untuk satu atau beberapa volume EBS yang ditentukan dalam permintaan.

Untuk lapisan keamanan tambahan, Anda harus mengaktifkan enkripsi untuk volume Amazon EBS. Operasi enkripsi kemudian terjadi pada server yang menghosting EC2 instans Amazon, yang membantu memastikan keamanan data saat istirahat dan data dalam transit antara instans dan penyimpanan EBS terlampir. Enkripsi Amazon EBS adalah solusi enkripsi langsung untuk sumber daya EBS yang terkait dengan instans Anda. EC2 Enkripsi EBS, Anda tidak perlu membangun, memelihara, dan mengamankan infrastruktur manajemen kunci Anda sendiri. Enkripsi EBS digunakan AWS KMS keys saat membuat volume terenkripsi.

IP Perbaikan

Tidak ada cara langsung untuk mengenkripsi volume Amazon EBS yang sudah ada dan tidak terenkripsi. Anda dapat mengenkripsi volume baru hanya saat Anda membuatnya.

Namun, jika Anda mengaktifkan enkripsi secara default, Amazon EBS mengenkripsi volume baru dengan menggunakan kunci default untuk enkripsi EBS. Jika Anda tidak mengaktifkan enkripsi secara default, Anda dapat mengaktifkan enkripsi saat Anda membuat volume individu. Dalam kedua kasus, Anda dapat mengganti kunci default untuk enkripsi EBS dan memilih pelanggan yang dikelola. AWS KMS key Untuk informasi selengkapnya tentang enkripsi EBS, lihat [enkripsi Amazon EBS](#) di Panduan Pengguna Amazon EBS.

Untuk informasi tentang membuat permintaan Armada EC2 Spot Amazon, lihat [Membuat Armada Spot](#) di Panduan Pengguna Amazon Elastic Compute Cloud.

[EC2.174] Set opsi EC2 DHCP harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: AWS::EC2::DHCPOptions

AWS Config aturan: [ec2-dhcp-options-tagged](#)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai yang Diizinkan	Security Hub
<code>requiredKeyTags</code>	Daftar kunci tag non-sistem yang harus ditetapkan ke sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS .	Tidak ada nilai default

Kontrol ini memeriksa apakah set opsi Amazon EC2 DHCP memiliki kunci tag yang ditentukan oleh `requiredKeyTags` parameter. Kontrol gagal jika set opsi tidak memiliki kunci tag, atau tidak memiliki semua kunci yang ditentukan oleh `requiredKeyTags` parameter. Jika Anda tidak menentukan nilai apa pun untuk `requiredKeyTags` parameter, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika set opsi tidak memiliki kunci tag. Kontrol mengabaikan tag sistem, yang diterapkan secara otomatis dan memiliki `aws:` awalan.

Tag adalah sebuah label yang Anda buat dan tetapkan ke sebuah AWS sumber daya. Setiap tanda terdiri dari kunci tanda yang diperlukan dan nilai tanda opsional. Anda dapat menggunakan tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Mereka membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Mereka juga dapat membantu Anda melacak pemilik sumber daya untuk tindakan dan pemberitahuan. Anda juga dapat menggunakan tag untuk menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi. Untuk informasi selengkapnya tentang strategi ABAC, lihat [Menentukan izin berdasarkan atribut dengan otorisasi ABAC](#) di Panduan Pengguna IAM. Untuk informasi lebih lanjut tentang penandaan, lihat [Panduan Pengguna AWS Penandaan dan Editor Tag](#).

Note

Jangan menyimpan informasi pengenalan pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses dari banyak orang Layanan AWS. Mereka tidak dimaksudkan untuk digunakan untuk data privat atau sensitif.

IP Perbaikan

Untuk informasi tentang menambahkan tag ke set opsi Amazon EC2 DHCP, lihat [Menandai EC2 sumber daya Amazon Anda](#) di Panduan EC2 Pengguna Amazon.

[EC2.175] templat EC2 peluncuran harus diberi tag

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: AWS::EC2::LaunchTemplate

AWS Config aturan: [ec2-launch-template-tagged](#)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai yang Diizinkan	Security Hub
<code>requiredKeyTags</code>	Daftar kunci tag non-sistem yang harus ditetapkan ke sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS .	Tidak ada nilai default

Kontrol ini memeriksa apakah template EC2 peluncuran Amazon memiliki kunci tag yang ditentukan oleh `requiredKeyTags` parameter. Kontrol gagal jika template peluncuran tidak memiliki kunci tag, atau tidak memiliki semua kunci yang ditentukan oleh `requiredKeyTags` parameter.

Jika Anda tidak menentukan nilai apa pun untuk `requiredKeyTags` parameter, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika templat peluncuran tidak memiliki kunci tag. Kontrol mengabaikan tag sistem, yang diterapkan secara otomatis dan memiliki `aws :` awalan.

Tag adalah sebuah label yang Anda buat dan tetapkan ke sebuah AWS sumber daya. Setiap tanda terdiri dari kunci tanda yang diperlukan dan nilai tanda opsional. Anda dapat menggunakan tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Mereka membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Mereka juga dapat membantu Anda melacak pemilik sumber daya untuk tindakan dan pemberitahuan. Anda juga dapat menggunakan tag untuk menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi. Untuk informasi selengkapnya tentang strategi ABAC, lihat [Menentukan izin berdasarkan atribut dengan otorisasi ABAC](#) di Panduan Pengguna IAM. Untuk informasi lebih lanjut tentang penandaan, lihat [Panduan Pengguna AWS Penandaan dan Editor Tag](#).

Note

Jangan menyimpan informasi pengenalan pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses dari banyak orang Layanan AWS. Mereka tidak dimaksudkan untuk digunakan untuk data privat atau sensitif.

IP Perbaikan

Untuk informasi tentang menambahkan tag ke templat EC2 peluncuran Amazon, lihat [Menandai EC2 sumber daya Amazon Anda](#) di Panduan EC2 Pengguna Amazon.

[EC2.176] daftar EC2 awalan harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::EC2::PrefixList`

AWS Config aturan: [ec2-prefix-list-tagged](#)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai yang Diizinkan	Security Hub
<code>requiredKeyTags</code>	Daftar kunci tag non-sistem yang harus ditetapkan ke sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS .	Tidak ada nilai default

Kontrol ini memeriksa apakah daftar EC2 awalan Amazon memiliki kunci tag yang ditentukan oleh `requiredKeyTags` parameter. Kontrol gagal jika daftar awalan tidak memiliki kunci tag, atau tidak memiliki semua kunci yang ditentukan oleh `requiredKeyTags` parameter. Jika Anda tidak menentukan nilai apa pun untuk `requiredKeyTags` parameter, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika daftar awalan tidak memiliki kunci tag. Kontrol mengabaikan tag sistem, yang diterapkan secara otomatis dan memiliki `aws` : awalan.

Tag adalah sebuah label yang Anda buat dan tetapkan ke sebuah AWS sumber daya. Setiap tanda terdiri dari kunci tanda yang diperlukan dan nilai tanda opsional. Anda dapat menggunakan tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Mereka membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Mereka juga dapat membantu Anda melacak pemilik sumber daya untuk tindakan dan pemberitahuan. Anda juga dapat menggunakan tag untuk menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi. Untuk informasi selengkapnya tentang strategi ABAC, lihat [Menentukan izin berdasarkan atribut dengan otorisasi ABAC](#) di Panduan Pengguna IAM. Untuk informasi lebih lanjut tentang penandaan, lihat [Panduan Pengguna AWS Penandaan dan Editor Tag](#).

Note

Jangan menyimpan informasi pengenalan pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses dari banyak orang Layanan AWS. Mereka tidak dimaksudkan untuk digunakan untuk data privat atau sensitif.

IP Perbaikan

Untuk informasi tentang menambahkan tag ke daftar EC2 awalan Amazon, lihat [Menandai EC2 sumber daya Amazon Anda](#) di Panduan EC2 Pengguna Amazon.

[EC2.177] Sesi cermin EC2 lalu lintas harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::EC2::TrafficMirrorSession`

AWS Config aturan: [ec2-traffic-mirror-session-tagged](#)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai yang Diizinkan	Security Hub
<code>requiredKeyTags</code>	Daftar kunci tag non-sistem yang harus ditetapkan ke sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS .	Tidak ada nilai default

Kontrol ini memeriksa apakah sesi cermin EC2 lalu lintas Amazon memiliki kunci tag yang ditentukan oleh `requiredKeyTags` parameter. Kontrol gagal jika sesi tidak memiliki kunci tag, atau tidak memiliki semua kunci yang ditentukan oleh `requiredKeyTags` parameter. Jika Anda tidak menentukan nilai apa pun untuk `requiredKeyTags` parameter, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika sesi tidak memiliki kunci tag. Kontrol mengabaikan tag sistem, yang diterapkan secara otomatis dan memiliki `aws:` awalan.

Tag adalah sebuah label yang Anda buat dan tetapkan ke sebuah AWS sumber daya. Setiap tanda terdiri dari kunci tanda yang diperlukan dan nilai tanda opsional. Anda dapat menggunakan tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Mereka membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Mereka juga dapat membantu Anda melacak pemilik sumber daya untuk tindakan dan pemberitahuan. Anda juga dapat menggunakan tag untuk menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi. Untuk informasi selengkapnya tentang strategi ABAC, lihat [Menentukan izin berdasarkan atribut dengan otorisasi ABAC](#) di Panduan Pengguna IAM. Untuk informasi lebih lanjut tentang penandaan, lihat [Panduan Pengguna AWS Penandaan dan Editor Tag](#).

Note

Jangan menyimpan informasi pengenalan pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses dari banyak orang Layanan AWS. Mereka tidak dimaksudkan untuk digunakan untuk data privat atau sensitif.

IP Perbaikan

Untuk informasi tentang menambahkan tag ke sesi cermin EC2 lalu lintas Amazon, lihat [Menandai EC2 sumber daya Amazon Anda](#) di Panduan EC2 Pengguna Amazon.

[EC2.178] Filter cermin EC2 lalu lintas harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::EC2::TrafficMirrorFilter`

AWS Config aturan: [ec2-traffic-mirror-filter-tagged](#)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai yang Diizinkan	Security Hub
<code>requiredKeyTags</code>	Daftar kunci tag non-sistem yang harus ditetapkan ke sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS .	Tidak ada nilai default

Kontrol ini memeriksa apakah filter cermin EC2 lalu lintas Amazon memiliki kunci tag yang ditentukan oleh `requiredKeyTags` parameter. Kontrol gagal jika filter tidak memiliki kunci tag, atau tidak memiliki semua kunci yang ditentukan oleh `requiredKeyTags` parameter. Jika Anda

tidak menentukan nilai apa pun untuk `requiredKeyTags` parameter, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika filter tidak memiliki kunci tag. Kontrol mengabaikan tag sistem, yang diterapkan secara otomatis dan memiliki `aws :` awalan.

Tag adalah sebuah label yang Anda buat dan tetapkan ke sebuah AWS sumber daya. Setiap tanda terdiri dari kunci tanda yang diperlukan dan nilai tanda opsional. Anda dapat menggunakan tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Mereka membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Mereka juga dapat membantu Anda melacak pemilik sumber daya untuk tindakan dan pemberitahuan. Anda juga dapat menggunakan tag untuk menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi. Untuk informasi selengkapnya tentang strategi ABAC, lihat [Menentukan izin berdasarkan atribut dengan otorisasi ABAC](#) di Panduan Pengguna IAM. Untuk informasi lebih lanjut tentang penandaan, lihat [Panduan Pengguna AWS Penandaan dan Editor Tag](#).

 Note

Jangan menyimpan informasi pengenalan pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses dari banyak orang Layanan AWS. Mereka tidak dimaksudkan untuk digunakan untuk data privat atau sensitif.

IP Perbaikan

Untuk informasi tentang menambahkan tag ke filter cermin EC2 lalu lintas Amazon, lihat [Menandai EC2 sumber daya Amazon Anda](#) di Panduan EC2 Pengguna Amazon.

[EC2.179] Target cermin EC2 lalu lintas harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::EC2::TrafficMirrorTarget`

AWS Config aturan: [ec2-traffic-mirror-target-tagged](#)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai yang Diizinkan	Security Hub
<code>requiredKeyTags</code>	Daftar kunci tag non-sistem yang harus ditetapkan ke sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS .	Tidak ada nilai default

Kontrol ini memeriksa apakah target mirror EC2 lalu lintas Amazon memiliki kunci tag yang ditentukan oleh `requiredKeyTags` parameter. Kontrol gagal jika target tidak memiliki kunci tag, atau tidak memiliki semua kunci yang ditentukan oleh `requiredKeyTags` parameter. Jika Anda tidak menentukan nilai apa pun untuk `requiredKeyTags` parameter, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika target tidak memiliki kunci tag. Kontrol mengabaikan tag sistem, yang diterapkan secara otomatis dan memiliki `aws:awalan`.

Tag adalah sebuah label yang Anda buat dan tetapkan ke sebuah AWS sumber daya. Setiap tanda terdiri dari kunci tanda yang diperlukan dan nilai tanda opsional. Anda dapat menggunakan tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Mereka membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Mereka juga dapat membantu Anda melacak pemilik sumber daya untuk tindakan dan pemberitahuan. Anda juga dapat menggunakan tag untuk menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi. Untuk informasi selengkapnya tentang strategi ABAC, lihat [Menentukan izin berdasarkan atribut dengan otorisasi ABAC](#) di Panduan Pengguna IAM. Untuk informasi lebih lanjut tentang penandaan, lihat [Panduan Pengguna AWS Penandaan dan Editor Tag](#).

Note

Jangan menyimpan informasi pengenalan pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses dari banyak orang Layanan AWS. Mereka tidak dimaksudkan untuk digunakan untuk data privat atau sensitif.

IP Perbaikan

Untuk informasi tentang menambahkan tag ke target cermin EC2 lalu lintas Amazon, lihat [Menandai EC2 sumber daya Amazon Anda](#) di Panduan EC2 Pengguna Amazon.

Kontrol Security Hub untuk Auto Scaling

Kontrol Security Hub ini mengevaluasi layanan dan EC2 sumber daya Amazon Auto Scaling.

Kontrol ini mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat [Ketersediaan kontrol berdasarkan Wilayah](#).

[AutoScaling.1] Grup Auto Scaling yang terkait dengan penyeimbang beban harus menggunakan pemeriksaan kesehatan ELB

Persyaratan terkait: PCI DSS v3.2.1/2.2., NIST.800-53.R5 CP-2 (2) NIST.800-53.r5 CA-7, NIST.800-53.R5 SI-2

Kategori: Identifikasi > Persediaan

Tingkat keparahan: Rendah

Jenis sumber daya: AWS::AutoScaling::AutoScalingGroup

AWS Config aturan: [autoscaling-group-elb-healthcheck-required](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah grup Amazon EC2 Auto Scaling yang terkait dengan penyeimbang beban menggunakan pemeriksaan kesehatan Elastic Load Balancing (ELB). Kontrol gagal jika grup Auto Scaling tidak menggunakan pemeriksaan kesehatan ELB.

Pemeriksaan kesehatan ELB membantu memastikan bahwa grup Auto Scaling dapat menentukan kesehatan instans berdasarkan tes tambahan yang disediakan oleh penyeimbang beban. Menggunakan pemeriksaan kesehatan Elastic Load Balancing juga membantu mendukung ketersediaan aplikasi yang menggunakan grup Auto EC2 Scaling.

Remediasi

Untuk menambahkan pemeriksaan kesehatan Elastic Load Balancing, lihat [Menambahkan pemeriksaan kesehatan Menambahkan Elastic Load Balancing di Panduan Pengguna Amazon Auto EC2 Scaling](#).

[AutoScaling.2] Grup EC2 Auto Scaling Amazon harus mencakup beberapa Availability Zone

Persyaratan terkait: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-2(2), NIST.800-53.r5 CP-6(2), NIST.800-53.r5 SC-3 6, NIST.800-53.r5 SC-5 (2), NIST.800-53.R5 SI-13 (5)

Kategori: Pulihkan > Ketahanan > Ketersediaan tinggi

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::AutoScaling::AutoScalingGroup

AWS Config aturan: [autoscaling-multiple-az](#)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub	
minAvailabilityZones	Jumlah minimum Availability Zone	Enum	2, 3, 4, 5, 6	2	

Kontrol ini memeriksa apakah grup EC2 Auto Scaling Amazon mencakup setidaknya jumlah Availability Zone () yang ditentukan. AZs Kontrol gagal jika grup Auto Scaling tidak menjangkau setidaknya jumlah yang ditentukan. AZs Kecuali Anda memberikan nilai parameter kustom untuk jumlah minimum AZs, Security Hub menggunakan nilai default dua AZs.

Grup Auto Scaling yang tidak menjangkau beberapa instans tidak AZs dapat meluncurkan instance di AZ lain untuk mengkompensasi jika AZ tunggal yang dikonfigurasi menjadi tidak tersedia. Namun, grup Auto Scaling dengan satu Availability Zone mungkin lebih disukai dalam beberapa kasus penggunaan, seperti pekerjaan batch atau ketika biaya transfer antar-AZ harus dijaga seminimal mungkin. Dalam kasus seperti itu, Anda dapat menonaktifkan kontrol ini atau menekan temuannya.

Remediasi

Untuk menambahkan AZs ke grup Auto Scaling yang ada, lihat [Menambahkan dan menghapus Availability Zone](#) di Panduan Pengguna Amazon Auto EC2 Scaling.

[AutoScaling.3] Konfigurasi peluncuran grup Auto Scaling harus EC2 mengonfigurasi instance agar memerlukan Layanan Metadata Instance Versi 2 () IMDSv2

Persyaratan terkait: NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (15), (7),, NIST.800-53.r5 AC-3 NIST.800-53.r5 CA-9 (1) NIST.800-53.r5 AC-6, Nist.800-53.R5 CM-2, PCI DSS v4.0.1/2.2.6

Kategori: Lindungi > Konfigurasi jaringan aman

Tingkat keparahan: Tinggi

Jenis sumber daya: AWS::AutoScaling::LaunchConfiguration

AWS Config aturan: [autoscaling-launchconfig-requires-imdsv2](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah IMDSv2 diaktifkan pada semua instans yang diluncurkan oleh grup EC2 Auto Scaling Amazon. Kontrol gagal jika versi Instance Metadata Service (IMDS) tidak disertakan dalam konfigurasi peluncuran atau dikonfigurasi sebagai `optional`, yang merupakan pengaturan yang memungkinkan salah satu atau. IMDSv1 IMDSv2

IMDS menyediakan data tentang instans yang dapat Anda gunakan untuk mengonfigurasi atau mengelola instance yang sedang berjalan.

IMDS versi 2 menambahkan perlindungan baru yang tidak tersedia IMDSv1 untuk melindungi instans Anda lebih lanjut. EC2

Remediasi

Grup Auto Scaling dikaitkan dengan satu konfigurasi peluncuran pada satu waktu. Anda tidak dapat mengubah konfigurasi peluncuran setelah Anda membuatnya. Untuk mengubah konfigurasi peluncuran untuk grup Auto Scaling, gunakan konfigurasi peluncuran yang ada sebagai dasar untuk konfigurasi peluncuran baru dengan IMDSv2 diaktifkan. Untuk informasi selengkapnya, lihat [Mengonfigurasi opsi metadata instans untuk instance baru](#) di Panduan Pengguna Amazon EC2 .

[AutoScaling.4] Konfigurasi peluncuran grup Auto Scaling seharusnya tidak memiliki batas hop respons metadata yang lebih besar dari 1

 Important

Security Hub menghentikan kontrol ini pada April 2024. Untuk informasi selengkapnya, lihat [Ubah log untuk kontrol CSPM Security Hub](#).

Persyaratan terkait: NIST.800-53.r5 CA-9 (1), Nist.800-53.R5 CM-2, Nist.800-53.R5 CM-2 (2)

Kategori: Lindungi > Konfigurasi jaringan aman

Tingkat keparahan: Tinggi

Jenis sumber daya: AWS::AutoScaling::LaunchConfiguration

AWS Config aturan: [autoscaling-launch-config-hop-limit](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa jumlah hop jaringan yang dapat ditempuh oleh token metadata. Kontrol gagal jika batas hop respons metadata lebih besar dari. 1

Layanan Metadata Instance (IMDS) menyediakan informasi metadata tentang EC2 instans Amazon dan berguna untuk konfigurasi aplikasi. Membatasi PUT respons HTTP untuk layanan metadata hanya untuk EC2 instance yang melindungi IMDS dari penggunaan yang tidak sah.

Bidang Time To Live (TTL) dalam paket IP dikurangi satu pada setiap hop. Pengurangan ini dapat digunakan untuk memastikan bahwa paket tidak bepergian ke luar EC2. IMDSv2 melindungi EC2 instance yang mungkin salah dikonfigurasi sebagai router terbuka, firewall lapisan 3, terowongan, atau perangkat NAT VPNs, yang mencegah pengguna yang tidak sah mengambil metadata. Dengan IMDSv2, PUT respons yang berisi token rahasia tidak dapat berjalan di luar instance karena batas hop respons metadata default disetel ke. 1 Namun, jika nilai ini lebih besar dari1, token dapat meninggalkan EC2 instance.

Remediasi

Untuk mengubah batas hop respons metadata untuk konfigurasi peluncuran yang ada, lihat [Memodifikasi opsi metadata instans untuk instance yang ada di Panduan Pengguna](#) Amazon. EC2

[Autoscaling.5] Instans EC2 Amazon yang diluncurkan menggunakan konfigurasi peluncuran grup Auto Scaling seharusnya tidak memiliki alamat IP Publik

Persyaratan terkait: NIST.800-53.r5 AC-2 1, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (9), PCI DSS v4.0.1/1.4.4

Kategori: Lindungi > Konfigurasi jaringan aman > Sumber daya tidak dapat diakses publik

Tingkat keparahan: Tinggi

Jenis sumber daya: AWS::AutoScaling::LaunchConfiguration

AWS Config aturan: [autoscaling-launch-config-public-ip-disabled](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah konfigurasi peluncuran terkait grup Auto Scaling menetapkan [alamat IP publik ke instans](#) grup. Kontrol gagal jika konfigurasi peluncuran terkait menetapkan alamat IP publik.

EC2 Instans Amazon dalam konfigurasi peluncuran grup Auto Scaling tidak boleh memiliki alamat IP publik terkait, kecuali dalam kasus edge terbatas. EC2 Instans Amazon seharusnya hanya dapat diakses dari belakang penyeimbang beban alih-alih langsung terpapar ke internet.

Remediasi

Grup Auto Scaling dikaitkan dengan satu konfigurasi peluncuran pada satu waktu. Anda tidak dapat mengubah konfigurasi peluncuran setelah Anda membuatnya. Untuk mengubah konfigurasi peluncuran untuk grup Auto Scaling, gunakan konfigurasi peluncuran yang ada sebagai dasar untuk konfigurasi peluncuran baru. Lalu, perbarui grup Auto Scaling Anda untuk menggunakan konfigurasi peluncuran baru. Untuk step-by-step petunjuknya, lihat [Mengubah konfigurasi peluncuran untuk grup Auto Scaling di Panduan](#) Pengguna Amazon Auto EC2 Scaling. Saat membuat konfigurasi peluncuran baru, di bawah Konfigurasi tambahan, untuk detail lanjutan, jenis alamat IP, pilih Jangan tetapkan alamat IP publik ke instance apa pun.

Setelah Anda mengubah konfigurasi peluncuran, Auto Scaling meluncurkan instance baru dengan opsi konfigurasi baru. Instance yang ada tidak terpengaruh. Untuk memperbarui instans yang ada,

kami sarankan Anda menyegarkan instans Anda, atau mengizinkan penskalaan otomatis untuk secara bertahap mengganti instans lama dengan instans yang lebih baru berdasarkan kebijakan penghentian Anda. Untuk informasi selengkapnya tentang memperbarui instans Auto Scaling, lihat [Memperbarui instans Auto Scaling di Panduan Pengguna Amazon Auto Scaling](#). EC2

[AutoScaling.6] Grup Auto Scaling harus menggunakan beberapa jenis instance di beberapa Availability Zone

Persyaratan terkait: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-2(2), NIST.800-53.r5 CP-6(2), NIST.800-53.r5 SC-3 6, NIST.800-53.r5 SC-5 (2), NIST.800-53.R5 SI-13 (5)

Kategori: Pulihkan > Ketahanan > Ketersediaan tinggi

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::AutoScaling::AutoScalingGroup

AWS Config aturan: [autoscaling-multiple-instance-types](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah grup EC2 Auto Scaling Amazon menggunakan beberapa jenis instans. Kontrol gagal jika grup Auto Scaling hanya memiliki satu jenis instance yang ditentukan.

Anda dapat meningkatkan ketersediaan dengan menerapkan aplikasi Anda di beberapa jenis instans yang berjalan di beberapa Availability Zone. Security Hub merekomendasikan penggunaan beberapa jenis instans agar grup Auto Scaling dapat meluncurkan tipe instans lain jika kapasitas instans tidak mencukupi di Availability Zone yang Anda pilih.

Remediasi

Untuk membuat grup Auto Scaling dengan beberapa jenis instans, lihat grup [Auto Scaling dengan beberapa jenis instans dan opsi pembelian](#) di Panduan Pengguna Amazon Auto EC2 Scaling.

[AutoScaling.9] Grup EC2 Auto Scaling Amazon harus menggunakan templat peluncuran Amazon EC2

Persyaratan terkait: NIST.800-53.r5 CA-9 (1), Nist.800-53.R5 CM-2, Nist.800-53.R5 CM-2 (2)

Kategori: Identifikasi > Konfigurasi Sumber Daya

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::AutoScaling::AutoScalingGroup`

AWS Config aturan: [autoscaling-launch-template](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah grup EC2 Auto Scaling Amazon dibuat dari template EC2 peluncuran. Kontrol ini gagal jika grup EC2 Auto Scaling Amazon tidak dibuat dengan templat peluncuran atau jika templat peluncuran tidak ditentukan dalam kebijakan instance campuran.

Grup EC2 Auto Scaling dapat dibuat dari template EC2 peluncuran atau konfigurasi peluncuran. Namun, menggunakan template peluncuran untuk membuat grup Auto Scaling memastikan bahwa Anda memiliki akses ke fitur dan peningkatan terbaru.

Remediasi

Untuk membuat grup Auto Scaling dengan template EC2 peluncuran, lihat [Membuat grup Auto Scaling menggunakan template peluncuran di Panduan Pengguna](#) Amazon Auto EC2 Scaling. Untuk informasi tentang cara mengganti konfigurasi peluncuran dengan templat peluncuran, lihat [Mengganti konfigurasi peluncuran dengan templat peluncuran](#) di Panduan EC2 Pengguna Amazon.

[AutoScaling.10] Grup EC2 Auto Scaling harus diberi tag

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::AutoScaling::AutoScalingGroup`

AWS Config aturan: `tagged-autoscaling-autoscalinggroup` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
<code>requiredTagKeys</code>	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS .	Tidak ada nilai default

Kontrol ini memeriksa apakah grup EC2 Auto Scaling Amazon memiliki tag dengan kunci spesifik yang ditentukan dalam parameter. `requiredTagKeys` Kontrol gagal jika grup Auto Scaling tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter. `requiredTagKeys` Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika grup Auto Scaling tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws :`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat [Untuk apa ABAC? AWS](#) di Panduan Pengguna IAM.

Note

Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat [Menandai AWS sumber daya Anda](#) di Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke grup Auto Scaling, lihat [Menandai grup dan instance Auto Scaling](#) di Panduan Pengguna Amazon EC2 Auto Scaling.

Kontrol Security Hub untuk Amazon ECR

Kontrol Security Hub ini mengevaluasi layanan dan sumber daya Amazon Elastic Container Registry (Amazon ECR).

Kontrol ini mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat [Ketersediaan kontrol berdasarkan Wilayah](#).

[ECR.1] Repositori pribadi ECR harus memiliki pemindaian gambar yang dikonfigurasi

Persyaratan terkait: NIST.800-53.r5 RA-5, PCI DSS v4.0.1/6.2.3, PCI DSS v4.0.1/6.2.4

Kategori: Identifikasi > Kerentanan, tambalan, dan manajemen versi

Tingkat keparahan: Tinggi

Jenis sumber daya: AWS::ECR::Repository

AWS Config aturan: [ecr-private-image-scanning-enabled](#)

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah repositori Amazon ECR pribadi memiliki pemindaian gambar yang dikonfigurasi. Kontrol gagal jika repositori ECR pribadi tidak dikonfigurasi untuk pemindaian saat push atau pemindaian berkelanjutan.

Pemindaian gambar ECR membantu mengidentifikasi kerentanan perangkat lunak dalam gambar kontainer Anda. Mengkonfigurasi pemindaian gambar pada repositori ECR menambahkan lapisan verifikasi untuk integritas dan keamanan gambar yang disimpan.

Remediasi

Untuk mengonfigurasi pemindaian gambar untuk repositori ECR, lihat [Pemindaian gambar](#) di Panduan Pengguna Amazon Elastic Container Registry.

[ECR.2] Repositori pribadi ECR harus memiliki kekekalan tag yang dikonfigurasi

Persyaratan terkait: NIST.800-53.r5 CA-9 (1), Nist.800-53.R5 CM-2, Nist.800-53.R5 CM-8 (1)

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::ECR::Repository

AWS Config aturan: [ecr-private-tag-immutability-enabled](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah repositori ECR pribadi memiliki kekekalan tag yang diaktifkan. Kontrol ini gagal jika repositori ECR pribadi menonaktifkan kekekalan tag. Aturan ini berlaku jika kekekalan tag diaktifkan dan memiliki nilai. IMMUTABLE

Amazon ECR Tag Immutability memungkinkan pelanggan untuk mengandalkan tag deskriptif gambar sebagai mekanisme yang andal untuk melacak dan mengidentifikasi gambar secara unik. Tag yang tidak dapat diubah bersifat statis, yang berarti setiap tag mengacu pada gambar yang unik. Ini meningkatkan keandalan dan skalabilitas karena penggunaan tag statis akan selalu menghasilkan gambar yang sama yang digunakan. Saat dikonfigurasi, kekekalan tag mencegah tag diganti, yang mengurangi permukaan serangan.

Remediasi

Untuk membuat repositori dengan tag yang tidak dapat diubah yang dikonfigurasi atau memperbarui setelan mutabilitas tag gambar untuk repositori yang ada, lihat Mutabilitas [tag gambar di Panduan Pengguna Registri Amazon Elastic Container](#).

[ECR.3] Repositori ECR harus memiliki setidaknya satu kebijakan siklus hidup yang dikonfigurasi

Persyaratan terkait: NIST.800-53.r5 CA-9 (1), Nist.800-53.R5 CM-2, Nist.800-53.R5 CM-2 (2)

Kategori: Identifikasi > Konfigurasi sumber daya

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::ECR::Repository

AWS Config aturan: [ecr-private-lifecycle-policy-configured](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah repositori Amazon ECR memiliki setidaknya satu kebijakan siklus hidup yang dikonfigurasi. Kontrol ini gagal jika repositori ECR tidak memiliki kebijakan siklus hidup yang dikonfigurasi.

Kebijakan siklus hidup Amazon ECR memungkinkan Anda untuk menentukan manajemen siklus hidup citra dalam repositori. Dengan mengonfigurasi kebijakan siklus hidup, Anda dapat mengotomatiskan pembersihan gambar yang tidak digunakan dan kedaluwarsa gambar berdasarkan usia atau hitungan. Mengotomatiskan tugas-tugas ini dapat membantu Anda menghindari penggunaan gambar usang secara tidak sengaja di repositori Anda.

Remediasi

Untuk mengonfigurasi kebijakan siklus hidup, lihat [Membuat pratinjau kebijakan siklus hidup di Panduan Pengguna Amazon Elastic Container Registry](#).

[ECR.4] Repositori publik ECR harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: AWS::ECR::PublicRepository

AWS Config aturan: tagged-ecr-publicrepository (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
<code>requiredTagKeys</code>	Daftar kunci tag non-sistem yang harus berisi sumber daya	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi	Tidak ada nilai default

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
	yang dievaluasi. Kunci tag peka huruf besar dan kecil.		persyaratan AWS .	

Kontrol ini memeriksa apakah repositori publik Amazon ECR memiliki tag dengan kunci tertentu yang ditentukan dalam parameter. `requiredTagKeys` Kontrol gagal jika repositori publik tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter. `requiredTagKeys` Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika repositori publik tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws :`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat [Untuk apa ABAC? AWS](#) di Panduan Pengguna IAM.

Note

Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat [Menandai AWS sumber daya Anda](#) di Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke repositori publik ECR, lihat [Menandai repositori publik Amazon ECR di Panduan Pengguna Registri Amazon Elastic Container](#).

[ECR.5] Repositori ECR harus dienkripsi dengan pelanggan yang dikelola AWS KMS keys

Persyaratan terkait: NIST.800-53.r5 SC-1 2 (2), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-1 3, 8, NIST.800-53.r5 SC-2 8 (1), (10), NIST.800-53.r5 SC-2 (1), NIST.800-53.r5 SC-7 Nist.800-53.R5 SI-7 NIST.800-53.r5 CA-9 (6), Nist.800-53.R5 AU-9

Kategori: Lindungi > Perlindungan Data > Enkripsi data-at-rest

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::ECR::Repository

AWS Config aturan: [ecr-repository-cmk-encryption-enabled](#)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
kmsKeyArns	Daftar Nama Sumber Daya Amazon (ARNs) AWS KMS keys untuk disertakan dalam evaluasi. Kontrol menghasilkan FAILED temuan jika repositori ECR tidak dienkripsi dengan kunci KMS dalam daftar.	StringList (maksimal 10 item)	1-10 kunci ARNs KMS yang ada. Misalnya: arn:aws:kms:us-west-2:11112223333:key/1234abcd-12ab-34cd-56ef-1234567890ab	Tidak ada nilai default

Kontrol ini memeriksa apakah repositori Amazon ECR dienkripsi saat istirahat dengan pelanggan yang dikelola. AWS KMS key Kontrol gagal jika repositori ECR tidak dienkripsi dengan kunci KMS

yang dikelola pelanggan. Anda dapat secara opsional menentukan daftar kunci KMS untuk kontrol untuk disertakan dalam evaluasi.

Secara default, Amazon ECR mengenkripsi data repositori dengan kunci terkelola Amazon S3 (SSE-S3), menggunakan algoritma AES-256. Untuk kontrol tambahan, Anda dapat mengonfigurasi Amazon ECR untuk mengenkripsi data dengan AWS KMS key (SSE-KMS atau DSSE-KMS) sebagai gantinya. Kunci KMS dapat berupa: sebuah Kunci yang dikelola AWS yang Amazon ECR buat dan kelola untuk Anda dan memiliki alias `saws/ecr`, atau kunci yang dikelola pelanggan yang Anda buat dan kelola di Anda. Akun AWS Dengan kunci KMS yang dikelola pelanggan, Anda memiliki kendali penuh atas kunci tersebut. Ini termasuk mendefinisikan dan memelihara kebijakan kunci, mengelola hibah, memutar materi kriptografi, menetapkan tag, membuat alias, dan mengaktifkan dan menonaktifkan kunci.

Note

AWS KMS mendukung akses lintas akun ke kunci KMS. Jika repositori ECR dienkripsi dengan kunci KMS yang dimiliki oleh akun lain, kontrol ini tidak melakukan pemeriksaan lintas akun saat mengevaluasi repositori. Kontrol tidak menilai apakah Amazon ECR dapat mengakses dan menggunakan kunci saat melakukan operasi kriptografi untuk repositori.

Remediasi

Anda tidak dapat mengubah pengaturan enkripsi untuk repositori ECR yang ada. Namun, Anda dapat menentukan pengaturan enkripsi yang berbeda untuk repositori ECR yang kemudian Anda buat. Amazon ECR mendukung penggunaan pengaturan enkripsi yang berbeda untuk masing-masing repositori.

Untuk informasi selengkapnya tentang opsi enkripsi untuk repositori ECR, lihat [Enkripsi saat istirahat di Panduan](#) Pengguna Amazon ECR. Untuk informasi selengkapnya tentang pelanggan yang dikelola AWS KMS keys, lihat [AWS KMS keys](#) di Panduan AWS Key Management Service Pengembang.

Kontrol Security Hub untuk Amazon ECS

Kontrol Security Hub ini mengevaluasi layanan dan sumber daya Amazon Elastic Container Service (Amazon ECS). Kontrol mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat [Ketersediaan kontrol berdasarkan Wilayah](#).

[ECS.1] Definisi tugas Amazon ECS harus memiliki mode jaringan yang aman dan definisi pengguna

Persyaratan terkait: NIST.800-53.r5 AC-2 (1) NIST.800-53.r5 AC-3,, NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-5, NIST.800-53.r5 AC-6

Kategori: Lindungi > Manajemen akses yang aman

Tingkat keparahan: Tinggi

Jenis sumber daya: AWS::ECS::TaskDefinition

AWS Config aturan: [ecs-task-definition-user-for-host-mode-check](#)

Jenis jadwal: Perubahan dipicu

Parameter:

- `SkipInactiveTaskDefinitions: true` (tidak dapat disesuaikan)

Kontrol ini memeriksa apakah definisi tugas Amazon ECS aktif dengan mode jaringan host memiliki `privileged` atau definisi user kontainer. Kontrol gagal untuk definisi tugas yang memiliki mode jaringan host dan definisi wadah `privileged=false`, kosong dan `user=root`, atau kosong.

Kontrol ini hanya mengevaluasi revisi aktif terbaru dari definisi tugas Amazon ECS.

Tujuan dari kontrol ini adalah untuk memastikan bahwa akses didefinisikan dengan sengaja ketika Anda menjalankan tugas yang menggunakan mode jaringan host. Jika definisi tugas memiliki hak istimewa yang tinggi, itu karena Anda telah memilih konfigurasi itu. Kontrol ini memeriksa eskalasi hak istimewa yang tidak terduga ketika definisi tugas mengaktifkan jaringan host, dan Anda tidak memilih hak istimewa yang ditinggikan.

Remediasi

Untuk informasi tentang cara memperbarui definisi tugas, lihat [Memperbarui definisi tugas](#) di Panduan Pengembang Layanan Amazon Elastic Container.

Saat Anda memperbarui definisi tugas, itu tidak memperbarui tugas yang sedang berjalan yang diluncurkan dari definisi tugas sebelumnya. Untuk memperbarui tugas yang sedang berjalan, Anda harus menerapkan ulang tugas dengan definisi tugas baru.

[ECS.2] Layanan ECS seharusnya tidak memiliki alamat IP publik yang ditetapkan kepadanya secara otomatis

Persyaratan terkait: NIST.800-53.r5 AC-2 1, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (9), PCI DSS v4.0.1/1.4.4

Kategori: Lindungi > Konfigurasi jaringan aman > Sumber daya tidak dapat diakses publik

Tingkat keparahan: Tinggi

Jenis sumber daya: AWS::ECS::Service

AWS Config aturan: `ecs-service-assign-public-ip-disabled` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah layanan Amazon ECS dikonfigurasi untuk secara otomatis menetapkan alamat IP publik. Kontrol ini gagal jika `AssignPublicIP` ada `ENABLED`. Kontrol ini lolos jika `AssignPublicIP` ada `DISABLED`.

Alamat IP publik adalah alamat IP yang dapat dijangkau dari internet. Jika Anda meluncurkan instans Amazon ECS Anda dengan alamat IP publik, maka instans Amazon ECS Anda dapat dijangkau dari internet. Layanan Amazon ECS tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke server aplikasi kontainer Anda.

Remediasi

Pertama, Anda harus membuat definisi tugas untuk cluster Anda yang menggunakan mode `awsvpc` jaringan dan menentukan `FARGATE` untuk `requiresCompatibilities`. Kemudian, untuk konfigurasi `Compute`, pilih `Launch type` dan `FARGATE`. Terakhir, untuk bidang `Jaringan`, matikan `IP Publik` untuk menonaktifkan penugasan IP publik otomatis untuk layanan Anda.

[ECS.3] Definisi tugas ECS tidak boleh membagikan namespace proses host

Persyaratan terkait: NIST.800-53.r5 CA-9 (1), Nist.800-53.R5 CM-2

Kategori: Identifikasi > Konfigurasi sumber daya

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::ECS::TaskDefinition`

AWS Config aturan: [ecs-task-definition-pid-mode-check](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah definisi tugas Amazon ECS dikonfigurasi untuk berbagi namespace proses host dengan kontainernya. Kontrol gagal jika definisi tugas membagikan namespace proses host dengan wadah yang berjalan di atasnya. Kontrol ini hanya mengevaluasi revisi aktif terbaru dari definisi tugas Amazon ECS.

Namespace ID proses (PID) menyediakan pemisahan antar proses. Ini mencegah proses sistem agar tidak terlihat, dan memungkinkan PIDs untuk digunakan kembali, termasuk PID 1. Jika namespace PID host dibagikan dengan kontainer, itu akan memungkinkan kontainer untuk melihat semua proses pada sistem host. Ini mengurangi manfaat isolasi tingkat proses antara host dan wadah. Keadaan ini dapat menyebabkan akses tidak sah ke proses pada host itu sendiri, termasuk kemampuan untuk memanipulasi dan menghentikannya. Pelanggan tidak boleh membagikan namespace proses host dengan wadah yang berjalan di atasnya.

Remediasi

Untuk mengonfigurasi definisi tugas, lihat [Parameter definisi tugas](#) di Panduan Pengembang Layanan Amazon Elastic Container. `pidMode`

[ECS.4] Kontainer ECS harus berjalan sebagai non-hak istimewa

Persyaratan terkait: NIST.800-53.r5 AC-2 (1) NIST.800-53.r5 AC-3,, NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-5, NIST.800-53.r5 AC-6

Kategori: Lindungi > Manajemen akses aman > Pembatasan akses pengguna root

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::ECS::TaskDefinition`

AWS Config aturan: [ecs-containers-nonprivileged](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah `privileged` parameter dalam definisi penampung Definisi Tugas Amazon ECS disetel ke `true`. Kontrol gagal jika parameter ini sama dengan `true`. Kontrol ini hanya mengevaluasi revisi aktif terbaru dari definisi tugas Amazon ECS.

Kami menyarankan Anda menghapus hak istimewa yang ditinggikan dari definisi tugas ECS Anda. Ketika parameter `privilege` adalah `true`, wadah diberikan hak istimewa yang ditinggikan pada instance wadah host (mirip dengan pengguna `root`).

Remediasi

Untuk mengonfigurasi `privileged` parameter pada definisi tugas, lihat [Parameter definisi kontainer lanjutan](#) di Panduan Pengembang Layanan Kontainer Elastis Amazon.

[ECS.5] Wadah ECS harus dibatasi pada akses hanya-baca ke sistem file root

Persyaratan terkait: NIST.800-53.r5 AC-2 (1) NIST.800-53.r5 AC-3,, NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-5, NIST.800-53.r5 AC-6

Kategori: Lindungi > Manajemen akses yang aman

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::ECS::TaskDefinition`

AWS Config aturan: [ecs-containers-readonly-access](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah wadah Amazon ECS memiliki akses hanya-baca ke sistem file root-nya. Kontrol gagal jika `readonlyRootFilesystem` parameter disetel ke `false`, atau parameter tidak ada dalam definisi wadah dalam definisi tugas. Kontrol ini hanya mengevaluasi revisi aktif terbaru dari definisi tugas Amazon ECS.

Jika `readonlyRootFilesystem` parameter disetel ke `true` dalam definisi tugas Amazon ECS, wadah ECS diberikan akses hanya-baca ke sistem file root-nya. Ini mengurangi vektor serangan keamanan karena sistem file root instance container tidak dapat dirusak atau ditulis tanpa mount volume eksplisit yang memiliki izin baca-tulis untuk folder dan direktori sistem file. Mengaktifkan opsi ini juga mematuhi prinsip hak istimewa paling sedikit.

Remediasi

Untuk memberikan akses read-only container Amazon ECS ke sistem file root, tambahkan `readonlyRootFilesystem` parameter ke definisi tugas untuk container, dan tetapkan nilai untuk parameter tersebut. `true` Untuk informasi tentang parameter definisi tugas dan cara menambahkannya ke definisi tugas, lihat definisi tugas [Amazon ECS dan Memperbarui definisi tugas](#) di Panduan Pengembang Layanan Amazon Elastic Container.

[ECS.8] Rahasia tidak boleh diteruskan sebagai variabel lingkungan kontainer

Persyaratan terkait: NIST.800-53.r5 CA-9 (1), Nist.800-53.R5 CM-2, PCI DSS v4.0.1/8.6.2

Kategori: Lindungi > Pengembangan aman > Kredensial tidak dikodekan dengan keras

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::ECS::TaskDefinition`

AWS Config aturan: [ecs-no-environment-secrets](#)

Jenis jadwal: Perubahan dipicu

Parameter: `secretKeys:AWS_ACCESS_KEY_ID,AWS_SECRET_ACCESS_KEY,ECS_ENGINE_AUTH_DATA` (tidak dapat disesuaikan)

Kontrol ini memeriksa apakah nilai kunci dari setiap variabel dalam `environment` parameter definisi kontainer termasuk `AWS_ACCESS_KEY_ID`, `AWS_SECRET_ACCESS_KEY`, atau `ECS_ENGINE_AUTH_DATA`. Kontrol ini gagal jika variabel lingkungan tunggal dalam definisi kontainer sama `AWS_ACCESS_KEY_ID`, `AWS_SECRET_ACCESS_KEY`, atau `ECS_ENGINE_AUTH_DATA`. Kontrol ini tidak mencakup variabel lingkungan yang diteruskan dari lokasi lain seperti Amazon S3. Kontrol ini hanya mengevaluasi revisi aktif terbaru dari definisi tugas Amazon ECS.

AWS Systems Manager Parameter Store dapat membantu Anda meningkatkan postur keamanan organisasi Anda. Sebaiknya gunakan Parameter Store untuk menyimpan rahasia dan kredensial alih-alih langsung meneruskannya ke instance container Anda atau hard coding ke dalam kode Anda.

Remediasi

Untuk membuat parameter menggunakan SSM, lihat [Membuat parameter Systems Manager](#) di Panduan AWS Systems Manager Pengguna. Untuk informasi selengkapnya tentang membuat definisi tugas yang menentukan rahasia, lihat Menentukan [data sensitif menggunakan Secrets Manager](#) di Panduan Pengembang Layanan Amazon Elastic Container.

[ECS.9] Definisi tugas ECS harus memiliki konfigurasi logging

Persyaratan terkait: NIST.800-53.r5 AC-4 (26),, NIST.800-53.r5 SC-7 (9) NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, NIST.800-53.R5 SI-7 (8)

Kategori: Identifikasi > Logging

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::ECS::TaskDefinition`

AWS Config aturan: `ecs-task-definition-log` [-konfigurasi](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah definisi tugas Amazon ECS aktif terbaru memiliki konfigurasi logging yang ditentukan. Kontrol gagal jika definisi tugas tidak memiliki `logConfiguration` properti yang ditentukan atau jika nilai untuk `logDriver` adalah nol dalam setidaknya satu definisi kontainer.

Logging membantu Anda menjaga keandalan, ketersediaan, dan kinerja Amazon ECS.

Mengumpulkan data dari definisi tugas memberikan visibilitas, yang dapat membantu Anda men-debug proses dan menemukan akar penyebab kesalahan. Jika Anda menggunakan solusi logging yang tidak harus didefinisikan dalam definisi tugas ECS (seperti solusi logging pihak ketiga), Anda dapat menonaktifkan kontrol ini setelah memastikan bahwa log Anda ditangkap dan dikirim dengan benar.

Remediasi

Untuk menentukan konfigurasi log untuk definisi tugas Amazon ECS Anda, lihat [Menentukan konfigurasi log dalam definisi tugas Anda di Panduan](#) Pengembang Layanan Amazon Elastic Container.

[ECS.10] Layanan ECS Fargate harus berjalan pada versi platform Fargate terbaru

Persyaratan terkait: NIST.800-53.R5 SI-2, NIST.800-53.R5 SI-2 (2), NIST.800-53.R5 SI-2 (4), Nist.800-53.R5 SI-2 (5), PCI DSS v4.0.1/6.3.3

Kategori: Identifikasi > Kerentanan, tambalan, dan manajemen versi

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::ECS::Service`

AWS Config aturan: [ecs-fargate-latest-platform-version](#)

Jenis jadwal: Perubahan dipicu

Parameter:

- `latestLinuxVersion: 1.4.0`(tidak dapat disesuaikan)
- `latestWindowsVersion: 1.0.0`(tidak dapat disesuaikan)

Kontrol ini memeriksa apakah layanan Amazon ECS Fargate menjalankan versi platform Fargate terbaru. Kontrol ini gagal jika versi platform bukan yang terbaru.

AWS Fargate Versi platform mengacu pada lingkungan runtime tertentu untuk infrastruktur tugas Fargate, yang merupakan kombinasi dari versi runtime kernel dan container. Versi platform baru dirilis saat lingkungan runtime berkembang. Misalnya, versi baru dapat dirilis untuk pembaruan kernel atau sistem operasi, fitur baru, perbaikan bug, atau pembaruan keamanan. Pembaruan dan tambalan keamanan diterapkan secara otomatis untuk tugas Fargate Anda. Jika ditemukan masalah keamanan yang memengaruhi versi platform, AWS tambal versi platform.

Remediasi

Untuk memperbarui layanan yang ada, termasuk versi platformnya, lihat [Memperbarui layanan](#) di Panduan Pengembang Layanan Amazon Elastic Container.

[ECS.12] Cluster ECS harus menggunakan Wawasan Kontainer

Persyaratan terkait: NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, NIST.800-53.R5 SI-2

Kategori: Identifikasi > Logging

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::ECS::Cluster`

AWS Config aturan: [ecs-container-insights-enabled](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah cluster ECS menggunakan Wawasan Kontainer. Kontrol ini gagal jika Wawasan Kontainer tidak disiapkan untuk klaster.

Pemantauan adalah bagian penting dalam menjaga keandalan, ketersediaan, dan kinerja klaster Amazon ECS. Gunakan CloudWatch Wawasan Kontainer untuk mengumpulkan, menggabungkan, dan meringkas metrik dan log dari aplikasi dan layanan mikro dalam kontainer Anda. CloudWatch Secara otomatis mengumpulkan metrik untuk banyak sumber daya, seperti CPU, memori, disk, dan jaringan. Wawasan Kontainer juga akan menyediakan informasi diagnostik, seperti kegagalan mengulang kembali kontainer, untuk membantu Anda melakukan isolasi atas masalah dan mengatasi masalah itu dengan cepat. Anda juga dapat menyetel CloudWatch alarm pada metrik yang dikumpulkan Container Insights.

Remediasi

Untuk menggunakan Wawasan Penampung, lihat [Memperbarui layanan](#) di Panduan CloudWatch Pengguna Amazon.

[ECS.13] Layanan ECS harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: AWS::ECS::Service

AWS Config aturan: tagged-ecs-service (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
<code>requiredTagKeys</code>	Daftar kunci tag non-sistem yang harus berisi sumber daya	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi	Tidak ada nilai default

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
	yang dievaluasi. Kunci tag peka huruf besar dan kecil.		persyaratan AWS .	

Kontrol ini memeriksa apakah layanan Amazon ECS memiliki tag dengan kunci spesifik yang ditentukan dalam parameter `requiredTagKeys`. Kontrol gagal jika layanan tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter `requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika layanan tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws :`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat [Untuk apa ABAC? AWS](#) di Panduan Pengguna IAM.

Note

Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat [Menandai AWS sumber daya Anda](#) di Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke layanan ECS, lihat [Menandai resource Amazon ECS Anda di Panduan Pengembang Layanan Amazon Elastic Container](#).

[ECS.14] Cluster ECS harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::ECS::Cluster`

AWS Config aturan: `tagged-ecs-cluster` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
<code>requiredTagKeys</code>	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS .	Tidak ada nilai default

Kontrol ini memeriksa apakah klaster Amazon ECS memiliki tag dengan kunci spesifik yang ditentukan dalam parameter `requiredTagKeys`. Kontrol gagal jika cluster tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter `requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika cluster tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke

AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat [Untuk apa ABAC? AWS](#) di Panduan Pengguna IAM.

Note

Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat [Menandai AWS sumber daya Anda](#) di Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke cluster ECS, lihat [Menandai resource Amazon ECS Anda di Panduan Pengembang Layanan Amazon Elastic Container](#).

[ECS.15] Definisi tugas ECS harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: AWS::ECS::TaskDefinition

AWS Config aturan: tagged-ecs-taskdefinition (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
requiredTagKeys	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi	Tidak ada nilai default

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
			persyaratan AWS	

Kontrol ini memeriksa apakah definisi tugas Amazon ECS memiliki tag dengan kunci tertentu yang ditentukan dalam parameter `requiredTagKeys`. Kontrol gagal jika definisi tugas tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter `requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika definisi tugas tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat [Untuk apa ABAC? AWS](#) di Panduan Pengguna IAM.

Note

Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat [Menandai AWS sumber daya Anda](#) di Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke definisi tugas ECS, lihat [Menandai resource Amazon ECS Anda di Panduan Pengembang Layanan Amazon Elastic](#) Container.

[ECS.16] Set tugas ECS seharusnya tidak secara otomatis menetapkan alamat IP publik

Persyaratan terkait: PCI DSS v4.0.1/1.4.4

Kategori: Lindungi > Konfigurasi jaringan aman > Sumber daya tidak dapat diakses publik

Tingkat keparahan: Tinggi

Jenis sumber daya: AWS::ECS::TaskSet

AWS Config aturan: `ecs-taskset-assign-public-ip-disabled` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah set tugas Amazon ECS dikonfigurasi untuk secara otomatis menetapkan alamat IP publik. Kontrol gagal jika `AssignPublicIP` disetel ke `ENABLED`.

Alamat IP publik dapat dijangkau dari internet. Jika Anda mengonfigurasi set tugas Anda dengan alamat IP publik, sumber daya yang terkait dengan kumpulan tugas dapat dijangkau dari internet. Kumpulan tugas ECS tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke server aplikasi kontainer Anda.

Remediasi

Untuk memperbarui set tugas ECS agar tidak menggunakan alamat IP publik, lihat [Memperbarui definisi tugas Amazon ECS menggunakan konsol di Panduan Pengembang](#) Layanan Amazon Elastic Container.

[ECS.17] Definisi tugas ECS tidak boleh menggunakan mode jaringan host

Persyaratan terkait: NIST.800-53.r5 AC-2 (1) NIST.800-53.r5 AC-3,, NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-5, NIST.800-53.r5 AC-6

Kategori: Lindungi > Konfigurasi jaringan aman

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::ECS::TaskDefinition

AWS Config aturan: [ecs-task-definition-network-mode-not-host](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah revisi aktif terbaru dari definisi tugas Amazon ECS menggunakan mode host jaringan. Kontrol gagal jika revisi aktif terbaru dari definisi tugas ECS menggunakan mode host jaringan.

Saat menggunakan mode host jaringan, jaringan wadah Amazon ECS terikat langsung ke host yang mendasari yang menjalankan penampung. Akibatnya, mode ini memungkinkan kontainer untuk terhubung ke layanan jaringan loopback pribadi pada host dan untuk meniru host. Kelemahan signifikan lainnya adalah tidak ada cara untuk memetakan ulang port kontainer saat menggunakan mode host jaringan, dan Anda tidak dapat menjalankan lebih dari satu instance tugas di setiap host.

Remediasi

Untuk informasi tentang mode jaringan dan opsi untuk tugas Amazon ECS yang dihosting di EC2 instans Amazon, lihat [opsi jaringan tugas Amazon ECS untuk jenis EC2 peluncuran di Panduan Pengembang](#) Layanan Kontainer Elastis Amazon. Untuk informasi tentang membuat revisi baru definisi tugas dan menentukan mode jaringan yang berbeda, lihat [Memperbarui definisi tugas Amazon ECS](#) dalam panduan tersebut.

Jika definisi tugas Amazon ECS dibuat oleh AWS Batch, lihat [Mode jaringan untuk AWS Batch pekerjaan untuk](#) mempelajari tentang mode jaringan dan penggunaan umum untuk jenis AWS Batch pekerjaan dan untuk memilih opsi yang aman.

Kontrol Security Hub untuk Amazon EFS

Kontrol Security Hub ini mengevaluasi layanan dan sumber daya Amazon Elastic File System (Amazon EFS).

Kontrol ini mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat [Ketersediaan kontrol berdasarkan Wilayah](#).

[EFS.1] Sistem File Elastis harus dikonfigurasi untuk mengenkripsi data file saat istirahat menggunakan AWS KMS

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v3.0.0/2.4.1, NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-1 3, 8, NIST.800-53.r5 SC-2 8 (1), (10), NIST.800-53.r5 SC-2 NIST.800-53.R5 SI-7 NIST.800-53.r5 SC-7 (6)

Kategori: Lindungi > Perlindungan Data > Enkripsi data-at-rest

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::EFS::FileSystem

AWS Config aturan: [efs-encrypted-check](#)

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah Amazon Elastic File System dikonfigurasi untuk mengenkripsi data file yang digunakan AWS KMS. Pemeriksaan gagal dalam kasus berikut.

- Encrypted diatur ke false dalam [DescribeFileSystems](#) respons.
- KmsKeyId Kunci dalam [DescribeFileSystems](#) respons tidak cocok dengan KmsKeyId parameter untuk [efs-encrypted-check](#).

Perhatikan bahwa kontrol ini tidak menggunakan KmsKeyId parameter untuk [efs-encrypted-check](#). Itu hanya memeriksa nilai Encrypted.

Untuk lapisan keamanan tambahan untuk data sensitif Anda di Amazon EFS, Anda harus membuat sistem file terenkripsi. Amazon EFS mendukung enkripsi untuk sistem file saat istirahat. Anda dapat mengaktifkan enkripsi data saat istirahat saat Anda membuat sistem file Amazon EFS. Untuk mempelajari lebih lanjut tentang enkripsi Amazon EFS, lihat [Enkripsi data di Amazon EFS](#) di Panduan Pengguna Amazon Elastic File System.

Remediasi

Untuk detail tentang cara mengenkripsi sistem file Amazon EFS baru, lihat [Mengekripsi data saat istirahat di Panduan Pengguna](#) Amazon Elastic File System.

[EFS.2] Volume Amazon EFS harus dalam rencana cadangan

Persyaratan terkait: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6, NIST.800-53.r5 CP-6(1), NIST.800-53.r5 CP-6(2), NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5 (2), NIST.800-53.R5 SI-12, NIST.800-53.R5 SI-13 (5)

Kategori: Pulihkan > Ketahanan > Cadangan

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::EFS::FileSystem

AWS Config aturan: [efs-in-backup-plan](#)

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah sistem file Amazon Elastic File System (Amazon EFS) ditambahkan ke paket cadangan AWS Backup. Kontrol gagal jika sistem file Amazon EFS tidak disertakan dalam paket cadangan.

Menyertakan sistem file EFS dalam paket cadangan membantu Anda melindungi data dari penghapusan dan kehilangan data.

Remediasi

Untuk mengaktifkan pencadangan otomatis untuk sistem file Amazon EFS yang ada, lihat [Memulai 4: Membuat cadangan otomatis Amazon EFS](#) di Panduan Pengembang.AWS Backup

[EFS.3] Titik akses EFS harus menegakkan direktori root

Persyaratan terkait: NIST.800-53.r5 AC-6 (10)

Kategori: Lindungi > Manajemen akses yang aman

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::EFS::AccessPoint

AWS Config aturan: [efs-access-point-enforce-root-directory](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah titik akses Amazon EFS dikonfigurasi untuk menerapkan direktori root. Kontrol gagal jika nilai Path diatur ke / (direktori root default dari sistem file).

Saat Anda menerapkan direktori root, klien NFS yang menggunakan titik akses menggunakan direktori root yang dikonfigurasi pada titik akses alih-alih direktori root sistem file. Menegakkan

direktori root untuk titik akses membantu membatasi akses data dengan memastikan bahwa pengguna titik akses hanya dapat menjangkau file dari subdirektori yang ditentukan.

Remediasi

Untuk petunjuk tentang cara menerapkan direktori root untuk jalur akses Amazon EFS, lihat [Menerapkan direktori root dengan titik akses](#) di Panduan Pengguna Amazon Elastic File System.

[EFS.4] Titik akses EFS harus menegakkan identitas pengguna

Persyaratan terkait: NIST.800-53.r5 AC-6 (2), PCI DSS v4.0.1/7.3.1

Kategori: Lindungi > Manajemen akses yang aman

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::EFS::AccessPoint

AWS Config aturan: [efs-access-point-enforce-user-identity](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah titik akses Amazon EFS dikonfigurasi untuk menegakkan identitas pengguna. Kontrol ini gagal jika identitas pengguna POSIX tidak ditentukan saat membuat titik akses EFS.

Titik akses Amazon EFS adalah titik masuk khusus aplikasi ke dalam sistem file EFS yang memudahkan pengelolaan akses aplikasi ke kumpulan data bersama. Titik akses dapat menerapkan identitas pengguna, termasuk grup POSIX pengguna, pada semua permintaan sistem file yang dibuat melalui titik akses. Titik akses juga dapat menerapkan direktori asal yang berbeda untuk sistem file sehingga klien hanya dapat mengakses data dalam direktori tertentu atau subdirektornya.

Remediasi

Untuk menerapkan identitas pengguna untuk jalur akses Amazon EFS, lihat [Menerapkan identitas pengguna menggunakan titik akses](#) di Panduan Pengguna Amazon Elastic File System.

[EFS.5] Titik akses EFS harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::EFS::AccessPoint`

AWS Config aturan: `tagged-efs-accesspoint` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
<code>requiredTagKeys</code>	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS.	Tidak ada nilai default

Kontrol ini memeriksa apakah titik akses Amazon EFS memiliki tag dengan kunci tertentu yang ditentukan dalam parameter `requiredTagKeys`. Kontrol gagal jika titik akses tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter `requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika titik akses tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat [Untuk apa ABAC? AWS](#) di Panduan Pengguna IAM.

 Note

Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat [Menandai AWS sumber daya Anda](#) di Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke titik akses EFS, lihat [Menandai resource Amazon EFS](#) di Panduan Pengguna Amazon Elastic File System.

[EFS.6] Target pemasangan EFS tidak boleh dikaitkan dengan subnet publik

Kategori: Lindungi > Konfigurasi jaringan aman > Sumber daya tidak dapat diakses publik

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::EFS::FileSystem`

AWS Config aturan: [efs-mount-target-public-accessible](#)

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah target pemasangan Amazon EFS dikaitkan dengan subnet pribadi. Kontrol gagal jika target pemasangan dikaitkan dengan subnet publik.

Secara default, sistem file hanya dapat diakses dari virtual private cloud (VPC) tempat Anda membuatnya. Sebaiknya buat target pemasangan EFS di subnet pribadi yang tidak dapat diakses dari internet. Ini membantu memastikan bahwa sistem file Anda hanya dapat diakses oleh pengguna yang berwenang dan tidak rentan terhadap akses atau serangan yang tidak sah.

Remediasi

Anda tidak dapat mengubah asosiasi antara target pemasangan EFS dan subnet setelah membuat target pemasangan. Untuk mengaitkan target mount yang ada dengan subnet yang berbeda, Anda harus membuat target mount baru di subnet pribadi dan kemudian menghapus target mount lama.

Untuk informasi tentang mengelola target mount, lihat [Membuat dan mengelola target mount dan grup keamanan](#) di Panduan Pengguna Amazon Elastic File System.

[EFS.7] Sistem file EFS harus mengaktifkan pencadangan otomatis

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::EFS::FileSystem`

AWS Config aturan: [efs-automatic-backups-enabled](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah sistem file Amazon EFS mengaktifkan pencadangan otomatis. Kontrol ini gagal jika sistem file EFS tidak mengaktifkan pencadangan otomatis.

Cadangan data adalah salinan sistem, konfigurasi, atau data aplikasi Anda yang disimpan secara terpisah dari aslinya. Mengaktifkan pencadangan reguler membantu Anda melindungi data berharga dari peristiwa tak terduga seperti kegagalan sistem, serangan siber, atau penghapusan yang tidak disengaja. Memiliki strategi cadangan yang kuat juga memfasilitasi pemulihan yang lebih cepat, kelangsungan bisnis, dan ketenangan pikiran dalam menghadapi potensi kehilangan data.

Remediasi

Untuk informasi tentang penggunaan AWS Backup untuk sistem file EFS, lihat [Mencadangkan sistem file EFS](#) di Panduan Pengguna Amazon Elastic File System

[EFS.8] Sistem file EFS harus dienkrpsi saat istirahat

Kategori: Lindungi > Perlindungan Data > Enkripsi data-at-rest

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::EFS::FileSystem`

AWS Config aturan: [efs-filesystem-ct-encrypted](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah sistem file Amazon EFS mengenkripsi data dengan AWS Key Management Service (AWS KMS). Kontrol gagal jika sistem file tidak dienkripsi.

Data saat istirahat mengacu pada data yang disimpan dalam penyimpanan persisten dan tidak mudah menguap untuk durasi berapa pun. Mengenkripsi data saat istirahat membantu Anda melindungi kerahasiaannya, yang mengurangi risiko bahwa pengguna yang tidak sah dapat mengaksesnya.

Remediasi

Untuk mengaktifkan enkripsi saat istirahat untuk sistem file EFS baru, lihat [Mengekripsi data saat istirahat di](#) Panduan Pengguna Amazon Elastic File System.

Kontrol Security Hub untuk Amazon EKS

Kontrol Security Hub ini mengevaluasi layanan dan sumber daya Amazon Elastic Kubernetes Service (Amazon EKS). Kontrol mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat [Ketersediaan kontrol berdasarkan Wilayah](#).

[EKS.1] Titik akhir kluster EKS seharusnya tidak dapat diakses publik

Persyaratan terkait: NIST.800-53.r5 AC-2 1, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21),, NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (9), PCI DSS v4.0.1/1.4.4

Kategori: Lindungi > Konfigurasi jaringan aman > Sumber daya tidak dapat diakses publik

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::EKS::Cluster`

AWS Config aturan: [eks-endpoint-no-public-access](#)

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah titik akhir kluster Amazon EKS dapat diakses publik. Kontrol gagal jika kluster EKS memiliki titik akhir yang dapat diakses publik.

Saat Anda membuat kluster baru, Amazon EKS membuat endpoint untuk server API Kubernetes terkelola yang Anda gunakan untuk berkomunikasi dengan kluster Anda. Secara default, titik akhir server API ini tersedia untuk umum di internet. Akses ke server API diamankan menggunakan kombinasi AWS Identity and Access Management (IAM) dan Kubernetes Role Based Access Control (RBAC) asli. Dengan menghapus akses publik ke titik akhir, Anda dapat menghindari eksposur yang tidak disengaja dan akses ke cluster Anda.

Remediasi

Untuk mengubah akses titik akhir untuk kluster EKS yang ada, lihat [Memodifikasi akses titik akhir kluster di Panduan](#) Pengguna Amazon EKS. Anda dapat mengatur akses titik akhir untuk kluster EKS baru saat membuatnya. Untuk petunjuk cara membuat kluster Amazon EKS baru, lihat [Membuat kluster Amazon EKS](#) di Panduan Pengguna Amazon EKS.

[EKS.2] Kluster EKS harus berjalan pada versi Kubernetes yang didukung

Persyaratan terkait: NIST.800-53.r5 CA-9 (1), NIST.800-53.R5 CM-2, NIST.800-53.R5 SI-2, NIST.800-53.R5 SI-2 (2), Nist.800-53.r5 SI-2 (4), Nist.800-53.R5 SI-2 (5), PCI DSS v4.0.1/12.3.4

Kategori: Identifikasi > Kerentanan, tambalan, dan manajemen versi

Tingkat keparahan: Tinggi

Jenis sumber daya: AWS::EKS::Cluster

AWS Config aturan: [eks-cluster-supported-version](#)

Jenis jadwal: Perubahan dipicu

Parameter:

- `oldestVersionSupported: 1.30` (tidak dapat disesuaikan)

Kontrol ini memeriksa apakah kluster Amazon Elastic Kubernetes Service (Amazon EKS) berjalan pada versi Kubernetes yang didukung. Kontrol gagal jika kluster EKS berjalan pada versi yang tidak didukung.

Jika aplikasi Anda tidak memerlukan versi Kubernetes tertentu, kami sarankan Anda menggunakan versi Kubernetes terbaru yang tersedia yang didukung oleh EKS untuk cluster Anda. Untuk informasi selengkapnya, lihat [kalender rilis Amazon EKS Kubernetes](#) dan [Memahami siklus hidup versi Kubernetes di Amazon EKS di Panduan Pengguna Amazon EKS](#).

Remediasi

Untuk memperbarui kluster EKS, lihat [Memperbarui klaster yang ada ke versi Kubernetes baru di Panduan](#) Pengguna Amazon EKS.

[EKS.3] Kluster EKS harus menggunakan rahasia Kubernetes terenkripsi

Persyaratan terkait: NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-1 2, NIST.800-53.r5 SC-1 3, NIST.800-53.r5 SC-2 8, PCI DSS v4.0.1/8.3.2

Kategori: Lindungi > Perlindungan Data > Enkripsi data-at-rest

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::EKS::Cluster

AWS Config aturan: [eks-cluster-secrets-encrypted](#)

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah kluster Amazon EKS menggunakan rahasia Kubernetes terenkripsi. Kontrol gagal jika rahasia Kubernetes cluster tidak dienkripsi.

Saat Anda mengenkripsi rahasia, Anda dapat menggunakan kunci AWS Key Management Service (AWS KMS) untuk menyediakan enkripsi amplop rahasia Kubernetes yang disimpan di etcd untuk kluster Anda. Enkripsi ini merupakan tambahan dari enkripsi volume EBS yang diaktifkan secara default untuk semua data (termasuk rahasia) yang disimpan dalam etcd sebagai bagian dari cluster EKS. Menggunakan enkripsi rahasia untuk kluster EKS Anda memungkinkan Anda untuk menerapkan strategi pertahanan secara mendalam untuk aplikasi Kubernetes dengan mengenkripsi rahasia Kubernetes dengan kunci KMS yang Anda tentukan dan kelola.

Remediasi

Untuk mengaktifkan enkripsi rahasia pada kluster EKS, lihat [Mengaktifkan enkripsi rahasia pada klaster yang ada](#) di Panduan Pengguna Amazon EKS.

[EKS.6] Kluster EKS harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::EKS::Cluster`

AWS Config aturan: `tagged-eks-cluster` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
<code>requiredTagKeys</code>	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS.	Tidak ada nilai default

Kontrol ini memeriksa apakah klaster Amazon EKS memiliki tag dengan kunci spesifik yang ditentukan dalam parameter `requiredTagKeys`. Kontrol gagal jika cluster tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter `requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika cluster tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat [Untuk apa ABAC? AWS](#) di Panduan Pengguna IAM.

Note

Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat [Menandai AWS sumber daya Anda](#) di Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke kluster EKS, lihat [Menandai resource Amazon EKS Anda](#) di Panduan Pengguna Amazon EKS.

[EKS.7] Konfigurasi penyedia identitas EKS harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::EKS::IdentityProviderConfig`

AWS Config aturan: `tagged-eks-identityproviderconfig` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
<code>requiredTagKeys</code>	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS .	Tidak ada nilai default

Kontrol ini memeriksa apakah konfigurasi penyedia identitas Amazon EKS memiliki tag dengan kunci spesifik yang ditentukan dalam parameter `requiredTagKeys`. Kontrol gagal jika

konfigurasi tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter `requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika konfigurasi tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengkategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat [Untuk apa ABAC? AWS](#) di Panduan Pengguna IAM.

Note

Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat [Menandai AWS sumber daya Anda](#) di Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke konfigurasi penyedia identitas EKS, lihat [Menandai resource Amazon EKS](#) Anda di Panduan Pengguna Amazon EKS.

[EKS.8] Kluster EKS harus mengaktifkan pencatatan audit

Persyaratan terkait: NIST.800-53.r5 AC-2 (12), (4), NIST.800-53.r5 AC-2 (26), (9),, NIST.800-53.r5 AC-4 (9), NIST.800-53.r5 AC-6 Nist.800-53.R5 SI-3 NIST.800-53.r5 SC-7 (8) NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 AU-9(7), NIST.800-53.r5 CA-7, Nist.800-53.r5 SI-4, Nist.800-53.r5 SI-4 (20), Nist.800-53.R5 SI-7 (8), PCI DSS v4.0.1/10.2.1

Kategori: Identifikasi > Logging

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::EKS::Cluster`

AWS Config aturan: [eks-cluster-log-enabled](#)

Jenis jadwal: Perubahan dipicu

Parameter:

- `logTypes: audit`(tidak dapat disesuaikan)

Kontrol ini memeriksa apakah klaster Amazon EKS telah mengaktifkan pencatatan audit. Kontrol gagal jika pencatatan audit tidak diaktifkan untuk klaster.

 Note

Kontrol ini tidak memeriksa apakah pencatatan audit Amazon EKS diaktifkan melalui Amazon Security Lake untuk Akun AWS.

Pencatatan pesawat kontrol EKS menyediakan log audit dan diagnostik langsung dari bidang kontrol EKS ke Amazon CloudWatch Logs di akun Anda. Anda dapat memilih jenis log yang Anda butuhkan, dan log dikirim sebagai aliran log ke grup untuk setiap kluster EKS. CloudWatch Logging memberikan visibilitas ke dalam akses dan kinerja kluster EKS. Dengan mengirimkan log pesawat kontrol EKS untuk kluster EKS Anda ke CloudWatch Log, Anda dapat merekam operasi untuk tujuan audit dan diagnostik di lokasi pusat.

Remediasi

Untuk mengaktifkan log audit untuk kluster EKS Anda, lihat [Mengaktifkan dan menonaktifkan log bidang kontrol di Panduan](#) Pengguna Amazon EKS.

Kontrol Security Hub untuk ElastiCache

AWS Security Hub Kontrol ini mengevaluasi ElastiCache layanan dan sumber daya Amazon.

Kontrol ini mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat [Ketersediaan kontrol berdasarkan Wilayah](#).

[ElastiCache.1] Cluster ElastiCache (Redis OSS) harus mengaktifkan pencadangan otomatis

Persyaratan terkait: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6, NIST.800-53.r5 CP-6(1), NIST.800-53.r5 CP-6(2), NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5 (2), NIST.800-53.R5 SI-12, NIST.800-53.R5 SI-13 (5)

Kategori: Pulih> Ketahanan > Cadangan diaktifkan

Tingkat keparahan: Tinggi

Jenis sumber daya: AWS::ElastiCache::CacheCluster,
AWS::ElastiCache::ReplicationGroup

AWS Config aturan: [elasticache-redis-cluster-automatic-backup-check](#)

Jenis jadwal: Periodik

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
snapshotRetentionPeriod	Periode retensi snapshot minimum dalam beberapa hari	Bilangan Bulat	1 untuk 35	1

Kontrol ini mengevaluasi apakah klaster Amazon ElastiCache (Redis OSS) memiliki cadangan otomatis yang dijadwalkan. Kontrol gagal jika SnapshotRetentionLimit untuk cluster Redis kurang dari periode waktu yang ditentukan. Kecuali Anda memberikan nilai parameter khusus untuk periode retensi snapshot, Security Hub menggunakan nilai default 1 hari.

Cluster Amazon ElastiCache (Redis OSS) dapat mencadangkan data mereka. Anda dapat menggunakan backup untuk memulihkan klaster atau menyemai klaster baru. Backup terdiri dari metadata klaster, beserta semua data di dalam klaster. Semua cadangan ditulis ke Amazon Simple Storage Service (Amazon S3), yang menyediakan penyimpanan durabel. Anda dapat memulihkan data Anda dengan membuat cluster Redis baru dan mengisinya dengan data dari cadangan. Anda

dapat mengelola backup menggunakan AWS Management Console, the AWS Command Line Interface (AWS CLI), dan API. ElastiCache

Remediasi

Untuk menjadwalkan pencadangan otomatis pada klaster ElastiCache (Redis OSS), lihat [Menjadwalkan pencadangan](#) otomatis di Panduan Pengguna Amazon. ElastiCache

[ElastiCache.2] ElastiCache cluster harus mengaktifkan peningkatan versi minor otomatis

Persyaratan terkait: NIST.800-53.R5 SI-2, NIST.800-53.R5 SI-2 (2), NIST.800-53.R5 SI-2 (4), Nist.800-53.R5 SI-2 (5) PCI DSS v4.0.1/6.3.3

Kategori: Identifikasi > Kerentanan, tambalan, dan manajemen versi

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::ElastiCache::CacheCluster`

AWS Config aturan: [elasticache-auto-minor-version-upgrade-check](#)

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini mengevaluasi apakah Amazon ElastiCache secara otomatis menerapkan upgrade versi minor ke cluster cache. Kontrol gagal jika cluster cache tidak memiliki upgrade versi minor yang diterapkan secara otomatis.

Note

Kontrol ini tidak berlaku untuk cluster ElastiCache Memcached.

Upgrade versi minor otomatis adalah fitur yang dapat Anda aktifkan di Amazon ElastiCache untuk secara otomatis meningkatkan cluster cache Anda ketika versi mesin cache minor baru tersedia. Upgrade ini mungkin termasuk patch keamanan dan perbaikan bug. Tetap up-to-date dengan instalasi patch adalah langkah penting dalam mengamankan sistem.

Remediasi

Untuk secara otomatis menerapkan upgrade versi minor ke cluster ElastiCache cache yang ada, lihat [Pengelolaan versi untuk ElastiCache](#) di Panduan ElastiCache Pengguna Amazon.

[ElastiCache.3] grup ElastiCache replikasi harus mengaktifkan failover otomatis

Persyaratan terkait: NIST.800-53.r5 CP-10, NIST.800-53.r5 SC-3 6, NIST.800-53.r5 SC-5 (2), NIST.800-53.R5 SI-13 (5)

Kategori: Pulihkan > Ketahanan > Ketersediaan tinggi

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::ElastiCache::ReplicationGroup

AWS Config aturan: [elasticache-repl-grp-auto-failover-enabled](#)

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah grup ElastiCache replikasi mengaktifkan failover otomatis. Kontrol gagal jika failover otomatis tidak diaktifkan untuk grup replikasi.

Ketika failover otomatis diaktifkan untuk grup replikasi, peran node utama akan secara otomatis gagal ke salah satu replika baca. Promosi failover dan replika ini memastikan bahwa Anda dapat melanjutkan penulisan ke primer baru setelah promosi selesai, yang mengurangi waktu henti secara keseluruhan jika terjadi kegagalan.

Remediasi

Untuk mengaktifkan failover otomatis untuk grup ElastiCache replikasi yang ada, lihat [Memodifikasi ElastiCache klaster di Panduan](#) Pengguna Amazon ElastiCache . Jika Anda menggunakan ElastiCache konsol, setel Auto failover ke diaktifkan.

[ElastiCache.4] grup ElastiCache replikasi harus dienkripsi saat istirahat

Persyaratan terkait: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-1 3, NIST.800-53.r5 SC-2 8, NIST.800-53.r5 SC-2 8 (1), NIST.800-53.r5 SC-7 (10), NIST.800-53.R5 SI-7 (6)

Kategori: Lindungi > Perlindungan Data > Enkripsi data-at-rest

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::ElasticCache::ReplicationGroup

AWS Config aturan: [elasticache-repl-grp-encrypted-at-rest](#)

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah grup ElasticCache replikasi dienkrpsi saat istirahat. Kontrol gagal jika grup replikasi tidak dienkrpsi saat istirahat.

Mengenkripsi data saat istirahat mengurangi risiko bahwa pengguna yang tidak diautentikasi mendapatkan akses ke data yang disimpan pada disk. ElasticCache (Redis OSS) grup replikasi harus dienkrpsi saat istirahat untuk lapisan keamanan tambahan.

Remediasi

Untuk mengonfigurasi enkripsi saat istirahat pada grup ElasticCache replikasi, lihat [Mengaktifkan enkripsi saat istirahat di Panduan Pengguna](#) Amazon. ElasticCache

[ElasticCache.5] grup ElasticCache replikasi harus dienkrpsi saat transit

Persyaratan terkait: NIST.800-53.r5 AC-1 7 (2),, NIST.800-53.r5 IA-5 (1) NIST.800-53.r5 AC-4, NIST.800-53.r5 SC-1 2 (3), 3, 3, NIST.800-53.r5 SC-1 3 (3), NIST.800-53.r5 SC-2 (4),, NIST.800-53.r5 SC-2 (1), NIST.800-53.r5 SC-7 (2) NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 Nist.800-53.r5 SI-7 NIST.800-53.r5 SC-8 (6), PCI DSS v4.0.1/4.2.1

Kategori: Lindungi > Perlindungan Data > Enkripsi data-in-transit

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::ElasticCache::ReplicationGroup

AWS Config aturan: [elasticache-repl-grp-encrypted-in-transit](#)

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah grup ElastiCache replikasi dienkripsi dalam perjalanan. Kontrol gagal jika grup replikasi tidak dienkripsi saat transit.

Mengenkripsi data dalam perjalanan mengurangi risiko bahwa pengguna yang tidak sah dapat menguping lalu lintas jaringan. Mengaktifkan enkripsi dalam transit pada grup ElastiCache replikasi mengenkripsi data Anda setiap kali data berpindah dari satu tempat ke tempat lain, seperti antar node di cluster Anda atau antara cluster Anda dan aplikasi Anda.

Remediasi

Untuk mengonfigurasi enkripsi dalam transit pada grup ElastiCache replikasi, lihat [Mengaktifkan enkripsi dalam transit di Panduan Pengguna](#) Amazon. ElastiCache

[ElastiCache.6] ElastiCache (Redis OSS) grup replikasi dari versi sebelumnya harus mengaktifkan Redis OSS AUTH

Persyaratan terkait: NIST.800-53.r5 AC-2 (1),, NIST.800-53.r5 AC-3 (15) NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-6, PCI DSS v4.0.1/8.3.1

Kategori: Lindungi > Manajemen akses yang aman

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::ElastiCache::ReplicationGroup

AWS Config aturan: [elasticache-repl-grp-redis-auth-enabled](#)

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah grup replikasi ElastiCache (Redis OSS) mengaktifkan Redis OSS AUTH. Kontrol gagal jika versi Redis OSS dari node grup replikasi di bawah 6.0 dan AuthToken tidak digunakan.

Saat Anda menggunakan token otentikasi Redis, atau kata sandi, Redis memerlukan kata sandi sebelum mengizinkan klien menjalankan perintah, yang meningkatkan keamanan data. Untuk Redis 6.0 dan versi yang lebih baru, sebaiknya gunakan Role-Based Access Control (RBAC). Karena RBAC tidak didukung untuk versi Redis lebih awal dari 6.0, kontrol ini hanya mengevaluasi versi yang tidak dapat menggunakan fitur RBAC.

Remediasi

Untuk menggunakan Redis AUTH pada grup replikasi ElastiCache (Redis OSS), lihat [Memodifikasi token AUTH pada klaster ElastiCache \(Redis OSS\) yang ada](#) di Panduan Pengguna Amazon ElastiCache.

[ElastiCache.7] ElastiCache cluster tidak boleh menggunakan grup subnet default

Persyaratan terkait: NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21) NIST.800-53.r5 SC-7,, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (5)

Kategori: Lindungi > Konfigurasi jaringan aman

Tingkat keparahan: Tinggi

Jenis sumber daya: AWS::ElastiCache::CacheCluster

AWS Config aturan: [elasticache-subnet-group-check](#)

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah ElastiCache cluster dikonfigurasi dengan grup subnet kustom. Kontrol gagal jika CacheSubnetGroupName untuk ElastiCache cluster memiliki nilai default.

Saat meluncurkan ElastiCache cluster, grup subnet default dibuat jika belum ada. Grup default menggunakan subnet dari Virtual Private Cloud (VPC) default. Sebaiknya gunakan grup subnet khusus yang lebih membatasi subnet tempat cluster berada, dan jaringan yang diwarisi cluster dari subnet.

Remediasi

Untuk membuat grup subnet baru untuk ElastiCache klaster, lihat [Membuat grup subnet](#) di ElastiCache Panduan Pengguna Amazon.

Kontrol Security Hub untuk Elastic Beanstalk

AWS Security Hub Kontrol ini mengevaluasi AWS Elastic Beanstalk layanan dan sumber daya.

Kontrol ini mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat [Ketersediaan kontrol berdasarkan Wilayah](#).

[ElasticBeanstalk.1] Lingkungan Elastic Beanstalk seharusnya mengaktifkan pelaporan kesehatan yang ditingkatkan

Persyaratan terkait: NIST.800-53.r5 CA-7, NIST.800-53.R5 SI-2

Kategori: Deteksi > Layanan deteksi > Pemantauan aplikasi

Tingkat keparahan: Rendah

Jenis sumber daya: AWS::ElasticBeanstalk::Environment

AWS Config aturan: [beanstalk-enhanced-health-reporting-enabled](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah pelaporan kesehatan yang ditingkatkan diaktifkan untuk AWS Elastic Beanstalk lingkungan Anda.

Pelaporan kesehatan yang ditingkatkan Elastic Beanstalk memungkinkan respons yang lebih cepat terhadap perubahan kesehatan infrastruktur yang mendasarinya. Perubahan ini dapat mengakibatkan kurangnya ketersediaan aplikasi.

Pelaporan kesehatan yang ditingkatkan Elastic Beanstalk menyediakan deskriptor status untuk mengukur tingkat keparahan masalah yang diidentifikasi dan mengidentifikasi kemungkinan penyebab untuk diselidiki. Agen kesehatan Elastic Beanstalk, termasuk dalam Amazon Machine Images (AMI) yang didukung, mengevaluasi log dan metrik contoh lingkungan. EC2

Untuk informasi tambahan, lihat [Pelaporan dan pemantauan kesehatan yang ditingkatkan](#) di Panduan AWS Elastic Beanstalk Pengembang.

Remediasi

Untuk petunjuk tentang cara mengaktifkan pelaporan kesehatan yang disempurnakan, lihat [Mengaktifkan pelaporan kesehatan yang disempurnakan menggunakan konsol Elastic Beanstalk di Panduan Pengembang.AWS Elastic Beanstalk](#)

[ElasticBeanstalk.2] Pembaruan platform yang dikelola Elastic Beanstalk harus diaktifkan

Persyaratan terkait: NIST.800-53.R5 SI-2, NIST.800-53.R5 SI-2 (2), NIST.800-53.R5 SI-2 (4), NIST.800-53.R5 SI-2 (5), PCI DSS v4.0.1/6.3.3

Kategori: Identifikasi > Kerentanan, tambalan, dan manajemen versi

Tingkat keparahan: Tinggi

Jenis sumber daya: AWS::ElasticBeanstalk::Environment

AWS Config aturan: [elastic-beanstalk-managed-updates-enabled](#)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
UpdateLevel	Tingkat pembaruan versi	Enum	minor, patch	Tidak ada nilai default

Kontrol ini memeriksa apakah pembaruan platform terkelola diaktifkan untuk lingkungan Elastic Beanstalk. Kontrol gagal jika tidak ada pembaruan platform terkelola yang diaktifkan. Secara default, kontrol lolos jika semua jenis pembaruan platform diaktifkan. Secara opsional, Anda dapat memberikan nilai parameter khusus untuk memerlukan tingkat pembaruan tertentu.

Mengaktifkan pembaruan platform terkelola memastikan bahwa perbaikan, pembaruan, dan fitur platform terbaru yang tersedia untuk lingkungan diinstal. Tetap up to date dengan instalasi patch adalah langkah penting dalam mengamankan sistem.

Remediasi

Untuk mengaktifkan pembaruan platform terkelola, lihat [Untuk mengonfigurasi pembaruan platform terkelola di bawah Pembaruan platform terkelola](#) di Panduan AWS Elastic Beanstalk Pengembang.

[ElasticBeanstalk.3] Elastic Beanstalk harus mengalirkan log ke CloudWatch

Persyaratan terkait: PCI DSS v4.0.1/10.4.2

Kategori: Identifikasi > Logging

Tingkat keparahan: Tinggi

Jenis sumber daya: AWS::ElasticBeanstalk::Environment

AWS Config aturan: [elastic-beanstalk-logs-to-cloudwatch](#)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
RetentionInDays	Jumlah hari untuk menyimpan peristiwa log sebelum kedaluwarsa	Enum	1, 3, 5, 7, 14, 30, 60, 90, 120, 150, 180, 365, 400, 545, 731, 1827, 3653	Tidak ada nilai default

Kontrol ini memeriksa apakah lingkungan Elastic Beanstalk dikonfigurasi untuk mengirim log ke Log. CloudWatch Kontrol gagal jika lingkungan Elastic Beanstalk tidak dikonfigurasi untuk mengirim log ke Log. CloudWatch Secara opsional, Anda dapat memberikan nilai kustom untuk RetentionInDays parameter jika Anda ingin kontrol lulus hanya jika log dipertahankan untuk jumlah hari tertentu sebelum kedaluwarsa.

CloudWatch membantu Anda mengumpulkan dan memantau berbagai metrik untuk aplikasi dan sumber daya infrastruktur Anda. Anda juga dapat menggunakan CloudWatch untuk mengonfigurasi tindakan alarm berdasarkan metrik tertentu. Kami merekomendasikan untuk mengintegrasikan Elastic Beanstalk dengan untuk meningkatkan visibilitas ke lingkungan Elastic CloudWatch Beanstalk Anda.

Log Elastic Beanstalk mencakup eb-activity.log, log akses dari server proxy nginx atau Apache lingkungan, dan log yang khusus untuk lingkungan.

Remediasi

Untuk mengintegrasikan Elastic CloudWatch Beanstalk dengan Log, [lihat Streaming CloudWatch log instance ke Log di Panduan Pengembang](#).AWS Elastic Beanstalk

Kontrol Security Hub untuk Elastic Load Balancing

AWS Security Hub Kontrol ini mengevaluasi layanan dan sumber daya Elastic Load Balancing. Tindakan Perbaikan mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat [Ketersediaan kontrol berdasarkan Wilayah](#).

[ELB.1] Application Load Balancer harus dikonfigurasi untuk mengalihkan semua permintaan HTTP ke HTTPS

Persyaratan terkait: PCI DSS v3.2.1/2.3, PCI DSS v3.2.1/4.1, NIST.800-53.r5 AC-1 7 (2), (1), 2 (3), 3, 3 NIST.800-53.r5 AC-4, 3 NIST.800-53.r5 IA-5 (3), (4), (1), NIST.800-53.r5 SC-1 NIST.800-53.r5 SC-2 (NIST.800-53.r5 SC-12), NIST.800-53.r5 SC-2 NIST.800-53.R5 SI-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-8 (6) NIST.800-53.r5 SC-8 NIST.800-53.r5 SC-8

Kategori: Deteksi > Layanan deteksi

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::ElasticLoadBalancingV2::LoadBalancer

AWS Config aturan: [alb-http-to-https-redirection-check](#)

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah pengalihan HTTP ke HTTPS dikonfigurasi pada semua pendengar HTTP Application Load Balancers. Kontrol gagal jika salah satu pendengar HTTP dari Application Load Balancers tidak memiliki pengalihan HTTP ke HTTPS yang dikonfigurasi.

Sebelum Anda mulai menggunakan Application Load Balancer, Anda harus menambahkan satu listener atau lebih. Seorang pendengar adalah proses yang menggunakan protokol dan port yang

dikonfigurasi untuk memeriksa permintaan koneksi. Pendengar mendukung protokol HTTP maupun HTTPS. Anda dapat menggunakan listener HTTPS untuk membongkar karya enkripsi dan dekripsi ke penyeimbang beban Anda. Untuk menerapkan enkripsi dalam perjalanan, Anda harus menggunakan tindakan pengalihan dengan Application Load Balancers untuk mengarahkan permintaan HTTP klien ke permintaan HTTPS pada port 443.

Untuk mempelajari selengkapnya, lihat [Pendengar untuk Application Load Balancer Anda di Panduan Pengguna untuk Application Load Balancers](#).

Tindakan Perbaikan

Untuk mengarahkan permintaan HTTP ke HTTPS, Anda harus menambahkan aturan pendengar Application Load Balancer atau mengedit aturan yang ada.

Untuk petunjuk tentang menambahkan aturan baru, lihat [Menambahkan aturan](#) di Panduan Pengguna untuk Penyeimbang Beban Aplikasi. Untuk Protokol: Port, pilih HTTP, lalu masukkan **80**. Untuk Add action, Redirect ke, pilih HTTPS, lalu masukkan **443**.

Untuk petunjuk cara mengedit aturan yang ada, lihat [Mengedit aturan](#) di Panduan Pengguna untuk Penyeimbang Beban Aplikasi. Untuk Protokol: Port, pilih HTTP, lalu masukkan **80**. Untuk Add action, Redirect ke, pilih HTTPS, lalu masukkan **443**.

[ELB.2] Classic Load Balancer dengan pendengar SSL/HTTPS harus menggunakan sertifikat yang disediakan oleh AWS Certificate Manager

Persyaratan terkait: NIST.800-53.r5 AC-1 7 (2),, NIST.800-53.r5 IA-5 (1) NIST.800-53.r5 AC-4, NIST.800-53.r5 SC-1 2 (3), 3, 3, 3 (5), NIST.800-53.r5 SC-1 NIST.800-53.r5 SC-2 (4),, NIST.800-53.r5 SC-2 (1), NIST.800-53.r5 SC-7 (2), NIST.800-53.r5 SC-8 Nist.800-53.r5 SI-7 NIST.800-53.r5 SC-8 (6), Nist.800-171.r2 3.13.8 NIST.800-53.r5 SC-8

Kategori: Lindungi > Perlindungan Data > Enkripsi data-in-transit

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::ElasticLoadBalancing::LoadBalancer

AWS Config aturan: [elb-acm-certificate-required](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah Classic Load Balancer menggunakan sertifikat HTTPS/SSL yang disediakan oleh (ACM). AWS Certificate Manager Kontrol gagal jika Classic Load Balancer yang dikonfigurasi dengan HTTPS/SSL listener tidak menggunakan sertifikat yang disediakan oleh ACM.

Untuk membuat sertifikat, Anda dapat menggunakan ACM atau alat yang mendukung protokol SSL dan TLS, seperti OpenSSL. Security Hub merekomendasikan agar Anda menggunakan ACM untuk membuat atau mengimpor sertifikat penyeimbang beban Anda.

ACM terintegrasi dengan Classic Load Balancer sehingga Anda dapat menyebarkan sertifikat pada penyeimbang beban Anda. Anda juga harus memperbarui sertifikat ini secara otomatis.

Tindakan Perbaikan

Untuk informasi tentang cara mengaitkan sertifikat ACM SSL/TLS dengan Classic Load Balancer, lihat artikel Pusat AWS Pengetahuan [Bagaimana cara mengaitkan sertifikat ACM SSL/TLS dengan Classic, Application, atau Network Load Balancer?](#)

[ELB.3] Pendengar Classic Load Balancer harus dikonfigurasi dengan penghentian HTTPS atau TLS

Persyaratan terkait: NIST.800-53.r5 AC-1 7 (2), (1) NIST.800-53.r5 AC-4, 2 NIST.800-53.r5 IA-5 (3), 3, 3, 3 (3), (4), NIST.800-53.r5 SC-1, NIST.800-53.r5 SC-2 (1), NIST.800-53.r5 SC-2 (NIST.800-53.r5 SC-12), NIST.800-53.r5 SC-7 Nist.800-53.r5 SI-7 NIST.800-53.r5 SC-8 (6) NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 Nist.800-171.r2 3.13.8, Nist.800-171.r2 3.13.15, PCI DSS v4.0.1/4.2.1

Kategori: Lindungi > Perlindungan Data > Enkripsi data-in-transit

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::ElasticLoadBalancing::LoadBalancer

AWS Config aturan: [elb-tls-https-listeners-only](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah pendengar Classic Load Balancer Anda dikonfigurasi dengan protokol HTTPS atau TLS untuk koneksi front-end (client to load balancer). Kontrol ini berlaku jika Classic

Load Balancer memiliki pendengar. Jika Classic Load Balancer Anda tidak memiliki listener yang dikonfigurasi, kontrol tidak melaporkan temuan apa pun.

Kontrol akan diteruskan jika pendengar Classic Load Balancer dikonfigurasi dengan TLS atau HTTPS untuk koneksi front-end.

Kontrol gagal jika pendengar tidak dikonfigurasi dengan TLS atau HTTPS untuk koneksi front-end.

Sebelum Anda mulai menggunakan penyeimbang beban, Anda harus menambahkan satu listener atau lebih. Seorang pendengar adalah proses yang menggunakan protokol dan port yang dikonfigurasi untuk memeriksa permintaan koneksi. Pendengar dapat mendukung protokol HTTP dan HTTPS/TLS. Anda harus selalu menggunakan pendengar HTTPS atau TLS, sehingga penyeimbang beban melakukan pekerjaan enkripsi dan dekripsi dalam perjalanan.

Tindakan Perbaikan

Untuk mengatasi masalah ini, perbarui pendengar Anda untuk menggunakan protokol TLS atau HTTPS.

Untuk mengubah semua pendengar yang tidak patuh menjadi pendengar TLS/HTTPS

1. Buka EC2 konsol Amazon di <https://console.aws.amazon.com/ec2/>.
2. Pada panel navigasi, di bawah Penyeimbangan Beban, pilih Penyeimbang Beban.
3. Pilih Classic Load Balancer Anda.
4. Pada tab Listeners, pilih Edit.
5. Untuk semua pendengar yang Protokol Load Balancer tidak disetel ke HTTPS atau SSL, ubah pengaturan ke HTTPS atau SSL.
6. Untuk semua pendengar yang dimodifikasi, pada tab Sertifikat, pilih Ubah default.
7. Untuk sertifikat ACM dan IAM, pilih sertifikat.
8. Pilih Simpan sebagai default.
9. Setelah Anda memperbarui semua pendengar, pilih Simpan.

[ELB.4] Application Load Balancer harus dikonfigurasi untuk menjatuhkan header http yang tidak valid

Persyaratan terkait: NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-8 (2), PCI DSS v4.0.1/6.2.4

Kategori: Lindungi > Keamanan Jaringan

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::ElasticLoadBalancingV2::LoadBalancer`

AWS Config aturan: [alb-http-drop-invalid-header-enabled](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini mengevaluasi apakah Application Load Balancer dikonfigurasi untuk menjatuhkan header HTTP yang tidak valid. Kontrol gagal jika nilai `routing.http.drop_invalid_header_fields.enabled` disetel ke `false`.

Secara default, Application Load Balancer tidak dikonfigurasi untuk menjatuhkan nilai header HTTP yang tidak valid. Menghapus nilai header ini mencegah serangan desync HTTP.

 Note

Sebaiknya nonaktifkan kontrol ini jika ELB.12 diaktifkan di akun Anda. Untuk informasi selengkapnya, lihat [\[ELB.12\] Application Load Balancer harus dikonfigurasi dengan mode mitigasi desync defensif atau paling ketat](#).

Tindakan Perbaikan

Untuk mengatasi masalah ini, konfigurasi penyeimbang beban Anda untuk menghapus bidang header yang tidak valid.

Untuk mengonfigurasi penyeimbang beban untuk menjatuhkan bidang header yang tidak valid

1. Buka EC2 konsol Amazon di <https://console.aws.amazon.com/ec2/>.
2. Di panel navigasi, pilih Penyeimbang beban.
3. Pilih Application Load Balancer.
4. Dari Tindakan, pilih Edit atribut.
5. Di bawah Jatuhkan Bidang Header Tidak Valid, pilih Aktifkan.
6. Pilih Simpan.

[ELB.5] Pencatatan aplikasi dan Classic Load Balancer harus diaktifkan

Persyaratan terkait: NIST.800-53.r5 AC-4 (26),, NIST.800-53.r5 SC-7 (9) NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, NIST.800-53.R5 SI-7 (8)

Kategori: Identifikasi > Logging

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::ElasticLoadBalancing::LoadBalancer,
AWS::ElasticLoadBalancingV2::LoadBalancer

AWS Config aturan: [elb-logging-enabled](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah Application Load Balancer dan Classic Load Balancer telah mengaktifkan logging. Kontrol gagal jika `access_logs.s3.enabled` adalah `false`.

Elastic Load Balancing memberikan log akses yang mengambil informasi mendetail tentang permintaan yang dikirim ke penyeimbang beban Anda. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server. Anda dapat menggunakan log akses ini untuk menganalisis pola lalu lintas dan memecahkan masalah.

Untuk mempelajari selengkapnya, lihat [Akses log untuk Classic Load Balancer](#) di Panduan Pengguna untuk Penyeimbang Beban Klasik.

Tindakan Perbaikan

Untuk mengaktifkan log akses, lihat [Langkah 3: Mengkonfigurasi log akses](#) di Panduan Pengguna untuk Penyeimbang Beban Aplikasi.

[ELB.6] Aplikasi, Gateway, dan Network Load Balancer harus mengaktifkan perlindungan penghapusan

Persyaratan terkait: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2(2), NIST.800-53.r5 CM-3, NIST.800-53.r5 SC-5 (2)

Kategori: Pulihkan > Ketahanan > Ketersediaan tinggi

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::ElasticLoadBalancingV2::LoadBalancer

AWS Config aturan: [elb-deletion-protection-enabled](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah Application, Gateway, atau Network Load Balancer telah mengaktifkan perlindungan penghapusan. Kontrol gagal jika perlindungan penghapusan dinonaktifkan.

Aktifkan perlindungan penghapusan untuk melindungi Aplikasi, Gateway, atau Network Load Balancer Anda dari penghapusan.

Tindakan Perbaikan

Untuk mencegah penyeimbang beban terhapus secara tidak sengaja, Anda dapat mengaktifkan perlindungan penghapusan. Secara default, perlindungan penghapusan dinonaktifkan untuk penyeimbang beban Anda.

Jika Anda mengaktifkan perlindungan penghapusan untuk penyeimbang beban, Anda harus menonaktifkan perlindungan penghapusan sebelum dapat menghapus penyeimbang beban.

Untuk mengaktifkan perlindungan penghapusan untuk Application Load Balancer, [lihat Perlindungan penghapusan](#) di Panduan Pengguna untuk Penyeimbang Beban Aplikasi. Untuk mengaktifkan perlindungan penghapusan untuk Load Balancer Gateway, [lihat Perlindungan penghapusan](#) di Panduan Pengguna untuk Penyeimbang Beban Gateway. Untuk mengaktifkan perlindungan penghapusan Network Load Balancer, [lihat Perlindungan penghapusan](#) di Panduan Pengguna untuk Network Load Balancer.

[ELB.7] Classic Load Balancers harus mengaktifkan pengurusan koneksi

Persyaratan terkait: NIST.800-53.r5 CA-9 (1), Nist.800-53.R5 CM-2

Kategori: Memulihkan > Ketahanan

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::ElasticLoadBalancing::LoadBalancer`

AWS Config aturan: `elb-connection-draining-enabled` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah Classic Load Balancer mengaktifkan pengurusan koneksi.

Mengaktifkan pengurusan koneksi pada Classic Load Balancer memastikan bahwa penyeimbang beban berhenti mengirim permintaan ke instans yang tidak terdaftar atau tidak sehat. Itu membuat koneksi yang ada tetap terbuka. Ini sangat berguna untuk instance di grup Auto Scaling, untuk memastikan bahwa koneksi tidak terputus secara tiba-tiba.

Tindakan Perbaikan

Untuk mengaktifkan koneksi yang menguras pada Classic Load Balancer, lihat [Konfigurasi koneksi untuk Classic Load Balancer Anda di Panduan Pengguna untuk Classic Load Balancers](#).

[ELB.8] Classic Load Balancer dengan pendengar SSL harus menggunakan kebijakan keamanan yang telah ditentukan sebelumnya yang memiliki urasi yang kuat AWS Config

Persyaratan terkait: NIST.800-53.r5 AC-1 7 (2), (1) NIST.800-53.r5 AC-4, 2 NIST.800-53.r5 IA-5 (3), 3, 3, 3 (3), (4), NIST.800-53.r5 SC-1, NIST.800-53.r5 SC-2 (1), NIST.800-53.r5 SC-2 (NIST.800-53.r5 SC-12), NIST.800-53.r5 SC-7 Nist.800-53.r5 SI-7 NIST.800-53.r5 SC-8 (6) NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 Nist.800-171.r2 3.13.8, Nist.800-171.r2 3.13.15, PCI DSS v4.0.1/4.2.1

Kategori: Lindungi > Perlindungan Data > Enkripsi data-in-transit

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::ElasticLoadBalancing::LoadBalancer`

AWS Config aturan: [elb-predefined-security-policy-ssl-check](#)

Jenis jadwal: Perubahan dipicu

Parameter:

- predefinedPolicyName: ELBSecurityPolicy-TLS-1-2-2017-01 (tidak dapat disesuaikan)

Kontrol ini memeriksa apakah pendengar Classic Load Balancer HTTPS/SSL Anda menggunakan kebijakan yang telah ditentukan sebelumnya. ELBSecurityPolicy-TLS-1-2-2017-01

Kontrol gagal jika Classic Load Balancer HTTPS/SSL pendengar tidak menggunakan.

ELBSecurityPolicy-TLS-1-2-2017-01

Kebijakan keamanan adalah kombinasi dari protokol SSL, sandi, dan opsi Server Order Preference. Kebijakan yang telah ditetapkan mengontrol cipher, protokol, dan perintah preferensi untuk mendukung selama negosiasi SSL antara klien dan penyeimbang beban.

Menggunakan ELBSecurityPolicy-TLS-1-2-2017-01 dapat membantu Anda memenuhi standar kepatuhan dan keamanan yang mengharuskan Anda menonaktifkan versi SSL dan TLS tertentu. Untuk informasi selengkapnya, lihat [Kebijakan keamanan SSL yang telah ditentukan sebelumnya untuk Classic Load Balancer](#) di Panduan Pengguna untuk Classic Load Balancer.

Tindakan Perbaikan

Untuk informasi tentang cara menggunakan kebijakan keamanan yang telah ditentukan sebelumnya ELBSecurityPolicy-TLS-1-2-2017-01 dengan Classic Load Balancer, [lihat Mengonfigurasi setelan keamanan](#) di Panduan Pengguna untuk Penyeimbang Beban Klasik.

[ELB.9] Classic Load Balancer harus mengaktifkan penyeimbangan beban lintas zona

Persyaratan terkait: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6(2), NIST.800-53.r5 SC-3 6, NIST.800-53.r5 SC-5 (2), NIST.800-53.R5 SI-13 (5)

Kategori: Pulihkan > Ketahanan > Ketersediaan tinggi

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::ElasticLoadBalancing::LoadBalancer

AWS Config aturan: [elb-cross-zone-load-balancing-enabled](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah load balancing lintas zona diaktifkan untuk Classic Load Balancers (). CLBs Kontrol gagal jika load balancing lintas zona tidak diaktifkan untuk CLB.

Sebuah simpul penyeimbang beban mendistribusikan lalu lintas hanya di target yang terdaftar di Availability Zone. Ketika load balancing lintas zona dinonaktifkan, setiap node Load Balancer mendistribusikan lalu lintas hanya di target yang telah terdaftar di Availability Zonenya. Jika jumlah target yang terdaftar tidak sama di seluruh Availability Zone, lalu lintas tidak akan didistribusikan secara merata dan contoh di satu zona mungkin berakhir lebih digunakan dibandingkan dengan contoh di zona lain. Dengan penyeimbangan beban lintas zona diaktifkan, setiap simpul penyeimbang beban untuk Classic Load Balancer Anda mendistribusikan permintaan secara merata ke seluruh instans terdaftar di semua Availability Zone yang diaktifkan. Untuk detailnya, lihat [Penyeimbang beban lintas zona di Panduan Pengguna Elastic Load Balancing](#).

Tindakan Perbaikan

Untuk mengaktifkan load balancing lintas zona di Classic Load Balancer, [lihat Aktifkan load balancing lintas zona di Panduan Pengguna untuk Classic Load Balancer](#).

[ELB.10] Classic Load Balancer harus menjangkau beberapa Availability Zone

Persyaratan terkait: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6(2), NIST.800-53.r5 SC-3 6, NIST.800-53.r5 SC-5 (2), NIST.800-53.R5 SI-13 (5)

Kategori: Pulihkan > Ketahanan > Ketersediaan tinggi

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::ElasticLoadBalancing::LoadBalancer

AWS Config aturan: [clb-multiple-az](#)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
minAvailabilityZones	Jumlah minimum Availability Zone	Enum	2, 3, 4, 5, 6	2

Kontrol ini memeriksa apakah Classic Load Balancer telah dikonfigurasi untuk menjangkau setidaknya jumlah Availability Zones () AZs yang ditentukan. Kontrol gagal jika Classic Load Balancer tidak mencakup setidaknya jumlah yang ditentukan. AZs Kecuali Anda memberikan nilai parameter kustom untuk jumlah minimum AZs, Security Hub menggunakan nilai default dua AZs.

Classic Load Balancer dapat disiapkan untuk mendistribusikan permintaan masuk di EC2 instans Amazon dalam satu Availability Zone atau beberapa Availability Zone. Classic Load Balancer yang tidak menjangkau beberapa Availability Zone tidak dapat mengarahkan lalu lintas ke target di Availability Zone lain jika Availability Zone yang dikonfigurasi menjadi tidak tersedia.

Tindakan Perbaikan

Untuk menambahkan Availability Zone ke Classic Load Balancer, lihat [Menambahkan atau menghapus subnet untuk Classic Load Balancer Anda di Panduan Pengguna untuk Classic Load Balancers](#).

[ELB.12] Application Load Balancer harus dikonfigurasi dengan mode mitigasi desync defensif atau paling ketat

Persyaratan terkait: NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 CA-9 (1), Nist.800-53.R5 CM-2, PCI DSS v4.0.1/6.2.4

Kategori: Lindungi > Perlindungan data > Integritas data

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::ElasticLoadBalancingV2::LoadBalancer

AWS Config aturan: [alb-desync-mode-check](#)

Jenis jadwal: Perubahan dipicu

Parameter:

- desyncMode: defensive, strictest (tidak dapat disesuaikan)

Kontrol ini memeriksa apakah Application Load Balancer dikonfigurasi dengan modus mitigasi desync defensif atau paling ketat. Kontrol gagal jika Application Load Balancer tidak dikonfigurasi dengan modus mitigasi desync defensif atau paling ketat.

Masalah HTTP Desync dapat menyebabkan penyelundupan permintaan dan membuat aplikasi rentan terhadap antrian permintaan atau keracunan cache. Pada gilirannya, kerentanan ini dapat menyebabkan isian kredensial atau eksekusi perintah yang tidak sah. Application Load Balancer yang dikonfigurasi dengan mode mitigasi desync defensif atau paling ketat melindungi aplikasi Anda dari masalah keamanan yang mungkin disebabkan oleh HTTP Desync.

Tindakan Perbaikan

Untuk memperbarui mode mitigasi desync dari Application Load Balancer, lihat Mode [mitigasi desync di Panduan Pengguna untuk Application Load Balancers](#).

[ELB.13] Penyeimbang Beban Aplikasi, Jaringan, dan Gateway harus mencakup beberapa Availability Zone

Persyaratan terkait: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6(2), NIST.800-53.r5 SC-3 6, NIST.800-53.r5 SC-5 (2), NIST.800-53.R5 SI-13 (5)

Kategori: Pulihkan > Ketahanan > Ketersediaan tinggi

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::ElasticLoadBalancingV2::LoadBalancer

AWS Config aturan: [elbv2-multiple-az](#)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
minAvailabilityZones	Jumlah minimum Availability Zone	Enum	2, 3, 4, 5, 6	2

Kontrol ini memeriksa apakah Elastic Load Balancer V2 (Application, Network, atau Gateway Load Balancer) telah mendaftarkan instans dari setidaknya jumlah Availability Zones () yang ditentukan.

AZs Kontrol gagal jika Elastic Load Balancer V2 tidak memiliki instance yang terdaftar setidaknya dalam jumlah yang ditentukan. AZs Kecuali Anda memberikan nilai parameter kustom untuk jumlah minimum AZs, Security Hub menggunakan nilai default dua AZs.

Elastic Load Balancing secara otomatis mendistribusikan lalu lintas masuk Anda ke beberapa target, seperti EC2 instans, kontainer, dan alamat IP, dalam satu atau beberapa Availability Zone. Elastic Load Balancing menskalakan load balancer Anda saat lalu lintas masuk Anda berubah seiring waktu. Disarankan untuk mengonfigurasi setidaknya dua zona ketersediaan untuk memastikan ketersediaan layanan, karena Elastic Load Balancer akan dapat mengarahkan lalu lintas ke zona ketersediaan lain jika salah satu tidak tersedia. Memiliki beberapa zona ketersediaan yang dikonfigurasi akan membantu menghilangkan satu titik kegagalan untuk aplikasi.

Tindakan Perbaikan

Untuk menambahkan Availability Zone ke Application Load Balancer, lihat [Availability Zone untuk Application Load Balancer](#) di Panduan Pengguna untuk Application Load Balancer. Untuk menambahkan Availability Zone ke Network Load Balancer, lihat [Network Load Balancers](#) di Panduan Pengguna untuk Network Load Balancer. Untuk menambahkan Availability Zone ke Load Balancer Gateway, lihat [Membuat Load Balancer Gateway di Panduan Pengguna untuk Penyeimbang Beban](#) Gateway.

[ELB.14] Classic Load Balancer harus dikonfigurasi dengan mode mitigasi desync defensif atau paling ketat

Persyaratan terkait: NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 CA-9 (1), Nist.800-53.R5 CM-2, PCI DSS v4.0.1/6.2.4

Kategori: Lindungi > Perlindungan data > Integritas data

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::ElasticLoadBalancing::LoadBalancer

AWS Config aturan: [clb-desync-mode-check](#)

Jenis jadwal: Perubahan dipicu

Parameter:

- desyncMode: defensive, strictest (tidak dapat disesuaikan)

Kontrol ini memeriksa apakah Classic Load Balancer dikonfigurasi dengan mode mitigasi desync defensif atau paling ketat. Kontrol gagal jika Classic Load Balancer tidak dikonfigurasi dengan mode mitigasi desync defensif atau paling ketat.

Masalah HTTP Desync dapat menyebabkan penyelundupan permintaan dan membuat aplikasi rentan terhadap antrian permintaan atau keracunan cache. Pada gilirannya, kerentanan ini dapat menyebabkan pembajakan kredensial atau eksekusi perintah yang tidak sah. Classic Load Balancer yang dikonfigurasi dengan mode mitigasi desync defensif atau paling ketat melindungi aplikasi Anda dari masalah keamanan yang mungkin disebabkan oleh HTTP Desync.

Tindakan Perbaikan

Untuk memperbarui mode mitigasi desync pada Classic Load Balancer, lihat [Memodifikasi mode mitigasi desync](#) di Panduan Pengguna untuk Penyeimbang Beban Klasik.

[ELB.16] Application Load Balancers harus dikaitkan dengan ACL web AWS WAF

Persyaratan terkait: NIST.800-53.r5 AC-4 (21)

Kategori: Lindungi > Layanan pelindung

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::ElasticLoadBalancingV2::LoadBalancer`

AWS Config aturan: [alb-waf-enabled](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah Application Load Balancer terkait dengan AWS WAF Classic atau daftar kontrol akses AWS WAF web (web ACL). Kontrol gagal jika Enabled bidang untuk AWS WAF konfigurasi diatur ke false.

AWS WAF adalah firewall aplikasi web yang membantu melindungi aplikasi web dan APIs dari serangan. Dengan AWS WAF, Anda dapat mengonfigurasi ACL web, yang merupakan seperangkat aturan yang mengizinkan, memblokir, atau menghitung permintaan web berdasarkan aturan dan ketentuan keamanan web yang dapat disesuaikan yang Anda tentukan. Sebaiknya kaitkan Application Load Balancer Anda dengan AWS WAF ACL web untuk membantu melindunginya dari serangan berbahaya.

Tindakan Perbaikan

Untuk mengaitkan Application Load Balancer dengan ACL web, lihat [Mengaitkan atau memisahkan ACL web dengan sumber daya di Panduan Pengembang](#). AWS WAF

[ELB.17] Aplikasi dan Penyeimbang Beban Jaringan dengan pendengar harus menggunakan kebijakan keamanan yang direkomendasikan

Persyaratan terkait: NIST.800-53.r5 AC-1 7 (2), NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5 (1), NIST.800-53.r5 SC-1 2 (3), 3, NIST.800-53.r5 SC-1 3, 3 (NIST.800-53.r5 SC-23), NIST.800-53.r5 SC-2 (4),, NIST.800-53.r5 SC-7 (1), NIST.800-53.r5 SC-8 (2) NIST.800-53.r5 SC-8, Nist.800-53.R5 SI-7 NIST.800-53.r5 SC-8 (6)

Kategori: Lindungi > Perlindungan Data > Enkripsi data-in-transit

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::ElasticLoadBalancingV2::Listener

AWS Config aturan: [elbv2-predefined-security-policy-ssl-check](#)

Jenis jadwal: Perubahan dipicu

Parameter:sslPolicies: ELBSecurityPolicy-TLS13-1-2-2021-06, ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04, ELBSecurityPolicy-TLS13-1-3-2021-06, ELBSecurityPolicy-TLS13-1-3-FIPS-2023-04, ELBSecurityPolicy-TLS13-1-2-Res-2021-06, ELBSecurityPolicy-TLS13-1-2-Res-FIPS-2023-04 (tidak dapat disesuaikan)

Kontrol ini memeriksa apakah pendengar HTTPS untuk Application Load Balancer atau pendengar TLS untuk Network Load Balancer dikonfigurasi untuk mengenkripsi data dalam perjalanan menggunakan kebijakan keamanan yang disarankan. Kontrol gagal jika pendengar HTTPS atau TLS untuk penyeimbang beban tidak dikonfigurasi untuk menggunakan kebijakan keamanan yang disarankan.

Elastic Load Balancing menggunakan konfigurasi negosiasi SSL, dikenal sebagai kebijakan keamanan, untuk menegosiasikan koneksi antara klien dan penyeimbang beban. Kebijakan keamanan menentukan kombinasi dari protokol dan sandi. Protokol membuat koneksi aman antara klien dan server. Sandi adalah algoritme enkripsi yang menggunakan kunci enkripsi untuk membuat pesan kode. Selama proses negosiasi koneksi, klien dan penyeimbang beban menyajikan daftar

sandi dan protokol yang masing-masing mendukung, dalam urutan preferensi. Menggunakan kebijakan keamanan yang direkomendasikan untuk menyeimbangkan beban dapat membantu Anda memenuhi standar kepatuhan dan keamanan.

Tindakan Perbaikan

[Untuk informasi tentang kebijakan keamanan yang direkomendasikan dan cara memperbarui pendengar, lihat bagian berikut dari Panduan Pengguna Elastic Load Balancing: Kebijakan keamanan untuk Application Load Balancer, Kebijakan keamanan untuk Network Load Balancer, Memperbarui listener HTTPS untuk Application Load Balancer, dan Memperbarui pendengar untuk Network Load Balancer Anda.](#)

Security Hub untuk Elasticsearch

AWS Security Hub Kontrol ini mengevaluasi layanan dan sumber daya Elasticsearch.

Kontrol ini mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat [Ketersediaan kontrol berdasarkan Wilayah](#).

[ES.1] Domain Elasticsearch harus mengaktifkan enkripsi saat istirahat

Persyaratan terkait: PCI DSS v3.2.1/3.4, NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-1 3, 8, NIST.800-53.r5 SC-2 8 (1), (10), NIST.800-53.r5 SC-2 NIST.800-53.R5 SI-7 NIST.800-53.r5 SC-7 (6)

Kategori: Lindungi > Perlindungan Data > Enkripsi data-at-rest

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::Elasticsearch::Domain

AWS Config aturan: [elasticsearch-encrypted-at-rest](#)

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah domain Elasticsearch memiliki enkripsi saat konfigurasi istirahat diaktifkan. Pemeriksaan gagal jika enkripsi saat istirahat tidak diaktifkan.

Untuk lapisan keamanan tambahan untuk data sensitif Anda di OpenSearch, Anda harus mengonfigurasi Anda OpenSearch untuk dienkripsi saat istirahat. Domain Elasticsearch menawarkan

enkripsi data saat istirahat. Fitur ini digunakan AWS KMS untuk menyimpan dan mengelola kunci enkripsi Anda. Untuk melakukan enkripsi, ia menggunakan algoritma Advanced Encryption Standard dengan kunci 256-bit (AES-256).

Untuk mempelajari lebih lanjut tentang OpenSearch enkripsi saat istirahat, lihat [Enkripsi data saat istirahat untuk OpenSearch Layanan Amazon](#) di Panduan Pengembang OpenSearch Layanan Amazon.

Jenis instans tertentu, seperti `t.small` dan `t.medium`, tidak mendukung enkripsi data saat istirahat. Untuk detailnya, lihat [Jenis instans yang didukung](#) di Panduan Pengembang OpenSearch Layanan Amazon.

Remediasi

Untuk mengaktifkan enkripsi saat istirahat untuk domain Elasticsearch baru dan yang sudah ada, lihat [Mengaktifkan enkripsi data saat istirahat di Panduan Pengembang](#) Layanan Amazon OpenSearch .

[ES.2] Domain Elasticsearch tidak boleh diakses publik

Persyaratan terkait: PCI DSS v3.2.1/1.2.1, PCI DSS v3.2.1/1.3.1, PCI DSS v3.2.1/1.3.2, PCI DSS v3.2.1/1.3.4, PCI DSS v3.2.1/1.3.6, NIST.800-53.r5 AC-2 1,, NIST.800-53.r5 AC-3 (7),, (21),,, (11), (16), (20), (21), (3), (4), (9) NIST.800-53.r5 AC-3 NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 PCI DSS v4.0.1/1.4.4 NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7

Kategori: Lindungi > Konfigurasi jaringan aman> Sumber daya dalam VPC

Tingkat keparahan: Kritis

Jenis sumber daya: AWS::Elasticsearch::Domain

AWS Config aturan: [elasticsearch-in-vpc-only](#)

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah domain Elasticsearch ada di VPC. Itu tidak mengevaluasi konfigurasi perutean subnet VPC untuk menentukan akses publik. Anda harus memastikan bahwa domain Elasticsearch tidak dilampirkan ke subnet publik. Lihat [Kebijakan berbasis sumber daya di Panduan](#)

[Pengembang](#) Layanan Amazon OpenSearch . Anda juga harus memastikan bahwa VPC Anda dikonfigurasi sesuai dengan praktik terbaik yang disarankan. Lihat [Praktik terbaik keamanan untuk VPC Anda](#) di Panduan Pengguna Amazon VPC.

Domain Elasticsearch yang digunakan dalam VPC dapat berkomunikasi dengan sumber daya VPC melalui jaringan AWS pribadi, tanpa perlu melintasi internet publik. Konfigurasi ini meningkatkan postur keamanan dengan membatasi akses ke data dalam perjalanan. VPCs menyediakan sejumlah kontrol jaringan untuk mengamankan akses ke domain Elasticsearch, termasuk ACL jaringan dan grup keamanan. Security Hub menyarankan agar Anda memigrasikan domain Elasticsearch publik VPCs untuk memanfaatkan kontrol ini.

Remediasi

Jika Anda membuat domain dengan titik akhir publik, Anda tidak dapat menempatkannya di dalam VPC nanti. Sebagai gantinya, Anda harus membuat domain baru dan memigrasi data Anda. Begitu juga sebaliknya. Jika Anda membuat domain dalam VPC, domain tersebut tidak dapat memiliki titik akhir publik. Sebagai gantinya, Anda harus [membuat domain lain](#) atau menonaktifkan kontrol ini.

Lihat [Meluncurkan domain OpenSearch Layanan Amazon Anda dalam VPC](#) di Panduan Pengembang Layanan OpenSearch Amazon.

[ES.3] Domain Elasticsearch harus mengenkripsi data yang dikirim antar node

Persyaratan terkait: NIST.800-53.r5 AC-4, NIST.800-53.r5 SC-1 3, NIST.800-53.r5 SC-2 3, 3 (NIST.800-53.r5 SC-23), (4),, NIST.800-53.r5 SC-7 (1) NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 NIST.800-53.r5 SC-8 (2), PCI DSS v4.0.1/4.2.1

Kategori: Lindungi > Perlindungan Data > Enkripsi data-in-transit

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::Elasticsearch::Domain

AWS Config aturan: [elasticsearch-node-to-node-encryption-check](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah domain Elasticsearch telah mengaktifkan node-to-node enkripsi. Kontrol gagal jika domain Elasticsearch tidak mengaktifkan node-to-node enkripsi. Kontrol juga

menghasilkan temuan yang gagal jika versi Elasticsearch tidak mendukung pemeriksaan node-to-node enkripsi.

HTTPS (TLS) dapat digunakan untuk membantu mencegah penyerang potensial menguping atau memanipulasi lalu lintas jaringan menggunakan atau serangan serupa. person-in-the-middle Hanya koneksi terenkripsi melalui HTTPS (TLS) yang diizinkan. Mengaktifkan node-to-node enkripsi untuk domain Elasticsearch memastikan bahwa komunikasi intra-cluster dienkripsi dalam perjalanan.

Mungkin ada penalti kinerja yang terkait dengan konfigurasi ini. Anda harus mengetahui dan menguji trade-off kinerja sebelum mengaktifkan opsi ini.

Remediasi

Untuk informasi tentang mengaktifkan node-to-node enkripsi pada domain baru dan yang sudah ada, lihat [Mengaktifkan node-to-node enkripsi di Panduan](#) Pengembang OpenSearch Layanan Amazon.

[ES.4] Kesalahan domain Elasticsearch yang masuk ke CloudWatch Log harus diaktifkan

Persyaratan terkait: NIST.800-53.r5 AC-2 (4), (26), NIST.800-53.r5 AC-4 (9),, NIST.800-53.r5 AC-6 (9), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7 NIST.800-53.R5 SI-3 NIST.800-53.r5 SC-7 (8), NIST.800-53.R5 SI-4 (20), NIST.800-53.R5 SI-7 (8)

Kategori: Identifikasi - Logging

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::Elasticsearch::Domain

AWS Config aturan: [elasticsearch-logs-to-cloudwatch](#)

Jenis jadwal: Perubahan dipicu

Parameter:

- logtype = 'error' (tidak dapat disesuaikan)

Kontrol ini memeriksa apakah domain Elasticsearch dikonfigurasi untuk mengirim log kesalahan ke Log. CloudWatch

Anda harus mengaktifkan log kesalahan untuk domain Elasticsearch dan mengirim log tersebut ke CloudWatch Log untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.

Remediasi

Untuk informasi tentang cara mengaktifkan penerbitan log, lihat [Mengaktifkan penerbitan log \(konsol\)](#) di Panduan Pengembang OpenSearch Layanan Amazon.

[ES.5] Domain Elasticsearch harus mengaktifkan pencatatan audit

Persyaratan terkait: NIST.800-53.r5 AC-2 (4), (26), NIST.800-53.r5 AC-4 (9), NIST.800-53.r5 AC-6 (9), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, NIST.800-53.R5 SI-3, NIST.800-53.r5 SC-7 (8), NIST.800-53.R5 SI-4 (20), NIST.800-53.R5 SI-7 (8), PCI DSS v4.0.1/10.4.2

Kategori: Identifikasi > Logging

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::Elasticsearch::Domain

AWS Config aturan: elasticsearch-audit-logging-enabled (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

- `cloudWatchLogsLogGroupArnList` (tidak dapat disesuaikan). Security Hub tidak mengisi parameter ini. Daftar grup CloudWatch log Log yang dipisahkan koma yang harus dikonfigurasi untuk log audit.

Aturan ini adalah NON_COMPLIANT jika grup CloudWatch log Log dari domain Elasticsearch tidak ditentukan dalam daftar parameter ini.

Kontrol ini memeriksa apakah domain Elasticsearch mengaktifkan pencatatan audit. Kontrol ini gagal jika domain Elasticsearch tidak mengaktifkan pencatatan audit.

Log audit sangat dapat disesuaikan. Mereka memungkinkan Anda melacak aktivitas pengguna di cluster Elasticsearch Anda, termasuk keberhasilan dan kegagalan otentikasi, permintaan, perubahan indeks OpenSearch, dan kueri penelusuran yang masuk.

Remediasi

Untuk petunjuk mendetail tentang mengaktifkan log audit, lihat [Mengaktifkan log audit di Panduan Pengembang OpenSearch Layanan Amazon](#).

[ES.6] Domain Elasticsearch harus memiliki setidaknya tiga node data

Persyaratan terkait: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6(2), NIST.800-53.r5 SC-3 6, NIST.800-53.r5 SC-5 (2), NIST.800-53.R5 SI-13 (5)

Kategori: Pulihkan > Ketahanan > Ketersediaan tinggi

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::Elasticsearch::Domain

AWS Config aturan: `elasticsearch-data-node-fault-tolerance` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah domain Elasticsearch dikonfigurasi dengan setidaknya tiga node data dan `is. zoneAwarenessEnabled true`

Domain Elasticsearch membutuhkan setidaknya tiga node data untuk ketersediaan tinggi dan toleransi kesalahan. Menerapkan domain Elasticsearch dengan setidaknya tiga node data memastikan operasi cluster jika node gagal.

Remediasi

Untuk memodifikasi jumlah node data dalam domain Elasticsearch

1. Buka konsol OpenSearch Layanan Amazon di <https://console.aws.amazon.com/aos/>.
2. Di bawah Domain, pilih nama domain yang ingin Anda edit.
3. Pilih Edit domain.
4. Di bawah Node data, atur Jumlah node ke angka yang lebih besar dari atau sama dengan 3.

Untuk tiga penerapan Availability Zone, atur ke kelipatan tiga untuk memastikan distribusi yang sama di seluruh Availability Zone.

5. Pilih Kirim.

[ES.7] Domain Elasticsearch harus dikonfigurasi dengan setidaknya tiga node master khusus

Persyaratan terkait: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6(2), NIST.800-53.r5 SC-3 6, NIST.800-53.r5 SC-5 (2), NIST.800-53.R5 SI-13 (5)

Kategori: Pulihkan > Ketahanan > Ketersediaan tinggi

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::Elasticsearch::Domain

AWS Config aturan: `elasticsearch-primary-node-fault-tolerance` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah domain Elasticsearch dikonfigurasi dengan setidaknya tiga node primer khusus. Kontrol ini gagal jika domain tidak menggunakan node primer khusus. Kontrol ini lolos jika domain Elasticsearch memiliki lima node primer khusus. Namun, menggunakan lebih dari tiga node primer mungkin tidak diperlukan untuk mengurangi risiko ketersediaan, dan akan menghasilkan biaya tambahan.

Domain Elasticsearch membutuhkan setidaknya tiga node primer khusus untuk ketersediaan tinggi dan toleransi kesalahan. Sumber daya node primer khusus dapat tegang selama blue/green penyebaran node data karena ada node tambahan untuk dikelola. Menerapkan domain Elasticsearch dengan setidaknya tiga node primer khusus memastikan kapasitas sumber daya node primer dan operasi cluster yang memadai jika sebuah node gagal.

Remediasi

Untuk memodifikasi jumlah node utama khusus dalam OpenSearch domain

1. Buka konsol OpenSearch Layanan Amazon di <https://console.aws.amazon.com/aos/>.
2. Di bawah Domain, pilih nama domain yang ingin Anda edit.
3. Pilih Edit domain.
4. Di bawah Node master khusus, setel tipe Instance ke tipe instans yang diinginkan.

5. Mengatur Jumlah node master sama dengan tiga atau lebih besar.
6. Pilih Kirim.

[ES.8] Koneksi ke domain Elasticsearch harus dienkripsi menggunakan kebijakan keamanan TLS terbaru

Persyaratan terkait: NIST.800-53.r5 AC-1 7 (2),, NIST.800-53.r5 IA-5 (1) NIST.800-53.r5 AC-4, NIST.800-53.r5 SC-1 2 (3), 3, 3, NIST.800-53.r5 SC-1 3 (3), NIST.800-53.r5 SC-2 (4),, NIST.800-53.r5 SC-2 (1), NIST.800-53.r5 SC-7 (2) NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 Nist.800-53.r5 SI-7 NIST.800-53.r5 SC-8 (6), PCI DSS v4.0.1/4.2.1

Kategori: Lindungi > Perlindungan Data > Enkripsi data-in-transit

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::Elasticsearch::Domain

AWS Config aturan: `elasticsearch-https-required` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah titik akhir domain Elasticsearch dikonfigurasi untuk menggunakan kebijakan keamanan TLS terbaru. Kontrol gagal jika titik akhir domain Elasticsearch tidak dikonfigurasi untuk menggunakan kebijakan terbaru yang didukung atau jika HTTPS tidak diaktifkan. Kebijakan keamanan TLS terbaru yang didukung saat ini adalah `Policy-Min-TLS-1-2-PFS-2023-10`.

HTTPS (TLS) dapat digunakan untuk membantu mencegah penyerang potensial menggunakan person-in-the-middle atau serangan serupa untuk menguping atau memanipulasi lalu lintas jaringan. Hanya koneksi terenkripsi melalui HTTPS (TLS) yang diizinkan. Mengenkripsi data dalam perjalanan dapat memengaruhi kinerja. Anda harus menguji aplikasi Anda dengan fitur ini untuk memahami profil kinerja dan dampak TLS. TLS 1.2 menyediakan beberapa peningkatan keamanan dibandingkan versi TLS sebelumnya.

Remediasi

Untuk mengaktifkan enkripsi TLS, gunakan operasi [UpdateDomainConfig](#) API untuk mengkonfigurasi [DomainEndpointOptions](#) objek. Ini menetapkan `TLSecurityPolicy`.

[ES.9] Domain Elasticsearch harus diberi tag

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: AWS::Elasticsearch::Domain

AWS Config aturan: tagged-elasticsearch-domain (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
<code>requiredTagKeys</code>	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS.	No default value

Kontrol ini memeriksa apakah domain Elasticsearch memiliki tag dengan kunci spesifik yang ditentukan dalam parameter. `requiredTagKeys` Kontrol gagal jika domain tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter `requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika domain tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke

AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat [Untuk apa ABAC? AWS](#) di Panduan Pengguna IAM.

Note

Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat [Menandai AWS sumber daya Anda](#) di Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke domain Elasticsearch, lihat [Bekerja dengan tag di Panduan Pengembang OpenSearch Layanan Amazon](#).

Kontrol Security Hub untuk Amazon EMR

AWS Security Hub Kontrol ini mengevaluasi layanan dan sumber daya Amazon EMR (sebelumnya disebut Amazon Elastic MapReduce). Kontrol mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat [Ketersediaan kontrol berdasarkan Wilayah](#).

[EMR.1] Node primer klaster EMR Amazon seharusnya tidak memiliki alamat IP publik

Persyaratan terkait: PCI DSS v3.2.1/1.2.1, PCI DSS v3.2.1/1.3.1, PCI DSS v3.2.1/1.3.2, PCI DSS v3.2.1/1.3.4, PCI DSS v3.2.1/1.3.6, PCI DSS v4.0.1/1.4.4, 1,, (7),, (21),,, (11), (16), (16), 20), (21), (3), (4), (9) NIST.800-53.r5 AC-2 NIST.800-53.r5 AC-3 NIST.800-53.r5 AC-3 NIST.800-53.r5 AC-4 NIST.800-53.r5 AC-4 NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7

Kategori: Lindungi > Konfigurasi jaringan aman

Tingkat keparahan: Tinggi

Jenis sumber daya: AWS::EMR::Cluster

AWS Config aturan: emr-master-no-public [-ip](#)

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah node master di kluster EMR Amazon memiliki alamat IP publik. Kontrol gagal jika alamat IP publik dikaitkan dengan salah satu instance node master.

Alamat IP publik ditunjuk di `PublicIp` bidang `NetworkInterfaces` konfigurasi untuk instance. Kontrol ini hanya memeriksa kluster EMR Amazon yang berada dalam status `atauRUNNING`. `WAITING`

Remediasi

Selama peluncuran, Anda dapat mengontrol apakah instance Anda di subnet default atau nondefault diberi alamat publik IPv4 . Secara default, subnet default memiliki atribut ini disetel ke `true`. Subnet nondefault memiliki atribut pengalamatan IPv4 publik yang disetel ke `false`, kecuali jika dibuat oleh wizard instance EC2 peluncuran Amazon. Dalam hal ini, atribut diatur ke `true`.

Setelah diluncurkan, Anda tidak dapat secara manual memisahkan IPv4 alamat publik dari instans Anda.

Untuk memulihkan temuan yang gagal, Anda harus meluncurkan cluster baru di VPC dengan subnet pribadi yang memiliki atribut pengalamatan publik yang IPv4 disetel ke `false` Untuk petunjuknya, lihat [Meluncurkan cluster ke dalam VPC](#) di Panduan Manajemen EMR Amazon.

[EMR.2] Pengaturan akses publik blok EMR Amazon harus diaktifkan

Persyaratan terkait: PCI DSS v4.0.1/1.4.4, NIST.800-53.r5 AC-2 1, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7),, NIST.800-53.r5 AC-4 (21) NIST.800-53.r5 AC-4,,, (11) NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), (4), NIST.800-53.r5 SC-7 (9) NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7

Kategori: Lindungi > Manajemen akses aman > Sumber daya tidak dapat diakses publik

Tingkat keparahan: Kritis

Jenis sumber daya: AWS : : : Account

AWS Config aturan: [emr-block-public-access](#)

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah akun Anda dikonfigurasi dengan Amazon EMR memblokir akses publik. Kontrol gagal jika pengaturan blokir akses publik tidak diaktifkan atau jika port apa pun selain port 22 diizinkan.

Amazon EMR memblokir akses publik mencegah Anda meluncurkan cluster di subnet publik jika cluster memiliki konfigurasi keamanan yang memungkinkan lalu lintas masuk dari alamat IP publik pada port. Saat pengguna dari Anda Akun AWS meluncurkan klaster, Amazon EMR memeriksa aturan port di grup keamanan untuk klaster dan membandingkannya dengan aturan lalu lintas masuk Anda. Jika grup keamanan memiliki aturan masuk yang membuka port ke alamat IP publik IPv4 0.0.0.0/0 atau IPv6 :::/0, dan port tersebut tidak ditentukan sebagai pengecualian untuk akun Anda, Amazon EMR tidak mengizinkan pengguna membuat cluster.

 Note

Blokir akses publik diaktifkan secara default. Untuk meningkatkan perlindungan akun, kami sarankan Anda tetap mengaktifkannya.

Remediasi

Untuk mengonfigurasi blokir akses publik untuk Amazon EMR, lihat Menggunakan [Amazon EMR memblokir akses publik di Panduan Manajemen](#) EMR Amazon.

[EMR.3] Konfigurasi keamanan Amazon EMR harus dienkripsi saat istirahat

Persyaratan terkait: NIST.800-53.r5 CA-9 (1), NIST.800-53.R5 CP-9 (8), NIST.800-53.R5 SI-12

Kategori: Lindungi > Perlindungan Data > Enkripsi data-at-rest

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::EMR::SecurityConfiguration

AWS Config aturan: [emr-security-configuration-encryption-rest](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah konfigurasi keamanan EMR Amazon mengaktifkan enkripsi saat istirahat. Kontrol gagal jika konfigurasi keamanan tidak mengaktifkan enkripsi saat istirahat.

Data saat istirahat mengacu pada data yang disimpan dalam penyimpanan persisten dan tidak mudah menguap untuk durasi berapa pun. Mengenkripsi data saat istirahat membantu Anda melindungi kerahasiaannya, yang mengurangi risiko bahwa pengguna yang tidak sah dapat mengaksesnya.

Remediasi

Untuk mengaktifkan enkripsi saat istirahat dalam konfigurasi keamanan Amazon EMR, lihat [Mengonfigurasi enkripsi data](#) di Panduan Manajemen EMR Amazon.

[EMR.4] Konfigurasi keamanan Amazon EMR harus dienkrpsi saat transit

Persyaratan terkait: NIST.800-53.r5 AC-4, NIST.800-53.r5 SC-7 (4) NIST.800-53.r5 SC-8,, NIST.800-53.r5 SC-8 (1), NIST.800-53.r5 SC-8 (2), NIST.800-53.r5 SC-1 3, NIST.800-53.r5 SC-2 3, NIST.800-53.r5 SC-2 3 (3)

Kategori: Lindungi > Perlindungan Data > Enkripsi data-in-transit

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::EMR::SecurityConfiguration

AWS Config aturan: [emr-security-configuration-encryption-transit](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah konfigurasi keamanan EMR Amazon mengaktifkan enkripsi saat transit. Kontrol gagal jika konfigurasi keamanan tidak mengaktifkan enkripsi dalam perjalanan.

Data dalam transit mengacu pada data yang berpindah dari satu lokasi ke lokasi lain, seperti antar node di cluster Anda atau antara cluster Anda dan aplikasi Anda. Data dapat bergerak di internet atau dalam jaringan pribadi. Mengenkripsi data dalam perjalanan mengurangi risiko bahwa pengguna yang tidak sah dapat menguping lalu lintas jaringan.

Remediasi

Untuk mengaktifkan enkripsi saat transit dalam konfigurasi keamanan Amazon EMR, lihat [Mengonfigurasi enkripsi data](#) di Panduan Manajemen EMR Amazon.

Kontrol Security Hub untuk EventBridge

AWS Security Hub Kontrol ini mengevaluasi EventBridge layanan dan sumber daya Amazon.

Kontrol ini mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat [Ketersediaan kontrol berdasarkan Wilayah](#).

[EventBridge.2] bus EventBridge acara harus diberi tag

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: AWS::Events::EventBus

AWS Config aturan: tagged-events-eventbus (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
<code>requiredTagKeys</code>	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS .	Tidak ada nilai default

Kontrol ini memeriksa apakah bus EventBridge acara Amazon memiliki tag dengan kunci tertentu yang ditentukan dalam parameter `requiredTagKeys`. Kontrol gagal jika bus acara tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter `requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci

tag dan gagal jika bus acara tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws :`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat [Untuk apa ABAC? AWS](#) di Panduan Pengguna IAM.

Note

Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat [Menandai AWS sumber daya Anda](#) di Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke bus EventBridge acara, lihat [EventBridge Tag Amazon](#) di Panduan EventBridge Pengguna Amazon.

[EventBridge.3] bus acara EventBridge khusus harus memiliki kebijakan berbasis sumber daya terlampir

Persyaratan terkait: NIST.800-53.r5 AC-2, NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (15), (7),,, NIST.800-53.r5 AC-3 NIST.800-53.r5 AC-6 (3) NIST.800-53.r5 AC-5 NIST.800-53.r5 AC-6, PCI DSS v4.0.1/10.3.1

Kategori: Lindungi > Manajemen akses aman > Sumber daya tidak dapat diakses publik

Tingkat keparahan: Rendah

Jenis sumber daya: AWS :: Events :: EventBus

AWS Config aturan: [custom-eventbus-policy-attached](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah bus acara EventBridge khusus Amazon memiliki kebijakan berbasis sumber daya yang dilampirkan. Kontrol ini gagal jika bus acara khusus tidak memiliki kebijakan berbasis sumber daya.

Secara default, bus acara EventBridge khusus tidak memiliki kebijakan berbasis sumber daya yang dilampirkan. Hal ini memungkinkan kepala sekolah di akun untuk mengakses bus acara. Dengan melampirkan kebijakan berbasis sumber daya ke bus acara, Anda dapat membatasi akses ke bus acara ke akun tertentu, serta dengan sengaja memberikan akses ke entitas di akun lain.

Remediasi

Untuk melampirkan kebijakan berbasis sumber daya ke bus peristiwa EventBridge khusus, lihat [Menggunakan kebijakan berbasis sumber daya untuk Amazon di Panduan Pengguna Amazon](#).
EventBridge EventBridge

[EventBridge.4] titik akhir EventBridge global harus mengaktifkan replikasi acara

Persyaratan terkait: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6(2), NIST.800-53.r5 SC-3 6, NIST.800-53.r5 SC-5 (2), NIST.800-53.R5 SI-13 (5)

Kategori: Pulihkan > Ketahanan > Ketersediaan tinggi

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::Events::Endpoint

AWS Config aturan: [global-endpoint-event-replication-enabled](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah replikasi peristiwa diaktifkan untuk titik akhir EventBridge global Amazon. Kontrol gagal jika replikasi peristiwa tidak diaktifkan untuk titik akhir global.

Titik akhir global membantu membuat aplikasi Anda toleran terhadap kesalahan regional. Untuk memulai, Anda menetapkan pemeriksaan kesehatan Amazon Route 53 ke titik akhir. Ketika failover

dimulai, pemeriksaan kesehatan melaporkan keadaan “tidak sehat”. Dalam beberapa menit setelah inisiasi failover, semua acara khusus diarahkan ke bus acara di Wilayah sekunder dan diproses oleh bus acara tersebut. Saat Anda menggunakan titik akhir global, Anda dapat mengaktifkan replikasi peristiwa. Replikasi acara mengirimkan semua peristiwa khusus ke bus acara di Wilayah primer dan sekunder menggunakan aturan terkelola. Sebaiknya aktifkan replikasi peristiwa saat menyiapkan titik akhir global. Replikasi acara membantu Anda memverifikasi bahwa titik akhir global Anda dikonfigurasi dengan benar. Replikasi peristiwa diperlukan untuk memulihkan secara otomatis dari peristiwa failover. Jika replikasi acara tidak diaktifkan, Anda harus mengatur ulang pemeriksaan kesehatan Route 53 secara manual ke “sehat” sebelum acara dialihkan kembali ke Wilayah utama.

Note

Jika Anda menggunakan bus acara khusus, Anda memerlukan bus genap khusus di setiap Wilayah dengan nama yang sama dan di akun yang sama agar failover berfungsi dengan baik. Mengaktifkan replikasi acara dapat meningkatkan biaya bulanan Anda. Untuk informasi tentang harga, lihat [EventBridge harga Amazon](#).

Remediasi

Untuk mengaktifkan replikasi peristiwa untuk titik akhir EventBridge global, lihat [Membuat titik akhir global di Panduan](#) Pengguna Amazon EventBridge . Untuk replikasi Acara, pilih Replikasi acara diaktifkan.

Kontrol Security Hub untuk Amazon Fraud Detector

Kontrol Security Hub ini mengevaluasi layanan dan sumber daya Amazon Fraud Detector.

Kontrol ini mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat [Ketersediaan kontrol berdasarkan Wilayah](#).

[FraudDetector.1] Jenis entitas Amazon Fraud Detector harus diberi tag

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::FraudDetector::EntityType`

AWS Config aturan: `frauddetector-entity-type-tagged`

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
<code>requiredKeyTags</code>	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS .	Tidak ada nilai default

Kontrol ini memeriksa apakah jenis entitas Amazon Fraud Detector memiliki tag dengan kunci spesifik yang ditentukan dalam parameter `requiredKeyTags`. Kontrol gagal jika tipe entitas tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter `requiredKeyTags`. Jika parameter `requiredKeyTags` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika tipe entitas tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat [Menentukan izin berdasarkan atribut dengan otorisasi ABAC di Panduan Pengguna IAM](#).

Note

Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS

Billing. Untuk mengetahui praktik terbaik penandaan lainnya, lihat [Praktik dan strategi terbaik](#) di Panduan Pengguna AWS Sumber Daya Penandaan dan Editor Tag.

Remediasi

Untuk menambahkan tag ke jenis entitas Amazon Fraud Detector (konsol)

1. Buka konsol Amazon Fraud Detector di <https://console.aws.amazon.com/frauddetector>.
2. Di panel navigasi, pilih Entitas.
3. Pilih jenis entitas dari daftar.
4. Di bagian tag tipe entitas, pilih Kelola tag.
5. Pilih Tambahkan tag baru. Masukkan kunci dan nilai untuk tanda tersebut. Ulangi untuk pasangan nilai kunci tambahan.
6. Setelah Anda selesai menambahkan tanda, pilih Simpan.

[FraudDetector.2] Label Amazon Fraud Detector harus diberi tag

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::FraudDetector::Label`

AWS Config aturan: `frauddetector-label-tagged`

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
<code>requiredKeyTags</code>	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi	Tidak ada nilai default

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
			persyaratan AWS	

Kontrol ini memeriksa apakah label Amazon Fraud Detector memiliki tag dengan kunci spesifik yang ditentukan dalam parameter `requiredKeyTags`. Kontrol gagal jika label tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter `requiredKeyTags`. Jika parameter `requiredKeyTags` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika label tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengkategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat [Menentukan izin berdasarkan atribut dengan otorisasi ABAC di Panduan Pengguna IAM](#).

Note

Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk mengetahui praktik terbaik penandaan lainnya, lihat [Praktik dan strategi terbaik di Panduan Pengguna AWS Sumber Daya Penandaan dan Editor Tag](#).

Remediasi

Untuk menambahkan tag ke label Amazon Fraud Detector (konsol)

1. Buka konsol Amazon Fraud Detector di <https://console.aws.amazon.com/frauddetector>.
2. Di panel navigasi, pilih Label.
3. Pilih label dari daftar.
4. Di bagian tag label, pilih Kelola tag.
5. Pilih Tambahkan tag baru. Masukkan kunci dan nilai untuk tanda tersebut. Ulangi untuk pasangan nilai kunci tambahan.
6. Setelah Anda selesai menambahkan tanda, pilih Simpan.

[FraudDetector.3] Hasil Amazon Fraud Detector harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::FraudDetector::Outcome`

AWS Config aturan: `frauddetector-outcome-tagged`

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
<code>requiredKeyTags</code>	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS .	Tidak ada nilai default

Kontrol ini memeriksa apakah hasil Amazon Fraud Detector memiliki tag dengan kunci spesifik yang ditentukan dalam parameter `requiredKeyTags`. Kontrol gagal jika hasilnya tidak memiliki kunci

tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter `requiredKeyTags`. Jika parameter `requiredKeyTags` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika hasilnya tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws :`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat [Menentukan izin berdasarkan atribut dengan otorisasi ABAC di Panduan Pengguna IAM](#).

Note

Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk mengetahui praktik terbaik penandaan lainnya, lihat [Praktik dan strategi terbaik di Panduan Pengguna AWS Sumber Daya Penandaan dan Editor Tag](#).

Remediasi

Untuk menambahkan tag ke hasil Amazon Fraud Detector (konsol)

1. Buka konsol Amazon Fraud Detector di <https://console.aws.amazon.com/frauddetector>.
2. Di panel navigasi, pilih Hasil.
3. Pilih hasil dari daftar.
4. Di bagian tag hasil, pilih Kelola tag.
5. Pilih Tambahkan tag baru. Masukkan kunci dan nilai untuk tanda tersebut. Ulangi untuk pasangan nilai kunci tambahan.
6. Setelah Anda selesai menambahkan tanda, pilih Simpan.

[FraudDetector.4] Variabel Amazon Fraud Detector harus diberi tag

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::FraudDetector::Variable`

AWS Config aturan: `frauddetector-variable-tagged`

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
<code>requiredKeyTags</code>	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS .	Tidak ada nilai default

Kontrol ini memeriksa apakah variabel Amazon Fraud Detector memiliki tag dengan kunci tertentu yang ditentukan dalam parameter `requiredKeyTags`. Kontrol gagal jika variabel tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter `requiredKeyTags`. Jika parameter `requiredKeyTags` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika variabel tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws :`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengkategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah

untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat [Menentukan izin berdasarkan atribut dengan otorisasi ABAC di Panduan Pengguna IAM](#).

Note

Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk mengetahui praktik terbaik penandaan lainnya, lihat [Praktik dan strategi terbaik di Panduan Pengguna AWS Sumber Daya Penandaan dan Editor Tag](#).

Remediasi

Untuk menambahkan tag ke variabel Amazon Fraud Detector (konsol)

1. Buka konsol Amazon Fraud Detector di <https://console.aws.amazon.com/frauddetector>.
2. Di panel navigasi, pilih Variabel.
3. Pilih variabel dari daftar.
4. Di bagian tag variabel, pilih Kelola tag.
5. Pilih Tambahkan tag baru. Masukkan kunci dan nilai untuk tanda tersebut. Ulangi untuk pasangan nilai kunci tambahan.
6. Setelah Anda selesai menambahkan tanda, pilih Simpan.

Kontrol Security Hub untuk Amazon FSx

AWS Security Hub Kontrol ini mengevaluasi FSx layanan dan sumber daya Amazon. Kontrol mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat [Ketersediaan kontrol berdasarkan Wilayah](#).

[FSx.1] FSx untuk sistem file OpenZFS harus dikonfigurasi untuk menyalin tag ke cadangan dan volume

Persyaratan terkait: NIST.800-53.r5 CA-9 (1), Nist.800-53.R5 CM-2, Nist.800-53.R5 CM-2 (2)

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: AWS::FSx::FileSystem

AWS Config aturan: [fsx-openzfs-copy-tags-enabled](#)

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah sistem file Amazon FSx untuk OpenZFS dikonfigurasi untuk menyalin tag ke cadangan dan volume. Kontrol gagal jika sistem file OpenZFS tidak dikonfigurasi untuk menyalin tag ke backup dan volume.

Identifikasi dan inventaris aset TI Anda merupakan aspek penting dari tata kelola dan keamanan. Tag membantu Anda mengkategorikan AWS sumber daya Anda dengan cara yang berbeda, misalnya, berdasarkan tujuan, pemilik, atau lingkungan. Ini berguna ketika Anda memiliki banyak sumber daya dari jenis yang sama karena Anda dapat dengan cepat mengidentifikasi sumber daya tertentu berdasarkan tag yang Anda tetapkan padanya.

Remediasi

Untuk informasi tentang mengonfigurasi sistem file FSx untuk OpenZFS untuk menyalin tag ke cadangan dan volume, lihat [Memperbarui sistem file di Amazon FSx untuk Panduan](#) Pengguna OpenZFS.

[FSx.2] FSx untuk sistem file Lustre harus dikonfigurasi untuk menyalin tag ke cadangan

Persyaratan terkait: Nist.800-53.r5 CP-9, NIST.800-53.R5 CM-8

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: AWS::FSx::FileSystem

AWS Config aturan: [fsx-lustre-copy-tags-to-backups](#)

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah sistem file Amazon FSx untuk Lustre dikonfigurasi untuk menyalin tag ke cadangan dan volume. Kontrol gagal jika sistem file Lustre tidak dikonfigurasi untuk menyalin tag ke backup dan volume.

Identifikasi dan inventaris aset TI Anda merupakan aspek penting dari tata kelola dan keamanan. Tag membantu Anda mengkategorikan AWS sumber daya Anda dengan cara yang berbeda, misalnya, berdasarkan tujuan, pemilik, atau lingkungan. Ini berguna ketika Anda memiliki banyak sumber daya dari jenis yang sama karena Anda dapat dengan cepat mengidentifikasi sumber daya tertentu berdasarkan tag yang Anda tetapkan padanya.

Remediasi

Untuk informasi tentang mengonfigurasi sistem file Lustre FSx untuk menyalin tag ke cadangan, lihat Menyalin [cadangan dalam hal yang sama Akun AWS di Amazon for Lustre User Guide](#). FSx

[FSx.3] FSx untuk sistem file OpenZFS harus dikonfigurasi untuk penyebaran Multi-AZ

Kategori: Pulihkan > Ketahanan > Ketersediaan tinggi

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::FSx::FileSystem

AWS Config aturan: [fsx-openzfs-deployment-type-check](#)

Jenis jadwal: Periodik

Parameter: deploymentTypes: MULTI_AZ_1 (tidak dapat disesuaikan)

Kontrol ini memeriksa apakah sistem file Amazon FSx untuk OpenZFS dikonfigurasi untuk menggunakan beberapa jenis penyebaran Availability Zones (Multi-AZ). Kontrol gagal jika sistem file tidak dikonfigurasi untuk menggunakan jenis penyebaran Multi-AZ.

Amazon FSx untuk OpenZFS mendukung beberapa jenis penyebaran untuk sistem file: Multi-AZ (HA), Single-AZ (HA), dan Single-AZ (non-HA). Jenis penyebaran menawarkan tingkat ketersediaan dan daya tahan yang berbeda. Sistem file multi-AZ (HA) terdiri dari sepasang server file ketersediaan tinggi (HA) yang tersebar di dua Availability Zones (AZs). Kami merekomendasikan penggunaan tipe penyebaran Multi-AZ (HA) untuk sebagian besar beban kerja produksi karena ketersediaan tinggi dan model daya tahan yang disediakannya.

Remediasi

Anda dapat mengonfigurasi sistem file Amazon FSx untuk OpenZFS untuk menggunakan jenis penyebaran Multi-AZ saat Anda membuat sistem file. Anda tidak dapat mengubah jenis penerapan untuk sistem file OpenZFS yang sudah ada FSx .

Untuk informasi tentang jenis dan opsi penerapan FSx untuk sistem file OpenZFS, lihat [Ketersediaan dan daya tahan Amazon FSx untuk OpenZFS dan Mengelola sumber daya sistem file di](#) Amazon FSx untuk Panduan Pengguna OpenZFS.

[FSx.4] FSx untuk sistem file NetApp ONTAP harus dikonfigurasi untuk penyebaran Multi-AZ

Kategori: Pulihkan > Ketahanan > Ketersediaan tinggi

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::FSx::FileSystem

AWS Config aturan: [fsx-ontap-deployment-type-check](#)

Jenis jadwal: Periodik

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
deploymentTypes	Daftar jenis penyebaran untuk disertakan dalam evaluasi. Kontrol menghasilkan FAILED temuan jika sistem file tidak dikonfigurasi untuk menggunakan jenis penerapan yang ditentukan dalam daftar.	Enum	MULTI_AZ_1 , MULTI_AZ_2	MULTI_AZ_1 , MULTI_AZ_2

Kontrol ini memeriksa apakah sistem file Amazon FSx untuk NetApp ONTAP dikonfigurasi untuk menggunakan beberapa jenis penyebaran Availability Zones (Multi-AZ). Kontrol gagal jika sistem file tidak dikonfigurasi untuk menggunakan jenis penyebaran multi-AZ. Anda dapat secara opsional menentukan daftar jenis penerapan yang akan disertakan dalam evaluasi.

Amazon FSx untuk NetApp ONTAP mendukung beberapa jenis penyebaran untuk sistem file: Single-AZ 1, Single-AZ 2, Multi-AZ 1, dan Multi-AZ 2. Jenis penyebaran menawarkan tingkat ketersediaan

dan daya tahan yang berbeda. Sebaiknya gunakan tipe penyebaran Multi-AZ untuk sebagian besar beban kerja produksi karena model ketersediaan dan daya tahan tinggi yang disediakan oleh tipe penerapan Multi-AZ. Sistem file Multi-AZ mendukung semua fitur ketersediaan dan daya tahan sistem file Single-AZ. Selain itu, mereka dirancang untuk menyediakan ketersediaan berkelanjutan ke data bahkan ketika Availability Zone (AZ) tidak tersedia.

Remediasi

Anda tidak dapat mengubah jenis penerapan untuk sistem file Amazon FSx untuk NetApp ONTAP yang ada. Namun, Anda dapat mencadangkan data, dan kemudian mengembalikannya pada sistem file baru yang menggunakan tipe penyebaran multi-AZ.

Untuk informasi tentang jenis dan opsi penerapan FSx untuk sistem file ONTAP, lihat [Opsi ketersediaan, daya tahan, dan penerapan serta Mengelola sistem file](#) di Panduan Pengguna FSx untuk ONTAP.

[FSx.5] FSx untuk sistem file Windows File Server harus dikonfigurasi untuk penyebaran Multi-AZ

Kategori: Pulihkan > Ketahanan > Ketersediaan tinggi

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::FSx::FileSystem

AWS Config aturan: [fsx-windows-deployment-type-check](#)

Jenis jadwal: Periodik

Parameter: deploymentTypes: MULTI_AZ_1 (tidak dapat disesuaikan)

Kontrol ini memeriksa apakah sistem file Amazon FSx untuk Windows File Server dikonfigurasi untuk menggunakan beberapa jenis penyebaran Availability Zones (Multi-AZ). Kontrol gagal jika sistem file tidak dikonfigurasi untuk menggunakan jenis penyebaran Multi-AZ.

Amazon FSx untuk Windows File Server mendukung dua jenis penyebaran untuk sistem file: Single-AZ dan Multi-AZ. Jenis penyebaran menawarkan tingkat ketersediaan dan daya tahan yang berbeda. Sistem file single-AZ terdiri dari satu instance server file Windows dan satu set volume penyimpanan dalam satu Availability Zone (AZ). Sistem file multi-AZ terdiri dari cluster server file Windows dengan ketersediaan tinggi yang tersebar di dua Availability Zone. Kami merekomendasikan penggunaan

tipe penyebaran Multi-AZ untuk sebagian besar beban kerja produksi karena ketersediaan tinggi dan model daya tahan yang disediakannya.

Remediasi

Anda dapat mengonfigurasi sistem file Amazon FSx untuk Windows File Server untuk menggunakan jenis penyebaran Multi-AZ saat Anda membuat sistem file. Anda tidak dapat mengubah jenis penerapan untuk sistem file Windows File Server yang sudah ada FSx .

Untuk informasi tentang jenis dan opsi penerapan FSx untuk sistem file Windows File Server, lihat [Ketersediaan dan daya tahan: Sistem file Single-AZ dan Multi-AZ](#) dan [Memulai Amazon FSx untuk Windows File Server](#) di Amazon FSx untuk Windows File Server Panduan Pengguna.

Kontrol Security Hub untuk Global Accelerator

AWS Security Hub Kontrol ini mengevaluasi AWS Global Accelerator layanan dan sumber daya.

Kontrol ini mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat [Ketersediaan kontrol berdasarkan Wilayah](#).

[GlobalAccelerator.1] Akselerator Akselerator Global harus diberi tag

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::GlobalAccelerator::Accelerator`

AWS Config aturan: `tagged-globalaccelerator-accelerator` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
<code>requiredTagKeys</code>	Daftar kunci tag non-sistem yang harus berisi sumber daya	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi	No default value

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
	yang dievaluasi. Kunci tag peka huruf besar dan kecil.		persyaratan AWS .	

Kontrol ini memeriksa apakah AWS Global Accelerator akselerator memiliki tag dengan kunci spesifik yang ditentukan dalam parameter `requiredTagKeys`. Kontrol gagal jika akselerator tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter `requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika akselerator tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws :`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat [Untuk apa ABAC? AWS](#) di Panduan Pengguna IAM.

Note

Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat [Menandai AWS sumber daya Anda](#) di Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke akselerator global Akselerator Global, lihat [Menandai AWS Global Accelerator di Panduan Pengembangan](#) AWS Global Accelerator .

Kontrol Security Hub untuk AWS Glue

AWS Security Hub Kontrol ini mengevaluasi AWS Glue layanan dan sumber daya. Kontrol mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat [Ketersediaan kontrol berdasarkan Wilayah](#).

AWS Glue Pekerjaan [Glue.1] harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: AWS::Glue::Job

AWS Config aturan: tagged-glue-job (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
<code>requiredTagKeys</code>	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS .	Tidak ada nilai default

Kontrol ini memeriksa apakah AWS Glue pekerjaan memiliki tag dengan kunci tertentu yang ditentukan dalam parameter `requiredTagKeys`. Kontrol gagal jika pekerjaan tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter `requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika pekerjaan tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengkategorikan sumber daya berdasarkan tujuan, pemilik,

lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat [Untuk apa ABAC? AWS](#) di Panduan Pengguna IAM.

Note

Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat [Menandai AWS sumber daya Anda](#) di Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke AWS Glue pekerjaan, lihat [AWS tag AWS Glue di](#) Panduan AWS Glue Pengguna.

[Glue.3] transformasi pembelajaran AWS Glue mesin harus dienkripsi saat istirahat

Kategori: Lindungi > Perlindungan Data > Enkripsi data-at-rest

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::Glue::MLTransform

AWS Config aturan: [glue-ml-transform-encrypted-at-rest](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak

Kontrol ini memeriksa apakah transformasi pembelajaran AWS Glue mesin dienkripsi saat istirahat. Kontrol gagal jika transformasi pembelajaran mesin tidak dienkripsi saat istirahat.

Data saat istirahat mengacu pada data yang disimpan dalam penyimpanan persisten dan tidak mudah menguap untuk durasi berapa pun. Mengenkripsi data saat istirahat membantu Anda melindungi kerahasiaannya, yang mengurangi risiko bahwa pengguna yang tidak sah dapat mengaksesnya.

Remediasi

Untuk mengonfigurasi enkripsi untuk transformasi pembelajaran AWS Glue mesin, lihat [Bekerja dengan transformasi pembelajaran mesin](#) di AWS Glue Panduan Pengguna.

[Glue.4] Pekerjaan AWS Glue percikan harus berjalan pada versi yang didukung AWS Glue

Persyaratan terkait: NIST.800-53.r5 CA-9 (1), NIST.800-53.R5 CM-2, NIST.800-53.R5 SI-2, NIST.800-53.R5 SI-2 (2), Nist.800-53.R5 SI-2 (4), NIST.800-53.R5 SI-2 (5)

Kategori: Identifikasi > Kerentanan, tambalan, dan manajemen versi

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::Glue::Job

AWS Config aturan: [glue-spark-job-supported-version](#)

Jenis jadwal: Perubahan dipicu

Parameter:minimumSupportedGlueVersion: 3.0 (tidak dapat disesuaikan)

Kontrol ini memeriksa apakah pekerjaan AWS Glue for Spark dikonfigurasi untuk berjalan pada versi yang didukung. AWS Glue Kontrol gagal jika pekerjaan Spark dikonfigurasi untuk berjalan pada versi yang lebih awal dari versi minimum yang didukung. AWS Glue

Note

Kontrol ini juga menghasilkan FAILED temuan untuk pekerjaan Spark jika properti AWS Glue version (GlueVersion) tidak ada atau null dalam item konfigurasi (CI) untuk pekerjaan tersebut. AWS Glue Dalam kasus seperti itu, temuan tersebut mencakup anotasi berikut: GlueVersion is null or missing in glueetl job configuration. Untuk mengatasi jenis FAILED temuan ini, tambahkan GlueVersion properti ke konfigurasi pekerjaan. Untuk daftar versi dan lingkungan runtime yang didukung, lihat [AWS Glue Versi](#) dalam Panduan AWS Glue Pengguna.

Menjalankan pekerjaan AWS Glue Spark pada versi saat ini AWS Glue dapat mengoptimalkan kinerja, keamanan, dan akses ke fitur terbaru. AWS Glue Ini juga dapat membantu melindungi terhadap kerentanan keamanan. Misalnya, versi baru mungkin dirilis untuk menyediakan pembaruan keamanan, mengatasi masalah, atau memperkenalkan fitur baru.

Remediasi

Untuk informasi tentang memigrasi pekerjaan Spark ke versi yang didukung AWS Glue, lihat [Memigrasi AWS Glue pekerjaan Spark](#) di Panduan Pengguna.AWS Glue

Kontrol Security Hub untuk Amazon GuardDuty

AWS Security Hub Kontrol ini mengevaluasi GuardDuty layanan dan sumber daya Amazon. Kontrol mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat [Ketersediaan kontrol berdasarkan Wilayah](#).

[GuardDuty.1] GuardDuty harus diaktifkan

Persyaratan terkait: NIST.800-53.r5 AC-2 (12), (4), 1 (1) NIST.800-53.r5 AU-6(1), NIST.800-53.r5 AU-6(5), NIST.800-53.r5 CA-7, NIST.800-53.r5 SA-1 1 NIST.800-53.r5 CM-8(3), NIST.800-53.r5 RA-3 (6), NIST.800-53.r5 SA-1 5 (2), 5 (8), (19), (21), (25), (NIST.800-53.r5 SA-11), (3), NIST.800-53.r5 SA-1 Nist.800-53.R5 SI-20, Nist.800-53.r5 SI-3 NIST.800-53.r5 SA-8 (8), NIST.800-53.r5 SA-8 Nist.800-53.r5 SI-4, NIST.800-53.r5 SA-8 Nist.800-53.R5 SI-4 NIST.800-53.r5 SC-5, Nist.800-53.r5 SI-4 .800-53.R5 SI-4 NIST.800-53.r5 SC-5 NIST.800-53.r5 SC-5 (1), NIST.800-53.R5 SI-4 (13), NIST.800-53.R5 SI-4 (2), NIST.800-53.R5 SI-4 (22), NIST.800-53.R5 SI-4 (25), NIST.800-53.R5 SI-4 (4), NIST.800-53.R5 3.R5 SI-4 (5), Nist.800-171.r2 3.4.2, Nist.800-171.r2 3.14.6, Nist.800-171.r2 3.14.7, PCI DSS v3.2.1/11.4 , PCI DSS v4.0.1/11.5.1

Kategori: Deteksi > Layanan deteksi

Tingkat keparahan: Tinggi

Jenis sumber daya: AWS : : : Account

AWS Config aturan: [guardduty-enabled-centralized](#)

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah Amazon GuardDuty diaktifkan di GuardDuty akun dan Wilayah Anda.

Sangat disarankan agar Anda mengaktifkan GuardDuty di semua AWS Wilayah yang didukung. Melakukan hal itu memungkinkan GuardDuty untuk menghasilkan temuan tentang aktivitas yang tidak sah atau tidak biasa, bahkan di Wilayah yang tidak aktif Anda gunakan. Ini juga memungkinkan GuardDuty untuk memantau CloudTrail peristiwa untuk global Layanan AWS seperti IAM.

Tindakan Perbaikan

Untuk mengaktifkan GuardDuty, lihat [Memulai GuardDuty](#) di Panduan GuardDuty Pengguna Amazon.

[GuardDuty.2] GuardDuty filter harus diberi tag

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::GuardDuty::Filter`

AWS Config aturan: `tagged-guardduty-filter` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai yang Diizinkan	Nilai default Security Hub
<code>requiredTagKeys</code>	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS .	No default value

Kontrol ini memeriksa apakah GuardDuty filter Amazon memiliki tag dengan kunci tertentu yang ditentukan dalam parameter `requiredTagKeys`. Kontrol gagal jika filter tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter `requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika filter tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws:`, diabaikan.

Tanda adalah sebuah label yang Anda tetapkan ke sebuah AWS sumber daya, dan itu terdiri dari sebuah kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat Anda menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat memasang tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk penanggung jawab IAM Anda. Anda dapat merancang kebijakan ABAC ini untuk memungkinkan operasi ketika tag penanggung jawab cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat [Untuk apa ABAC untuk? AWS](#) di Panduan Pengguna IAM.

Note

Jangan menambahkan informasi pengenalan pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat [Menandai AWS sumber daya Anda](#) di Referensi Umum AWS

Tindakan Perbaikan

Untuk menambahkan tag ke GuardDuty filter, lihat [TagResource](#) di Referensi Amazon GuardDuty API.

[GuardDuty.3] GuardDuty IPSets harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: AWS::GuardDuty::IPSet

AWS Config aturan: tagged-guardduty-ipset (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai yang Diizinkan	Nilai default Security Hub
<code>requiredTagKeys</code>	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS .	No default value

Kontrol ini memeriksa apakah Amazon GuardDuty IPSet memiliki tag dengan kunci tertentu yang ditentukan dalam parameter `requiredTagKeys`. Kontrol gagal jika IPSet tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter `requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika IPSet tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws :`, diabaikan.

Tanda adalah sebuah label yang Anda tetapkan ke sebuah AWS sumber daya, dan itu terdiri dari sebuah kunci dan nilai opsional. Anda dapat membuat tag untuk mengkategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat Anda menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat memasang tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk penanggung jawab IAM Anda. Anda dapat merancang kebijakan ABAC ini untuk memungkinkan operasi ketika tag penanggung jawab cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat [Untuk apa ABAC untuk? AWS](#) di Panduan Pengguna IAM.

Note

Jangan menambahkan informasi pengenalan pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat [Menandai AWS sumber daya Anda](#) di Referensi Umum AWS

Tindakan Perbaikan

Untuk menambahkan tag ke a GuardDuty IPSet, lihat [TagResource](#) di Referensi Amazon GuardDuty API.

[GuardDuty.4] GuardDuty detektor harus diberi tag

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: AWS::GuardDuty::Detector

AWS Config aturan: tagged-guardduty-detector (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai yang Diizinkan	Nilai default Security Hub
<code>requiredTagKeys</code>	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS .	No default value

Kontrol ini memeriksa apakah GuardDuty detektor Amazon memiliki tag dengan kunci tertentu yang ditentukan dalam parameter `requiredTagKeys`. Kontrol gagal jika detektor tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter `requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika detektor tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws:`, diabaikan.

Tanda adalah sebuah label yang Anda tetapkan ke sebuah AWS sumber daya, dan itu terdiri dari sebuah kunci dan nilai opsional. Anda dapat membuat tag untuk mengkategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik

sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat memasang tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk penanggung jawab IAM Anda. Anda dapat merancang kebijakan ABAC ini untuk memungkinkan operasi ketika tag penanggung jawab cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat Untuk [apa ABAC untuk? AWS](#) di Panduan Pengguna IAM.

Note

Jangan menambahkan informasi pengenalan pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat [Menandai AWS sumber daya Anda](#) di Referensi Umum AWS

Tindakan Perbaikan

Untuk menambahkan tag ke GuardDuty detektor, lihat [TagResource](#) di Referensi Amazon GuardDuty API.

[GuardDuty.5] Pemantauan Log Audit GuardDuty EKS harus diaktifkan

Kategori: Deteksi > Layanan deteksi

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::GuardDuty::Detector`

AWS Config aturan: [guardduty-eks-protection-audit-enabled](#)

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah Pemantauan Log Audit GuardDuty EKS diaktifkan. Untuk akun mandiri, kontrol gagal jika Pemantauan Log Audit GuardDuty EKS dinonaktifkan di akun. Dalam lingkungan multi-akun, kontrol gagal jika akun GuardDuty administrator yang didelegasikan dan semua akun anggota tidak mengaktifkan Pemantauan Log Audit EKS.

Di lingkungan multi-akun, kontrol menghasilkan temuan hanya di akun GuardDuty administrator yang didelegasikan. Hanya administrator yang didelegasikan yang dapat mengaktifkan atau menonaktifkan fitur Pemantauan Log Audit EKS untuk akun anggota di organisasi. GuardDuty Akun anggota tidak dapat mengubah konfigurasi ini dari akun mereka. Kontrol ini menghasilkan FAILED temuan jika GuardDuty administrator yang didelegasikan memiliki akun anggota yang ditangguhkan yang tidak mengaktifkan Pemantauan Log Audit GuardDuty EKS. Untuk menerima PASSED temuan, administrator yang didelegasikan harus memisahkan akun yang ditangguhkan ini. GuardDuty

GuardDuty EKS Audit Log Monitoring membantu Anda mendeteksi aktivitas yang berpotensi mencurigakan di kluster Amazon Elastic Kubernetes Service (Amazon EKS) Anda. EKS Audit Log Monitoring menggunakan log audit Kubernetes untuk menangkap aktivitas kronologis dari pengguna, aplikasi yang menggunakan Kubernetes API, dan control plane.

Tindakan Perbaikan

Untuk mengaktifkan Pemantauan Log Audit GuardDuty [EKS, lihat Pemantauan Log Audit EKS](#) di Panduan GuardDuty Pengguna Amazon.

[GuardDuty.6] Perlindungan GuardDuty Lambda harus diaktifkan

Persyaratan terkait: PCI DSS v4.0.1/11.5.1

Kategori: Deteksi > Layanan deteksi

Tingkat keparahan: Tinggi

Jenis sumber daya: AWS::GuardDuty::Detector

AWS Config aturan: [guardduty-lambda-protection-enabled](#)

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah Perlindungan GuardDuty Lambda diaktifkan. Untuk akun mandiri, kontrol gagal jika Perlindungan GuardDuty Lambda dinonaktifkan di akun. Di lingkungan multi-akun, kontrol gagal jika akun GuardDuty administrator yang didelegasikan dan semua akun anggota tidak mengaktifkan Perlindungan Lambda.

Di lingkungan multi-akun, kontrol menghasilkan temuan hanya di akun GuardDuty administrator yang didelegasikan. Hanya administrator yang didelegasikan yang dapat mengaktifkan atau menonaktifkan fitur Perlindungan Lambda untuk akun anggota di organisasi. GuardDuty Akun anggota tidak

dapat mengubah konfigurasi ini dari akun mereka. Kontrol ini menghasilkan FAILED temuan jika GuardDuty administrator yang didelegasikan memiliki akun anggota yang ditangguhkan yang tidak mengaktifkan Perlindungan GuardDuty Lambda. Untuk menerima PASSED temuan, administrator yang didelegasikan harus memisahkan akun yang ditangguhkan ini. GuardDuty

GuardDuty Lambda Protection membantu Anda mengidentifikasi potensi ancaman keamanan saat suatu AWS Lambda fungsi dipanggil. Setelah Anda mengaktifkan Perlindungan Lambda, GuardDuty mulai memantau log aktivitas jaringan Lambda yang terkait dengan fungsi Lambda di Anda. Akun AWS Ketika fungsi Lambda dipanggil dan GuardDuty mengidentifikasi lalu lintas jaringan mencurigakan yang menunjukkan adanya potongan kode yang berpotensi berbahaya dalam fungsi Lambda Anda, menghasilkan temuan. GuardDuty

Tindakan Perbaikan

Untuk mengaktifkan Perlindungan GuardDuty Lambda, lihat [Mengonfigurasi Perlindungan Lambda di Panduan Pengguna](#) Amazon. GuardDuty

[GuardDuty.7] GuardDuty EKS Runtime Monitoring harus diaktifkan

Persyaratan terkait: PCI DSS v4.0.1/11.5.1

Kategori: Deteksi > Layanan Deteksi

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::GuardDuty::Detector

AWS Config aturan: [guardduty-eks-protection-runtime-enabled](#)

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah GuardDuty EKS Runtime Monitoring dengan manajemen agen otomatis diaktifkan. Untuk akun mandiri, kontrol gagal jika GuardDuty EKS Runtime Monitoring dengan manajemen agen otomatis dinonaktifkan di akun. Dalam lingkungan multi-akun, kontrol gagal jika akun GuardDuty administrator yang didelegasikan dan semua akun anggota tidak memiliki EKS Runtime Monitoring dengan manajemen agen otomatis diaktifkan.

Di lingkungan multi-akun, kontrol menghasilkan temuan hanya di akun GuardDuty administrator yang didelegasikan. Hanya administrator yang didelegasikan yang dapat mengaktifkan atau menonaktifkan fitur EKS Runtime Monitoring dengan manajemen agen otomatis untuk akun anggota

di organisasi. GuardDuty Akun anggota tidak dapat mengubah konfigurasi ini dari akun mereka. Kontrol ini menghasilkan FAILED temuan jika GuardDuty administrator yang didelegasikan memiliki akun anggota yang ditangguhkan yang tidak mengaktifkan GuardDuty EKS Runtime Monitoring. Untuk menerima PASSED temuan, administrator yang didelegasikan harus memisahkan akun yang ditangguhkan ini. GuardDuty

Perlindungan EKS di Amazon GuardDuty menyediakan cakupan deteksi ancaman untuk membantu Anda melindungi kluster Amazon EKS di AWS lingkungan Anda. EKS Runtime Monitoring menggunakan peristiwa tingkat sistem operasi untuk membantu Anda mendeteksi potensi ancaman di node dan kontainer EKS dalam kluster EKS Anda.

Tindakan Perbaikan

Untuk mengaktifkan Pemantauan Runtime EKS dengan manajemen agen otomatis, lihat [Mengaktifkan Pemantauan GuardDuty Runtime](#) di Panduan Pengguna Amazon GuardDuty .

[GuardDuty.8] Perlindungan GuardDuty Malware untuk EC2 harus diaktifkan

Kategori: Deteksi > Layanan deteksi

Tingkat keparahan: Tinggi

Jenis sumber daya: AWS::GuardDuty::Detector

AWS Config aturan: [guardduty-malware-protection-enabled](#)

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah Perlindungan GuardDuty Malware diaktifkan. Untuk akun mandiri, kontrol gagal jika Perlindungan GuardDuty Malware dinonaktifkan di akun. Dalam lingkungan multi-akun, kontrol gagal jika akun GuardDuty administrator yang didelegasikan dan semua akun anggota tidak mengaktifkan Perlindungan Malware.

Di lingkungan multi-akun, kontrol menghasilkan temuan hanya di akun GuardDuty administrator yang didelegasikan. Hanya administrator yang didelegasikan yang dapat mengaktifkan atau menonaktifkan fitur Perlindungan Malware untuk akun anggota di organisasi. GuardDuty Akun anggota tidak dapat mengubah konfigurasi ini dari akun mereka. Kontrol ini menghasilkan FAILED temuan jika GuardDuty administrator yang didelegasikan memiliki akun anggota yang ditangguhkan yang tidak mengaktifkan Perlindungan GuardDuty Malware. Untuk menerima PASSED temuan, administrator yang didelegasikan harus memisahkan akun yang ditangguhkan ini. GuardDuty

GuardDuty Perlindungan Malware for EC2 membantu Anda mendeteksi potensi keberadaan malware dengan memindai volume Amazon Elastic Block Store (Amazon EBS) yang dilampirkan ke instans Amazon Elastic Compute Cloud (EC2Amazon) dan beban kerja kontainer. Perlindungan Malware menyediakan opsi pemindaian di mana Anda dapat memutuskan apakah Anda ingin menyertakan atau mengecualikan EC2 instance dan beban kerja kontainer tertentu pada saat pemindaian. Ini juga menyediakan opsi untuk menyimpan snapshot volume EBS yang dilampirkan ke EC2 instance atau beban kerja kontainer, di akun Anda. GuardDuty Cuplikan disimpan hanya ketika malware ditemukan dan temuan Perlindungan Malware dihasilkan.

Tindakan Perbaikan

Untuk mengaktifkan Perlindungan GuardDuty Malware EC2, lihat [Mengonfigurasi GuardDuty pemindaian malware yang dimulai](#) di Panduan Pengguna Amazon GuardDuty .

[GuardDuty.9] Perlindungan GuardDuty RDS harus diaktifkan

Persyaratan terkait: PCI DSS v4.0.1/11.5.1

Kategori: Deteksi > Layanan deteksi

Tingkat keparahan: Tinggi

Jenis sumber daya: AWS::GuardDuty::Detector

AWS Config aturan: [guardduty-rds-protection-enabled](#)

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah Perlindungan GuardDuty RDS diaktifkan. Untuk akun mandiri, kontrol gagal jika Perlindungan GuardDuty RDS dinonaktifkan di akun. Dalam lingkungan multi-akun, kontrol gagal jika akun GuardDuty administrator yang didelegasikan dan semua akun anggota tidak mengaktifkan Perlindungan RDS.

Di lingkungan multi-akun, kontrol menghasilkan temuan hanya di akun GuardDuty administrator yang didelegasikan. Hanya administrator yang didelegasikan yang dapat mengaktifkan atau menonaktifkan fitur Perlindungan RDS untuk akun anggota di organisasi. GuardDuty Akun anggota tidak dapat mengubah konfigurasi ini dari akun mereka. Kontrol ini menghasilkan FAILED temuan jika GuardDuty administrator yang didelegasikan memiliki akun anggota yang ditangguhkan yang tidak mengaktifkan Perlindungan GuardDuty RDS. Untuk menerima PASSED temuan, administrator yang didelegasikan harus memisahkan akun yang ditangguhkan ini. GuardDuty

Perlindungan RDS dalam GuardDuty analisis dan profil Aktivitas login RDS untuk potensi ancaman akses ke database Amazon Aurora Anda (Edisi yang kompatibel dengan Aurora MySQL dan Edisi yang kompatibel dengan Aurora PostgreSQL). Fitur ini memungkinkan Anda mengidentifikasi perilaku login yang berpotensi mencurigakan. Perlindungan RDS tidak memerlukan infrastruktur tambahan; itu dirancang agar tidak mempengaruhi kinerja instance database Anda. Ketika RDS Protection mendeteksi upaya login yang berpotensi mencurigakan atau anomali yang menunjukkan ancaman terhadap database Anda, GuardDuty menghasilkan temuan baru dengan detail tentang database yang berpotensi dikompromikan.

Tindakan Perbaikan

Untuk mengaktifkan Perlindungan GuardDuty RDS, lihat [Perlindungan GuardDuty RDS](#) di GuardDuty Panduan Pengguna Amazon.

[GuardDuty.10] Perlindungan GuardDuty S3 harus diaktifkan

Persyaratan terkait: PCI DSS v4.0.1/11.5.1

Kategori: Deteksi > Layanan deteksi

Tingkat keparahan: Tinggi

Jenis sumber daya: AWS::GuardDuty::Detector

AWS Config aturan: [guardduty-s3-protection-enabled](#)

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah Perlindungan GuardDuty S3 diaktifkan. Untuk akun mandiri, kontrol gagal jika Perlindungan GuardDuty S3 dinonaktifkan di akun. Dalam lingkungan multi-akun, kontrol gagal jika akun GuardDuty administrator yang didelegasikan dan semua akun anggota tidak mengaktifkan Perlindungan S3.

Di lingkungan multi-akun, kontrol menghasilkan temuan hanya di akun GuardDuty administrator yang didelegasikan. Hanya administrator yang didelegasikan yang dapat mengaktifkan atau menonaktifkan fitur Perlindungan S3 untuk akun anggota di organisasi. GuardDuty Akun anggota tidak dapat mengubah konfigurasi ini dari akun mereka. Kontrol ini menghasilkan FAILED temuan jika GuardDuty administrator yang didelegasikan memiliki akun anggota yang ditangguhkan yang tidak mengaktifkan Perlindungan GuardDuty S3. Untuk menerima PASSED temuan, administrator yang didelegasikan harus memisahkan akun yang ditangguhkan ini. GuardDuty

Perlindungan S3 memungkinkan GuardDuty untuk memantau operasi API tingkat objek untuk mengidentifikasi potensi risiko keamanan data dalam bucket Amazon Simple Storage Service (Amazon S3) Anda. GuardDuty memantau ancaman terhadap sumber daya S3 Anda dengan menganalisis peristiwa AWS CloudTrail manajemen dan peristiwa data CloudTrail S3.

Tindakan Perbaikan

Untuk mengaktifkan Perlindungan GuardDuty S3, lihat Perlindungan [Amazon S3 di GuardDuty Amazon di](#) Panduan Pengguna GuardDuty Amazon.

[GuardDuty.11] GuardDuty Runtime Monitoring harus diaktifkan

Kategori: Deteksi > Layanan Deteksi

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::GuardDuty::Detector`

AWS Config aturan: [guardduty-runtime-monitoring-enabled](#)

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah Runtime Monitoring diaktifkan di Amazon GuardDuty. Untuk akun mandiri, kontrol gagal jika GuardDuty Runtime Monitoring dinonaktifkan untuk akun tersebut. Dalam lingkungan multi-akun, kontrol gagal jika GuardDuty Runtime Monitoring dinonaktifkan untuk akun GuardDuty administrator yang didelegasikan dan semua akun anggota.

Dalam lingkungan multi-akun, hanya GuardDuty administrator yang didelegasikan yang dapat mengaktifkan atau menonaktifkan GuardDuty Runtime Monitoring untuk akun di organisasi mereka. Selain itu, hanya GuardDuty administrator yang dapat mengonfigurasi dan mengelola agen keamanan yang GuardDuty digunakan untuk pemantauan runtime AWS beban kerja dan sumber daya untuk akun di organisasi. GuardDuty akun anggota tidak dapat mengaktifkan, mengonfigurasi, atau menonaktifkan Runtime Monitoring untuk akun mereka sendiri.

GuardDuty Runtime Monitoring mengamati dan menganalisis tingkat sistem operasi, jaringan, dan peristiwa file untuk membantu Anda mendeteksi potensi ancaman dalam beban kerja tertentu AWS di lingkungan Anda. Ini menggunakan agen GuardDuty keamanan yang menambahkan visibilitas ke dalam perilaku runtime, seperti akses file, eksekusi proses, argumen baris perintah, dan koneksi jaringan. Anda dapat mengaktifkan dan mengelola agen keamanan untuk setiap jenis sumber daya

yang ingin Anda pantau untuk potensi ancaman, seperti kluster Amazon EKS dan EC2 instans Amazon.

Tindakan Perbaikan

Untuk informasi tentang mengonfigurasi dan mengaktifkan GuardDuty Runtime Monitoring, lihat Runtime [Monitoring dan Mengaktifkan GuardDuty Runtime Monitoring di GuardDuty Panduan Pengguna Amazon. GuardDuty](#)

[GuardDuty.12] GuardDuty ECS Runtime Monitoring harus diaktifkan

Kategori: Deteksi > Layanan Deteksi

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::GuardDuty::Detector

AWS Config aturan: [guardduty-ecs-protection-runtime-enabled](#)

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah agen keamanan GuardDuty otomatis Amazon diaktifkan untuk pemantauan runtime kluster Amazon ECS aktif. AWS Fargate Untuk akun mandiri, kontrol gagal jika agen keamanan dinonaktifkan untuk akun tersebut. Dalam lingkungan multi-akun, kontrol gagal jika agen keamanan dinonaktifkan untuk akun GuardDuty administrator yang didelegasikan dan semua akun anggota.

Di lingkungan multi-akun, kontrol ini hanya menghasilkan temuan di akun GuardDuty administrator yang didelegasikan. Ini karena hanya GuardDuty administrator yang didelegasikan yang dapat mengaktifkan atau menonaktifkan Runtime Monitoring sumber daya ECS-Fargate untuk akun di organisasi mereka. GuardDuty Akun anggota tidak dapat melakukan ini untuk akun mereka sendiri. Selain itu, kontrol ini menghasilkan FAILED temuan jika GuardDuty ditangguhkan untuk akun anggota dan Runtime Monitoring sumber daya ECS-Fargate dinonaktifkan untuk akun anggota. Untuk menerima PASSED temuan, GuardDuty administrator harus memisahkan akun anggota yang ditangguhkan dari akun administrator mereka dengan menggunakan GuardDuty.

GuardDuty Runtime Monitoring mengamati dan menganalisis tingkat sistem operasi, jaringan, dan peristiwa file untuk membantu Anda mendeteksi potensi ancaman dalam beban kerja tertentu AWS di lingkungan Anda. Ini menggunakan agen GuardDuty keamanan yang menambahkan visibilitas

ke dalam perilaku runtime, seperti akses file, eksekusi proses, argumen baris perintah, dan koneksi jaringan. Anda dapat mengaktifkan dan mengelola agen keamanan untuk setiap jenis sumber daya yang ingin Anda pantau untuk potensi ancaman. Ini termasuk kluster Amazon ECS di. AWS Fargate

Tindakan Perbaikan

Untuk mengaktifkan dan mengelola agen keamanan untuk GuardDuty Runtime Monitoring sumber daya ECS-Fargate, Anda harus menggunakannya secara langsung. GuardDuty Anda tidak dapat mengaktifkan atau mengelolanya secara manual untuk sumber daya ECS-Fargate. Untuk informasi tentang mengaktifkan dan mengelola agen keamanan, lihat [Prasyarat untuk dukungan AWS Fargate \(khusus Amazon ECS\)](#) dan [Mengelola agen keamanan otomatis untuk AWS Fargate \(khusus Amazon ECS\)](#) di [Panduan Pengguna Amazon](#). GuardDuty

[GuardDuty.13] GuardDuty EC2 Runtime Monitoring harus diaktifkan

Kategori: Deteksi > Layanan Deteksi

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::GuardDuty::Detector

AWS Config aturan: [guardduty-ec2-protection-runtime-enabled](#)

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah agen keamanan GuardDuty otomatis Amazon diaktifkan untuk pemantauan runtime EC2 instans Amazon. Untuk akun mandiri, kontrol gagal jika agen keamanan dinonaktifkan untuk akun tersebut. Dalam lingkungan multi-akun, kontrol gagal jika agen keamanan dinonaktifkan untuk akun GuardDuty administrator yang didelegasikan dan semua akun anggota.

Di lingkungan multi-akun, kontrol ini hanya menghasilkan temuan di akun GuardDuty administrator yang didelegasikan. Ini karena hanya GuardDuty administrator yang didelegasikan yang dapat mengaktifkan atau menonaktifkan Pemantauan Waktu Proses EC2 instans Amazon untuk akun di organisasi mereka. GuardDuty Akun anggota tidak dapat melakukan ini untuk akun mereka sendiri. Selain itu, kontrol ini menghasilkan FAILED temuan jika GuardDuty ditangguhkan untuk akun anggota dan Pemantauan Runtime EC2 instance dinonaktifkan untuk akun anggota. Untuk menerima PASSED temuan, GuardDuty administrator harus memisahkan akun anggota yang ditangguhkan dari akun administrator mereka dengan menggunakan GuardDuty.

GuardDuty Runtime Monitoring mengamati dan menganalisis tingkat sistem operasi, jaringan, dan peristiwa file untuk membantu Anda mendeteksi potensi ancaman dalam beban kerja tertentu AWS di lingkungan Anda. Ini menggunakan agen GuardDuty keamanan yang menambahkan visibilitas ke dalam perilaku runtime, seperti akses file, eksekusi proses, argumen baris perintah, dan koneksi jaringan. Anda dapat mengaktifkan dan mengelola agen keamanan untuk setiap jenis sumber daya yang ingin Anda pantau untuk potensi ancaman. Ini termasuk EC2 contoh Amazon.

Tindakan Perbaikan

Untuk informasi tentang mengonfigurasi dan mengelola agen keamanan otomatis untuk Pemantauan GuardDuty Waktu Proses EC2 instans, lihat [Prasyarat untuk dukungan instans EC2 Amazon dan Mengaktifkan agen keamanan otomatis untuk instans Amazon di Panduan Pengguna EC2 Amazon](#). GuardDuty

Kontrol Security Hub untuk AWS Identity and Access Management

AWS Security Hub Kontrol ini mengevaluasi layanan dan sumber daya AWS Identity and Access Management (IAM). Kontrol mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat [Ketersediaan kontrol berdasarkan Wilayah](#).

[IAM.1] Kebijakan IAM seharusnya tidak mengizinkan hak administratif “*” penuh

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v1.2.0/1.22, Tolok Ukur AWS Yayasan CIS v1.4.0/1.16,, NIST.800-53.r5 AC-2 (1), (15), (7), NIST.800-53.r5 AC-2,, (10), (2) NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (3), NIST.800-53.r5 AC-3 NIST.800-171.R2 3.1.4 NIST.800-53.r5 AC-5 NIST.800-53.r5 AC-6, NIST.800-53.r5 AC-6 PCI DSS v3.2.1/7.2.1 NIST.800-53.r5 AC-6 NIST.800-53.r5 AC-6

Kategori: Lindungi > Manajemen akses yang aman

Tingkat keparahan: Tinggi

Jenis sumber daya: AWS::IAM::Policy

AWS Config aturan: [iam-policy-no-statements-with-admin-access](#)

Jenis jadwal: Perubahan dipicu

Parameter:

- `excludePermissionBoundaryPolicy: true`(tidak dapat disesuaikan)

Kontrol ini memeriksa apakah versi default kebijakan IAM (juga dikenal sebagai kebijakan yang dikelola pelanggan) memiliki akses administrator dengan menyertakan pernyataan dengan "Effect": "Allow" with "Action": "*" over "Resource": "*". Kontrol gagal jika Anda memiliki kebijakan IAM dengan pernyataan seperti itu.

Kontrol hanya memeriksa kebijakan terkelola pelanggan yang Anda buat. Itu tidak memeriksa kebijakan sebaris dan AWS terkelola.

Kebijakan IAM mendefinisikan serangkaian hak istimewa yang diberikan kepada pengguna, grup, atau peran. Mengikuti saran keamanan standar, Anda AWS merekomendasikan agar Anda memberikan hak istimewa paling rendah, yang berarti hanya memberikan izin yang diperlukan untuk melakukan tugas. Bila Anda memberikan hak administratif penuh alih-alih set izin minimum yang dibutuhkan pengguna, Anda mengekspos sumber daya ke tindakan yang mungkin tidak diinginkan.

Alih-alih mengizinkan hak administratif penuh, tentukan apa yang perlu dilakukan pengguna dan kemudian buat kebijakan yang memungkinkan pengguna hanya melakukan tugas tersebut. Lebih aman untuk memulai dengan serangkaian izin minimum dan memberikan izin tambahan sesuai kebutuhan. Jangan memulai dengan izin yang terlalu lunak, lalu coba kencangkan nanti.

Anda harus menghapus kebijakan IAM yang memiliki pernyataan dengan "Effect": "Allow" with "Action": "*" over "Resource": "*".

Note

AWS Config harus diaktifkan di semua Wilayah tempat Anda menggunakan Security Hub. Namun, perekaman sumber daya global dapat diaktifkan dalam satu Wilayah. Jika Anda hanya merekam sumber daya global dalam satu Wilayah, maka Anda dapat menonaktifkan kontrol ini di semua Wilayah kecuali Wilayah tempat Anda merekam sumber daya global.

Tindakan Perbaikan

Untuk mengubah kebijakan IAM Anda sehingga tidak mengizinkan hak administratif "*" penuh, lihat [Mengedit kebijakan IAM](#) di Panduan Pengguna IAM.

[IAM.2] Pengguna IAM seharusnya tidak memiliki kebijakan IAM yang dilampirkan

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v3.0.0/1.15, Tolok Ukur Yayasan CIS AWS v1.2.0/1.16,, NIST.800-53.r5 AC-2 (1), (15), (7), (3), Nist.800-171.r2 3.1.1 NIST.800-53.r5 AC-2, Nist.800-171.r2 3.1.2 NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 Nist.800-171.r2

3.1.7, NIST.800-53.r5 AC-3 Nist.800-171.r2 3.3.9 NIST.800-53.r5 AC-6, NIST.800-53.r5 AC-6 Nist.800-171.r2 3.13.3, PCI DSS v3.2.1/7.2.1

Kategori: Lindungi > Manajemen akses yang aman

Tingkat keparahan: Rendah

Jenis sumber daya: AWS : : IAM : : User

AWS Config aturan: [iam-user-no-policies-check](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah pengguna IAM Anda memiliki kebijakan yang dilampirkan. Kontrol gagal jika pengguna IAM Anda memiliki kebijakan yang dilampirkan. Sebagai gantinya, pengguna IAM harus mewarisi izin dari grup IAM atau mengambil peran.

Secara default, pengguna, grup, dan peran IAM tidak memiliki akses ke AWS sumber daya. Kebijakan IAM memberikan hak istimewa kepada pengguna, grup, atau peran. Kami menyarankan Anda menerapkan kebijakan IAM secara langsung ke grup dan peran tetapi tidak untuk pengguna. Menetapkan hak istimewa di grup atau tingkat peran mengurangi kompleksitas manajemen akses seiring bertambahnya jumlah pengguna. Mengurangi kompleksitas manajemen akses pada gilirannya dapat mengurangi kesempatan bagi kepala sekolah untuk secara tidak sengaja menerima atau mempertahankan hak istimewa yang berlebihan.

Note

AWS Config harus diaktifkan di semua Wilayah tempat Anda menggunakan Security Hub. Namun, perekaman sumber daya global dapat diaktifkan dalam satu Wilayah. Jika Anda hanya merekam sumber daya global dalam satu Wilayah, Anda dapat menonaktifkan kontrol ini di semua Wilayah kecuali Wilayah tempat Anda merekam sumber daya global.

Tindakan Perbaikan

Untuk mengatasi masalah ini, [buat grup IAM](#), dan lampirkan kebijakan ke grup. Kemudian, [tambahkan pengguna ke grup](#). Kebijakan ini diterapkan ke setiap pengguna dalam grup. Untuk menghapus kebijakan yang dilampirkan langsung ke pengguna, lihat [Menambahkan dan menghapus izin identitas IAM](#) di Panduan Pengguna IAM.

[IAM.3] Kunci akses pengguna IAM harus diputar setiap 90 hari atau kurang

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v3.0.0/1.14, Tolok Ukur Yayasan CIS v1.4.0/1.14, Tolok Ukur AWS Yayasan CIS v1.2.0/1.4, (1), (3), NIST.800-53.r5 AC-2 (15), PCI DSS AWS v4.0.1/8.3.9, PCI DSS v4.0.1/8.6.3 NIST.800-53.r5 AC-2 NIST.800-53.r5 AC-3

Kategori: Lindungi > Manajemen akses yang aman

Tingkat keparahan: Sedang

Jenis sumber daya: AWS : : IAM : : User

AWS Config aturan: [access-keys-rotated](#)

Jenis jadwal: Periodik

Parameter:

- `maxAccessKeyAge`: 90 (tidak dapat disesuaikan)

Kontrol ini memeriksa apakah kunci akses aktif diputar dalam 90 hari.

Kami sangat menyarankan Anda untuk tidak membuat dan menghapus semua access key di akun Anda. Sebaliknya, praktik terbaik yang disarankan adalah membuat satu atau lebih peran IAM atau menggunakan [federasi](#) melalui AWS IAM Identity Center. Anda dapat menggunakan metode ini untuk memungkinkan pengguna Anda mengakses AWS Management Console dan AWS CLI.

Setiap pendekatan memiliki kasus penggunaannya. Federasi umumnya lebih baik untuk perusahaan yang memiliki direktori pusat yang ada atau berencana untuk membutuhkan lebih dari batas saat ini pada pengguna IAM. Aplikasi yang berjalan di luar AWS lingkungan membutuhkan kunci akses untuk akses terprogram ke AWS sumber daya.

Namun, jika sumber daya yang membutuhkan akses terprogram berjalan di dalam AWS, praktik terbaik adalah menggunakan peran IAM. Peran memungkinkan Anda memberikan akses sumber daya tanpa melakukan hardcoding ID kunci akses dan secret access key ke dalam konfigurasi.

Untuk mempelajari selengkapnya tentang melindungi kunci akses dan akun Anda, lihat [Praktik terbaik untuk mengelola kunci AWS akses](#) di Referensi Umum AWS. Lihat juga [pedoman posting blog untuk melindungi Anda Akun AWS saat menggunakan akses terprogram](#).

Jika Anda sudah memiliki kunci akses, Security Hub merekomendasikan agar Anda memutar kunci akses setiap 90 hari. Memutar kunci akses mengurangi kemungkinan kunci akses yang terkait

dengan akun yang disusupi atau dihentikan digunakan. Ini juga memastikan bahwa data tidak dapat diakses dengan kunci lama yang mungkin telah hilang, retak, atau dicuri. Selalu perbarui aplikasi Anda setelah Anda memutar tombol akses.

Access key ini terdiri dari access key ID dan secret access key. Mereka digunakan untuk menandatangani permintaan terprogram yang Anda buat untuk AWS. Pengguna memerlukan kunci akses mereka sendiri untuk melakukan panggilan terprogram AWS dari AWS CLI, Alat untuk Windows PowerShell AWS SDKs, atau panggilan HTTP langsung menggunakan operasi API untuk individu Layanan AWS.

Jika organisasi Anda menggunakan AWS IAM Identity Center (Pusat Identitas IAM), pengguna Anda dapat masuk ke Active Directory, direktori Pusat Identitas IAM bawaan, atau [penyedia identitas lain \(iDP\) yang terhubung ke Pusat Identitas IAM](#). Mereka kemudian dapat dipetakan ke peran IAM yang memungkinkan mereka menjalankan AWS CLI perintah atau memanggil operasi AWS API tanpa perlu kunci akses. Untuk mempelajari lebih lanjut, lihat [Mengonfigurasi AWS CLI yang akan digunakan AWS IAM Identity Center](#) dalam Panduan AWS Command Line Interface Pengguna.

Note

AWS Config harus diaktifkan di semua Wilayah tempat Anda menggunakan Security Hub. Namun, perekaman sumber daya global dapat diaktifkan dalam satu Wilayah. Jika Anda hanya merekam sumber daya global dalam satu Wilayah, maka Anda dapat menonaktifkan kontrol ini di semua Wilayah kecuali Wilayah tempat Anda merekam sumber daya global.

Tindakan Perbaikan

Untuk memutar tombol akses yang lebih tua dari 90 hari, lihat [Memutar kunci akses](#) di Panduan Pengguna IAM. Ikuti petunjuk untuk setiap pengguna dengan usia kunci Access lebih dari 90 hari.

[IAM.4] Kunci akses pengguna root IAM seharusnya tidak ada

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v3.0.0/1.4, Tolok Ukur AWS Yayasan CIS v1.4.0/1.4, Tolok Ukur Yayasan CIS AWS v1.2.0/1.12, PCI DSS v3.2.1/2.1, PCI DSS v3.2.1/2.2, PCI DSS v3.2.1/7.2.1, (1), (15), (7),, (10), (2) NIST.800-53.r5 AC-2 NIST.800-53.r5 AC-3 NIST.800-53.r5 AC-3 NIST.800-53.r5 AC-6 NIST.800-53.r5 AC-6 NIST.800-53.r5 AC-6

Kategori: Lindungi > Manajemen akses yang aman

Tingkat keparahan: Kritis

Jenis sumber daya: AWS:::Account

AWS Config aturan: [iam-root-access-key-check](#)

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah kunci akses pengguna root ada.

Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. AWS access key menyediakan akses terprogram ke akun tertentu.

Security Hub merekomendasikan agar Anda menghapus semua kunci akses yang terkait dengan pengguna root. Ini membatasi vektor yang dapat digunakan untuk membahayakan akun Anda. Ini juga mendorong pembuatan dan penggunaan akun berbasis peran yang paling tidak memiliki hak istimewa.

Tindakan Perbaikan

Untuk menghapus kunci akses pengguna root, lihat [Menghapus kunci akses untuk pengguna root di Panduan Pengguna](#) IAM. Untuk menghapus kunci akses pengguna root dari Akun AWS dalam AWS GovCloud (US), lihat [Menghapus kunci akses pengguna root AWS GovCloud \(US\) akun saya](#) di Panduan AWS GovCloud (US) Pengguna.

[IAM.5] MFA harus diaktifkan untuk semua pengguna IAM yang memiliki kata sandi konsol

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v3.0.0/1.10, Tolok Ukur AWS Yayasan CIS v1.4.0/1.10, Tolok Ukur AWS Yayasan CIS v1.2.0/1.2, (1), (15), NIST.800-53.r5 AC-2 (1), (2), (6), (8), PCI NIST.800-53.r5 AC-3 DSS v4.0.1/8.4.2 NIST.800-53.r5 IA-2 NIST.800-53.r5 IA-2 NIST.800-53.r5 IA-2 NIST.800-53.r5 IA-2

Kategori: Lindungi > Manajemen akses yang aman

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::IAM::User

AWS Config aturan: [mfa-enabled-for-iam-console-access](#)

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah autentikasi AWS multi-faktor (MFA) diaktifkan untuk semua pengguna IAM yang menggunakan kata sandi konsol.

Autentikasi Multi-Faktor (MFA) menambahkan lapisan perlindungan ekstra di atas nama pengguna dan kata sandi. Dengan MFA diaktifkan, ketika pengguna masuk ke AWS situs web, mereka diminta untuk nama pengguna dan kata sandi mereka. Selain itu, mereka diminta untuk kode otentikasi dari perangkat MFA AWS mereka.

Kami menyarankan Anda mengaktifkan MFA untuk semua akun yang memiliki kata sandi konsol. MFA dirancang untuk memberikan peningkatan keamanan untuk akses konsol. Prinsipal otentikasi harus memiliki perangkat yang memancarkan kunci sensitif waktu dan harus memiliki pengetahuan tentang kredensi.

 Note

AWS Config harus diaktifkan di semua Wilayah tempat Anda menggunakan Security Hub. Namun, perekaman sumber daya global dapat diaktifkan dalam satu Wilayah. Jika Anda hanya merekam sumber daya global dalam satu Wilayah, maka Anda dapat menonaktifkan kontrol ini di semua Wilayah kecuali Wilayah tempat Anda merekam sumber daya global.

Tindakan Perbaikan

Untuk menambahkan MFA untuk pengguna IAM, lihat [Menggunakan autentikasi multi-faktor \(MFA\)](#) di Panduan Pengguna IAM. AWS

Kami menawarkan kunci keamanan MFA gratis untuk pelanggan yang memenuhi syarat. [Lihat apakah Anda memenuhi syarat, dan pesan kunci gratis Anda.](#)

[IAM.6] MFA perangkat keras harus diaktifkan untuk pengguna root

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v3.0.0/1.6, Tolok Ukur AWS Yayasan CIS v1.4.0/1.6, Tolok Ukur AWS Yayasan CIS v1.2.0/1.14, PCI DSS v3.2.1/8.3.1, (1), (15), NIST.800-53.r5 AC-2 (1), (2), (6), (8), PCI DSS v4.0.1/8.4.2 NIST.800-53.r5 AC-3 NIST.800-53.r5 IA-2 NIST.800-53.r5 IA-2 NIST.800-53.r5 IA-2 NIST.800-53.r5 IA-2

Kategori: Lindungi > Manajemen akses yang aman

Tingkat keparahan: Kritis

Jenis sumber daya: AWS:::Account

AWS Config aturan: [root-account-hardware-mfa-enabled](#)

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah Anda Akun AWS diaktifkan untuk menggunakan perangkat autentikasi multi-faktor perangkat keras (MFA) untuk masuk dengan kredensial pengguna root. Kontrol gagal jika MFA perangkat keras tidak diaktifkan atau perangkat MFA virtual diizinkan untuk masuk dengan kredensial pengguna root.

MFA virtual mungkin tidak menyediakan tingkat kerahasiaan yang sama dengan perangkat keras MFA. Kami menyarankan Anda menggunakan perangkat MFA virtual hanya saat Anda menunggu persetujuan pembelian perangkat keras atau perangkat keras Anda tiba. Untuk mempelajari selengkapnya, lihat [Menetapkan perangkat MFA virtual \(konsol\)](#) di Panduan Pengguna IAM.

Note

Security Hub mengevaluasi kontrol ini berdasarkan keberadaan kredensial pengguna root (profil login) di file. Akun AWS Kontrol menghasilkan PASSED temuan dalam kasus-kasus berikut:

- Kredensial pengguna root hadir di akun dan perangkat keras MFA diaktifkan untuk pengguna root.
- Kredensial pengguna root tidak ada di akun.

Kontrol menghasilkan FAILED temuan jika kredensial pengguna root ada di akun dan MFA perangkat keras tidak diaktifkan untuk pengguna root.

Tindakan Perbaikan

Untuk informasi tentang mengaktifkan MFA perangkat keras untuk pengguna root, [lihat Autentikasi multi-faktor untuk Pengguna root akun AWS](#) di Panduan Pengguna IAM.

Kami menawarkan kunci keamanan MFA gratis untuk pelanggan yang memenuhi syarat. Untuk menentukan apakah Anda memenuhi syarat, lihat Program [Kunci Keamanan MFA](#). FAQs

[IAM.7] Kebijakan kata sandi untuk pengguna IAM harus memiliki konfigurasi yang kuat

Persyaratan terkait: NIST.800-53.r5 AC-2 (1), (3), (15), NIST.800-53.r5 AC-2 (1), Nist.800-171.r2 3.5.2, NIST.800-53.r5 IA-5 Nist.800-171.r2 3.5.7, Nist.800-171.r2 3.5.8, Nist.800-171.r2 3.5.9, PCI DSS v4.0.1/8.3.6, PCI DSS v4.0.1/8.3.7 NIST.800-53.r5 AC-3

Kategori: Lindungi > Manajemen akses yang aman

Tingkat keparahan: Sedang

Jenis sumber daya: AWS:::Account

AWS Config aturan: [iam-password-policy](#)

Jenis jadwal: Periodik

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
RequireUppercaseCharacters	Diperlukan setidaknya satu karakter huruf besar	Boolean	true atau false	true
RequireLowercaseCharacters	Diperlukan setidaknya satu karakter kecil dalam kata sandi	Boolean	true atau false	true
RequireSymbols	Diperlukan setidaknya satu simbol dalam kata sandi	Boolean	true atau false	true
RequireNumbers	Diperlukan setidaknya satu angka dalam kata sandi	Boolean	true atau false	true
MinimumPasswordLength	Jumlah karakter minimum dalam kata sandi	Bilangan Bulat	8 untuk 128	8

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
PasswordReusePrevention	Jumlah rotasi kata sandi sebelum kata sandi lama dapat digunakan kembali	Bilangan Bulat	12 untuk 24	Tidak ada nilai default
MaxPasswordAge	Jumlah hari sebelum kedaluwarsa kata sandi	Bilangan Bulat	1 untuk 90	Tidak ada nilai default

Kontrol ini memeriksa apakah kebijakan kata sandi akun untuk pengguna IAM menggunakan konfigurasi yang kuat. Kontrol gagal jika kebijakan kata sandi tidak menggunakan konfigurasi yang kuat. Kecuali Anda memberikan nilai parameter khusus, Security Hub menggunakan nilai default yang disebutkan dalam tabel sebelumnya. `MaxPasswordAgeParameter` `PasswordReusePrevention` dan tidak memiliki nilai default, jadi jika Anda mengecualikan parameter ini, Security Hub mengabaikan jumlah rotasi kata sandi dan usia kata sandi saat mengevaluasi kontrol ini.

Untuk mengakses AWS Management Console, pengguna IAM memerlukan kata sandi. Sebagai praktik terbaik, Security Hub sangat merekomendasikan bahwa alih-alih membuat pengguna IAM, Anda menggunakan federasi. Federasi memungkinkan pengguna untuk menggunakan kredensi perusahaan mereka yang ada untuk masuk ke AWS Management Console. Gunakan AWS IAM Identity Center (IAM Identity Center) untuk membuat atau menyatukan pengguna, dan kemudian mengambil peran IAM ke dalam akun.

Untuk mempelajari lebih lanjut tentang penyedia identitas dan federasi, lihat [Penyedia identitas dan federasi](#) di Panduan Pengguna IAM. Untuk mempelajari selengkapnya tentang Pusat Identitas IAM, lihat [Panduan AWS IAM Identity Center Pengguna](#).

Jika Anda perlu menggunakan pengguna IAM, Security Hub menyarankan agar Anda menerapkan pembuatan kata sandi pengguna yang kuat. Anda dapat mengatur kebijakan kata sandi Akun AWS untuk menentukan persyaratan periode rotasi wajib untuk kata sandi. Saat Anda membuat atau mengubah kebijakan kata sandi, sebagian besar pengaturan kebijakan kata sandinya diterapkan saat pengguna mengubah kata sandinya. Beberapa pengaturan diterapkan dengan segera.

Tindakan Perbaikan

Untuk memperbarui kebijakan kata sandi, lihat [Menyetel kebijakan kata sandi akun untuk pengguna IAM](#) di Panduan Pengguna IAM.

[IAM.8] Kredensi pengguna IAM yang tidak digunakan harus dihapus

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v1.2.0/1.3,, NIST.800-53.r5 AC-2 (1), (3), NIST.800-53.r5 AC-2, (15), NIST.800-53.r5 AC-3 (7),, NIST.800-53.r5 AC-2 Nist.800-171.r2 3.1.2, PCI DSS v3.2.1/8.1.4 NIST.800-53.r5 AC-6, PCI DSS v4.0.1/8.2.6 NIST.800-53.r5 AC-3 NIST.800-53.r5 AC-3

Kategori: Lindungi > Manajemen akses yang aman

Tingkat keparahan: Sedang

Jenis sumber daya: AWS : : IAM : : User

AWS Config aturan: [iam-user-unused-credentials-check](#)

Jenis jadwal: Periodik

Parameter:

- `maxCredentialUsageAge`: 90 (tidak dapat disesuaikan)

Kontrol ini memeriksa apakah pengguna IAM Anda memiliki kata sandi atau kunci akses aktif yang belum digunakan selama 90 hari.

Pengguna IAM dapat mengakses AWS sumber daya menggunakan berbagai jenis kredensial, seperti kata sandi atau kunci akses.

Security Hub menyarankan agar Anda menghapus atau menonaktifkan semua kredensial yang tidak digunakan selama 90 hari atau lebih. Menonaktifkan atau menghapus kredensi yang tidak perlu mengurangi jendela peluang untuk kredensi yang terkait dengan akun yang disusupi atau ditinggalkan untuk digunakan.

Note

AWS Config harus diaktifkan di semua Wilayah tempat Anda menggunakan Security Hub. Namun, perekaman sumber daya global dapat diaktifkan dalam satu Wilayah. Jika Anda

hanya merekam sumber daya global dalam satu Wilayah, maka Anda dapat menonaktifkan kontrol ini di semua Wilayah kecuali Wilayah tempat Anda merekam sumber daya global.

Tindakan Perbaikan

Saat Anda melihat informasi pengguna di konsol IAM, ada kolom untuk usia kunci Access, Usia kata sandi, dan Aktivitas terakhir. Jika nilai di salah satu kolom ini lebih besar dari 90 hari, buat kredensial untuk pengguna tersebut tidak aktif.

Anda juga dapat menggunakan [laporan kredensi](#) untuk memantau pengguna dan mengidentifikasi mereka yang tidak memiliki aktivitas selama 90 hari atau lebih. Anda dapat mengunduh laporan kredensi dalam .csv format dari konsol IAM.

Setelah Anda mengidentifikasi akun yang tidak aktif atau kredensi yang tidak digunakan, nonaktifkan akun tersebut. Untuk instruksi, lihat [Membuat, mengubah, atau menghapus kata sandi pengguna IAM](#).

[IAM.9] MFA harus diaktifkan untuk pengguna root

Persyaratan terkait: PCI DSS v3.2.1/8.3.1, PCI DSS v4.0.1/8.4.2, Tolok Ukur Yayasan CIS v3.0.0/1.5, Tolok Ukur AWS Yayasan CIS v1.4.0/1.5, Tolok Ukur AWS Yayasan CIS v1.2.0/1.13, (1), (15), (1), (2), (6), (8) AWS NIST.800-53.r5 AC-2 NIST.800-53.r5 AC-3 NIST.800-53.r5 IA-2 NIST.800-53.r5 IA-2 NIST.800-53.r5 IA-2 NIST.800-53.r5 IA-2

Kategori: Lindungi > Manajemen akses yang aman

Tingkat keparahan: Kritis

Jenis sumber daya: AWS :: Account

AWS Config aturan: [root-account-mfa-enabled](#)

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah autentikasi multi-faktor (MFA) diaktifkan untuk pengguna akar IAM untuk masuk Akun AWS ke. AWS Management Console Kontrol gagal jika MFA tidak diaktifkan untuk pengguna root akun.

Pengguna root IAM Akun AWS memiliki akses lengkap ke semua layanan dan sumber daya di akun. Jika MFA diaktifkan, pengguna harus memasukkan nama pengguna, kata sandi, dan kode otentikasi dari perangkat AWS MFA mereka untuk masuk ke AWS Management Console MFA menambahkan lapisan perlindungan ekstra di atas nama pengguna dan kata sandi.

Kontrol ini menghasilkan PASSED temuan dalam kasus-kasus berikut:

- Kredensi pengguna root ada di akun dan MFA diaktifkan untuk pengguna root.
- Kredensi pengguna root tidak ada di akun.

Kontrol menghasilkan FAILED temuan jika kredensi pengguna root ada di akun dan MFA tidak diaktifkan untuk pengguna root.

Tindakan Perbaikan

Untuk informasi tentang mengaktifkan MFA untuk pengguna root, [lihat Autentikasi multi-faktor untuk Pengguna root akun AWS](#) Panduan Pengguna. Akun AWS Identity and Access Management

[IAM.10] Kebijakan kata sandi untuk pengguna IAM harus memiliki konfigurasi yang kuat

Persyaratan terkait: Nist.800-171.r2 3.5.2, Nist.800-171.r2 3.5.7, Nist.800-171.r2 3.5.8, Nist.800-171.r2 3.5.9, PCI DSS v3.2.1/8.1.4, PCI DSS v3.2.1/8.2.3, PCI DSS v3.2.1/8.2.4, PCI DSS v3.3.2.1/8.2.5

Kategori: Lindungi > Manajemen akses yang aman

Tingkat keparahan: Sedang

Jenis sumber daya: AWS :: Account

AWS Config aturan: [iam-password-policy](#)

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah kebijakan kata sandi akun untuk pengguna IAM menggunakan konfigurasi DSS PCI minimum berikut.

- `RequireUppercaseCharacters`— Memerlukan setidaknya satu karakter huruf besar dalam kata sandi. (Default = `true`)
- `RequireLowercaseCharacters`— Memerlukan setidaknya satu karakter huruf kecil dalam kata sandi. (Default = `true`)
- `RequireNumbers`— Diperlukan setidaknya satu angka dalam kata sandi. (Default = `true`)
- `MinimumPasswordLength`— Panjang minimum kata sandi. (Default = 7 atau lebih lama)
- `PasswordReusePrevention`— Jumlah kata sandi sebelum mengizinkan penggunaan kembali. (Default = 4)
- `MaxPasswordAge`— Jumlah hari sebelum kedaluwarsa kata sandi. (Default = 90)

 Note

Pada 30 Mei 2025, Security Hub menghapus kontrol ini dari standar PCI DSS v4.0.1. PCI DSS v4.0.1 sekarang membutuhkan kata sandi untuk memiliki minimal 8 karakter. Kontrol ini terus berlaku untuk standar PCI DSS v3.2.1, yang memiliki persyaratan kata sandi yang berbeda.

[Untuk mengevaluasi kebijakan kata sandi akun terhadap persyaratan PCI DSS v4.0.1, Anda dapat menggunakan kontrol IAM.7.](#) Kontrol ini membutuhkan kata sandi untuk memiliki minimal 8 karakter. Ini juga mendukung nilai khusus untuk panjang kata sandi dan parameter lainnya. Kontrol IAM.7 adalah bagian dari standar PCI DSS v4.0.1 di Security Hub.

Tindakan Perbaikan

Untuk memperbarui kebijakan kata sandi agar menggunakan konfigurasi yang disarankan, lihat [Menyetel kebijakan kata sandi akun untuk pengguna IAM](#) di Panduan Pengguna IAM.

[IAM.11] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu huruf besar

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v1.2.0/1.5, Nist.800-171.r2 3.5.2, Nist.800-171.r2 3.5.7, Nist.800-171.r2 3.5.8, Nist.800-171.r2 3.5.9, PCI DSS v4.0.1/8.3.6

Kategori: Lindungi > Manajemen akses yang aman

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS:::Account`

AWS Config aturan: [iam-password-policy](#)

Jenis jadwal: Periodik

Parameter: Tidak ada

Kebijakan kata sandi, sebagian, menegakkan persyaratan kompleksitas kata sandi. Gunakan kebijakan kata sandi IAM untuk memastikan bahwa kata sandi menggunakan kumpulan karakter yang berbeda.

CIS merekomendasikan bahwa kebijakan kata sandi memerlukan setidaknya satu huruf besar. Menyetel kebijakan kompleksitas kata sandi meningkatkan ketahanan akun terhadap upaya login brute force.

Tindakan Perbaikan

Untuk mengubah kebijakan kata sandi, lihat [Menyetel kebijakan kata sandi akun untuk pengguna IAM](#) di Panduan Pengguna IAM. Untuk kekuatan Kata Sandi, pilih Diperlukan setidaknya satu huruf besar dari alfabet Latin (A—Z).

[IAM.12] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu huruf kecil

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v1.2.0/1.6, Nist.800-171.r2 3.5.2, Nist.800-171.r2 3.5.7, Nist.800-171.r2 3.5.8, Nist.800-171.r2 3.5.9, PCI DSS v4.0.1/8.3.6

Kategori: Lindungi > Manajemen akses yang aman

Tingkat keparahan: Sedang

Jenis sumber daya: AWS :: Account

AWS Config aturan: [iam-password-policy](#)

Jenis jadwal: Periodik

Parameter: Tidak ada

Kebijakan kata sandi, sebagian, menegakkan persyaratan kompleksitas kata sandi. Gunakan kebijakan kata sandi IAM untuk memastikan bahwa kata sandi menggunakan kumpulan karakter yang berbeda. CIS merekomendasikan bahwa kebijakan kata sandi memerlukan setidaknya satu huruf kecil. Menyetel kebijakan kompleksitas kata sandi meningkatkan ketahanan akun terhadap upaya login brute force.

Tindakan Perbaikan

Untuk mengubah kebijakan kata sandi, lihat [Menyetel kebijakan kata sandi akun untuk pengguna IAM](#) di Panduan Pengguna IAM. Untuk kekuatan Kata Sandi, pilih Diperlukan setidaknya satu huruf kecil dari alfabet Latin (A—Z).

[IAM.13] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu simbol

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v1.2.0/1.7, Nist.800-171.r2 3.5.2, Nist.800-171.r2 3.5.7, Nist.800-171.r2 3.5.8, Nist.800-171.r2 3.5.9, PCI DSS v4.0.1/8.3.6

Kategori: Lindungi > Manajemen akses yang aman

Tingkat keparahan: Sedang

Jenis sumber daya: AWS:::Account

AWS Config aturan: [iam-password-policy](#)

Jenis jadwal: Periodik

Parameter: Tidak ada

Kebijakan kata sandi, sebagian, menegakkan persyaratan kompleksitas kata sandi. Gunakan kebijakan kata sandi IAM untuk memastikan bahwa kata sandi menggunakan kumpulan karakter yang berbeda.

CIS merekomendasikan bahwa kebijakan kata sandi memerlukan setidaknya satu simbol. Menyetel kebijakan kompleksitas kata sandi meningkatkan ketahanan akun terhadap upaya login brute force.

Tindakan Perbaikan

Untuk mengubah kebijakan kata sandi, lihat [Menyetel kebijakan kata sandi akun untuk pengguna IAM](#) di Panduan Pengguna IAM. Untuk kekuatan Password, pilih Memerlukan setidaknya satu karakter nonalfanumerik.

[IAM.14] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu nomor

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v1.2.0/1.8, Nist.800-171.r2 3.5.2, Nist.800-171.r2 3.5.7, Nist.800-171.r2 3.5.8, Nist.800-171.r2 3.5.9, PCI DSS v4.0.1/8.3.6

Kategori: Lindungi > Manajemen akses yang aman

Tingkat keparahan: Sedang

Jenis sumber daya: AWS :: Account

AWS Config aturan: [iam-password-policy](#)

Jenis jadwal: Periodik

Parameter: Tidak ada

Kebijakan kata sandi, sebagian, menegakkan persyaratan kompleksitas kata sandi. Gunakan kebijakan kata sandi IAM untuk memastikan bahwa kata sandi menggunakan kumpulan karakter yang berbeda.

CIS merekomendasikan bahwa kebijakan kata sandi memerlukan setidaknya satu nomor. Menyetel kebijakan kompleksitas kata sandi meningkatkan ketahanan akun terhadap upaya login brute force.

Tindakan Perbaikan

Untuk mengubah kebijakan kata sandi, lihat [Menyetel kebijakan kata sandi akun untuk pengguna IAM](#) di Panduan Pengguna IAM. Untuk kekuatan Kata Sandi, pilih Memerlukan setidaknya satu nomor.

[IAM.15] Pastikan kebijakan kata sandi IAM membutuhkan panjang kata sandi minimum 14 atau lebih

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v3.0.0/1.8, Tolok Ukur Yayasan CIS v1.4.0/1.8, Tolok Ukur AWS Yayasan CIS v1.2.0/1.9, Nist.800-171.r2 3.5.2, Nist.800-171.r2 3.5.7, Nist.800-171.r2 3.5.8, AWS Nist.800-171.r2 3.5.9

Kategori: Lindungi > Manajemen akses yang aman

Tingkat keparahan: Sedang

Jenis sumber daya: AWS :: Account

AWS Config aturan: [iam-password-policy](#)

Jenis jadwal: Periodik

Parameter: Tidak ada

Kebijakan kata sandi, sebagian, menegakkan persyaratan kompleksitas kata sandi. Gunakan kebijakan kata sandi IAM untuk memastikan bahwa kata sandi setidaknya memiliki panjang tertentu.

CIS merekomendasikan bahwa kebijakan kata sandi memerlukan panjang kata sandi minimum 14 karakter. Menyetel kebijakan kompleksitas kata sandi meningkatkan ketahanan akun terhadap upaya login brute force.

Tindakan Perbaikan

Untuk mengubah kebijakan kata sandi, lihat [Menyetel kebijakan kata sandi akun untuk pengguna IAM](#) di Panduan Pengguna IAM. Untuk panjang minimum Kata Sandi, masukkan **14** atau nomor yang lebih besar.

[IAM.16] Pastikan kebijakan kata sandi IAM mencegah penggunaan kembali kata sandi

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v3.0.0/1.9, Tolok Ukur Yayasan CIS v1.4.0/1.9, Tolok Ukur AWS Yayasan CIS v1.2.0/1.10, Nist.800-171.r2 3.5.2, AWS Nist.800-171.r2 3.5.7, Nist.800-171.r2 3.5.8, Nist.800-171.r2 3.5.9, PCI DSS v4.0.1/8.3.7

Kategori: Lindungi > Manajemen akses yang aman

Tingkat keparahan: Rendah

Jenis sumber daya: AWS :: Account

AWS Config aturan: [iam-password-policy](#)

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah jumlah kata sandi yang harus diingat diatur ke 24. Kontrol gagal jika nilainya tidak 24.

Kebijakan kata sandi IAM dapat mencegah penggunaan kembali kata sandi yang diberikan oleh pengguna yang sama.

CIS merekomendasikan agar kebijakan kata sandi mencegah penggunaan kembali kata sandi. Mencegah penggunaan kembali kata sandi meningkatkan ketahanan akun terhadap upaya login brute force.

Tindakan Perbaikan

Untuk mengubah kebijakan kata sandi, lihat [Menyetel kebijakan kata sandi akun untuk pengguna IAM](#) di Panduan Pengguna IAM. Untuk Mencegah penggunaan kembali kata sandi, masukkan **24**.

[IAM.17] Pastikan kebijakan kata sandi IAM kedaluwarsa kata sandi dalam waktu 90 hari atau kurang

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v1.2.0/1.11, Nist.800-171.r2 3.5.2, Nist.800-171.r2 3.5.7, Nist.800-171.r2 3.5.8, Nist.800-171.r2 3.5.9, PCI DSS v4.0.1/8.3.9

Kategori: Lindungi > Manajemen akses yang aman

Tingkat keparahan: Rendah

Jenis sumber daya: AWS :: Account

AWS Config aturan: [iam-password-policy](#)

Jenis jadwal: Periodik

Parameter: Tidak ada

Kebijakan kata sandi IAM dapat mengharuskan kata sandi diputar atau kedaluwarsa setelah beberapa hari tertentu.

CIS merekomendasikan agar kebijakan kata sandi kedaluwarsa kata sandi setelah 90 hari atau kurang. Mengurangi masa pakai kata sandi meningkatkan ketahanan akun terhadap upaya login brute force. Mengharuskan perubahan kata sandi reguler juga membantu dalam skenario berikut:

- Kata sandi dapat dicuri atau dikompromikan tanpa sepengetahuan Anda. Ini dapat terjadi melalui kompromi sistem, kerentanan perangkat lunak, atau ancaman internal.
- Filter web perusahaan dan pemerintah tertentu atau server proxy dapat mencegat dan merekam lalu lintas bahkan jika itu dienkripsi.
- Banyak orang menggunakan kata sandi yang sama untuk banyak sistem seperti pekerjaan, email, dan pribadi.
- Workstation pengguna akhir yang dikompromikan mungkin memiliki keystroke logger.

Tindakan Perbaikan

Untuk mengubah kebijakan kata sandi, lihat [Menyetel kebijakan kata sandi akun untuk pengguna IAM](#) di Panduan Pengguna IAM. Untuk Aktifkan kedaluwarsa kata sandi, masukkan **90** atau nomor yang lebih kecil.

[IAM.18] Memastikan peran dukungan telah dibuat untuk mengelola insiden dengan AWS Dukungan

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v3.0.0/1.17, Tolok Ukur Yayasan CIS v1.4.0/1.17, Tolok Ukur AWS Yayasan CIS v1.2.0/1.20, NIST.800-171.R2 3.1.2, PCI DSS v4.0.1/12.10.3 AWS

Kategori: Lindungi > Manajemen akses yang aman

Tingkat keparahan: Rendah

Jenis sumber daya: AWS:::Account

AWS Config aturan: [iam-policy-in-use](#)

Jenis jadwal: Periodik

Parameter:

- policyARN: arn:*partition*:iam::aws:policy/AWSSupportAccess (tidak dapat disesuaikan)
- policyUsageType: ANY (tidak dapat disesuaikan)

AWS menyediakan pusat dukungan yang dapat digunakan untuk pemberitahuan dan respons insiden, serta dukungan teknis dan layanan pelanggan.

Buat peran IAM untuk memungkinkan pengguna yang berwenang mengelola insiden dengan Support AWS . Dengan menerapkan hak istimewa terkecil untuk kontrol akses, peran IAM akan memerlukan kebijakan IAM yang sesuai untuk memungkinkan akses pusat dukungan untuk mengelola insiden dengan. Dukungan

Note

AWS Config harus diaktifkan di semua Wilayah tempat Anda menggunakan Security Hub. Namun, perekaman sumber daya global dapat diaktifkan dalam satu Wilayah. Jika Anda hanya merekam sumber daya global dalam satu Wilayah, maka Anda dapat menonaktifkan kontrol ini di semua Wilayah kecuali Wilayah tempat Anda merekam sumber daya global.

Tindakan Perbaikan

Untuk mengatasi masalah ini, buat peran untuk memungkinkan pengguna yang berwenang mengelola Dukungan insiden.

Untuk membuat peran yang akan digunakan untuk Dukungan akses

1. Buka konsol IAM di <https://console.aws.amazon.com/iam/>.
2. Di panel navigasi IAM, pilih Peran, lalu pilih Buat peran.
3. Untuk tipe Peran, pilih Yang Lain Akun AWS.
4. Untuk ID Akun, masukkan Akun AWS ID yang Akun AWS ingin Anda beri akses ke sumber daya Anda.

Jika pengguna atau grup yang akan mengambil peran ini berada di akun yang sama, maka masukkan nomor akun lokal.

Note

Administrator akun yang ditentukan dapat memberikan izin untuk mengasumsikan peran ini kepada setiap pengguna dalam akun tersebut. Untuk melakukannya, administrator melampirkan kebijakan kepada pengguna atau grup yang memberikan izin untuk tindakan `sts:AssumeRole`. Dalam kebijakan itu, sumber daya harus menjadi peran ARN.

5. Pilih Berikutnya: Izin.
6. Cari kebijakan terkelola `AWSSupportAccess`.
7. Pilih kotak centang untuk kebijakan `AWSSupportAccess` terkelola.
8. Pilih Berikutnya: Tanda.
9. (Opsional) Untuk menambahkan metadata ke peran, lampirkan tag sebagai pasangan nilai kunci.

Untuk informasi selengkapnya tentang penggunaan tag di IAM, lihat [Menandai pengguna dan peran IAM dalam Panduan](#) Pengguna IAM.

10. Pilih Berikutnya: Tinjauan.
11. Untuk Nama peran, masukkan nama peran Anda.

Nama peran harus unik di Akun AWS. Mereka tidak peka dengan huruf besar/kecil.

12. (Opsional) Untuk Deskripsi peran, masukkan deskripsi.

13. Tinjau peran, lalu pilih Buat peran.

[IAM.19] MFA harus diaktifkan untuk semua pengguna IAM

Persyaratan terkait: NIST.800-53.r5 AC-2 (1), (15), (1), NIST.800-53.r5 AC-3 (2), (6), NIST.800-53.r5 IA-2 (8), Nist.800-171.r2 3.3.8, NIST.800-53.r5 IA-2 Nist.800-171.r2 3.5.3, NIST.800-53.r5 IA-2 Nist.800-171.r2 3.5.4, Nist.800-171.r2 3.7.5, PCI DSS v3.2.1/8.3.1, PCI DSS v3.2.1/8.3.1, PCI DSS v4.0.1/8.4.2, NIST.800-53.r5 IA-2

Kategori: Lindungi > Manajemen akses yang aman

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::IAM::User

AWS Config aturan: [iam-user-mfa-enabled](#)

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah pengguna IAM mengaktifkan autentikasi multi-faktor (MFA).

Note

AWS Config harus diaktifkan di semua Wilayah tempat Anda menggunakan Security Hub. Namun, perekaman sumber daya global dapat diaktifkan dalam satu Wilayah. Jika Anda hanya merekam sumber daya global dalam satu Wilayah, maka Anda dapat menonaktifkan kontrol ini di semua Wilayah kecuali Wilayah tempat Anda merekam sumber daya global.

Tindakan Perbaikan

Untuk menambahkan MFA bagi pengguna IAM, lihat Mengaktifkan [perangkat MFA untuk pengguna di AWS Panduan Pengguna](#) IAM.

[IAM.20] Hindari penggunaan pengguna root

Important

Security Hub menghentikan kontrol ini pada April 2024. Untuk informasi selengkapnya, lihat [Ubah log untuk kontrol CSPM Security Hub](#).

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v1.2.0/1.1

Kategori: Lindungi > Manajemen akses yang aman

Tingkat keparahan: Rendah

Jenis sumber daya: AWS::IAM::User

AWS Config aturan: use-of-root-account-test (aturan Security Hub khusus)

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah akun AWS memiliki batasan pada penggunaan pengguna root. Kontrol mengevaluasi sumber daya berikut:

- Topik Amazon Simple Notification Service (Amazon SNS)
- AWS CloudTrail Jejak
- Filter metrik yang terkait dengan CloudTrail jejak
- CloudWatch Alarm Amazon berdasarkan filter

Pemeriksaan ini menghasilkan FAILED temuan jika satu atau lebih pernyataan berikut ini benar:

- Tidak ada CloudTrail jejak di akun.
- CloudTrail Jejak diaktifkan, tetapi tidak dikonfigurasi dengan setidaknya satu jejak Multi-wilayah yang mencakup acara manajemen baca dan tulis.
- CloudTrail Jejak diaktifkan, tetapi tidak terkait dengan grup CloudWatch log Log.
- Filter metrik yang tepat yang ditentukan oleh Pusat Keamanan Internet (CIS) tidak digunakan. Filter metrik yang ditentukan adalah '`${.userIdentity.type="Root" && $.userIdentity.invokedBy NOT EXISTS && $.eventType != "AwsServiceEvent"}`'.

- Tidak ada CloudWatch alarm berdasarkan filter metrik di akun.
- CloudWatch alarm yang dikonfigurasi untuk mengirim notifikasi ke topik SNS terkait tidak dipicu berdasarkan kondisi alarm.
- Topik SNS tidak sesuai dengan [kendala untuk mengirim pesan ke](#) topik SNS.
- Topik SNS tidak memiliki setidaknya satu pelanggan.

Pemeriksaan ini menghasilkan status kontrol NO_DATA jika satu atau lebih pernyataan berikut ini benar:

- Jejak multi-wilayah berbasis di Wilayah yang berbeda. Security Hub hanya dapat menghasilkan temuan di Wilayah tempat jejak itu berada.
- Jejak multi-wilayah milik akun yang berbeda. Security Hub hanya dapat menghasilkan temuan untuk akun yang memiliki jejak.

Pemeriksaan ini menghasilkan status kontrol WARNING jika satu atau lebih pernyataan berikut ini benar:

- Akun saat ini tidak memiliki topik SNS yang direferensikan dalam alarm. CloudWatch
- Akun saat ini tidak memiliki akses ke topik SNS saat menjalankan ListSubscriptionsByTopic SNS API.

Note

Sebaiknya gunakan jejak organisasi untuk mencatat peristiwa dari banyak akun di suatu organisasi. Jejak organisasi adalah jalur Multi-wilayah secara default dan hanya dapat dikelola oleh akun AWS Organizations manajemen atau akun administrator yang CloudTrail didelegasikan. Menggunakan jejak organisasi menghasilkan status kontrol NO_DATA untuk kontrol yang dievaluasi di akun anggota organisasi. Di akun anggota, Security Hub hanya menghasilkan temuan untuk sumber daya milik anggota. Temuan yang berkaitan dengan jejak organisasi dihasilkan di akun pemilik sumber daya. Anda dapat melihat temuan ini di akun administrator yang didelegasikan Security Hub menggunakan agregasi lintas wilayah.

Sebagai praktik terbaik, gunakan kredensial pengguna akar Anda hanya saat diperlukan untuk [melakukan tugas manajemen akun dan layanan](#). Terapkan kebijakan IAM secara langsung ke grup

dan peran tetapi tidak untuk pengguna. Untuk instruksi pengaturan administrator untuk penggunaan sehari-hari, lihat [Membuat pengguna dan grup admin IAM pertama Anda](#) dalam Panduan Pengguna IAM.

Tindakan Perbaikan

Langkah-langkah untuk mengatasi masalah ini termasuk menyiapkan topik Amazon SNS, jejak, CloudTrail filter metrik, dan alarm untuk filter metrik.

Untuk membuat topik Amazon SNS

1. [Buka konsol Amazon SNS di https://console.aws.amazon.com/sns/v3/home](https://console.aws.amazon.com/sns/v3/home).
2. Buat topik Amazon SNS yang menerima semua alarm CIS.

Buat setidaknya satu pelanggan ke topik. Untuk informasi lebih lanjut, lihat [Memulai dengan Amazon SNS](#) di Panduan Developer Amazon Simple Notification Service.

Selanjutnya, siapkan aktif CloudTrail yang berlaku untuk semua Wilayah. Untuk melakukannya, ikuti langkah-langkah perbaikan di [the section called “\[CloudTrail.1\] CloudTrail harus diaktifkan dan dikonfigurasi dengan setidaknya satu jejak Multi-wilayah yang mencakup acara manajemen baca dan tulis”](#).

Catat nama grup CloudWatch log Log yang Anda kaitkan dengan CloudTrail jejak. Anda membuat filter metrik untuk grup log tersebut.

Terakhir, buat filter metrik dan alarm.

Untuk membuat filter metrik dan alarm

1. Buka CloudWatch konsol di <https://console.aws.amazon.com/cloudwatch/>.
2. Pada panel navigasi, pilih Grup log.
3. Pilih kotak centang untuk grup CloudWatch log Log yang terkait dengan CloudTrail jejak yang Anda buat.
4. Dari Tindakan, pilih Buat Filter Metrik.
5. Di bawah Definisikan pola, lakukan hal berikut:
 - a. Salin pola berikut, lalu tempelkan ke bidang Pola Filter.

```
{$.userIdentity.type="Root" && $.userIdentity.invokedBy NOT EXISTS && $.eventType != "AwsServiceEvent"}
```

- b. Pilih Berikutnya.
6. Di Assign Metrik, lakukan hal berikut:
 - a. Di Nama filter, masukkan nama untuk filter metrik Anda.
 - b. Untuk Metric Namespace, masukkan. **LogMetrics**

Jika Anda menggunakan namespace yang sama untuk semua filter metrik log CIS Anda, maka semua metrik Benchmark CIS dikelompokkan bersama.
 - c. Untuk Metric Name (Nama metrik), masukkan nama untuk metrik. Ingat nama metrik. Anda harus memilih metrik saat Anda membuat alarm.
 - d. Untuk Metric value (Nilai metrik), masukkan **1**.
 - e. Pilih Berikutnya.
7. Di bawah Tinjau dan buat, verifikasi informasi yang Anda berikan untuk filter metrik baru. Kemudian, pilih Buat filter metrik.
8. Di panel navigasi, pilih Grup log, lalu pilih filter yang Anda buat di bawah Filter metrik.
9. Pilih kotak centang untuk filter. Pilih Buat alarm.
10. Di Bawah Tentukan metrik dan kondisi, lakukan hal berikut:
 - a. Di bawah Kondisi, untuk Ambang Batas, pilih Statis.
 - b. Untuk Tentukan kondisi alarm, pilih Greater/Equal.
 - c. Untuk Tentukan nilai ambang batas, masukkan **1**.
 - d. Pilih Berikutnya.
11. Di bawah Mengkonfigurasi tindakan, lakukan hal berikut:
 - a. Di bawah Pemicu status alarm, pilih Dalam alarm.
 - b. Di bawah Pilih topik SNS, pilih Pilih topik SNS yang sudah ada.
 - c. Untuk Kirim notifikasi ke, masukkan nama topik SNS yang Anda buat di prosedur sebelumnya.
 - d. Pilih Berikutnya.
12. Di bawah Tambahkan nama dan deskripsi, masukkan Nama dan Deskripsi untuk alarm, seperti **CIS-1.1-RootAccountUsage**. Lalu pilih Selanjutnya.

13. Di bawah Pratinjau dan buat, tinjau konfigurasi alarm. Kemudian pilih Buat alarm.

[IAM.21] Kebijakan terkelola pelanggan IAM yang Anda buat seharusnya tidak mengizinkan tindakan wildcard untuk layanan

Persyaratan terkait: NIST.800-53.r5 AC-2, NIST.800-53.r5 AC-2 (1),, (15), (7),,, (10) NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (2), NIST.800-53.r5 AC-6 (3), NIST.800-53.r5 AC-3 Nist.800-171.r2 3.1.1, Nist.800-171.r2 3.1.2 NIST.800-53.r5 AC-5 NIST.800-53.r5 AC-6, NIST.800-53.r5 AC-6 Nist.800-171.r2 3.1.5, NIST.800-53.r5 AC-6 Nist.800-171.r2 3.1.7, Nist.800-171.r2 3.3.8, Nist.800-171.r2 3.3.8, Nist.800-171.r2 St.800-171.r2 3.3.9, Nist.800-171.r2 3.13.3, Nist.800-171.r2 3.13.4

Kategori: Deteksi > Manajemen akses aman

Tingkat keparahan: Rendah

Jenis sumber daya: AWS::IAM::Policy

AWS Config aturan: [iam-policy-no-statements-with-full-access](#)

Jenis jadwal: Perubahan dipicu

Parameter:

- `excludePermissionBoundaryPolicy`: True (tidak dapat disesuaikan)

Kontrol ini memeriksa apakah kebijakan berbasis identitas IAM yang Anda buat memiliki pernyataan Izinkan yang menggunakan wildcard * untuk memberikan izin untuk semua tindakan pada layanan apa pun. Kontrol gagal jika ada pernyataan kebijakan yang disertakan "Effect": "Allow" dengan "Action": "Service:*".

Misalnya, pernyataan berikut dalam kebijakan menghasilkan temuan yang gagal.

```
"Statement": [
{
  "Sid": "EC2-Wildcard",
  "Effect": "Allow",
  "Action": "ec2:*",
  "Resource": "*"
}
```

```
}
```

Kontrol juga gagal jika Anda menggunakannya "Effect": "Allow""NotAction": "**service**: *". Dalam hal ini, NotAction elemen menyediakan akses ke semua tindakan dalam Layanan AWS, kecuali untuk tindakan yang ditentukan dalamNotAction.

Kontrol ini hanya berlaku untuk kebijakan IAM yang dikelola pelanggan. Ini tidak berlaku untuk kebijakan IAM yang dikelola oleh AWS.

Saat Anda menetapkan izin Layanan AWS, penting untuk mencakup tindakan IAM yang diizinkan dalam kebijakan IAM Anda. Anda harus membatasi tindakan IAM hanya pada tindakan yang diperlukan. Ini membantu Anda memberikan izin hak istimewa paling sedikit. Kebijakan yang terlalu permisif dapat menyebabkan eskalasi hak istimewa jika kebijakan tersebut dilampirkan pada prinsipal IAM yang mungkin tidak memerlukan izin.

Dalam beberapa kasus, Anda mungkin ingin mengizinkan tindakan IAM yang memiliki awalan serupa, seperti DescribeFlowLogs dan. DescribeAvailabilityZones Dalam kasus resmi ini, Anda dapat menambahkan wildcard akhiran ke awalan umum. Misalnya, ec2:Describe*.

Kontrol ini lolos jika Anda menggunakan tindakan IAM awalan dengan wildcard berakhiran. Misalnya, pernyataan berikut dalam kebijakan menghasilkan temuan yang dilewatkan.

```
"Statement": [  
  {  
    "Sid": "EC2-Wildcard",  
    "Effect": "Allow",  
    "Action": "ec2:Describe*",  
    "Resource": "*"   
  }  
]
```

Saat mengelompokkan tindakan IAM terkait dengan cara ini, Anda juga dapat menghindari melebihi batas ukuran kebijakan IAM.

Note

AWS Config harus diaktifkan di semua Wilayah tempat Anda menggunakan Security Hub. Namun, perekaman sumber daya global dapat diaktifkan dalam satu Wilayah. Jika Anda hanya merekam sumber daya global dalam satu Wilayah, maka Anda dapat menonaktifkan kontrol ini di semua Wilayah kecuali Wilayah tempat Anda merekam sumber daya global.

Tindakan Perbaikan

Untuk mengatasi masalah ini, perbarui kebijakan IAM Anda sehingga tidak mengizinkan hak administratif “*” penuh. Untuk detail tentang cara mengedit kebijakan IAM, lihat [Mengedit kebijakan IAM di Panduan Pengguna IAM](#).

[IAM.22] Kredensi pengguna IAM yang tidak digunakan selama 45 hari harus dihapus

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v3.0.0/1.12, Tolok Ukur Yayasan CIS v1.4.0/1.12, NIST.800-171.R2 3.1.2 AWS

Kategori: Lindungi > Manajemen akses yang aman

Tingkat keparahan: Sedang

Jenis sumber daya: AWS : : IAM : : User

AWS Config aturan: [iam-user-unused-credentials-check](#)

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah pengguna IAM Anda memiliki kata sandi atau kunci akses aktif yang belum digunakan selama 45 hari atau lebih. Untuk melakukannya, ia memeriksa apakah `maxCredentialUsageAge` parameter AWS Config aturan sama dengan 45 atau lebih.

Pengguna dapat mengakses AWS sumber daya menggunakan berbagai jenis kredensial, seperti kata sandi atau kunci akses.

CIS merekomendasikan agar Anda menghapus atau menonaktifkan semua kredensial yang telah tidak digunakan selama 45 hari atau lebih. Menonaktifkan atau menghapus kredensi yang tidak perlu mengurangi jendela peluang untuk kredensi yang terkait dengan akun yang disusupi atau ditinggalkan untuk digunakan.

AWS Config Aturan untuk kontrol ini menggunakan operasi [GenerateCredentialReport](#) API [GetCredentialReport](#) dan, yang hanya diperbarui setiap empat jam. Perubahan pada pengguna IAM dapat memakan waktu hingga empat jam untuk dapat dilihat oleh kontrol ini.

Note

AWS Config harus diaktifkan di semua Wilayah tempat Anda menggunakan Security Hub. Namun, Anda dapat mengaktifkan perekaman sumber daya global dalam satu Wilayah.

Jika Anda hanya merekam sumber daya global dalam satu Wilayah, maka Anda dapat menonaktifkan kontrol ini di semua Wilayah kecuali Wilayah tempat Anda merekam sumber daya global.

Tindakan Perbaikan

Saat Anda melihat informasi pengguna di konsol IAM, ada kolom untuk usia kunci Access, Usia kata sandi, dan Aktivitas terakhir. Jika nilai di salah satu kolom ini lebih besar dari 45 hari, buat kredensial untuk pengguna tersebut tidak aktif.

Anda juga dapat menggunakan [laporan kredensi](#) untuk memantau pengguna dan mengidentifikasi mereka yang tidak memiliki aktivitas selama 45 hari atau lebih. Anda dapat mengunduh laporan kredensi dalam .csv format dari konsol IAM.

Setelah Anda mengidentifikasi akun yang tidak aktif atau kredensi yang tidak digunakan, nonaktifkan akun tersebut. Untuk instruksi, lihat [Membuat, mengubah, atau menghapus kata sandi pengguna IAM](#).

[IAM.23] Penganalisis Akses IAM harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: AWS::AccessAnalyzer::Analyzer

AWS Config aturan: tagged-accessanalyzer-analyzer (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
requiredTagKeys	Daftar kunci tag non-sistem yang harus berisi sumber daya	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi	No default value

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
	yang dievaluasi. Kunci tag peka huruf besar dan kecil.		persyaratan AWS .	

Kontrol ini memeriksa apakah penganalisis yang dikelola oleh AWS Identity and Access Management Access Analyzer (IAM Access Analyzer) memiliki tag dengan kunci tertentu yang ditentukan dalam parameter `requiredTagKeys`. Kontrol gagal jika penganalisis tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter `requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika penganalisis tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws:`, diabaikan.

Tanda adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengkategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat Anda menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk penanggung jawab IAM Anda. Anda dapat merancang kebijakan ABAC ini untuk memungkinkan operasi ketika tag penanggung jawab cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat [Untuk apa ABAC untuk? AWS](#) di Panduan Pengguna IAM.

Note

Jangan menambahkan informasi pengenalan pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat [Menandai AWS sumber daya Anda](#) di Referensi Umum AWS.

Tindakan Perbaikan

Untuk menambahkan tag ke analyzer, lihat [TagResource](#) di Referensi API AWS IAM Access Analyzer.

[IAM.24] Peran IAM harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: AWS::IAM::Role

AWS Config aturan: tagged-iam-role (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
<code>requiredTagKeys</code>	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS .	No default value

Kontrol ini memeriksa apakah peran AWS Identity and Access Management (IAM) memiliki tag dengan kunci tertentu yang ditentukan dalam parameter `requiredTagKeys`. Kontrol gagal jika peran tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter `requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika peran tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws:`, diabaikan.

Tanda adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat Anda menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian

kebijakan terpisah untuk penanggung jawab IAM Anda. Anda dapat merancang kebijakan ABAC ini untuk memungkinkan operasi ketika tag penanggung jawab cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat Untuk [apa ABAC untuk? AWS](#) di Panduan Pengguna IAM.

Note

Jangan menambahkan informasi pengenalan pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat [Menandai AWS sumber daya Anda](#) di Referensi Umum AWS

Tindakan Perbaikan

Untuk menambahkan tag ke peran IAM, lihat [Menandai sumber daya IAM di Panduan](#) Pengguna IAM.

[IAM.25] Pengguna IAM harus diberi tag

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: AWS::IAM::User

AWS Config aturan: tagged-iam-user (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
requiredTagKeys	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS	No default value

Kontrol ini memeriksa apakah pengguna AWS Identity and Access Management (IAM) memiliki tag dengan kunci tertentu yang ditentukan dalam `parameterrequiredTagKeys`. Kontrol gagal jika pengguna tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam `parameterrequiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika pengguna tidak diberi tag dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws :`, diabaikan.

Tanda adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat Anda menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk penanggung jawab IAM Anda. Anda dapat merancang kebijakan ABAC ini untuk memungkinkan operasi ketika tag penanggung jawab cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat [Untuk apa ABAC untuk? AWS](#) di Panduan Pengguna IAM.

Note

Jangan menambahkan informasi pengenalan pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat [Menandai AWS sumber daya Anda](#) di Referensi Umum AWS

Tindakan Perbaikan

Untuk menambahkan tag ke pengguna IAM, lihat [Menandai sumber daya IAM](#) di Panduan Pengguna IAM.

[IAM.26] Sertifikat SSL/TLS kedaluwarsa yang dikelola di IAM harus dihapus

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v3.0.0/1.19

Kategori: Identifikasi > Kepatuhan

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::IAM::ServerCertificate`

AWS Config aturan: [iam-server-certificate-expiration-check](#)

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah sertifikat SSL/TLS server certificate that is managed in IAM has expired. The control fails if the expired SSL/TLS server aktif tidak dihapus.

Untuk mengaktifkan koneksi HTTPS ke situs web atau aplikasi Anda di AWS, Anda memerlukan sertifikat server SSL/TLS. Anda dapat menggunakan IAM atau AWS Certificate Manager (ACM) untuk menyimpan dan menyebarkan sertifikat server. Gunakan IAM sebagai manajer sertifikat hanya ketika Anda harus mendukung koneksi HTTPS di Wilayah AWS yang tidak didukung oleh ACM. IAM mengenkripsi kunci pribadi Anda dengan aman dan menyimpan versi terenkripsinya dalam penyimpanan sertifikat IAM SSL. IAM mendukung penyebaran sertifikat server di semua Wilayah, tetapi Anda harus mendapatkan sertifikat dari penyedia eksternal untuk digunakan. AWS Anda tidak dapat mengunggah sertifikat ACM ke IAM. Sebagai tambahan, Anda tidak dapat mengelola sertifikat Anda dari konsol IAM. Menghapus sertifikat SSL/TLS yang kedaluwarsa menghilangkan risiko bahwa sertifikat yang tidak valid disebarkan secara tidak sengaja ke sumber daya, yang dapat merusak kredibilitas aplikasi atau situs web yang mendasarinya.

Tindakan Perbaikan

Untuk menghapus sertifikat server dari IAM, lihat [Mengelola sertifikat server di IAM](#) di Panduan Pengguna IAM.

[IAM.27] Identitas IAM seharusnya tidak memiliki kebijakan yang dilampirkan `AWSCloud ShellFullAccess`

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v3.0.0/1.22

Kategori: Lindungi > Manajemen akses aman > Kebijakan IAM yang aman

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::IAM::Role`, `AWS::IAM::User`, `AWS::IAM::Group`

AWS Config aturan: [iam-policy-blacklisted-check](#)

Jenis jadwal: Perubahan dipicu

Parameter:

- “PolicyArns”: “arn:iam: :aws:iam:” policy/AWSCloudShellFullAccess,arn:aws-cn:iam::aws:policy/AWSCloudShellFullAccess, arn:aws-us-gov:iam::aws:policy/AWSCloudShellFullAccess

Kontrol ini memeriksa apakah identitas IAM (pengguna, peran, atau grup) memiliki kebijakan AWS terkelola `AWSCloudShellFullAccess`. Kontrol gagal jika identitas IAM memiliki `AWSCloudShellFullAccess` kebijakan yang dilampirkan.

AWS CloudShell menyediakan cara mudah untuk menjalankan perintah CLI terhadap Layanan AWS. Kebijakan AWS terkelola `AWSCloudShellFullAccess` menyediakan akses penuh CloudShell, yang memungkinkan kemampuan mengunggah dan mengunduh file antara sistem lokal pengguna dan CloudShell lingkungan. Dalam CloudShell lingkungan, pengguna memiliki izin sudo, dan dapat mengakses internet. Akibatnya, melampirkan kebijakan terkelola ini ke identitas IAM memberi mereka kemampuan untuk menginstal perangkat lunak transfer file dan memindahkan data dari CloudShell ke server internet eksternal. Sebaiknya ikuti prinsip hak istimewa paling sedikit dan melampirkan izin yang lebih sempit ke identitas IAM Anda.

Tindakan Perbaikan

Untuk melepaskan `AWSCloudShellFullAccess` kebijakan dari identitas IAM, lihat [Menambahkan dan menghapus izin identitas IAM](#) di Panduan Pengguna IAM.

[IAM.28] IAM Access Analyzer penganalisis akses eksternal harus diaktifkan

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v3.0.0/1.20

Kategori: Deteksi > Layanan deteksi > Pemantauan penggunaan istimewa

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::AccessAnalyzer::Analyzer`

AWS Config aturan: [iam-external-access-analyzer-enabled](#)

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah Akun AWS penganalisis akses eksternal IAM Access Analyzer diaktifkan. Kontrol gagal jika akun tidak mengaktifkan penganalisis akses eksternal di pilihan Wilayah AWS Anda saat ini.

IAM Access Analyzer membantu mengidentifikasi sumber daya, seperti bucket Amazon Simple Storage Service (Amazon S3) atau peran IAM, yang dibagikan dengan entitas eksternal. Hal ini membantu Anda menghindari akses yang tidak diinginkan ke sumber daya dan data Anda. IAM Access Analyzer bersifat Regional dan harus diaktifkan di setiap Wilayah. Untuk mengidentifikasi sumber daya yang dibagi dengan kepala sekolah eksternal, analisis akses menggunakan penalaran berbasis logika untuk menganalisis kebijakan berbasis sumber daya di lingkungan Anda. AWS Saat Anda membuat penganalisis akses eksternal, Anda dapat membuat dan mengaktifkannya untuk seluruh organisasi atau akun individual Anda.

Note

Jika akun merupakan bagian dari organisasi AWS Organizations, kontrol ini tidak memfaktorkan penganalisis akses eksternal yang menentukan organisasi sebagai zona kepercayaan dan diaktifkan untuk organisasi di Wilayah saat ini. Jika organisasi Anda menggunakan jenis konfigurasi ini, pertimbangkan untuk menonaktifkan kontrol ini untuk akun anggota individual di organisasi Anda di Wilayah.

Tindakan Perbaikan

Untuk informasi tentang mengaktifkan penganalisis akses eksternal di Wilayah tertentu, lihat [Memulai IAM Access Analyzer di Panduan Pengguna IAM](#). Anda harus mengaktifkan penganalisis di setiap Wilayah yang ingin Anda gunakan untuk memantau akses ke sumber daya Anda.

Kontrol Security Hub untuk Amazon Inspector

AWS Security Hub Kontrol ini mengevaluasi layanan dan sumber daya Amazon Inspector.

Kontrol ini mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat [Ketersediaan kontrol berdasarkan Wilayah](#).

[Inspektor.1] Pemindaian Amazon Inspector harus diaktifkan EC2

Persyaratan terkait: PCI DSS v4.0.1/11.3.1

Kategori: Deteksi > Layanan deteksi

Tingkat keparahan: Tinggi

Jenis sumber daya: AWS :: Account

AWS Config aturan: [inspector-ec2-scan-enabled](#)

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah EC2 pemindaian Amazon Inspector diaktifkan. Untuk akun mandiri, kontrol gagal jika pemindaian Amazon EC2 Inspector dinonaktifkan di akun. Di lingkungan multi-akun, kontrol gagal jika akun administrator Amazon Inspector yang didelegasikan dan semua akun anggota tidak EC2 mengaktifkan pemindaian.

Dalam lingkungan multi-akun, kontrol menghasilkan temuan hanya di akun administrator Amazon Inspector yang didelegasikan. Hanya administrator yang didelegasikan yang dapat mengaktifkan atau menonaktifkan fitur EC2 pemindaian untuk akun anggota di organisasi. Akun anggota Amazon Inspector tidak dapat mengubah konfigurasi ini dari akun mereka. Kontrol ini menghasilkan FAILED temuan jika administrator yang didelegasikan memiliki akun anggota yang ditangguhkan yang tidak mengaktifkan pemindaian Amazon EC2 Inspector. Untuk menerima PASSED temuan, administrator yang didelegasikan harus memisahkan akun yang ditangguhkan ini di Amazon Inspector.

EC2 Pemindaian Amazon Inspector mengekstrak metadata dari instans Amazon Elastic Compute Cloud (EC2Amazon) Anda, lalu membandingkan metadata ini dengan aturan yang dikumpulkan dari penasihat keamanan untuk menghasilkan temuan. Amazon Inspector memindai instans untuk kerentanan paket dan masalah jangkauan jaringan. Untuk informasi tentang sistem operasi yang didukung, termasuk sistem operasi mana yang dapat dipindai tanpa agen SSM, lihat [Sistem operasi yang didukung: Pemindaian Amazon EC2](#) .

Remediasi

Untuk mengaktifkan pemindaian Amazon Inspector, lihat [Mengaktifkan EC2 pemindaian di Panduan Pengguna](#) Amazon Inspector.

[Inspektor.2] Pemindaian ECR Amazon Inspector harus diaktifkan

Persyaratan terkait: PCI DSS v4.0.1/11.3.1

Kategori: Deteksi > Layanan deteksi

Tingkat keparahan: Tinggi

Jenis sumber daya: AWS : : : Account

AWS Config aturan: [inspector-ecr-scan-enabled](#)

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah pemindaian Amazon Inspector ECR diaktifkan. Untuk akun mandiri, kontrol gagal jika pemindaian Amazon Inspector ECR dinonaktifkan di akun. Di lingkungan multi-akun, kontrol gagal jika akun administrator Amazon Inspector yang didelegasikan dan semua akun anggota tidak mengaktifkan pemindaian ECR.

Dalam lingkungan multi-akun, kontrol menghasilkan temuan hanya di akun administrator Amazon Inspector yang didelegasikan. Hanya administrator yang didelegasikan yang dapat mengaktifkan atau menonaktifkan fitur pemindaian ECR untuk akun anggota di organisasi. Akun anggota Amazon Inspector tidak dapat mengubah konfigurasi ini dari akun mereka. Kontrol ini menghasilkan FAILED temuan jika administrator yang didelegasikan memiliki akun anggota yang ditangguhkan yang tidak mengaktifkan pemindaian Amazon Inspector ECR. Untuk menerima PASSED temuan, administrator yang didelegasikan harus memisahkan akun yang ditangguhkan ini di Amazon Inspector.

Amazon Inspector memindai gambar kontainer yang disimpan di Amazon Elastic Container Registry (Amazon ECR) untuk mencari kerentanan perangkat lunak untuk menghasilkan temuan kerentanan paket. Saat mengaktifkan pemindaian Amazon Inspector untuk Amazon ECR, Anda menetapkan Amazon Inspector sebagai layanan pemindaian pilihan untuk registri pribadi Anda. Ini menggantikan pemindaian dasar, yang disediakan tanpa biaya oleh Amazon ECR, dengan pemindaian yang disempurnakan, yang disediakan dan ditagih melalui Amazon Inspector. Pemindaian yang disempurnakan memberi Anda manfaat pemindaian kerentanan untuk sistem operasi dan paket bahasa pemrograman di tingkat registri. Anda dapat meninjau temuan yang ditemukan menggunakan pemindaian yang disempurnakan pada tingkat gambar, untuk setiap lapisan gambar, di konsol Amazon ECR. Selain itu, Anda dapat meninjau dan bekerja dengan temuan ini di layanan lain yang tidak tersedia untuk temuan pemindaian dasar, termasuk AWS Security Hub dan Amazon EventBridge.

Remediasi

Untuk mengaktifkan pemindaian Amazon Inspector ECR, lihat [Mengaktifkan pemindaian di Panduan Pengguna Amazon Inspector](#).

[Inspektor.3] Pemindaian kode Amazon Inspector Lambda harus diaktifkan

Persyaratan terkait: PCI DSS v4.0.1/6.2.4, PCI DSS v4.0.1/6.3.1

Kategori: Deteksi > Layanan deteksi

Tingkat keparahan: Tinggi

Jenis sumber daya: AWS :: Account

AWS Config aturan: [inspector-lambda-code-scan-enabled](#)

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah pemindaian kode Amazon Inspector Lambda diaktifkan. Untuk akun mandiri, kontrol gagal jika pemindaian kode Amazon Inspector Lambda dinonaktifkan di akun. Di lingkungan multi-akun, kontrol gagal jika akun administrator Amazon Inspector yang didelegasikan dan semua akun anggota tidak mengaktifkan pemindaian kode Lambda.

Dalam lingkungan multi-akun, kontrol menghasilkan temuan hanya di akun administrator Amazon Inspector yang didelegasikan. Hanya administrator yang didelegasikan yang dapat mengaktifkan atau menonaktifkan fitur pemindaian kode Lambda untuk akun anggota di organisasi. Akun anggota Amazon Inspector tidak dapat mengubah konfigurasi ini dari akun mereka. Kontrol ini menghasilkan FAILED temuan jika administrator yang didelegasikan memiliki akun anggota yang ditangguhkan yang tidak mengaktifkan pemindaian kode Amazon Inspector Lambda. Untuk menerima PASSED temuan, administrator yang didelegasikan harus memisahkan akun yang ditangguhkan ini di Amazon Inspector.

Pemindaian kode Amazon Inspector Lambda memindai kode aplikasi khusus dalam AWS Lambda fungsi untuk kerentanan kode berdasarkan praktik terbaik keamanan. AWS Pemindaian kode Lambda dapat mendeteksi kekurangan injeksi, kebocoran data, kriptografi lemah, atau enkripsi yang hilang dalam kode Anda. Fitur ini [Wilayah AWS hanya tersedia secara spesifik](#). Anda dapat mengaktifkan pemindaian kode Lambda bersama dengan pemindaian standar Lambda (lihat).

[\[Inspektor.4\] Pemindaian standar Amazon Inspector Lambda harus diaktifkan](#)

Remediasi

Untuk mengaktifkan pemindaian kode Amazon Inspector Lambda, lihat [Mengaktifkan pemindaian di Panduan Pengguna Amazon Inspector](#).

[Inspektor.4] Pemindaian standar Amazon Inspector Lambda harus diaktifkan

Persyaratan terkait: PCI DSS v4.0.1/6.2.4, PCI DSS v4.0.1/6.3.1

Kategori: Deteksi > Layanan deteksi

Tingkat keparahan: Tinggi

Jenis sumber daya: AWS :: Account

AWS Config aturan: [inspector-lambda-standard-scan-enabled](#)

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah pemindaian standar Amazon Inspector Lambda diaktifkan. Untuk akun mandiri, kontrol gagal jika pemindaian standar Amazon Inspector Lambda dinonaktifkan di akun. Di lingkungan multi-akun, kontrol gagal jika akun administrator Amazon Inspector yang didelegasikan dan semua akun anggota tidak mengaktifkan pemindaian standar Lambda.

Dalam lingkungan multi-akun, kontrol menghasilkan temuan hanya di akun administrator Amazon Inspector yang didelegasikan. Hanya administrator yang didelegasikan yang dapat mengaktifkan atau menonaktifkan fitur pemindaian standar Lambda untuk akun anggota di organisasi. Akun anggota Amazon Inspector tidak dapat mengubah konfigurasi ini dari akun mereka. Kontrol ini menghasilkan FAILED temuan jika administrator yang didelegasikan memiliki akun anggota yang ditangguhkan yang tidak mengaktifkan pemindaian standar Amazon Inspector Lambda. Untuk menerima PASSED temuan, administrator yang didelegasikan harus memisahkan akun yang ditangguhkan ini di Amazon Inspector.

Pemindaian standar Amazon Inspector Lambda mengidentifikasi kerentanan perangkat lunak dalam dependensi paket aplikasi yang Anda tambahkan ke kode fungsi dan lapisan Anda. AWS Lambda Jika Amazon Inspector mendeteksi kerentanan dalam dependensi paket aplikasi fungsi Lambda Anda, Amazon Inspector menghasilkan temuan tipe terperinci. Package Vulnerability Anda dapat mengaktifkan pemindaian kode Lambda bersama dengan pemindaian standar Lambda (lihat). [\[Inspektor.3\] Pemindaian kode Amazon Inspector Lambda harus diaktifkan](#)

Remediasi

Untuk mengaktifkan pemindaian standar Amazon Inspector Lambda, lihat [Mengaktifkan pemindaian di](#) Panduan Pengguna Amazon Inspector.

Kontrol Security Hub untuk AWS IoT

AWS Security Hub Kontrol ini mengevaluasi AWS IoT layanan dan sumber daya.

Kontrol ini mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat [Ketersediaan kontrol berdasarkan Wilayah](#).

[IoT.1] profil AWS IoT Device Defender keamanan harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::IoT::SecurityProfile`

AWS Config aturan: `tagged-iot-securityprofile` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
<code>requiredTagKeys</code>	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS .	No default value

Kontrol ini memeriksa apakah profil AWS IoT Device Defender keamanan memiliki tag dengan kunci tertentu yang ditentukan dalam parameter `requiredTagKeys`. Kontrol gagal jika profil keamanan tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter `requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika profil keamanan tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke

AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat [Untuk apa ABAC? AWS](#) di Panduan Pengguna IAM.

Note

Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat [Menandai AWS sumber daya Anda](#) di Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke profil AWS IoT Device Defender keamanan, lihat [Menandai AWS IoT sumber daya Anda](#) di Panduan AWS IoT Pengembang.

[IoT.2] tindakan AWS IoT Core mitigasi harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::IoT::MitigationAction`

AWS Config aturan: `tagged-iot-mitigationaction` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
<code>requiredTagKeys</code>	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi	No default value

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
			persyaratan AWS	

Kontrol ini memeriksa apakah tindakan AWS IoT Core mitigasi memiliki tag dengan kunci spesifik yang ditentukan dalam parameter. `requiredTagKeys` Kontrol gagal jika tindakan mitigasi tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter. `requiredTagKeys` Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika tindakan mitigasi tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengkategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat [Untuk apa ABAC? AWS](#) di Panduan Pengguna IAM.

Note

Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat [Menandai AWS sumber daya Anda](#) di Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke tindakan AWS IoT Core mitigasi, lihat [Menandai AWS IoT sumber daya Anda di Panduan Pengembang](#).AWS IoT

AWS IoT Core Dimensi [IoT.3] harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::IoT::Dimension`

AWS Config aturan: `tagged-iot-dimension` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
<code>requiredTagKeys</code>	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS .	No default value

Kontrol ini memeriksa apakah AWS IoT Core dimensi memiliki tag dengan kunci tertentu yang ditentukan dalam parameter `requiredTagKeys`. Kontrol gagal jika dimensi tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter `requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika dimensi tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws :`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke

AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat [Untuk apa ABAC? AWS](#) di Panduan Pengguna IAM.

Note

Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat [Menandai AWS sumber daya Anda](#) di Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke AWS IoT Core dimensi, lihat [Menandai AWS IoT sumber daya Anda](#) di Panduan AWS IoT Pengembang.

[IoT.4] AWS IoT Core otorisasi harus diberi tag

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::IoT::Authorizer`

AWS Config aturan: `tagged-iot-authorizer` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
<code>requiredTagKeys</code>	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi	No default value

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
			persyaratan AWS	

Kontrol ini memeriksa apakah AWS IoT Core otorisasi memiliki tag dengan kunci tertentu yang ditentukan dalam parameter `requiredTagKeys`. Kontrol gagal jika otorisasi tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter `requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika otorisasi tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws :`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat [Untuk apa ABAC? AWS](#) di Panduan Pengguna IAM.

Note

Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat [Menandai AWS sumber daya Anda](#) di Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke AWS IoT Core otorisasi, lihat [Menandai AWS IoT sumber daya Anda di Panduan AWS IoT](#) Pengembang.

[IoT.5] alias AWS IoT Core peran harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::IoT::RoleAlias`

AWS Config aturan: `tagged-iot-rolealias` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
<code>requiredTagKeys</code>	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS .	No default value

Kontrol ini memeriksa apakah alias AWS IoT Core peran memiliki tag dengan kunci tertentu yang ditentukan dalam parameter `requiredTagKeys`. Kontrol gagal jika alias peran tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter `requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika alias peran tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengkategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan

terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat [Untuk apa ABAC? AWS](#) di Panduan Pengguna IAM.

Note

Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat [Menandai AWS sumber daya Anda](#) di Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke alias AWS IoT Core peran, lihat [Menandai AWS IoT sumber daya Anda di Panduan AWS IoT](#) Pengembang.

AWS IoT Core Kebijakan [IoT.6] harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::IoT::Policy`

AWS Config aturan: `tagged-iot-policy` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
<code>requiredTagKeys</code>	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS .	No default value

Kontrol ini memeriksa apakah AWS IoT Core kebijakan memiliki tag dengan kunci spesifik yang ditentukan dalam parameter `requiredTagKeys`. Kontrol gagal jika kebijakan tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter `requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika kebijakan tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws :`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat [Untuk apa ABAC? AWS](#) di Panduan Pengguna IAM.

Note

Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat [Menandai AWS sumber daya Anda](#) di Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke AWS IoT Core kebijakan, lihat [Menandai AWS IoT sumber daya Anda](#) di Panduan AWS IoT Pengembang.

Kontrol Security Hub untuk AWS IoT Events

AWS Security Hub Kontrol ini mengevaluasi layanan dan AWS sumber daya IoT Events.

Kontrol ini mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat [Ketersediaan kontrol berdasarkan Wilayah](#).

[Io TEvents .1] Input Peristiwa AWS IoT harus diberi tag

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: AWS::IoTEvents::Input

AWS Config aturan: iotevents-input-tagged

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
<code>requiredKeyTags</code>	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS .	Tidak ada nilai default

Kontrol ini memeriksa apakah input AWS IoT Events memiliki tag dengan kunci spesifik yang ditentukan dalam parameter `requiredKeyTags`. Kontrol gagal jika input tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter `requiredKeyTags`. Jika parameter `requiredKeyTags` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika input tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS

sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat [Menentukan izin berdasarkan atribut dengan otorisasi ABAC di Panduan Pengguna IAM](#).

Note

Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk mengetahui praktik terbaik penandaan lainnya, lihat [Praktik dan strategi terbaik di Panduan Pengguna AWS Sumber Daya Penandaan dan Editor Tag](#).

Remediasi

Untuk menambahkan tag ke input Peristiwa AWS IoT, [lihat Menandai sumber daya AWS IoT Events Anda](#) di Panduan AWS IoT Events Pengembang.

[IoTEvents .2] Model detektor Acara AWS IoT harus diberi tag

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::IoTEvents::DetectorModel`

AWS Config aturan: `iotevents-detector-model-tagged`

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
<code>requiredKeyTags</code>	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi	Tidak ada nilai default

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
			persyaratan AWS	

Kontrol ini memeriksa apakah model detektor Peristiwa AWS IoT memiliki tag dengan kunci spesifik yang ditentukan dalam parameter. `requiredKeyTags` Kontrol gagal jika model detektor tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter `requiredKeyTags`. Jika parameter `requiredKeyTags` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika model detektor tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws :`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat [Menentukan izin berdasarkan atribut dengan otorisasi ABAC di Panduan Pengguna IAM](#).

Note

Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk mengetahui praktik terbaik penandaan lainnya, lihat [Praktik dan strategi terbaik di Panduan Pengguna AWS Sumber Daya Penandaan dan Editor Tag](#).

Remediasi

Untuk menambahkan tag ke model detektor Peristiwa AWS IoT, [lihat Menandai sumber daya AWS IoT Events Anda](#) di Panduan AWS IoT Events Pengembang.

[IoTEvents .3] Model alarm AWS IoT Events harus diberi tag

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::IoTEvents::AlarmModel`

AWS Config aturan: `iotevents-alarm-model-tagged`

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
<code>requiredKeyTags</code>	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS .	Tidak ada nilai default

Kontrol ini memeriksa apakah model alarm AWS IoT Events memiliki tag dengan kunci spesifik yang ditentukan dalam parameter. `requiredKeyTags` Kontrol gagal jika model alarm tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter `requiredKeyTags`. Jika parameter `requiredKeyTags` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika model alarm tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS

sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat [Menentukan izin berdasarkan atribut dengan otorisasi ABAC di Panduan Pengguna IAM](#).

Note

Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk mengetahui praktik terbaik penandaan lainnya, lihat [Praktik dan strategi terbaik di Panduan Pengguna AWS Sumber Daya Penandaan dan Editor Tag](#).

Remediasi

Untuk menambahkan tag ke model alarm Peristiwa AWS IoT, [lihat Menandai sumber daya AWS IoT Events Anda](#) di Panduan AWS IoT Events Pengembang.

Kontrol Security Hub untuk AWS IoT SiteWise

AWS Security Hub Kontrol ini mengevaluasi SiteWise layanan dan AWS sumber daya IoT.

Kontrol ini mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat [Ketersediaan kontrol berdasarkan Wilayah](#).

[IoT Site Wise.1] Model aset AWS IoT harus ditandai SiteWise

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::IoTSiteWise::AssetModel`

AWS Config aturan: `iotsitewise-asset-model-tagged`

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
<code>requiredKeyTags</code>	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS .	Tidak ada nilai default

Kontrol ini memeriksa apakah model SiteWise aset AWS IoT memiliki tag dengan kunci spesifik yang ditentukan dalam parameter. `requiredKeyTags` Kontrol gagal jika model aset tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter `requiredKeyTags`. Jika parameter `requiredKeyTags` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika model aset tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat [Menentukan izin berdasarkan atribut dengan otorisasi ABAC di Panduan Pengguna IAM](#).

Note

Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk mengetahui praktik terbaik penandaan lainnya, lihat [Praktik dan strategi terbaik di Panduan Pengguna AWS Sumber Daya Penandaan dan Editor Tag](#).

Remediasi

Untuk menambahkan tag ke model SiteWise aset AWS IoT, lihat [Menandai AWS IoT SiteWise sumber daya Anda](#) di AWS IoT SiteWise Panduan Pengguna.

[IoT Site Wise.2] Dasbor AWS IoT harus diberi tag SiteWise

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: AWS::IoTSiteWise::Dashboard

AWS Config aturan: iotsitewise-dashboard-tagged

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
requiredKeyTags	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS .	Tidak ada nilai default

Kontrol ini memeriksa apakah SiteWise dasbor AWS IoT memiliki tag dengan kunci spesifik yang ditentukan dalam parameter. `requiredKeyTags` Kontrol gagal jika dasbor tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter `requiredKeyTags`. Jika parameter `requiredKeyTags` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika dasbor tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengkategorikan sumber daya berdasarkan tujuan, pemilik,

lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat [Menentukan izin berdasarkan atribut dengan otorisasi ABAC di Panduan Pengguna IAM](#).

Note

Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk mengetahui praktik terbaik penandaan lainnya, lihat [Praktik dan strategi terbaik di Panduan Pengguna AWS Sumber Daya Penandaan dan Editor Tag](#).

Remediasi

Untuk menambahkan tag ke SiteWise dasbor AWS IoT, lihat [Menandai AWS IoT SiteWise sumber daya Anda](#) di AWS IoT SiteWise Panduan Pengguna.

[IoT Site Wise.3] Gateway AWS IoT harus diberi tag SiteWise

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: AWS::IoTSiteWise::Gateway

AWS Config aturan: iotsitewise-gateway-tagged

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
<code>requiredKeyTags</code>	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS .	Tidak ada nilai default

Kontrol ini memeriksa apakah SiteWise gateway AWS IoT memiliki tag dengan kunci spesifik yang ditentukan dalam parameter. `requiredKeyTags` Kontrol gagal jika gateway tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter `requiredKeyTags`. Jika parameter `requiredKeyTags` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika gateway tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws :`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat [Menentukan izin berdasarkan atribut dengan otorisasi ABAC di Panduan Pengguna IAM](#).

Note

Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk mengetahui praktik terbaik penandaan lainnya, lihat [Praktik dan strategi terbaik di Panduan Pengguna AWS Sumber Daya Penandaan dan Editor Tag](#).

Remediasi

Untuk menambahkan tag ke SiteWise gateway AWS IoT, lihat [Menandai AWS IoT SiteWise sumber daya Anda](#) di AWS IoT SiteWise Panduan Pengguna.

[IoT SiteWise.4] Portal AWS IoT harus diberi tag SiteWise

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::IoTSiteWise::Portal`

AWS Config aturan: `iotsitewise-portal-tagged`

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
<code>requiredKeyTags</code>	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS .	Tidak ada nilai default

Kontrol ini memeriksa apakah SiteWise portal AWS IoT memiliki tag dengan kunci spesifik yang ditentukan dalam parameter. `requiredKeyTags` Kontrol gagal jika portal tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter `requiredKeyTags`. Jika parameter `requiredKeyTags` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika portal tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengkategorikan sumber daya berdasarkan tujuan, pemilik,

lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat [Menentukan izin berdasarkan atribut dengan otorisasi ABAC di Panduan Pengguna IAM](#).

Note

Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk mengetahui praktik terbaik penandaan lainnya, lihat [Praktik dan strategi terbaik di Panduan Pengguna AWS Sumber Daya Penandaan dan Editor Tag](#).

Remediasi

Untuk menambahkan tag ke SiteWise portal AWS IoT, lihat [Menandai AWS IoT SiteWise sumber daya Anda](#) di AWS IoT SiteWise Panduan Pengguna.

[IoT Site Wise.5] Proyek AWS IoT harus diberi tag SiteWise

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::IoTSiteWise::Project`

AWS Config aturan: `iotsitewise-project-tagged`

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
<code>requiredKeyTags</code>	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS .	Tidak ada nilai default

Kontrol ini memeriksa apakah SiteWise proyek AWS IoT memiliki tag dengan kunci spesifik yang ditentukan dalam parameter. `requiredKeyTags` Kontrol gagal jika proyek tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter `requiredKeyTags`. Jika parameter `requiredKeyTags` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika proyek tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws :`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat [Menentukan izin berdasarkan atribut dengan otorisasi ABAC di Panduan Pengguna IAM](#).

Note

Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk mengetahui praktik terbaik penandaan lainnya, lihat [Praktik dan strategi terbaik di Panduan Pengguna AWS Sumber Daya Penandaan dan Editor Tag](#).

Remediasi

Untuk menambahkan tag ke SiteWise proyek AWS IoT, lihat [Menandai AWS IoT SiteWise sumber daya Anda](#) di AWS IoT SiteWise Panduan Pengguna.

Kontrol Security Hub untuk AWS IoT TwinMaker

AWS Security Hub Kontrol ini mengevaluasi TwinMaker layanan dan AWS sumber daya IoT.

Kontrol ini mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat [Ketersediaan kontrol berdasarkan Wilayah](#).

[IoT Twin Maker.1] Pekerjaan sinkronisasi AWS IoT harus ditandai TwinMaker

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::IoT::TwinMaker::SyncJob`

AWS Config aturan: `iottwinmaker-sync-job-tagged`

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
<code>requiredKeyTags</code>	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS .	Tidak ada nilai default

Kontrol ini memeriksa apakah pekerjaan TwinMaker sinkronisasi AWS IoT memiliki tag dengan kunci spesifik yang ditentukan dalam parameter. `requiredKeyTags` Kontrol gagal jika pekerjaan

sinkronisasi tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter `requiredKeyTags`. Jika parameter `requiredKeyTags` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika pekerjaan sinkronisasi tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws :`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat [Menentukan izin berdasarkan atribut dengan otorisasi ABAC di Panduan Pengguna IAM](#).

Note

Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk mengetahui praktik terbaik penandaan lainnya, lihat [Praktik dan strategi terbaik di Panduan Pengguna AWS Sumber Daya Penandaan dan Editor Tag](#).

Remediasi

Untuk menambahkan tag ke pekerjaan TwinMaker sinkronisasi AWS IoT, lihat [TagResource](#) di Panduan Pengguna AWS IoT TwinMaker .

[IoT Twin Maker.2] Ruang kerja AWS IoT harus diberi tag TwinMaker

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::IoT::TwinMaker::Workspace`

AWS Config aturan: `iottwinmaker-workspace-tagged`

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
<code>requiredKeyTags</code>	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS .	Tidak ada nilai default

Kontrol ini memeriksa apakah TwinMaker ruang kerja AWS IoT memiliki tag dengan kunci spesifik yang ditentukan dalam parameter. `requiredKeyTags` Kontrol gagal jika ruang kerja tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter `requiredKeyTags`. Jika parameter `requiredKeyTags` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika ruang kerja tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat [Menentukan izin berdasarkan atribut dengan otorisasi ABAC di Panduan Pengguna IAM](#).

Note

Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS

Billing. Untuk mengetahui praktik terbaik penandaan lainnya, lihat [Praktik dan strategi terbaik](#) di Panduan Pengguna AWS Sumber Daya Penandaan dan Editor Tag.

Remediasi

Untuk menambahkan tag ke ruang TwinMaker kerja AWS IoT, lihat [TagResource](#) di Panduan Pengguna AWS IoT TwinMaker .

[IoT Twin Maker.3] Adegan AWS IoT harus diberi tag TwinMaker

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::IoT::TwinMaker::Scene`

AWS Config aturan: `iottwinmaker-scene-tagged`

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
<code>requiredKeyTags</code>	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS .	Tidak ada nilai default

Kontrol ini memeriksa apakah TwinMaker adegan AWS IoT memiliki tag dengan kunci spesifik yang ditentukan dalam parameter. `requiredKeyTags` Kontrol gagal jika adegan tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter `requiredKeyTags`. Jika parameter `requiredKeyTags` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika adegan tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws :`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat [Menentukan izin berdasarkan atribut dengan otorisasi ABAC di Panduan Pengguna IAM](#).

Note

Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk mengetahui praktik terbaik penandaan lainnya, lihat [Praktik dan strategi terbaik di Panduan Pengguna AWS Sumber Daya Penandaan dan Editor Tag](#).

Remediasi

Untuk menambahkan tag ke TwinMaker adegan AWS IoT, lihat [TagResource](#) di Panduan Pengguna AWS IoT TwinMaker .

[Io TTwin Maker.4] Entitas AWS IoT harus diberi tag TwinMaker

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::IoT::TwinMaker::Entity`

AWS Config aturan: `iottwinmaker-entity-tagged`

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
<code>requiredKeyTags</code>	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS .	Tidak ada nilai default

Kontrol ini memeriksa apakah TwinMaker entitas AWS IoT memiliki tag dengan kunci spesifik yang ditentukan dalam parameter. `requiredKeyTags` Kontrol gagal jika entitas tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter `requiredKeyTags`. Jika parameter `requiredKeyTags` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika entitas tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws :`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat [Menentukan izin berdasarkan atribut dengan otorisasi ABAC di Panduan Pengguna IAM](#).

Note

Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk mengetahui praktik terbaik penandaan lainnya, lihat [Praktik dan strategi terbaik di Panduan Pengguna AWS Sumber Daya Penandaan dan Editor Tag](#).

Remediasi

Untuk menambahkan tag ke TwinMaker entitas AWS IoT, lihat [TagResource](#) di Panduan Pengguna AWS IoT TwinMaker .

Kontrol Security Hub untuk AWS IoT Wireless

AWS Security Hub Kontrol ini mengevaluasi layanan dan AWS sumber daya IoT Wireless.

Kontrol ini mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat [Ketersediaan kontrol berdasarkan Wilayah](#).

[Io TWireless .1] Grup multicast Nirkabel AWS IoT harus diberi tag

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::IoTWireless::MulticastGroup`

AWS Config aturan: `iotwireless-multicast-group-tagged`

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
<code>requiredKeyTags</code>	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS .	Tidak ada nilai default

Kontrol ini memeriksa apakah grup multicast Nirkabel AWS IoT memiliki tag dengan kunci spesifik yang ditentukan dalam parameter. `requiredKeyTags` Kontrol gagal jika grup multicast

tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter. `requiredKeyTags` Jika parameter `requiredKeyTags` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika grup multicast tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat [Menentukan izin berdasarkan atribut dengan otorisasi ABAC di Panduan Pengguna IAM](#).

Note

Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk mengetahui praktik terbaik penandaan lainnya, lihat [Praktik dan strategi terbaik di Panduan Pengguna AWS Sumber Daya Penandaan dan Editor Tag](#).

Remediasi

Untuk menambahkan tag ke grup multicast Nirkabel AWS IoT, [lihat Menandai sumber daya AWS IoT Wireless Anda](#) di Panduan Pengembang AWS IoT Wireless

[IoT Wireless .2] Profil layanan AWS IoT Wireless harus diberi tag

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::IoTWireless::ServiceProfile`

AWS Config aturan: `iotwireless-service-profile-tagged`

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
<code>requiredKeyTags</code>	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS.	Tidak ada nilai default

Kontrol ini memeriksa apakah profil layanan AWS IoT Wireless memiliki tag dengan kunci spesifik yang ditentukan dalam parameter. `requiredKeyTags` Kontrol gagal jika profil layanan tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter `requiredKeyTags`. Jika parameter `requiredKeyTags` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika profil layanan tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat [Menentukan izin berdasarkan atribut dengan otorisasi ABAC di Panduan Pengguna IAM](#).

Note

Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS

Billing. Untuk mengetahui praktik terbaik penandaan lainnya, lihat [Praktik dan strategi terbaik](#) di Panduan Pengguna AWS Sumber Daya Penandaan dan Editor Tag.

Remediasi

Untuk menambahkan tag ke profil layanan Nirkabel AWS IoT, [lihat Menandai sumber daya AWS IoT Wireless Anda](#) di Panduan AWS IoT Wireless Pengembang.

[Io TWireless .3] Tugas AWS IoT FUOTA harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: AWS::IoTWireless::FuotaTask

AWS Config aturan: iotwireless-fuota-task-tagged

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
requiredKeyTags	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS .	Tidak ada nilai default

Kontrol ini memeriksa apakah tugas over-the-air pembaruan firmware Nirkabel AWS IoT (FUOTA) memiliki tag dengan kunci spesifik yang ditentukan dalam parameter. `requiredKeyTags` Kontrol gagal jika tugas FUOTA tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter `requiredKeyTags`. Jika parameter `requiredKeyTags` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika tugas FUOTA tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat [Menentukan izin berdasarkan atribut dengan otorisasi ABAC di Panduan Pengguna IAM](#).

Note

Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk mengetahui praktik terbaik penandaan lainnya, lihat [Praktik dan strategi terbaik di Panduan Pengguna AWS Sumber Daya Penandaan dan Editor Tag](#).

Remediasi

Untuk menambahkan tag ke tugas FUOTA Nirkabel AWS IoT, [lihat Menandai sumber daya AWS IoT Wireless Anda](#) di AWS IoT Wireless Panduan Pengembang.

Kontrol Security Hub untuk Amazon IVS

AWS Security Hub Kontrol ini mengevaluasi layanan dan sumber daya Amazon Interactive Video Service (IVS).

Kontrol ini mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat [Ketersediaan kontrol berdasarkan Wilayah](#).

[IVS.1] Pasangan kunci pemutaran IVS harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::IVS::PlaybackKeyPair`

AWS Config aturan: `ivs-playback-key-pair-tagged`

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
<code>requiredKeyTags</code>	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS .	Tidak ada nilai default

Kontrol ini memeriksa apakah key pair Amazon IVS playback memiliki tag dengan kunci spesifik yang ditentukan dalam parameter `requiredKeyTags`. Kontrol gagal jika playback key pair tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter `requiredKeyTags`. Jika parameter `requiredKeyTags` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika key pair playback tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat [Menentukan izin berdasarkan atribut dengan otorisasi ABAC di Panduan Pengguna IAM](#).

Note

Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk mengetahui praktik terbaik penandaan lainnya, lihat [Praktik dan strategi terbaik](#) di Panduan Pengguna AWS Sumber Daya Penandaan dan Editor Tag.

Remediasi

Untuk menambahkan tag ke key pair IVS playback, lihat [TagResource](#) di Referensi API Streaming Waktu Nyata Amazon IVS.

[IVS.2] Konfigurasi perekaman IVS harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::IVS::RecordingConfiguration`

AWS Config aturan: `ivs-recording configuration-tagged`

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
<code>requiredKeyTags</code>	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS .	Tidak ada nilai default

Kontrol ini memeriksa apakah konfigurasi perekaman Amazon IVS memiliki tag dengan kunci spesifik yang ditentukan dalam parameter `requiredKeyTags`. Kontrol gagal jika konfigurasi

perekaman tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter `requiredKeyTags`. Jika parameter `requiredKeyTags` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika konfigurasi perekaman tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat [Menentukan izin berdasarkan atribut dengan otorisasi ABAC di Panduan Pengguna IAM](#).

Note

Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk mengetahui praktik terbaik penandaan lainnya, lihat [Praktik dan strategi terbaik di Panduan Pengguna AWS Sumber Daya Penandaan dan Editor Tag](#).

Remediasi

Untuk menambahkan tag ke konfigurasi perekaman IVS, lihat [TagResource](#) di Referensi API Streaming Waktu Nyata Amazon IVS.

[IVS.3] Saluran IVS harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::IVS::Channel`

AWS Config aturan: `ivs-channel-tagged`

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
<code>requiredKeyTags</code>	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS .	Tidak ada nilai default

Kontrol ini memeriksa apakah saluran Amazon IVS memiliki tag dengan kunci spesifik yang ditentukan dalam parameter `requiredKeyTags`. Kontrol gagal jika saluran tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter `requiredKeyTags`. Jika parameter `requiredKeyTags` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika saluran tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws :`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat [Menentukan izin berdasarkan atribut dengan otorisasi ABAC di Panduan Pengguna IAM](#).

Note

Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS

Billing. Untuk mengetahui praktik terbaik penandaan lainnya, lihat [Praktik dan strategi terbaik](#) di Panduan Pengguna AWS Sumber Daya Penandaan dan Editor Tag.

Remediasi

Untuk menambahkan tag ke saluran IVS, lihat [TagResource](#) di Referensi API Streaming Waktu Nyata Amazon IVS.

Kontrol Security Hub untuk Amazon Keyspaces

AWS Security Hub Kontrol ini mengevaluasi layanan dan sumber daya Amazon Keyspaces.

Kontrol ini mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat [Ketersediaan kontrol berdasarkan Wilayah](#).

[Keyspaces.1] Ruang kunci Amazon Keyspaces harus diberi tag

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: AWS::Cassandra::Keyspace

AWS Config aturan: cassandra-keyspace-tagged

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
requiredKeyTags	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS .	Tidak ada nilai default

Kontrol ini memeriksa apakah ruang kunci Amazon Keyspaces memiliki tag dengan kunci tertentu yang ditentukan dalam parameter. `requiredKeyTags` Kontrol gagal jika ruang kunci tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter `requiredKeyTags`. Jika parameter `requiredKeyTags` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika ruang kunci tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws :`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat [Menentukan izin berdasarkan atribut dengan otorisasi ABAC di Panduan Pengguna IAM](#).

Note

Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk mengetahui praktik terbaik penandaan lainnya, lihat [Praktik dan strategi terbaik di Panduan Pengguna AWS Sumber Daya Penandaan dan Editor Tag](#).

Remediasi

Untuk menambahkan tag ke ruang kunci Amazon Keyspaces, lihat [Menambahkan tag ke ruang kunci di Panduan](#) Pengembang Amazon Keyspaces.

Kontrol Security Hub untuk Kinesis

AWS Security Hub Kontrol ini mengevaluasi layanan dan sumber daya Amazon Kinesis.

Kontrol ini mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat [Ketersediaan kontrol berdasarkan Wilayah](#).

[Kinesis.1] Aliran kinesis harus dienkripsi saat istirahat

Persyaratan terkait: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-1 3, NIST.800-53.r5 SC-2 8, NIST.800-53.r5 SC-2 8 (1), NIST.800-53.r5 SC-7 (10), NIST.800-53.R5 SI-7 (6)

Kategori: Lindungi > Perlindungan Data > Enkripsi data-at-rest

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::Kinesis::Stream

AWS Config aturan: [kinesis-stream-encrypted](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah Kinesis Data Streams dienkripsi saat istirahat dengan enkripsi sisi server. Kontrol ini gagal jika aliran Kinesis tidak dienkripsi saat istirahat dengan enkripsi sisi server.

Enkripsi sisi server adalah fitur di Amazon Kinesis Data Streams yang secara otomatis mengenkripsi data sebelum diam dengan menggunakan file. AWS KMS key Data dienkripsi sebelum ditulis ke lapisan penyimpanan aliran Kinesis, dan didekripsi setelah diambil dari penyimpanan. Akibatnya, data Anda dienkripsi saat istirahat dalam layanan Amazon Kinesis Data Streams.

Remediasi

Untuk informasi tentang mengaktifkan enkripsi sisi server untuk aliran Kinesis, lihat [Bagaimana cara memulai enkripsi sisi server?](#) di Panduan Pengembang Amazon Kinesis.

[Kinesis.2] Aliran kinesis harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: AWS::Kinesis::Stream

AWS Config aturan: tagged-kinesis-stream (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
<code>requiredTagKeys</code>	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS.	Tidak ada nilai default

Kontrol ini memeriksa apakah aliran data Amazon Kinesis memiliki tag dengan kunci tertentu yang ditentukan dalam parameter. `requiredTagKeys` Kontrol gagal jika aliran data tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter `requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika aliran data tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat [Untuk apa ABAC? AWS](#) di Panduan Pengguna IAM.

Note

Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS

Billing. Untuk praktik terbaik penandaan lainnya, lihat [Menandai AWS sumber daya Anda](#) di Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke aliran data Kinesis, lihat [Menandai aliran Anda di Amazon Kinesis Data Streams di Panduan Pengembang Amazon Kinesis](#).

[Kinesis.3] Aliran kinesis harus memiliki periode retensi data yang memadai

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::Kinesis::Stream`

AWS Config aturan: [kinesis-stream-backup-retention-check](#)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
<code>minimumBackupRetentionPeriod</code>	Jumlah jam minimum data harus disimpan.	String	24 hingga 8760	168

Kontrol ini memeriksa apakah aliran data Amazon Kinesis memiliki periode retensi data yang lebih besar dari atau sama dengan kerangka waktu yang ditentukan. Kontrol gagal jika periode retensi data kurang dari kerangka waktu yang ditentukan. Kecuali Anda memberikan nilai parameter khusus untuk periode penyimpanan data, Security Hub menggunakan nilai default 168 jam.

Dalam Kinesis Data Streams, aliran data adalah urutan catatan data yang dimaksudkan untuk ditulis dan dibaca secara real time. Catatan data disimpan dalam pecahan di aliran Anda sementara. Periode waktu dari saat catatan ditambahkan ke saat tidak lagi dapat diakses disebut periode retensi. Kinesis Data Streams segera membuat catatan yang lebih tua dari periode retensi

baru tidak dapat diakses setelah mengurangi periode retensi. Misalnya, mengubah periode retensi dari 24 jam menjadi 48 jam berarti rekaman yang ditambahkan ke aliran 23 jam 55 menit sebelumnya masih tersedia setelah 24 jam.

Remediasi

Untuk mengubah periode retensi cadangan untuk Kinesis Data Streams, [lihat Mengubah periode retensi data di Panduan Pengembang](#) Amazon Kinesis Data Streams.

Kontrol Security Hub untuk AWS KMS

AWS Security Hub Kontrol ini mengevaluasi AWS Key Management Service (AWS KMS) layanan dan sumber daya. Kontrol mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat [Ketersediaan kontrol berdasarkan Wilayah](#).

[KMS.1] Kebijakan yang dikelola pelanggan IAM tidak boleh mengizinkan tindakan dekripsi pada semua kunci KMS

Persyaratan terkait: NIST.800-53.r5 AC-2, NIST.800-53.r5 AC-2 (1) NIST.800-53.r5 AC-3,, NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-5, NIST.800-53.r5 AC-6, NIST.800-53.r5 AC-6 (3)

Kategori: Lindungi > Manajemen akses yang aman

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::IAM::Policy

AWS Config aturan: [iam-customer-policy-blocked-kms-actions](#)

Jenis jadwal: Perubahan dipicu

Parameter:

- `blockedActionsPatterns: kms:ReEncryptFrom, kms:Decrypt`(tidak dapat disesuaikan)
- `excludePermissionBoundaryPolicy: True` (tidak dapat disesuaikan)

Memeriksa apakah versi default dari kebijakan terkelola pelanggan IAM mengizinkan prinsipal untuk menggunakan tindakan AWS KMS dekripsi pada semua sumber daya. Kontrol gagal jika kebijakan cukup terbuka untuk mengizinkan `kms:Decrypt` atau `kms:ReEncryptFrom` tindakan pada semua kunci KMS.

Kontrol hanya memeriksa kunci KMS dalam elemen Resource dan tidak memperhitungkan persyaratan apa pun dalam elemen Kondisi kebijakan. Selain itu, kontrol mengevaluasi kebijakan terkelola pelanggan yang terlampir dan tidak terikat. Itu tidak memeriksa kebijakan sebaris atau kebijakan AWS terkelola.

Dengan AWS KMS, Anda mengontrol siapa yang dapat menggunakan kunci KMS Anda dan mendapatkan akses ke data terenkripsi Anda. Kebijakan IAM menentukan tindakan identitas (pengguna, grup, atau peran) yang dapat dilakukan pada sumber daya mana. Mengikuti praktik terbaik keamanan, AWS merekomendasikan agar Anda mengizinkan hak istimewa paling sedikit. Dengan kata lain, Anda harus memberikan identitas hanya `kms:ReEncryptFrom` izin `kms:Decrypt` atau dan hanya untuk kunci yang diperlukan untuk melakukan tugas. Jika tidak, pengguna mungkin menggunakan kunci yang tidak sesuai untuk data Anda.

Alih-alih memberikan izin untuk semua kunci, tentukan kumpulan kunci minimum yang dibutuhkan pengguna untuk mengakses data terenkripsi. Kemudian desain kebijakan yang memungkinkan pengguna untuk hanya menggunakan kunci tersebut. Misalnya, jangan izinkan `kms:Decrypt` izin pada semua kunci KMS. Sebagai gantinya, izinkan `kms:Decrypt` hanya pada kunci di Wilayah tertentu untuk akun Anda. Dengan mengadopsi prinsip hak istimewa terkecil, Anda dapat mengurangi risiko pengungkapan data Anda yang tidak diinginkan.

Remediasi

Untuk mengubah kebijakan terkelola pelanggan IAM, lihat [Mengedit kebijakan yang dikelola pelanggan](#) di Panduan Pengguna IAM. Saat mengedit kebijakan Anda, untuk Resource bidang tersebut, berikan Nama Sumber Daya Amazon (ARN) kunci atau kunci tertentu yang ingin Anda izinkan untuk mengaktifkan tindakan dekripsi.

[KMS.2] Prinsipal IAM tidak boleh memiliki kebijakan inline IAM yang memungkinkan tindakan dekripsi pada semua kunci KMS

Persyaratan terkait: NIST.800-53.r5 AC-2, NIST.800-53.r5 AC-2 (1) NIST.800-53.r5 AC-3,, NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-5, NIST.800-53.r5 AC-6, NIST.800-53.r5 AC-6 (3)

Kategori: Lindungi > Manajemen akses yang aman

Tingkat keparahan: Sedang

Jenis sumber daya:

- `AWS::IAM::Group`
- `AWS::IAM::Role`
- `AWS::IAM::User`

AWS Config aturan: [iam-inline-policy-blocked-kms-actions](#)

Jenis jadwal: Perubahan dipicu

Parameter:

- `blockedActionsPatterns`: `kms:ReEncryptFrom`, `kms:Decrypt`(tidak dapat disesuaikan)

Kontrol ini memeriksa apakah kebijakan inline yang disematkan dalam identitas IAM Anda (peran, pengguna, atau grup) memungkinkan tindakan AWS KMS dekripsi dan enkripsi ulang pada semua kunci KMS. Kontrol gagal jika kebijakan cukup terbuka untuk mengizinkan `kms:Decrypt` atau `kms:ReEncryptFrom` tindakan pada semua kunci KMS.

Kontrol hanya memeriksa kunci KMS dalam elemen Resource dan tidak memperhitungkan persyaratan apa pun dalam elemen Kondisi kebijakan.

Dengan AWS KMS, Anda mengontrol siapa yang dapat menggunakan kunci KMS Anda dan mendapatkan akses ke data terenkripsi Anda. Kebijakan IAM menentukan tindakan identitas (pengguna, grup, atau peran) yang dapat dilakukan pada sumber daya mana. Mengikuti praktik terbaik keamanan, AWS merekomendasikan agar Anda mengizinkan hak istimewa paling sedikit. Dengan kata lain, Anda harus memberikan identitas hanya izin yang mereka butuhkan dan hanya untuk kunci yang diperlukan untuk melakukan tugas. Jika tidak, pengguna mungkin menggunakan kunci yang tidak sesuai untuk data Anda.

Alih-alih memberikan izin untuk semua kunci, tentukan kumpulan kunci minimum yang dibutuhkan pengguna untuk mengakses data terenkripsi. Kemudian desain kebijakan yang memungkinkan pengguna untuk hanya menggunakan kunci tersebut. Misalnya, jangan izinkan `kms:Decrypt` izin pada semua kunci KMS. Sebagai gantinya, izinkan izin hanya pada kunci tertentu di Wilayah tertentu untuk akun Anda. Dengan mengadopsi prinsip hak istimewa terkecil, Anda dapat mengurangi risiko pengungkapan data Anda yang tidak diinginkan.

Remediasi

Untuk mengubah kebijakan sebaris IAM, lihat [Mengedit kebijakan sebaris di Panduan Pengguna IAM](#). Saat mengedit kebijakan Anda, untuk Resource bidang tersebut, berikan Nama Sumber

Daya Amazon (ARN) kunci atau kunci tertentu yang ingin Anda izinkan untuk mengaktifkan tindakan dekripsi.

[KMS.3] tidak AWS KMS keys boleh dihapus secara tidak sengaja

Persyaratan terkait: NIST.800-53.r5 SC-1 2, NIST.800-53.r5 SC-1 2 (2)

Kategori: Lindungi > Perlindungan data > Perlindungan penghapusan data

Tingkat keparahan: Kritis

Jenis sumber daya: AWS : : KMS : : Key

AWS Config aturan: kms-cmk-not-scheduled-for-deletion-2 (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah kunci KMS dijadwalkan untuk dihapus. Kontrol gagal jika kunci KMS dijadwalkan untuk dihapus.

Kunci KMS tidak dapat dipulihkan setelah dihapus. Data yang dienkrpsi di bawah kunci KMS juga tidak dapat dipulihkan secara permanen jika kunci KMS dihapus. Jika data bermakna telah dienkrpsi di bawah kunci KMS yang dijadwalkan untuk dihapus, pertimbangkan untuk mendekripsi data atau mengenkripsi ulang data di bawah kunci KMS baru kecuali Anda sengaja melakukan penghapusan kriptografi.

Ketika kunci KMS dijadwalkan untuk dihapus, periode tunggu wajib diberlakukan untuk memberikan waktu untuk membalikkan penghapusan, jika dijadwalkan dalam kesalahan. Masa tunggu default adalah 30 hari, tetapi dapat dikurangi menjadi sesingkat 7 hari ketika kunci KMS dijadwalkan untuk dihapus. Selama masa tunggu, penghapusan yang dijadwalkan dapat dibatalkan dan kunci KMS tidak akan dihapus.

Untuk informasi tambahan mengenai menghapus kunci KMS, lihat [Menghapus kunci KMS](#) di Panduan Pengembang.AWS Key Management Service

Remediasi

Untuk membatalkan penghapusan kunci KMS terjadwal, lihat Untuk membatalkan penghapusan kunci di bawah Penjadwalan dan pembatalan penghapusan [kunci](#) (konsol) di Panduan Pengembang.AWS Key Management Service

[KMS.4] rotasi AWS KMS tombol harus diaktifkan

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v3.0.0/3.6, Tolok Ukur Yayasan CIS v1.4.0/3.8, Tolok Ukur AWS Yayasan CIS v1.2.0/2.8, 2, 2 (2), 8 (3), PCI DSS AWS v3.2.1/3.6.4, NIST.800-53.r5 SC-1 PCI DSS v4.0.1/3.7.4 NIST.800-53.r5 SC-1 NIST.800-53.r5 SC-2

Kategori: Lindungi > Perlindungan Data > Enkripsi data-at-rest

Tingkat keparahan: Sedang

Jenis sumber daya: AWS : : KMS : : Key

AWS Config aturan: [cmk-backing-key-rotation-enabled](#)

Jenis jadwal: Periodik

Parameter: Tidak ada

AWS KMS memungkinkan pelanggan untuk memutar kunci dukungan, yang merupakan bahan kunci yang disimpan AWS KMS dan diikat ke ID kunci kunci KMS. Ini adalah kunci pendukung yang digunakan untuk melakukan operasi kriptografi seperti enkripsi dan dekripsi. Rotasi kunci otomatis saat ini mempertahankan semua kunci pendukung sebelumnya sehingga dekripsi data terenkripsi dapat berlangsung secara transparan.

CIS merekomendasikan agar Anda mengaktifkan rotasi kunci KMS. Memutar kunci enkripsi membantu mengurangi dampak potensial dari kunci yang dikompromikan karena data yang dienkripsi dengan kunci baru tidak dapat diakses dengan kunci sebelumnya yang mungkin telah diekspos.

Remediasi

Untuk mengaktifkan rotasi tombol KMS, lihat [Cara mengaktifkan dan menonaktifkan rotasi tombol otomatis](#) di Panduan AWS Key Management Service Pengembang.

[KMS.5] Kunci KMS tidak boleh diakses publik

Kategori: Lindungi > Konfigurasi jaringan aman > Sumber daya tidak dapat diakses publik

Tingkat keparahan: Kritis

Jenis sumber daya: AWS : : KMS : : Key

AWS Config aturan: [kms-key-policy-no-public-access](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa AWS KMS key apakah an dapat diakses publik. Kontrol gagal jika kunci KMS dapat diakses publik.

Menerapkan akses hak istimewa paling sedikit sangat penting untuk mengurangi risiko keamanan dan dampak kesalahan atau niat jahat. Jika kebijakan kunci untuk AWS KMS key mengizinkan akses dari akun eksternal, pihak ketiga mungkin dapat mengenkripsi dan mendekripsi data dengan menggunakan kunci. Hal ini dapat mengakibatkan ancaman internal atau eksternal yang mengeksfiltrasi data dari Layanan AWS yang menggunakan kunci.

Note

Kontrol ini juga mengembalikan FAILED temuan AWS KMS key jika konfigurasi Anda AWS Config mencegah merekam kebijakan kunci di Item Konfigurasi (CI) untuk kunci KMS. AWS Config Untuk mengisi kebijakan kunci di CI untuk kunci KMS, [AWS Config peran](#) harus memiliki akses untuk membaca kebijakan kunci menggunakan panggilan [GetKeyPolicy](#) API. Untuk mengatasi jenis FAILED temuan ini, periksa kebijakan yang dapat mencegah AWS Config peran memiliki akses baca ke kebijakan kunci untuk kunci KMS. Misalnya, periksa yang berikut ini:

- Kebijakan kunci untuk kunci KMS.
- [Kebijakan kontrol layanan \(SCPs\)](#) dan [kebijakan kontrol sumber daya \(RCPs\)](#) AWS Organizations yang berlaku untuk akun Anda.
- Izin untuk AWS Config peran tersebut, jika Anda tidak menggunakan peran [AWS Config terkait layanan](#).

Selain itu, kontrol ini tidak mengevaluasi kondisi kebijakan yang menggunakan karakter atau variabel wildcard. Untuk menghasilkan PASSED temuan, kondisi dalam kebijakan kunci hanya boleh menggunakan nilai tetap, yaitu nilai yang tidak mengandung karakter wildcard atau variabel kebijakan. Untuk informasi tentang variabel kebijakan, lihat [Variabel dan tag](#) di Panduan AWS Identity and Access Management Pengguna.

Remediasi

Untuk informasi tentang memperbarui kebijakan kunci AWS KMS key, lihat [Kebijakan kunci AWS KMS di](#) Panduan AWS Key Management Service Pengembang.

Kontrol Security Hub untuk AWS Lambda

AWS Security Hub Kontrol ini mengevaluasi AWS Lambda layanan dan sumber daya. Kontrol mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat [Ketersediaan kontrol berdasarkan Wilayah](#).

[Lambda.1] Kebijakan fungsi Lambda harus melarang akses publik

Persyaratan terkait: NIST.800-53.r5 AC-2 1,, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-3,, (21),, NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (11), (16) NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (20), (21), NIST.800-53.r5 SC-7 (3), (4), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SC-7 PCI DSS v3.2.1/1.2.1, NIST.800-53.r5 SC-7 PCI DSS v3.2.1/1.3.1, PCI DSS v3.2.1/1.3.2, PCI DSS v3.2.1/1.3.4, PCI DSS v3.2.1/7.2.1, PCI DSS v4.0.1/7.2.1 NIST.800-53.r5 SC-7

Kategori: Lindungi > Konfigurasi jaringan aman

Tingkat keparahan: Kritis

Jenis sumber daya: AWS::Lambda::Function

AWS Config aturan: [lambda-function-public-access-prohibited](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah kebijakan berbasis sumber daya fungsi Lambda melarang akses publik di luar akun Anda. Kontrol gagal jika akses publik diizinkan. Kontrol juga gagal jika fungsi Lambda dipanggil dari Amazon S3, dan kebijakan tidak menyertakan kondisi untuk membatasi akses publik, seperti. AWS::SourceAccount Sebaiknya gunakan kondisi S3 lainnya beserta AWS::SourceAccount kebijakan bucket Anda untuk akses yang lebih disempurnakan.

Note

Kontrol ini tidak mengevaluasi kondisi kebijakan yang menggunakan karakter atau variabel wildcard. Untuk menghasilkan PASSED temuan, kondisi dalam kebijakan untuk fungsi Lambda hanya boleh menggunakan nilai tetap, yaitu nilai yang tidak mengandung karakter wildcard atau variabel kebijakan. Untuk informasi tentang variabel kebijakan, lihat [Variabel dan tag](#) di Panduan AWS Identity and Access Management Pengguna.

Fungsi Lambda tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke kode fungsi Anda.

Remediasi

Untuk mengatasi masalah ini, Anda harus memperbarui kebijakan berbasis sumber daya fungsi Anda untuk menghapus izin atau menambahkan kondisi. AWS:SourceAccount Anda hanya dapat memperbarui kebijakan berbasis sumber daya dari Lambda API atau AWS CLI

Untuk memulai, [tinjau kebijakan berbasis sumber daya di](#) konsol Lambda. Identifikasi pernyataan kebijakan yang memiliki nilai Principal bidang yang membuat kebijakan publik, seperti "*" atau { "AWS": "*" }.

Anda tidak dapat mengedit kebijakan dari konsol. Untuk menghapus izin dari fungsi, jalankan [remove-permission](#) perintah dari file. AWS CLI

```
$ aws lambda remove-permission --function-name <function-name> --statement-id <statement-id>
```

Ganti *<function-name>* dengan nama fungsi Lambda, dan *<statement-id>* dengan pernyataan ID (Sid) dari pernyataan yang ingin Anda hapus.

[Lambda.2] Fungsi Lambda harus menggunakan runtime yang didukung

Persyaratan terkait: NIST.800-53.r5 CA-9 (1), NIST.800-53.R5 CM-2, NIST.800-53.R5 SI-2, NIST.800-53.R5 SI-2 (2), Nist.800-53.r5 SI-2 (4), Nist.800-53.R5 SI-2 (5), PCI DSS v4.0.1/12.3.4

Kategori: Lindungi > Pengembangan aman

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::Lambda::Function

AWS Config aturan: [lambda-function-settings-check](#)

Jenis jadwal: Perubahan dipicu

Parameter:

- runtime: dotnet8, java21, java17, java11, java8.al2, nodejs22.x, nodejs20.x, nodejs18.x, python3.13, python3.12, python3.11, python3.10, python3.9, ruby3.4, ruby3.3, ruby3.2 (tidak dapat disesuaikan)

Kontrol ini memeriksa apakah setelan runtime AWS Lambda fungsi cocok dengan nilai yang diharapkan yang ditetapkan untuk runtime yang didukung dalam setiap bahasa. Kontrol gagal jika fungsi Lambda tidak menggunakan runtime yang didukung, seperti yang tercantum di bagian Parameter. Security Hub mengabaikan fungsi yang memiliki tipe paket. Image

Lambda runtime dibangun di sekitar kombinasi sistem operasi, bahasa pemrograman, dan pustaka perangkat lunak yang tunduk pada pemeliharaan dan pembaruan keamanan. Jika komponen runtime tidak lagi didukung untuk pembaruan keamanan, Lambda menghentikan runtime. Meskipun Anda tidak dapat membuat fungsi yang menggunakan runtime yang tidak digunakan lagi, fungsi tersebut masih tersedia untuk memproses peristiwa pemanggilan. Sebaiknya pastikan bahwa fungsi Lambda Anda terkini dan tidak menggunakan lingkungan runtime yang tidak digunakan lagi. Untuk daftar runtime yang didukung, lihat runtime [Lambda](#) di AWS Lambda Panduan Pengembang.

Remediasi

Untuk informasi selengkapnya tentang runtime yang didukung dan jadwal penghentian, lihat kebijakan penghentian [waktu proses di Panduan Pengembang](#). AWS Lambda Saat Anda memigrasikan runtime ke versi terbaru, ikuti sintaks dan panduan dari penerbit bahasa tersebut. Kami juga merekomendasikan untuk menerapkan [pembaruan runtime](#) untuk membantu mengurangi risiko dampak pada beban kerja Anda jika terjadi ketidakcocokan versi runtime yang jarang terjadi.

[Lambda.3] Fungsi Lambda harus dalam VPC

Persyaratan terkait: PCI DSS v3.2.1/1.2.1, PCI DSS v3.2.1/1.3.1, PCI DSS v3.2.1/1.3.2, PCI DSS v3.2.1/1.3.4, NIST.800-53.r5 AC-2 1,, NIST.800-53.r5 AC-3 (7),, (21),,, (11), (16), (20) NIST.800-53.r5 AC-3, (21), (3) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (4), NIST.800-53.r5 AC-6 (9) NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7

Kategori: Lindungi > Konfigurasi jaringan aman

Tingkat keparahan: Rendah

Jenis sumber daya: AWS::Lambda::Function

AWS Config aturan: [lambda-inside-vpc](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah fungsi Lambda digunakan di cloud pribadi virtual (VPC). Kontrol gagal jika fungsi Lambda tidak diterapkan di VPC. Security Hub tidak mengevaluasi konfigurasi perutean subnet VPC untuk menentukan jangkauan publik. Anda mungkin melihat temuan yang gagal untuk sumber daya Lambda @Edge.

Menyebarkan sumber daya dalam VPC memperkuat keamanan dan kontrol atas konfigurasi jaringan. Penerapan tersebut juga menawarkan skalabilitas dan toleransi kesalahan yang tinggi di beberapa Availability Zone. Anda dapat menyesuaikan penerapan VPC untuk memenuhi beragam persyaratan aplikasi.

Remediasi

Untuk mengonfigurasi fungsi yang ada untuk terhubung ke subnet pribadi di VPC Anda, lihat [Mengonfigurasi akses VPC](#) di Panduan Pengembang AWS Lambda. Sebaiknya pilih setidaknya dua subnet pribadi untuk ketersediaan tinggi dan setidaknya satu grup keamanan yang memenuhi persyaratan konektivitas fungsi.

[Lambda.5] Fungsi VPC Lambda harus beroperasi di beberapa Availability Zone

Persyaratan terkait: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6(2), NIST.800-53.r5 SC-3 6, NIST.800-53.r5 SC-5 (2), NIST.800-53.R5 SI-13 (5)

Kategori: Pulihkan > Ketahanan > Ketersediaan tinggi

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::Lambda::Function

AWS Config aturan: [lambda-vpc-multi-az-check](#)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
availabilityZones	Jumlah minimum Availability Zone	Enum	2, 3, 4, 5, 6	2

Kontrol ini memeriksa apakah AWS Lambda fungsi yang terhubung ke virtual private cloud (VPC) beroperasi setidaknya dalam jumlah Availability Zone (AZs) yang ditentukan. Kontrol gagal jika fungsi tidak beroperasi setidaknya dalam jumlah yang ditentukan AZs. Kecuali Anda memberikan nilai parameter kustom untuk jumlah minimum AZs, Security Hub menggunakan nilai default dua AZs.

Menyebarkan sumber daya di beberapa AZs adalah praktik AWS terbaik untuk memastikan ketersediaan tinggi dalam arsitektur Anda. Ketersediaan adalah pilar inti dalam kerahasiaan, integritas, dan model keamanan triad ketersediaan. Semua fungsi Lambda yang terhubung ke VPC harus memiliki penerapan Multi-AZ untuk memastikan bahwa satu zona kegagalan tidak menyebabkan gangguan total operasi.

Remediasi

Jika Anda mengonfigurasi fungsi Anda untuk terhubung ke VPC di akun Anda, tentukan subnet dalam beberapa AZs untuk memastikan ketersediaan tinggi. Untuk petunjuk, lihat [Mengonfigurasi akses VPC](#) di Panduan AWS Lambda Pengembang.

Lambda secara otomatis menjalankan fungsi lain dalam beberapa AZs untuk memastikan bahwa itu tersedia untuk memproses peristiwa jika terjadi gangguan layanan dalam satu zona.

[Lambda.6] Fungsi Lambda harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: AWS::Lambda::Function

AWS Config aturan: tagged-lambda-function (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
requiredTagKeys	Daftar kunci tag non-sistem yang harus berisi sumber daya	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi	No default value

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
	yang dievaluasi. Kunci tag peka huruf besar dan kecil.		persyaratan AWS .	

Kontrol ini memeriksa apakah suatu AWS Lambda fungsi memiliki tag dengan kunci tertentu yang ditentukan dalam parameter `requiredTagKeys`. Kontrol gagal jika fungsi tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter `requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika fungsi tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws :`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat [Untuk apa ABAC? AWS](#) di Panduan Pengguna IAM.

Note

Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat [Menandai AWS sumber daya Anda](#) di Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke fungsi Lambda, lihat [Menggunakan tag pada fungsi Lambda](#) di Panduan Pengembang AWS Lambda

Kontrol Security Hub untuk Macie

AWS Security Hub Kontrol ini mengevaluasi layanan Amazon Macie.

Kontrol ini mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat [Ketersediaan kontrol berdasarkan Wilayah](#).

[Macie.1] Amazon Macie harus diaktifkan

Persyaratan terkait: NIST.800-53.r5 CA-7, NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 SA-8 (19) NIST.800-53.r5 RA-5, NIST.800-53.R5 SI-4

Kategori: Deteksi > Layanan deteksi

Tingkat keparahan: Sedang

Jenis sumber daya: AWS : : : Account

AWS Config aturan: [macie-status-check](#)

Jenis jadwal: Periodik

Kontrol ini memeriksa apakah Amazon Macie diaktifkan untuk sebuah akun. Kontrol gagal jika Macie tidak diaktifkan untuk akun.

Amazon Macie menemukan data sensitif menggunakan pembelajaran mesin dan pencocokan pola, memberikan visibilitas ke risiko keamanan data, dan memungkinkan perlindungan otomatis terhadap risiko tersebut. Macie secara otomatis dan terus-menerus mengevaluasi bucket Amazon Simple Storage Service (Amazon S3) Anda untuk keamanan dan kontrol akses, serta menghasilkan temuan untuk memberi tahu Anda tentang potensi masalah terkait keamanan atau privasi data Amazon S3 Anda. Macie juga mengotomatiskan penemuan dan pelaporan data sensitif, seperti informasi identitas pribadi (PII), untuk memberi Anda pemahaman yang lebih baik tentang data yang Anda simpan di Amazon S3. Untuk mempelajari lebih lanjut, lihat [Panduan Pengguna Amazon Macie](#).

Remediasi

Untuk mengaktifkan Macie, lihat [Mengaktifkan Macie](#) di Panduan Pengguna Amazon Macie.

[Macie.2] Penemuan data sensitif otomatis Macie harus diaktifkan

Persyaratan terkait: NIST.800-53.r5 CA-7, NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 SA-8 (19) NIST.800-53.r5 RA-5, NIST.800-53.R5 SI-4

Kategori: Deteksi > Layanan deteksi

Tingkat keparahan: Tinggi

Jenis sumber daya: AWS :: Account

AWS Config aturan: [macie-auto-sensitive-data-discovery-check](#)

Jenis jadwal: Periodik

Kontrol ini memeriksa apakah penemuan data sensitif otomatis diaktifkan untuk akun administrator Amazon Macie. Kontrol gagal jika penemuan data sensitif otomatis tidak diaktifkan untuk akun administrator Macie. Kontrol ini hanya berlaku untuk akun administrator.

Macie mengotomatiskan penemuan dan pelaporan data sensitif, seperti informasi identitas pribadi (PII), di bucket Amazon Simple Storage Service (Amazon S3). Dengan penemuan data sensitif otomatis, Macie terus mengevaluasi inventaris bucket Anda dan menggunakan teknik pengambilan sampel untuk mengidentifikasi dan memilih objek S3 yang representatif dari bucket Anda. Macie kemudian menganalisis objek yang dipilih, memeriksanya untuk data sensitif. Seiring kemajuan analisis, Macie memperbarui statistik, data inventaris, dan informasi lain yang diberikannya tentang data S3 Anda. Macie juga menghasilkan temuan untuk melaporkan data sensitif yang ditemukannya.

Remediasi

Untuk membuat dan mengonfigurasi tugas penemuan data sensitif otomatis untuk menganalisis objek di bucket S3, lihat [Mengonfigurasi penemuan data sensitif otomatis untuk akun Anda](#) di Panduan Pengguna Amazon Macie.

Kontrol Security Hub untuk Amazon MSK

AWS Security Hub Kontrol ini mengevaluasi layanan dan sumber daya Amazon Managed Streaming for Apache Kafka (Amazon MSK).

Kontrol ini mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat [Ketersediaan kontrol berdasarkan Wilayah](#).

[MSK.1] Kluster MSK harus dienkripsi saat transit di antara node broker

Persyaratan terkait: NIST.800-53.r5 AC-4, NIST.800-53.r5 SC-1 3, NIST.800-53.r5 SC-2 3, 3 (NIST.800-53.r5 SC-23), (4),, NIST.800-53.r5 SC-7 (1) NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 NIST.800-53.r5 SC-8 (2), PCI DSS v4.0.1/4.2.1

Kategori: Lindungi > Perlindungan Data > Enkripsi data-in-transit

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::MSK::Cluster`

AWS Config aturan: [msk-in-cluster-node-require-tls](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah kluster MSK Amazon dienkripsi dalam perjalanan dengan HTTPS (TLS) di antara node broker cluster. Kontrol gagal jika komunikasi teks biasa diaktifkan untuk koneksi node broker cluster.

HTTPS menawarkan lapisan keamanan ekstra karena menggunakan TLS untuk memindahkan data dan dapat digunakan untuk membantu mencegah penyerang potensial menggunakan person-in-the-middle atau serangan serupa untuk menguping atau memanipulasi lalu lintas jaringan. Secara default, Amazon MSK mengenkripsi data dalam perjalanan dengan TLS. Namun, Anda dapat mengganti default ini pada saat Anda membuat cluster. Sebaiknya gunakan koneksi terenkripsi melalui HTTPS (TLS) untuk koneksi node broker.

Remediasi

Untuk memperbarui setelan enkripsi untuk kluster MSK, lihat [Memperbarui setelan keamanan klaster di Panduan Pengembang](#) Amazon Managed Streaming for Apache Kafka.

[MSK.2] Kluster MSK seharusnya telah meningkatkan pemantauan yang dikonfigurasi

Persyaratan terkait: NIST.800-53.r5 CA-7, NIST.800-53.R5 SI-2

Kategori: Deteksi > Layanan deteksi

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::MSK::Cluster`

AWS Config aturan: [msk-enhanced-monitoring-enabled](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah klaster MSK Amazon telah meningkatkan pemantauan yang dikonfigurasi, yang ditentukan oleh tingkat pemantauan setidaknya `PER_TOPIC_PER_BROKER`. Kontrol gagal jika tingkat pemantauan untuk cluster diatur ke `DEFAULT` atau `PER_BROKER`.

Tingkat `PER_TOPIC_PER_BROKER` pemantauan memberikan wawasan yang lebih terperinci tentang kinerja klaster MSK Anda, dan juga menyediakan metrik yang terkait dengan pemanfaatan sumber daya, seperti penggunaan CPU dan memori. Ini membantu Anda mengidentifikasi kemacetan kinerja dan pola pemanfaatan sumber daya untuk masing-masing topik dan broker. Visibilitas ini, pada gilirannya, dapat mengoptimalkan kinerja broker Kafka Anda.

Remediasi

Untuk mengonfigurasi pemantauan yang disempurnakan untuk klaster MSK, selesaikan langkah-langkah berikut:

1. Buka konsol MSK Amazon di <https://console.aws.amazon.com/msk/rumah?region=us-east-1#/home/>.
2. Pada panel navigasi, silakan pilih Klaster. Kemudian, pilih cluster.
3. Untuk Tindakan, pilih Edit pemantauan.
4. Pilih opsi untuk pemantauan tingkat topik yang ditingkatkan.
5. Pilih Simpan perubahan.

Untuk informasi selengkapnya tentang tingkat pemantauan, lihat [Memperbarui setelan keamanan klaster](#) di Panduan Pengembang Amazon Managed Streaming for Apache Kafka.

[MSK.3] Konektor MSK Connect harus dienkripsi saat transit

Persyaratan terkait: PCI DSS v4.0.1/4.2.1

Kategori: Lindungi > Perlindungan Data > Enkripsi data-in-transit

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::KafkaConnect::Connector`

AWS Config aturan: `msk-connect-connector-encrypted` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah konektor Amazon MSK Connect dienkripsi saat transit. Kontrol ini gagal jika konektor tidak dienkripsi saat transit.

Data dalam transit mengacu pada data yang berpindah dari satu lokasi ke lokasi lain, seperti antar node di cluster Anda atau antara cluster dan aplikasi Anda. Data dapat bergerak di internet atau dalam jaringan pribadi. Mengenkripsi data dalam perjalanan mengurangi risiko bahwa pengguna yang tidak sah dapat menguping lalu lintas jaringan.

Remediasi

Anda dapat mengaktifkan enkripsi saat transit saat Anda membuat konektor MSK Connect. Anda tidak dapat mengubah pengaturan enkripsi setelah membuat konektor. Untuk informasi selengkapnya, lihat [Membuat konektor](#) di Panduan Pengembang Amazon Managed Streaming for Apache Kafka.

Kontrol Security Hub untuk Amazon MQ

AWS Security Hub Kontrol ini mengevaluasi layanan dan sumber daya Amazon MQ.

Kontrol ini mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat [Ketersediaan kontrol berdasarkan Wilayah](#).

[MQ.2] Broker ActiveMQ harus mengalirkan log audit ke CloudWatch

Persyaratan terkait: Nist.800-53.r5 AU-2, Nist.800-53.R5 AU-3, Nist.800-53.R5 AU-12, Nist.800-53.r5 SI-4, PCI DSS v4.0.1/10.3.3

Kategori: Identifikasi > Logging

Tingkat keparahan: Sedang

Jenis sumber daya: AWS : : AmazonMQ : : Broker

AWS Config aturan: [mq-cloudwatch-audit-log-enabled](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah broker Amazon MQ ActiveMQ mengalirkan log audit ke Amazon Logs. CloudWatch Kontrol gagal jika broker tidak mengalirkan log audit ke CloudWatch Log.

Dengan menerbitkan log broker ActiveMQ CloudWatch ke Log, Anda dapat CloudWatch membuat alarm dan metrik yang meningkatkan visibilitas informasi terkait keamanan.

Remediasi

Untuk melakukan streaming log broker ActiveMQ CloudWatch ke Log, lihat [Mengonfigurasi Amazon MQ untuk log ActiveMQ di Panduan Pengembang Amazon MQ](#).

[MQ.3] Broker Amazon MQ harus mengaktifkan peningkatan versi minor otomatis

Persyaratan terkait: NIST.800-53.R5 CM-3, NIST.800-53.R5 SI-2, PCI DSS v4.0.1/6.3.3

Kategori: Identifikasi > Kerentanan, tambalan, dan manajemen versi

Tingkat keparahan: Rendah

Jenis sumber daya: AWS : : AmazonMQ : : Broker

AWS Config aturan: [mq-auto-minor-version-upgrade-enabled](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah broker Amazon MQ mengaktifkan peningkatan versi minor otomatis. Kontrol gagal jika broker tidak mengaktifkan peningkatan versi minor otomatis.

Saat Amazon MQ merilis dan mendukung versi mesin broker baru, perubahan tersebut kompatibel dengan aplikasi yang ada dan tidak menghentikan fungsionalitas yang ada. Pembaruan versi mesin broker otomatis melindungi Anda dari risiko keamanan, membantu memperbaiki bug, dan meningkatkan fungsionalitas.

Note

Ketika broker yang terkait dengan peningkatan versi minor otomatis berada di tambalan terbaru dan menjadi tidak didukung, Anda harus mengambil tindakan manual untuk meningkatkan.

Remediasi

Untuk mengaktifkan pemutakhiran versi minor otomatis untuk broker MQ, lihat [Memutakhirkan versi mesin minor secara otomatis](#) di Panduan Pengembang Amazon MQ.

[MQ.4] Broker Amazon MQ harus diberi tag

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: AWS::AmazonMQ::Broker

AWS Config aturan: tagged-amazonmq-broker (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
<code>requiredTagKeys</code>	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS .	No default value

Kontrol ini memeriksa apakah broker Amazon MQ memiliki tag dengan kunci spesifik yang ditentukan dalam parameter. `requiredTagKeys` Kontrol gagal jika broker tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter `requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika broker tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengkategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan

terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat [Untuk apa ABAC? AWS](#) di Panduan Pengguna IAM.

 Note

Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat [Menandai AWS sumber daya Anda](#) di Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke broker Amazon MQ, lihat [Menandai sumber daya](#) di Panduan Pengembang Amazon MQ.

[MQ.5] Broker ActiveMQ harus menggunakan mode penerapan aktif/siaga

Persyaratan terkait: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6(2), NIST.800-53.r5 SC-3 6, NIST.800-53.r5 SC-5 (2), NIST.800-53.R5 SI-13 (5)

Kategori: Pulihkan > Ketahanan > Ketersediaan tinggi

Tingkat keparahan: Rendah

Jenis sumber daya: AWS : : AmazonMQ : : Broker

AWS Config aturan: [mq-active-deployment-mode](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah mode penerapan untuk broker Amazon MQ ActiveMQ diatur ke aktif/siaga. Kontrol gagal jika broker instans tunggal (diaktifkan secara default) ditetapkan sebagai mode penerapan.

Penerapan aktif/siaga menyediakan ketersediaan tinggi untuk broker Amazon MQ ActiveMQ Anda di file. Wilayah AWS Mode penerapan aktif/siaga mencakup dua instance broker di dua Availability Zone yang berbeda, dikonfigurasi dalam pasangan redundan. Pialang ini berkomunikasi secara

serempak dengan aplikasi Anda, yang dapat mengurangi waktu henti dan kehilangan data jika terjadi kegagalan.

Remediasi

Untuk membuat broker ActiveMQ baru dengan mode penerapan aktif/siaga, lihat [Membuat dan mengonfigurasi broker ActiveMQ di Panduan Pengembang Amazon MQ](#). Untuk mode Deployment, pilih broker aktif/siaga. Anda tidak dapat mengubah mode penerapan untuk broker yang ada. Sebagai gantinya, Anda harus membuat broker baru dan menyalin pengaturan dari broker lama.

[MQ.6] Broker RabbitMQ harus menggunakan mode penerapan cluster

Persyaratan terkait: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6(2), NIST.800-53.r5 SC-3 6, NIST.800-53.r5 SC-5 (2), NIST.800-53.R5 SI-13 (5)

Kategori: Pulihkan > Ketahanan > Ketersediaan tinggi

Tingkat keparahan: Rendah

Jenis sumber daya: AWS :: AmazonMQ :: Broker

AWS Config aturan: [mq-rabbit-deployment-mode](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah mode penerapan untuk broker Amazon MQ RabbitMQ disetel ke penerapan cluster. Kontrol gagal jika broker instans tunggal (diaktifkan secara default) ditetapkan sebagai mode penerapan.

Penerapan cluster memberikan ketersediaan tinggi untuk broker Amazon MQ RabbitMQ Anda di file. Wilayah AWS Penyebaran cluster adalah pengelompokan logis dari tiga node broker RabbitMQ, masing-masing dengan volume Amazon Elastic Block Store (Amazon EBS) sendiri dan status bersama. Penyebaran cluster memastikan bahwa data direplikasi ke semua node di cluster, yang dapat mengurangi waktu henti dan hilangnya data jika terjadi kegagalan.

Remediasi

Untuk membuat broker RabbitMQ baru dengan mode penerapan cluster, lihat [Membuat dan menghubungkan ke broker RabbitMQ di Panduan Pengembang Amazon MQ](#). Untuk mode Deployment, pilih Penerapan cluster. Anda tidak dapat mengubah mode penerapan untuk broker

yang ada. Sebagai gantinya, Anda harus membuat broker baru dan menyalin pengaturan dari broker lama.

Kontrol Security Hub untuk Neptuneus

AWS Security Hub Kontrol ini mengevaluasi layanan dan sumber daya Amazon Neptuneus.

Kontrol ini mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat [Ketersediaan kontrol berdasarkan Wilayah](#).

[Neptuneus.1] Cluster DB Neptuneus harus dienkripsi saat istirahat

Persyaratan terkait: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-1 3, NIST.800-53.r5 SC-2 8, NIST.800-53.r5 SC-2 8 (1), NIST.800-53.r5 SC-7 (10), NIST.800-53.R5 SI-7 (6)

Kategori: Lindungi > Perlindungan Data > Enkripsi data-at-rest

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::RDS::DBCluster

AWS Config aturan: [neptune-cluster-encrypted](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah cluster DB Neptuneus dienkripsi saat istirahat. Kontrol gagal jika cluster DB Neptuneus tidak dienkripsi saat istirahat.

Data saat istirahat mengacu pada data apa pun yang disimpan dalam penyimpanan persisten dan tidak mudah menguap untuk durasi berapa pun. Enkripsi membantu Anda melindungi kerahasiaan data tersebut, mengurangi risiko bahwa pengguna yang tidak sah dapat mengaksesnya. Mengenkripsi kluster DB Neptuneus Anda melindungi data dan metadata Anda dari akses yang tidak sah. Ini juga memenuhi persyaratan kepatuhan untuk data-at-rest enkripsi sistem file produksi.

Remediasi

Anda dapat mengaktifkan enkripsi saat istirahat saat Anda membuat cluster DB Neptuneus. Anda tidak dapat mengubah pengaturan enkripsi setelah membuat cluster. Untuk informasi selengkapnya, lihat [Mengekripsi sumber daya Neptuneus saat istirahat di Panduan Pengguna Neptuneus](#).

[Neptune.2] Cluster DB Neptune harus menerbitkan log audit ke Log CloudWatch

Persyaratan terkait: NIST.800-53.r5 AC-2 (4), (26), (9), NIST.800-53.r5 AC-4 NIST.800-53.r5 AC-6 (9), NIST.800-53.R5 SI-20 NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(1), NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 AU-6(5), NIST.800-53.r5 AU-7(1), NIST.800-53.r5 AU-9(7), NIST.800-53.r5 CA-7, NIST.800-53.R5 SI-3 NIST.800-53.r5 SC-7 (8), Nist.800-53.R5 SI-4 (20), NIST.800-53.R5 SI-4 (5), NIST.800-53.R5 SI-7 (8), PCI DSS v4.0.1/10.3.3

Kategori: Identifikasi > Logging

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::RDS::DBCluster

AWS Config aturan: [neptune-cluster-cloudwatch-log-export-enabled](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah kluster DB Neptune menerbitkan log audit ke Amazon Logs. CloudWatch Kontrol gagal jika kluster DB Neptune tidak mempublikasikan log audit ke Log. CloudWatch EnableCloudWatchLogsExport harus diatur ke Audit.

Amazon Neptune dan CloudWatch Amazon terintegrasi sehingga Anda dapat mengumpulkan dan menganalisis metrik kinerja. Neptune secara otomatis mengirimkan metrik CloudWatch ke dan juga mendukung Alarm. CloudWatch Log audit sangat dapat disesuaikan. Saat Anda mengaudit database, setiap operasi pada data dapat dipantau dan dicatat ke jejak audit, termasuk informasi tentang cluster database mana yang diakses dan bagaimana caranya. Kami merekomendasikan pengiriman log ini CloudWatch untuk membantu Anda memantau cluster DB Neptune Anda.

Remediasi

Untuk memublikasikan log audit Neptune CloudWatch ke Log, lihat [Menerbitkan log Neptune ke Log CloudWatch Amazon di Panduan Pengguna Neptune](#). Di bagian Log ekspor, pilih Audit.

[Neptune.3] Snapshot cluster Neptune DB seharusnya tidak publik

Persyaratan terkait: NIST.800-53.r5 AC-2 1, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 AC-6 NIST.800-53.r5

SC-7, NIST.800-53.r5 SC-7 (11), (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (9), PCI DSS v4.0.1/1.4.4

Kategori: Lindungi > Konfigurasi jaringan aman > Sumber daya tidak dapat diakses publik

Tingkat keparahan: Kritis

Jenis sumber daya: AWS::RDS::DBClusterSnapshot

AWS Config aturan: [neptune-cluster-snapshot-public-prohibited](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah snapshot cluster DB manual Neptunus bersifat publik. Kontrol gagal jika snapshot cluster DB manual Neptunus bersifat publik.

Snapshot manual cluster Neptunus DB tidak boleh dipublikasikan kecuali dimaksudkan. Jika Anda membagikan snapshot manual yang tidak terenkripsi sebagai publik, snapshot tersedia untuk semua. Akun AWS Cuplikan publik dapat mengakibatkan eksposur data yang tidak diinginkan.

Remediasi

Untuk menghapus akses publik untuk snapshot kluster DB manual Neptunus, [lihat Berbagi snapshot cluster DB](#) di Panduan Pengguna Neptunus.

[Neptunus.4] Cluster DB Neptunus harus mengaktifkan perlindungan penghapusan

Persyaratan terkait: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2(2), NIST.800-53.r5 CM-3, NIST.800-53.r5 SC-5 (2)

Kategori: Lindungi > Perlindungan data > Perlindungan penghapusan data

Tingkat keparahan: Rendah

Jenis sumber daya: AWS::RDS::DBCluster

AWS Config aturan: [neptune-cluster-deletion-protection-enabled](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah cluster DB Neptuneus mengaktifkan perlindungan penghapusan. Kontrol gagal jika cluster DB Neptuneus tidak mengaktifkan perlindungan penghapusan.

Mengaktifkan perlindungan penghapusan klaster menawarkan lapisan perlindungan tambahan terhadap penghapusan atau penghapusan database yang tidak disengaja oleh pengguna yang tidak sah. Cluster DB Neptuneus tidak dapat dihapus saat perlindungan penghapusan diaktifkan. Anda harus menonaktifkan perlindungan penghapusan terlebih dahulu sebelum permintaan penghapusan berhasil.

Remediasi

Untuk mengaktifkan perlindungan penghapusan klaster DB Neptuneus yang ada, lihat [Memodifikasi cluster DB menggunakan konsol, CLI, dan API di](#) Panduan Pengguna Amazon Aurora.

[Neptuneus.5] Cluster DB Neptuneus harus mengaktifkan cadangan otomatis

Persyaratan terkait: NIST.800-53.R5 SI-12

Kategori: Pulih> Ketahanan > Cadangan diaktifkan

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::RDS::DBCluster

AWS Config aturan: [neptune-cluster-backup-retention-check](#)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub	
minimumBackupRetention	Periode retensi cadangan minimum dalam beberapa hari	Bilangan Bulat	7 untuk 35	7	

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub	
RetentionPeriod					

Kontrol ini memeriksa apakah cluster DB Neptune telah mengaktifkan pencadangan otomatis, dan periode retensi cadangan lebih besar dari atau sama dengan kerangka waktu yang ditentukan. Kontrol gagal jika cadangan tidak diaktifkan untuk cluster DB Neptune, atau jika periode retensi kurang dari kerangka waktu yang ditentukan. Kecuali Anda memberikan nilai parameter khusus untuk periode penyimpanan cadangan, Security Hub menggunakan nilai default 7 hari.

Pencadangan membantu Anda pulih lebih cepat dari insiden keamanan dan memperkuat ketahanan sistem Anda. Dengan mengotomatiskan cadangan untuk cluster DB Neptune Anda, Anda akan dapat memulihkan sistem Anda ke titik waktu tertentu dan meminimalkan waktu henti dan kehilangan data.

Remediasi

Untuk mengaktifkan pencadangan otomatis dan menetapkan periode retensi cadangan untuk kluster DB Neptune Anda, lihat Mengaktifkan [pencadangan otomatis](#) di Panduan Pengguna Amazon RDS. Untuk periode retensi Backup, pilih nilai yang lebih besar dari atau sama dengan 7.

[Neptune.6] Snapshot cluster Neptune DB harus dienkripsi saat istirahat

Persyaratan terkait: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-1 3, NIST.800-53.r5 SC-2 8, NIST.800-53.r5 SC-2 8 (1), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SC-7 (18)

Kategori: Lindungi > Perlindungan Data > Enkripsi data-at-rest

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::RDS::DBClusterSnapshot

AWS Config aturan: [neptune-cluster-snapshot-encrypted](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah snapshot cluster Neptune DB dienkripsi saat istirahat. Kontrol gagal jika cluster DB Neptune tidak dienkripsi saat istirahat.

Data saat istirahat mengacu pada data apa pun yang disimpan dalam penyimpanan persisten dan tidak mudah menguap untuk durasi berapa pun. Enkripsi membantu Anda melindungi kerahasiaan data tersebut, mengurangi risiko bahwa pengguna yang tidak sah mendapatkan akses ke sana. Data dalam snapshot cluster DB Neptune harus dienkripsi saat istirahat untuk lapisan keamanan tambahan.

Remediasi

Anda tidak dapat mengenkripsi snapshot cluster Neptune DB yang ada. Sebagai gantinya, Anda harus mengembalikan snapshot ke cluster DB baru dan mengaktifkan enkripsi pada cluster. Anda dapat membuat snapshot terenkripsi dari cluster terenkripsi. Untuk petunjuknya, lihat [Memulihkan dari snapshot cluster DB dan Membuat snapshot cluster DB di Neptune di Panduan Pengguna Neptune](#).

[Neptune.7] Cluster DB Neptune harus mengaktifkan otentikasi basis data IAM

Persyaratan terkait: NIST.800-53.r5 AC-2 (1) NIST.800-53.r5 AC-3,, NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-6

Kategori: Lindungi > Manajemen akses aman > Otentikasi tanpa kata sandi

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::RDS::DBCluster

AWS Config aturan: [neptune-cluster-iam-database-authentication](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah cluster DB Neptune memiliki otentikasi database IAM diaktifkan. Kontrol gagal jika otentikasi database IAM tidak diaktifkan untuk cluster DB Neptune.

Autentikasi database IAM untuk kluster database Amazon Neptune menghilangkan kebutuhan untuk menyimpan kredensial pengguna dalam konfigurasi database karena otentikasi dikelola secara

eksternal menggunakan IAM. Ketika autentikasi database IAM diaktifkan, setiap permintaan harus ditandatangani menggunakan AWS Signature Version 4.

Remediasi

Secara default, otentikasi database IAM dinonaktifkan saat Anda membuat cluster DB Neptune. Untuk mengaktifkannya, lihat [Mengaktifkan otentikasi database IAM di Neptune di Panduan Pengguna Neptune](#).

[Neptunus.8] Cluster DB Neptune harus dikonfigurasi untuk menyalin tag ke snapshot

Persyaratan terkait: NIST.800-53.r5 CA-9 (1), Nist.800-53.R5 CM-2, Nist.800-53.R5 CM-2 (2)

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: AWS::RDS::DBCluster

AWS Config aturan: [neptune-cluster-copy-tags-to-snapshot-enabled](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah cluster DB Neptune dikonfigurasi untuk menyalin semua tag ke snapshot saat snapshot dibuat. Kontrol gagal jika cluster DB Neptune tidak dikonfigurasi untuk menyalin tag ke snapshot.

Identifikasi dan inventaris aset TI Anda adalah aspek penting dari tata kelola dan keamanan. Anda harus menandai snapshot dengan cara yang sama seperti cluster database Amazon RDS induknya. Menyalin tag memastikan bahwa metadata untuk snapshot DB cocok dengan cluster database induk, dan kebijakan akses untuk snapshot DB juga cocok dengan instans DB induk.

Remediasi

Untuk menyalin tag ke snapshot untuk kluster DB Neptune, lihat [Menyalin tag di Neptune di Panduan Pengguna Neptune](#).

[Neptunus.9] Cluster DB Neptune harus digunakan di beberapa Availability Zone

Persyaratan terkait: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6(2), NIST.800-53.r5 SC-3 6, NIST.800-53.r5 SC-5 (2), NIST.800-53.R5 SI-13 (5)

Kategori: Pulihkan > Ketahanan > Ketersediaan tinggi

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::RDS::DBCluster

AWS Config aturan: [neptune-cluster-multi-az-enabled](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah klaster DB Amazon Neptune memiliki instance baca-replika di beberapa Availability Zones (). AZs Kontrol gagal jika cluster digunakan hanya dalam satu AZ.

Jika AZ tidak tersedia dan selama peristiwa pemeliharaan rutin, replika baca berfungsi sebagai target failover untuk instance utama. Artinya, jika instans primer gagal, Neptune mempromosikan instans replika baca menjadi instans primer. Sebaliknya, jika klaster DB Anda tidak menyertakan instans replika baca, klaster DB Anda tetap tidak tersedia ketika instans primer gagal sampai telah dibuat ulang. Membuat ulang instans primer membutuhkan waktu lebih lama daripada mempromosikan replika baca. Untuk memastikan ketersediaan yang tinggi, sebaiknya Anda membuat satu atau lebih instance read-replica yang memiliki kelas instans DB yang sama dengan instance utama dan terletak berbeda AZs dari instance primer.

Remediasi

Untuk menerapkan cluster DB Neptune dalam AZs beberapa, [lihat Instance DB Read-replika di cluster DB Neptune di Panduan Pengguna Neptune](#).

Kontrol Security Hub untuk AWS Network Firewall

AWS Security Hub Kontrol ini mengevaluasi AWS Network Firewall layanan dan sumber daya. Kontrol mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat [Ketersediaan kontrol berdasarkan Wilayah](#).

[NetworkFirewall.1] Firewall Jaringan harus digunakan di beberapa Availability Zone

Persyaratan terkait: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6(2), NIST.800-53.r5 SC-3 6, NIST.800-53.r5 SC-5 (2), NIST.800-53.R5 SI-13 (5)

Kategori: Pulihkan > Ketahanan > Ketersediaan tinggi

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::NetworkFirewall::Firewall

AWS Config aturan: [netfw-multi-az-enabled](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini mengevaluasi apakah firewall yang dikelola AWS Network Firewall dikerahkan di beberapa Availability Zones (AZs). Kontrol gagal jika firewall digunakan hanya dalam satu AZ.

AWS Infrastruktur global mencakup banyak Wilayah AWS. AZs Secara fisik terpisah, lokasi terisolasi di setiap Wilayah yang terhubung oleh jaringan latensi rendah, throughput tinggi, dan sangat redundan. Dengan menerapkan firewall Network Firewall di beberapa AZs, Anda dapat menyeimbangkan dan mengalihkan lalu lintas di antaranya AZs, yang membantu Anda merancang solusi yang sangat tersedia.

Remediasi

Menerapkan firewall Network Firewall di beberapa AZs

1. Buka konsol Amazon VPC di. <https://console.aws.amazon.com/vpc/>
2. Di panel navigasi, di bawah Network Firewall, pilih Firewall.
3. Pada halaman Firewall, pilih firewall yang ingin Anda edit.
4. Pada halaman detail Firewall, pilih tab Detail Firewall.
5. Di bagian Kebijakan terkait dan VPC, pilih Edit
6. Untuk menambahkan AZ baru, pilih Add New Subnet. Pilih AZ dan subnet yang ingin Anda gunakan. Pastikan Anda memilih setidaknya dua AZs.
7. Pilih Simpan.

[NetworkFirewall.2] Pencatatan Firewall Jaringan harus diaktifkan

Persyaratan terkait: NIST.800-53.r5 AC-2 (12), (4), (26), NIST.800-53.r5 AC-2 (9),, NIST.800-53.r5 AC-4 (9), Nist.800-53.R5 SI-3 NIST.800-53.r5 AC-6 (8) NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5

AU-6(4), NIST.800-53.r5 AU-9(7), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 Nist.800-53.r5 SI-4, Nist.800-53.r5 SI-4 (20), Nist.800-53.r5 SI-7 (8), Nist.800-171.r2 3.1.20, Nist.800-171.r2 3.13.1

Kategori: Identifikasi > Logging

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::NetworkFirewall::LoggingConfiguration

AWS Config aturan: [netfw-logging-enabled](#)

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah logging diaktifkan untuk AWS Network Firewall firewall. Kontrol gagal jika logging tidak diaktifkan untuk setidaknya satu jenis log atau jika tujuan logging tidak ada.

Logging membantu Anda menjaga keandalan, ketersediaan, dan performa Firewall Anda. Di Network Firewall, logging memberikan informasi rinci tentang lalu lintas jaringan, termasuk waktu yang mesin stateful menerima aliran paket, informasi rinci tentang aliran paket, dan setiap tindakan aturan stateful diambil terhadap aliran paket.

Remediasi

Untuk mengaktifkan logging untuk firewall, lihat [Memperbarui konfigurasi logging firewall](#) di Panduan AWS Network Firewall Pengembang.

[NetworkFirewall.3] Kebijakan Network Firewall harus memiliki setidaknya satu kelompok aturan yang terkait

Persyaratan terkait: NIST.800-53.r5 CA-9 (1), Nist.800-53.r5 CM-2, Nist.800-171.r2 3.1.3, Nist.800-171.r2 3.13.1

Kategori: Lindungi > Konfigurasi Jaringan Aman

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::NetworkFirewall::FirewallPolicy

AWS Config aturan: [netfw-policy-rule-group-associated](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah kebijakan Network Firewall memiliki grup aturan stateful atau stateless yang terkait. Kontrol gagal jika kelompok aturan stateless atau stateful tidak ditugaskan.

Kebijakan Firewall menentukan cara Firewall Anda memonitor dan menangani lalu lintas di Amazon Virtual Private Cloud (Amazon VPC). Konfigurasi kelompok aturan stateless dan stateful membantu memfilter paket dan arus lalu lintas, dan mendefinisikan penanganan lalu lintas default.

Remediasi

Untuk menambahkan grup aturan ke kebijakan Network Firewall, lihat [Memperbarui kebijakan firewall](#) di Panduan AWS Network Firewall Pengembang. Untuk informasi tentang membuat dan mengelola grup aturan, lihat [Grup aturan di AWS Network Firewall](#).

[NetworkFirewall.4] Tindakan stateless default untuk kebijakan Network Firewall harus drop atau forward untuk paket penuh

Persyaratan terkait: NIST.800-53.r5 CA-9 (1), Nist.800-53.R5 CM-2

Kategori: Lindungi > Konfigurasi Jaringan Aman

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::NetworkFirewall::FirewallPolicy

AWS Config aturan: [netfw-policy-default-action-full-packets](#)

Jenis jadwal: Perubahan dipicu

Parameter:

- `statelessDefaultActions`: `aws:drop,aws:forward_to_sfe`(tidak dapat disesuaikan)

Kontrol ini memeriksa apakah tindakan stateless default untuk paket penuh untuk kebijakan Network Firewall adalah drop atau forward. Kontrol lolos jika Drop atau Forward dipilih, dan gagal jika Pass dipilih.

Kebijakan firewall menentukan bagaimana firewall Anda memantau dan menangani lalu lintas di Amazon VPC. Anda mengonfigurasi grup aturan stateless dan stateful untuk memfilter paket dan arus lalu lintas. Default untuk Pass dapat memungkinkan lalu lintas yang tidak diinginkan.

Remediasi

Untuk mengubah kebijakan firewall, lihat [Memperbarui kebijakan firewall](#) di Panduan AWS Network Firewall Pengembang. Untuk tindakan default Stateless, pilih Edit. Kemudian, pilih Jatuhkan atau Teruskan ke grup aturan stateful sebagai Tindakan.

[NetworkFirewall.5] Tindakan stateless default untuk kebijakan Network Firewall harus drop atau forward untuk paket yang terfragmentasi

Persyaratan terkait: NIST.800-53.r5 CA-9 (1), Nist.800-53.r5 CM-2, Nist.800-171.r2 3.1.3, Nist.800-171.r2 3.1.14, Nist.800-171.r2 3.13.1, Nist.800-171.r2 3.13.6

Kategori: Lindungi > Konfigurasi Jaringan Aman

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::NetworkFirewall::FirewallPolicy

AWS Config aturan: [netfw-policy-default-action-fragment-packets](#)

Jenis jadwal: Perubahan dipicu

Parameter:

- `statelessFragDefaultActions` (Required) : `aws:drop`, `aws:forward_to_sfe`(tidak dapat disesuaikan)

Kontrol ini memeriksa apakah tindakan stateless default untuk paket terfragmentasi untuk kebijakan Network Firewall adalah drop atau forward. Kontrol lolos jika Drop atau Forward dipilih, dan gagal jika Pass dipilih.

Kebijakan firewall menentukan bagaimana firewall Anda memantau dan menangani lalu lintas di Amazon VPC. Anda mengonfigurasi grup aturan stateless dan stateful untuk memfilter paket dan arus lalu lintas. Default untuk Pass dapat memungkinkan lalu lintas yang tidak diinginkan.

Remediasi

Untuk mengubah kebijakan firewall, lihat [Memperbarui kebijakan firewall](#) di Panduan AWS Network Firewall Pengembang. Untuk tindakan default Stateless, pilih Edit. Kemudian, pilih Jatuhkan atau Teruskan ke grup aturan stateful sebagai Tindakan.

[NetworkFirewall.6] Grup aturan Stateless Network Firewall tidak boleh kosong

Persyaratan terkait: NIST.800-53.r5 AC-4 (21), (11), (16) NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (5), NIST.800-53.r5 SC-7 Nist.800-171.r2 3.1.3, NIST.800-53.r5 SC-7 Nist.800-171.r2 3.1.14, Nist.800-171.r2 3.13.1, Nist.800-171.r2 3.13.6

Kategori: Lindungi > Konfigurasi Jaringan Aman

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::NetworkFirewall::RuleGroup

AWS Config aturan: [netfw-stateless-rule-group-not-empty](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah grup aturan stateless AWS Network Firewall berisi aturan. Kontrol gagal jika tidak ada aturan di grup aturan.

Grup aturan berisi aturan yang menentukan bagaimana firewall Anda memproses lalu lintas di VPC Anda. Grup aturan stateless kosong, ketika ada dalam kebijakan firewall, mungkin memberi kesan bahwa grup aturan akan memproses lalu lintas. Namun, ketika grup aturan stateless kosong, itu tidak memproses lalu lintas.

Remediasi

Untuk menambahkan aturan ke grup aturan Firewall Jaringan, lihat [Memperbarui grup aturan stateful di Panduan AWS Network Firewall](#) Pengembang. Pada halaman detail firewall, untuk grup aturan Stateless, pilih Edit untuk menambahkan aturan.

[NetworkFirewall.7] Firewall Jaringan harus diberi tag

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: AWS::NetworkFirewall::Firewall

AWS Config aturan: tagged-networkfirewall-firewall (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
<code>requiredTagKeys</code>	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS.	No default value

Kontrol ini memeriksa apakah AWS Network Firewall firewall memiliki tag dengan kunci spesifik yang ditentukan dalam parameter `requiredTagKeys`. Kontrol gagal jika firewall tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter `requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika firewall tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke sebuah AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat Anda menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk penanggung jawab IAM Anda. Anda dapat merancang kebijakan ABAC ini untuk memungkinkan operasi ketika tag penanggung jawab cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat [Untuk apa ABAC untuk? AWS](#) di Panduan Pengguna IAM.

Note

Jangan menambahkan informasi pengenalan pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS

Billing. Untuk praktik terbaik penandaan lainnya, lihat [Menandai AWS sumber daya Anda](#) di Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke firewall Network Firewall, lihat [Menandai AWS Network Firewall sumber daya](#) di Panduan AWS Network Firewall Pengembang.

[NetworkFirewall.8] Kebijakan firewall Network Firewall harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::NetworkFirewall::FirewallPolicy`

AWS Config aturan: `tagged-networkfirewall-firewallpolicy` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
<code>requiredTagKeys</code>	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS .	No default value

Kontrol ini memeriksa apakah kebijakan AWS Network Firewall firewall memiliki tag dengan kunci spesifik yang ditentukan dalam parameter `requiredTagKeys`. Kontrol gagal jika kebijakan firewall tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter `requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika kebijakan firewall tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke sebuah AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat Anda menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk penanggung jawab IAM Anda. Anda dapat merancang kebijakan ABAC ini untuk memungkinkan operasi ketika tag penanggung jawab cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat [Untuk apa ABAC untuk? AWS](#) di Panduan Pengguna IAM.

Note

Jangan menambahkan informasi pengenalan pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat [Menandai AWS sumber daya Anda](#) di Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke kebijakan Network Firewall, lihat [Menandai AWS Network Firewall sumber daya](#) di Panduan AWS Network Firewall Pengembang.

[NetworkFirewall.9] Firewall Jaringan harus mengaktifkan perlindungan penghapusan

Persyaratan terkait: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2(2), NIST.800-53.r5 CM-3, NIST.800-53.r5 SC-5 (2)

Kategori: Lindungi > Keamanan Jaringan

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::NetworkFirewall::Firewall

AWS Config aturan: [netfw-deletion-protection-enabled](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah AWS Network Firewall Firewall memiliki perlindungan penghapusan diaktifkan. Kontrol gagal jika perlindungan penghapusan tidak diaktifkan untuk firewall.

AWS Network Firewall adalah firewall jaringan stateful, dikelola dan layanan deteksi intrusi yang memungkinkan Anda untuk memeriksa dan memfilter lalu lintas ke, dari, atau antara Virtual Private Clouds () Anda. VPCs Pengaturan perlindungan penghapusan melindungi terhadap penghapusan firewall yang tidak disengaja.

Remediasi

Untuk mengaktifkan proteksi penghapusan pada firewall Network Firewall yang ada, lihat [Memperbarui firewall](#) di Panduan AWS Network Firewall Pengembang. Untuk Ubah perlindungan, pilih Aktifkan. Anda juga dapat mengaktifkan perlindungan penghapusan dengan menjalankan [UpdateFirewallDeleteProtection](#) API dan menyetel bidang ke. `DeleteProtection true`

[NetworkFirewall.10] Firewall Jaringan harus mengaktifkan perlindungan perubahan subnet

Persyaratan terkait: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2(2), NIST.800-53.r5 CM-3, NIST.800-53.r5 SC-5 (2)

Kategori: Lindungi > Keamanan Jaringan

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::NetworkFirewall::Firewall`

AWS Config aturan: [netfw-subnet-change-protection-enabled](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah perlindungan perubahan subnet diaktifkan untuk AWS Network Firewall firewall. Kontrol gagal jika perlindungan perubahan subnet tidak diaktifkan untuk firewall.

AWS Network Firewall adalah firewall jaringan stateful yang dikelola dan layanan deteksi intrusi yang dapat Anda gunakan untuk memeriksa dan memfilter lalu lintas ke, dari, atau di antara Virtual

Private Clouds () Anda. VPCs Jika Anda mengaktifkan perlindungan perubahan subnet untuk firewall Network Firewall, Anda dapat melindungi firewall terhadap perubahan yang tidak disengaja pada asosiasi subnet firewall.

Remediasi

Untuk informasi tentang mengaktifkan perlindungan perubahan subnet untuk firewall Network Firewall yang ada, lihat [Memperbarui firewall di Panduan AWS Network Firewall](#) Pengembang.

Kontrol Security Hub untuk Amazon OpenSearch Service

AWS Security Hub Kontrol ini mengevaluasi OpenSearch layanan dan sumber daya Amazon OpenSearch Service (Service). Kontrol mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat [Ketersediaan kontrol berdasarkan Wilayah](#).

[Opensearch.1] OpenSearch domain harus mengaktifkan enkripsi saat istirahat

Persyaratan terkait: PCI DSS v3.2.1/1.2.1, PCI DSS v3.2.1/1.3.1, PCI DSS v3.2.1/1.3.4, PCI DSS v3.2.1/7.2.1, (1), 3, 8, 8 (1), NIST.800-53.R5 SI-7 (6) NIST.800-53.r5 CA-9 NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-1 NIST.800-53.r5 SC-2 NIST.800-53.r5 SC-2

Kategori: Lindungi > Perlindungan Data > Enkripsi data-at-rest

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::OpenSearch::Domain

AWS Config aturan: [opensearch-encrypted-at-rest](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah OpenSearch domain memiliki encryption-at-rest konfigurasi yang diaktifkan. Pemeriksaan gagal jika enkripsi saat istirahat tidak diaktifkan.

Untuk lapisan keamanan tambahan untuk data sensitif, Anda harus mengonfigurasi domain OpenSearch Layanan Anda untuk dienkrpsi saat istirahat. Saat Anda mengonfigurasi enkripsi data saat istirahat, AWS KMS menyimpan dan mengelola kunci enkripsi Anda. Untuk melakukan enkripsi, AWS KMS gunakan algoritma Advanced Encryption Standard dengan kunci 256-bit (AES-256).

Untuk mempelajari lebih lanjut tentang enkripsi OpenSearch Layanan saat istirahat, lihat [Enkripsi data saat istirahat untuk OpenSearch Layanan Amazon](#) di Panduan Pengembang OpenSearch Layanan Amazon.

Remediasi

Untuk mengaktifkan enkripsi saat istirahat untuk OpenSearch domain baru dan yang sudah ada, lihat [Mengaktifkan enkripsi data saat istirahat di](#) Panduan Pengembang OpenSearch Layanan Amazon.

[Opensearch.2] OpenSearch domain tidak boleh diakses publik

Persyaratan terkait: PCI DSS v3.2.1/1.2.1, PCI DSS v3.2.1/1.3.1, PCI DSS v3.2.1/1.3.2, PCI DSS v3.2.1/1.3.4, PCI DSS v3.2.1/1.3.6, NIST.800-53.r5 AC-2 1,, (7),, (21),,, (11), (16), (20), (21), (3), (4 NIST.800-53.r5 AC-3) NIST.800-53.r5 AC-3, (9) NIST.800-53.r5 AC-4 NIST.800-53.r5 AC-4 NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7

Kategori: Lindungi > Konfigurasi jaringan aman> Sumber daya dalam VPC

Tingkat keparahan: Kritis

Jenis sumber daya: AWS::OpenSearch::Domain

AWS Config aturan: [opensearch-in-vpc-only](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah OpenSearch domain berada dalam VPC. Itu tidak mengevaluasi konfigurasi perutean subnet VPC untuk menentukan akses publik.

Anda harus memastikan bahwa OpenSearch domain tidak dilampirkan ke subnet publik. Lihat [Kebijakan berbasis sumber daya di Panduan Pengembang](#) Layanan Amazon OpenSearch . Anda juga harus memastikan bahwa VPC Anda dikonfigurasi sesuai dengan praktik terbaik yang disarankan. Lihat [Praktik terbaik keamanan untuk VPC Anda](#) di Panduan Pengguna Amazon VPC.

OpenSearch domain yang digunakan dalam VPC dapat berkomunikasi dengan sumber daya VPC melalui AWS jaringan pribadi, tanpa perlu melintasi internet publik. Konfigurasi ini meningkatkan

postur keamanan dengan membatasi akses ke data dalam perjalanan. VPCs menyediakan sejumlah kontrol jaringan untuk mengamankan akses ke OpenSearch domain, termasuk ACL jaringan dan grup keamanan. Security Hub menyarankan agar Anda memigrasikan OpenSearch domain publik VPCs untuk memanfaatkan kontrol ini.

Remediasi

Jika Anda membuat domain dengan titik akhir publik, Anda tidak dapat menempatkannya di dalam VPC nanti. Sebagai gantinya, Anda harus membuat domain baru dan memigrasi data Anda. Begitu juga sebaliknya. Jika Anda membuat domain dalam VPC, domain tersebut tidak dapat memiliki titik akhir publik. Sebagai gantinya, Anda harus [membuat domain lain](#) atau menonaktifkan kontrol ini.

Untuk petunjuknya, lihat [Meluncurkan domain OpenSearch Layanan Amazon Anda dalam VPC](#) di Panduan Pengembang Layanan OpenSearch Amazon.

[Opensearch.3] OpenSearch domain harus mengenkripsi data yang dikirim antar node

Persyaratan terkait: NIST.800-53.r5 AC-4, NIST.800-53.r5 SC-1 3, NIST.800-53.r5 SC-2 3, NIST.800-53.r5 SC-2 3 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 (1), NIST.800-53.r5 SC-8 (2)

Kategori: Lindungi > Perlindungan Data > Enkripsi data-in-transit

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::OpenSearch::Domain

AWS Config aturan: [opensearch-node-to-node-encryption-check](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah OpenSearch domain telah mengaktifkan node-to-node enkripsi. Kontrol ini gagal jika node-to-node enkripsi dinonaktifkan pada domain.

HTTPS (TLS) dapat digunakan untuk membantu mencegah penyerang potensial menguping atau memanipulasi lalu lintas jaringan menggunakan atau serangan serupa. person-in-the-middle Hanya koneksi terenkripsi melalui HTTPS (TLS) yang diizinkan. Mengaktifkan node-to-node enkripsi untuk OpenSearch domain memastikan bahwa komunikasi intra-cluster dienkripsi dalam perjalanan.

Mungkin ada penalti kinerja yang terkait dengan konfigurasi ini. Anda harus mengetahui dan menguji trade-off kinerja sebelum mengaktifkan opsi ini.

Remediasi

Untuk mengaktifkan node-to-node enkripsi pada OpenSearch domain, lihat [Mengaktifkan node-to-node enkripsi](#) di Panduan Pengembang OpenSearch Layanan Amazon.

[Opensearch.4] login kesalahan OpenSearch domain ke Log harus diaktifkan CloudWatch

Persyaratan terkait: NIST.800-53.r5 AC-2 (4), (26), NIST.800-53.r5 AC-4 (9),, NIST.800-53.r5 AC-6 (9), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7 NIST.800-53.R5 SI-3 NIST.800-53.r5 SC-7 (8), NIST.800-53.R5 SI-4 (20), NIST.800-53.R5 SI-7 (8)

Kategori: Identifikasi > Logging

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::OpenSearch::Domain

AWS Config aturan: [opensearch-logs-to-cloudwatch](#)

Jenis jadwal: Perubahan dipicu

Parameter:

- logtype = 'error' (tidak dapat disesuaikan)

Kontrol ini memeriksa apakah OpenSearch domain dikonfigurasi untuk mengirim log kesalahan ke CloudWatch Log. Kontrol ini gagal jika error logging ke tidak CloudWatch diaktifkan untuk domain.

Anda harus mengaktifkan log kesalahan untuk OpenSearch domain dan mengirim log tersebut ke CloudWatch Log untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.

Remediasi

Untuk mengaktifkan penerbitan log, lihat [Mengaktifkan penerbitan log \(konsol\)](#) di Panduan Pengembang OpenSearch Layanan Amazon.

[Opensearch.5] OpenSearch domain harus mengaktifkan pencatatan audit

Persyaratan terkait: NIST.800-53.r5 AC-2 (4), (26), NIST.800-53.r5 AC-4 (9),, NIST.800-53.r5 AC-6 (9), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7 Nist.800-53.R5 SI-3 NIST.800-53.r5 SC-7 (8), Nist.800-53.r5 SI-4 (20), Nist.800-53.R5 SI-7 (8), PCI DSS v4.0.1/10.2.1

Kategori: Identifikasi > Logging

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::OpenSearch::Domain

AWS Config aturan: [opensearch-audit-logging-enabled](#)

Jenis jadwal: Perubahan dipicu

Parameter:

- `cloudWatchLogsLogGroupArnList`(tidak dapat disesuaikan) - Security Hub tidak mengisi parameter ini. Daftar grup CloudWatch log Log yang dipisahkan koma yang harus dikonfigurasi untuk log audit.

Kontrol ini memeriksa apakah OpenSearch domain telah mengaktifkan pencatatan audit. Kontrol ini gagal jika OpenSearch domain tidak mengaktifkan pencatatan audit.

Log audit sangat dapat disesuaikan. Mereka memungkinkan Anda melacak aktivitas pengguna di OpenSearch kluster Anda, termasuk keberhasilan dan kegagalan otentikasi, permintaan, perubahan indeksOpenSearch, dan kueri penelusuran yang masuk.

Remediasi

Untuk petunjuk cara mengaktifkan log audit, lihat [Mengaktifkan log audit di Panduan](#) Pengembang OpenSearch Layanan Amazon.

[Opensearch.6] OpenSearch domain harus memiliki setidaknya tiga node data

Persyaratan terkait: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6(2), NIST.800-53.r5 SC-3 6, NIST.800-53.r5 SC-5 (2), NIST.800-53.R5 SI-13 (5)

Kategori: Pulihkan > Ketahanan > Ketersediaan tinggi

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::OpenSearch::Domain

AWS Config aturan: [opensearch-data-node-fault-tolerance](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah OpenSearch domain dikonfigurasi dengan setidaknya tiga node data dan `zoneAwarenessEnabled` adalah `true`. Kontrol ini gagal untuk OpenSearch domain jika `instanceCount` kurang dari 3 atau `zoneAwarenessEnabled` kurang `false`.

Untuk mencapai ketersediaan tinggi tingkat cluster dan toleransi kesalahan, OpenSearch domain harus memiliki setidaknya tiga node data. Menyebarkan OpenSearch domain dengan setidaknya tiga node data memastikan operasi cluster jika node gagal.

Remediasi

Untuk memodifikasi jumlah node data dalam OpenSearch domain

1. Masuk ke AWS konsol dan buka konsol OpenSearch Layanan Amazon di <https://console.aws.amazon.com/aos/>.
2. Di bawah Domain saya, pilih nama domain yang akan diedit, dan pilih Edit.
3. Di bawah Data node mengatur Jumlah node ke angka yang lebih besar dari 3. Jika Anda menerapkan ke tiga Availability Zone, setel nomor ke kelipatan tiga untuk memastikan distribusi yang sama di seluruh Availability Zone.
4. Pilih Kirim.

[Opensearch.7] OpenSearch domain harus mengaktifkan kontrol akses berbutir halus

Persyaratan terkait: NIST.800-53.r5 AC-2 (1) NIST.800-53.r5 AC-3,, NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-5, NIST.800-53.r5 AC-6

Kategori: Lindungi > Manajemen Akses Aman > Tindakan API sensitif dibatasi

Tingkat keparahan: Tinggi

Jenis sumber daya: AWS::OpenSearch::Domain

AWS Config aturan: [opensearch-access-control-enabled](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah OpenSearch domain memiliki kontrol akses berbutir halus yang diaktifkan. Kontrol gagal jika kontrol akses berbutir halus tidak diaktifkan. Kontrol akses berbutir halus membutuhkan OpenSearch parameter `advanced-security-options` yang akan diaktifkan `update-domain-config`.

Kontrol akses berbutir halus menawarkan cara tambahan untuk mengontrol akses ke data Anda di Layanan Amazon. OpenSearch

Remediasi

Untuk mengaktifkan kontrol akses berbutir halus, lihat Kontrol akses [berbutir halus di OpenSearch Layanan Amazon di Panduan Pengembang Layanan Amazon](#). OpenSearch

[Opensearch.8] Koneksi ke OpenSearch domain harus dienkripsi menggunakan kebijakan keamanan TLS terbaru

Persyaratan terkait: NIST.800-53.r5 AC-1 7 (2), NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5 (1), NIST.800-53.r5 SC-1 2 (3), 3, NIST.800-53.r5 SC-1 3, 3 (NIST.800-53.r5 SC-23), NIST.800-53.r5 SC-2 (4),, NIST.800-53.r5 SC-7 (1), NIST.800-53.r5 SC-8 (2) NIST.800-53.r5 SC-8, Nist.800-53.R5 SI-7 NIST.800-53.r5 SC-8 (6)

Kategori: Lindungi > Perlindungan Data > Enkripsi data-in-transit

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::OpenSearch::Domain

AWS Config aturan: [opensearch-https-required](#)

Jenis jadwal: Perubahan dipicu

Parameter:

- `tlsPolicies: Policy-Min-TLS-1-2-PFS-2023-10`(tidak dapat disesuaikan)

Kontrol ini memeriksa apakah titik akhir domain OpenSearch Layanan Amazon dikonfigurasi untuk menggunakan kebijakan keamanan TLS terbaru. Kontrol gagal jika titik akhir OpenSearch domain tidak dikonfigurasi untuk menggunakan kebijakan terbaru yang didukung atau jika HTTPS tidak diaktifkan.

HTTPS (TLS) dapat digunakan untuk membantu mencegah penyerang potensial menggunakan person-in-the-middle atau serangan serupa untuk menguping atau memanipulasi lalu lintas jaringan. Hanya koneksi terenkripsi melalui HTTPS (TLS) yang diizinkan. Mengenkripsi data dalam perjalanan dapat memengaruhi kinerja. Anda harus menguji aplikasi Anda dengan fitur ini untuk memahami profil kinerja dan dampak TLS. TLS 1.2 menyediakan beberapa peningkatan keamanan dibandingkan versi TLS sebelumnya.

Remediasi

Untuk mengaktifkan enkripsi TLS, gunakan operasi [UpdateDomainConfig](#) API. Konfigurasi [DomainEndpointOptions](#) bidang untuk menentukan nilai untuk `TLSecurityPolicy`. Untuk informasi selengkapnya, lihat [Node-to-node enkripsi](#) di Panduan Pengembang OpenSearch Layanan Amazon.

[Opensearch.9] domain harus ditandai OpenSearch

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::OpenSearch::Domain`

AWS Config aturan: `tagged-opensearch-domain` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
<code>requiredTagKeys</code>	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi	No default value

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub

[persyaratan AWS](#).

Kontrol ini memeriksa apakah domain OpenSearch Layanan Amazon memiliki tag dengan kunci tertentu yang ditentukan dalam parameter `requiredTagKeys`. Kontrol gagal jika domain tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter `requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika domain tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat [Untuk apa ABAC? AWS](#) di Panduan Pengguna IAM.

Note

Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat [Menandai AWS sumber daya Anda](#) di Referensi Umum AWS.

Remediasi

Untuk menambahkan tag ke domain OpenSearch Layanan, lihat [Bekerja dengan tag](#) di Panduan Pengembang OpenSearch Layanan Amazon.

[Opensearch.10] OpenSearch domain harus menginstal pembaruan perangkat lunak terbaru

Persyaratan terkait: NIST.800-53.R5 SI-2, NIST.800-53.R5 SI-2 (2), NIST.800-53.R5 SI-2 (4), NIST.800-53.R5 SI-2 (5), PCI DSS v4.0.1/6.3.3

Kategori: Identifikasi > Kerentanan, tambalan, dan manajemen versi

Tingkat keparahan: Rendah

Jenis sumber daya: AWS::OpenSearch::Domain

AWS Config aturan: [opensearch-update-check](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah domain OpenSearch Layanan Amazon memiliki pembaruan perangkat lunak terbaru yang diinstal. Kontrol gagal jika pembaruan perangkat lunak tersedia tetapi tidak diinstal untuk domain.

OpenSearch Pembaruan perangkat lunak layanan menyediakan perbaikan, pembaruan, dan fitur platform terbaru yang tersedia untuk lingkungan. Menjaga up-to-date instalasi patch membantu menjaga keamanan dan ketersediaan domain. Jika tidak ada tindakan yang diambil pada pembaruan yang diperlukan, perangkat lunak layanan diperbarui secara otomatis (biasanya setelah 2 minggu). Kami merekomendasikan penjadwalan pembaruan selama waktu lalu lintas rendah ke domain untuk meminimalkan gangguan layanan.

Remediasi

Untuk menginstal pembaruan perangkat lunak untuk OpenSearch domain, lihat [Memulai pembaruan](#) di Panduan Pengembang OpenSearch Layanan Amazon.

[Opensearch.11] OpenSearch domain harus memiliki setidaknya tiga node primer khusus

Persyaratan terkait: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-2, NIST.800-53.r5 SC-5, NIST.800-53.r5 SC-3 6, NIST.800-53.R5 SI-13

Kategori: Pulihkan > Ketahanan > Ketersediaan tinggi

Tingkat keparahan: Rendah

Jenis sumber daya: AWS::OpenSearch::Domain

AWS Config aturan: [opensearch-primary-node-fault-tolerance](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah domain OpenSearch Layanan Amazon dikonfigurasi dengan setidaknya tiga node utama khusus. Kontrol gagal jika domain memiliki kurang dari tiga node utama khusus.

OpenSearch Layanan menggunakan node primer khusus untuk meningkatkan stabilitas cluster. Node utama khusus melakukan tugas manajemen kluster, tetapi tidak menyimpan data atau menanggapi permintaan unggahan data. Kami menyarankan Anda menggunakan Multi-AZ dengan standby, yang menambahkan tiga node utama khusus untuk setiap domain produksi OpenSearch .

Remediasi

Untuk mengubah jumlah node utama untuk OpenSearch domain, lihat [Membuat dan mengelola domain OpenSearch Layanan Amazon](#) di Panduan Pengembang OpenSearch Layanan Amazon.

Kontrol Security Hub untuk AWS Private CA

AWS Security Hub Kontrol ini mengevaluasi AWS Private Certificate Authority (AWS Private CA) layanan dan sumber daya.

Kontrol ini mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat [Ketersediaan kontrol berdasarkan Wilayah](#).

[PCA.1] otoritas sertifikat AWS Private CA root harus dinonaktifkan

Persyaratan terkait: NIST.800-53.r5 CA-9 (1), Nist.800-53.R5 CM-2

Kategori: Lindungi > Konfigurasi jaringan aman

Tingkat keparahan: Rendah

Jenis sumber daya: AWS::ACMPCA::CertificateAuthority

AWS Config aturan: [acm-pca-root-ca-disabled](#)

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah AWS Private CA memiliki otoritas sertifikat root (CA) yang dinonaktifkan. Kontrol gagal jika root CA diaktifkan.

Dengan AWS Private CA, Anda dapat membuat hierarki CA yang mencakup CA root dan bawahan CAs. Anda harus meminimalkan penggunaan CA root untuk tugas sehari-hari, terutama di lingkungan produksi. Root CA seharusnya hanya digunakan untuk menerbitkan sertifikat untuk perantara CAs. Hal ini memungkinkan CA root disimpan di luar bahaya sementara perantara CAs melakukan tugas harian menerbitkan sertifikat entitas akhir.

Remediasi

Untuk menonaktifkan root CA, lihat [Memperbarui status CA](#) di Panduan AWS Private Certificate Authority Pengguna.

[PCA.2] Otoritas sertifikat CA AWS swasta harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::ACMPCA::CertificateAuthority`

AWS Config aturan: `acmpca-certificate-authority-tagged`

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
<code>requiredKeyTags</code>	Daftar kunci tag non-sistem yang harus berisi sumber daya	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi	Tidak ada nilai default

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
	yang dievaluasi. Kunci tag peka huruf besar dan kecil.		persyaratan AWS .	

Kontrol ini memeriksa apakah otoritas sertifikat CA AWS Pribadi memiliki tag dengan kunci spesifik yang ditentukan dalam parameter `requiredKeyTags`. Kontrol gagal jika otoritas sertifikat tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter `requiredKeyTags`. Jika parameter `requiredKeyTags` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika otoritas sertifikat tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat [Menentukan izin berdasarkan atribut dengan otorisasi ABAC di Panduan Pengguna IAM](#).

Note

Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk mengetahui praktik terbaik penandaan lainnya, lihat [Praktik dan strategi terbaik di Panduan Pengguna AWS Sumber Daya Penandaan dan Editor Tag](#).

Remediasi

Untuk menambahkan tag ke otoritas CA AWS Pribadi, lihat [Menambahkan tag untuk CA pribadi Anda di Panduan AWS Private Certificate Authority Pengguna](#).

Kontrol Security Hub untuk Amazon RDS

AWS Security Hub Kontrol ini mengevaluasi layanan dan sumber daya Amazon Relational Database Service (Amazon RDS). Kontrol mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat [Ketersediaan kontrol berdasarkan Wilayah](#).

[RDS.1] Snapshot RDS harus bersifat pribadi

Persyaratan terkait: PCI DSS v3.2.1/1.2.1, PCI DSS v3.2.1/1.3.1, PCI DSS v3.2.1/1.3.4, PCI DSS v3.2.1/1.3.6, PCI DSS v3.2.1/7.2.1, NIST.800-53.r5 AC-2 1,, (7),, (21),,, (11), (16), (20), (21), (3), (4 NIST.800-53.r5 AC-3) NIST.800-53.r5 AC-3, (9) NIST.800-53.r5 AC-4 NIST.800-53.r5 AC-4 NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7

Kategori: Lindungi > Konfigurasi jaringan aman

Tingkat keparahan: Kritis

Jenis sumber daya: AWS::RDS::DBClusterSnapshot, AWS::RDS::DBSnapshot

AWS Config aturan: [rds-snapshots-public-prohibited](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah snapshot Amazon RDS bersifat publik. Kontrol gagal jika snapshot RDS bersifat publik. Kontrol ini mengevaluasi instans RDS, instans Aurora DB, instans DB Neptune, dan cluster Amazon DocumentDB.

Snapshot RDS digunakan untuk mencadangkan data pada instans RDS Anda pada titik waktu tertentu. Mereka dapat digunakan untuk mengembalikan status instans RDS sebelumnya.

Snapshot RDS tidak boleh bersifat publik kecuali dimaksudkan. Jika Anda membagikan snapshot manual yang tidak terenkripsi sebagai publik, ini membuat snapshot tersedia untuk semua. Akun AWS Hal ini dapat mengakibatkan paparan data yang tidak diinginkan dari instans RDS Anda.

Perhatikan bahwa jika konfigurasi diubah untuk mengizinkan akses publik, AWS Config aturan mungkin tidak dapat mendeteksi perubahan hingga 12 jam. Sampai AWS Config aturan mendeteksi perubahan, cek lolos meskipun konfigurasi melanggar aturan.

Untuk mempelajari lebih lanjut tentang berbagi snapshot DB, lihat [Berbagi snapshot DB](#) di Panduan Pengguna Amazon RDS.

Remediasi

Untuk menghapus akses publik dari snapshot RDS, lihat [Berbagi snapshot di Panduan Pengguna Amazon RDS](#). Untuk visibilitas snapshot DB, kami memilih Private.

[RDS.2] Instans RDS DB harus melarang akses publik, sebagaimana ditentukan oleh konfigurasi PubliclyAccessible

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v3.0.0/2.3.3,, (21),, (11), (16), NIST.800-53.r5 AC-4 (21) NIST.800-53.r5 AC-4, (4), NIST.800-53.r5 SC-7 (5) NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 PCI DSS v3.2.1/1.2.1, NIST.800-53.r5 SC-7 PCI DSS v3.2.1/1.3.1, NIST.800-53.r5 SC-7 PCI DSS v3.2.1/1.3.2, PCI DSS v3.2.1/1.3.4, PCI DSS v3.2.1/1.4, PCI DSS v3.2.1/1.3.6, PCI DSS v3.2.1/7.2.1, PCI DSS v4.0.1/1.4.4 NIST.800-53.r5 SC-7

Kategori: Lindungi > Konfigurasi jaringan aman

Tingkat keparahan: Kritis

Jenis sumber daya: AWS::RDS::DBInstance

AWS Config aturan: [rds-instance-public-access-check](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah instans Amazon RDS dapat diakses publik dengan mengevaluasi PubliclyAccessible bidang dalam item konfigurasi instans.

Instans Neptune DB dan cluster Amazon DocumentDB tidak memiliki bendera dan tidak dapat dievaluasi. PubliclyAccessible Namun, kontrol ini masih dapat menghasilkan temuan untuk sumber daya ini. Anda dapat menekan temuan ini.

PubliclyAccessibleNilai dalam konfigurasi instans RDS menunjukkan apakah instans DB dapat diakses publik. Ketika instans DB dikonfigurasi denganPubliclyAccessible, itu adalah instance yang menghadap Internet dengan nama DNS yang dapat diselesaikan secara publik, yang diselesaikan ke alamat IP publik. Ketika instans DB tidak dapat diakses publik, itu adalah instance internal dengan nama DNS yang menyelesaikan ke alamat IP pribadi.

Kecuali jika Anda bermaksud agar instans RDS Anda dapat diakses publik, instans RDS tidak boleh dikonfigurasi dengan nilai `PubliclyAccessible`. Melakukannya mungkin memungkinkan lalu lintas yang tidak perlu ke instance database Anda.

Remediasi

Untuk menghapus akses publik dari instans RDS DB, lihat [Memodifikasi instans Amazon RDS DB di Panduan Pengguna](#) Amazon RDS. Untuk akses Publik, pilih No.

[RDS.3] Instans RDS DB harus mengaktifkan enkripsi saat istirahat

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v3.0.0/2.3.1, Tolok Ukur AWS Yayasan CIS v1.4.0/2.3.1, (1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-1 3, 8, NIST.800-53.r5 SC-2 8, NIST.800-53.r5 CA-9 (1), (10), NIST.800-53.R5 SI-7 (NIST.800-53.r5 SC-26) NIST.800-53.r5 SC-7

Kategori: Lindungi > Perlindungan Data > Enkripsi data-at-rest

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::RDS::DBInstance

AWS Config aturan: [rds-storage-encrypted](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah enkripsi penyimpanan diaktifkan untuk instans Amazon RDS DB Anda.

Kontrol ini ditujukan untuk instans RDS DB. Namun, itu juga dapat menghasilkan temuan untuk instans Aurora DB, instans DB Neptune, dan cluster Amazon DocumentDB. Jika temuan ini tidak berguna, maka Anda bisa menekannya.

Untuk lapisan keamanan tambahan untuk data sensitif Anda dalam instans RDS DB, Anda harus mengonfigurasi instans RDS DB Anda untuk dienkripsi saat istirahat. Untuk mengenkripsi instans dan snapshot RDS DB Anda saat istirahat, aktifkan opsi enkripsi untuk instans RDS DB Anda. Data yang dienkripsi saat istirahat mencakup penyimpanan yang mendasari untuk instans DB, pencadangan otomatisnya, replika baca, dan snapshot.

Instans DB terenkripsi RDS menggunakan algoritme enkripsi AES-256 standar terbuka untuk mengenkripsi data Anda di server yang menghosting instans RDS DB Anda. Setelah data Anda

dienkripsi, Amazon RDS menangani otentikasi akses dan dekripsi data Anda secara transparan dengan dampak minimal pada kinerja. Anda tidak perlu memodifikasi aplikasi klien database Anda untuk menggunakan enkripsi.

Enkripsi Amazon RDS saat ini tersedia untuk semua mesin database dan jenis penyimpanan. Enkripsi Amazon RDS tersedia untuk sebagian besar kelas instans DB. Untuk mempelajari tentang kelas instans DB yang tidak mendukung enkripsi Amazon RDS, lihat Mengenakripsi [sumber daya Amazon RDS di Panduan Pengguna Amazon RDS](#).

Remediasi

Untuk informasi tentang mengenkripsi instans DB di Amazon RDS, lihat Mengenakripsi [sumber daya Amazon RDS di Panduan Pengguna Amazon RDS](#).

[RDS.4] Snapshot cluster RDS dan snapshot database harus dienkripsi saat istirahat

Persyaratan terkait: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-1 3, NIST.800-53.r5 SC-2 8, NIST.800-53.r5 SC-2 8 (1), NIST.800-53.r5 SC-7 (10), NIST.800-53.R5 SI-7 (6)

Kategori: Lindungi > Perlindungan Data > Enkripsi data-at-rest

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::RDS::DBClusterSnapshot, AWS::RDS::DBSnapshot

AWS Config aturan: [rds-snapshot-encrypted](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah snapshot RDS DB dienkripsi. Kontrol gagal jika snapshot RDS DB tidak dienkripsi.

Kontrol ini ditujukan untuk instans RDS DB. Namun, ini juga dapat menghasilkan temuan untuk snapshot instans Aurora DB, instans DB Neptune, dan cluster Amazon DocumentDB. Jika temuan ini tidak berguna, maka Anda bisa menekannya.

Mengenakripsi data saat istirahat mengurangi risiko bahwa pengguna yang tidak diautentikasi mendapatkan akses ke data yang disimpan pada disk. Data dalam snapshot RDS harus dienkripsi saat istirahat untuk lapisan keamanan tambahan.

Remediasi

Untuk mengenkripsi snapshot RDS, lihat Mengenkripsi [sumber daya Amazon RDS di Panduan Pengguna Amazon RDS](#). Saat Anda mengenkripsi instans RDS DB, data terenkripsi mencakup penyimpanan yang mendasari untuk instance, pencadangan otomatisnya, replika baca, dan snapshot.

Anda hanya dapat mengenkripsi instans RDS DB saat Anda membuatnya, bukan setelah instans DB dibuat. Namun, karena Anda dapat mengenkripsi salinan snapshot yang tidak dienkripsi, Anda dapat menambahkan enkripsi secara efektif ke instans DB yang tidak terenkripsi. Artinya, Anda dapat membuat snapshot instans DB, lalu membuat salinan terenkripsi dari snapshot tersebut. Anda kemudian dapat memulihkan instans DB dari snapshot terenkripsi untuk menghasilkan salinan terenkripsi dari instans DB asli.

[RDS.5] Instans RDS DB harus dikonfigurasi dengan beberapa Availability Zone

Persyaratan terkait: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6(2), NIST.800-53.r5 SC-3 6, NIST.800-53.r5 SC-5 (2), NIST.800-53.R5 SI-13 (5)

Kategori: Pulihkan > Ketahanan > Ketersediaan tinggi

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::RDS::DBInstance

AWS Config aturan: [rds-multi-az-support](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah ketersediaan tinggi diaktifkan untuk instans RDS DB Anda. Kontrol gagal jika instans RDS DB tidak dikonfigurasi dengan beberapa Availability Zones (AZs). Kontrol ini tidak berlaku untuk instans RDS DB yang merupakan bagian dari penerapan cluster DB multi-AZ.

Mengonfigurasi instans Amazon RDS DB dengan AZs membantu memastikan ketersediaan data yang disimpan. Penerapan multi-AZ memungkinkan failover otomatis jika ada masalah dengan ketersediaan AZ dan selama pemeliharaan RDS reguler.

Remediasi

Untuk menerapkan instans DB Anda dalam beberapa kali AZs, [Memodifikasi instans DB menjadi penerapan instans DB multi-AZ](#) di Panduan Pengguna Amazon RDS.

[RDS.6] Pemantauan yang ditingkatkan harus dikonfigurasi untuk instans RDS DB

Persyaratan terkait: NIST.800-53.r5 CA-7, NIST.800-53.R5 SI-2

Kategori: Deteksi > Layanan deteksi

Tingkat keparahan: Rendah

Jenis sumber daya: AWS::RDS::DBInstance

AWS Config aturan: [rds-enhanced-monitoring-enabled](#)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub	
monitoringInterval	Jumlah detik antara pemantauan interval pengumpulan metrik	Enum	1, 5, 10, 15, 30, 60	Tidak ada nilai default	

Kontrol ini memeriksa apakah pemantauan yang disempurnakan diaktifkan untuk instans DB Amazon Relational Database Service (Amazon RDS). Kontrol gagal jika pemantauan yang ditingkatkan tidak diaktifkan untuk instance. Jika Anda memberikan nilai khusus untuk `monitoringInterval` parameter, kontrol hanya akan diteruskan jika metrik pemantauan yang disempurnakan dikumpulkan untuk instance pada interval yang ditentukan.

Di Amazon RDS, Enhanced Monitoring memungkinkan respons yang lebih cepat terhadap perubahan kinerja di infrastruktur yang mendasarinya. Perubahan kinerja ini dapat mengakibatkan kurangnya ketersediaan data. Enhanced Monitoring menyediakan metrik real-time dari sistem operasi yang dijalankan instans RDS DB Anda. Agen diinstal pada instance. Agen dapat memperoleh metrik lebih akurat daripada yang mungkin dari lapisan hypervisor.

Metrik Pemantauan Ditingkatkan berguna ketika Anda ingin melihat bagaimana proses atau thread yang berbeda pada instans DB menggunakan CPU. Untuk informasi selengkapnya, lihat [Pemantauan yang Ditingkatkan](#) di Panduan Pengguna Amazon RDS.

Remediasi

Untuk petunjuk mendetail tentang mengaktifkan Pemantauan yang Ditingkatkan untuk instans DB Anda, lihat [Menyiapkan dan mengaktifkan Pemantauan yang Ditingkatkan](#) di Panduan Pengguna Amazon RDS.

[RDS.7] Cluster RDS harus mengaktifkan perlindungan penghapusan

Persyaratan terkait: NIST.800-53.r5 CM-3, NIST.800-53.r5 SC-5 (2)

Kategori: Lindungi > Perlindungan data > Perlindungan penghapusan data

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::RDS::DBCluster`

AWS Config aturan: [rds-cluster-deletion-protection-enabled](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah klaster RDS DB memiliki perlindungan penghapusan yang diaktifkan. Kontrol gagal jika cluster RDS DB tidak mengaktifkan perlindungan penghapusan.

Kontrol ini ditujukan untuk instans RDS DB. Namun, itu juga dapat menghasilkan temuan untuk instans Aurora DB, instans DB Neptune, dan cluster Amazon DocumentDB. Jika temuan ini tidak berguna, maka Anda bisa menekannya.

Mengaktifkan perlindungan penghapusan klaster adalah lapisan perlindungan tambahan terhadap penghapusan atau penghapusan database yang tidak disengaja oleh entitas yang tidak sah.

Ketika perlindungan penghapusan diaktifkan, klaster RDS tidak dapat dihapus. Sebelum permintaan penghapusan berhasil, perlindungan penghapusan harus dinonaktifkan.

Remediasi

Untuk mengaktifkan perlindungan penghapusan klaster RDS DB, lihat [Memodifikasi cluster DB menggunakan konsol, CLI, dan API di](#) Panduan Pengguna Amazon RDS. Untuk perlindungan penghapusan, pilih Aktifkan perlindungan penghapusan.

[RDS.8] Instans RDS DB harus mengaktifkan perlindungan penghapusan

Persyaratan terkait: NIST.800-53.r5 CM-3, NIST.800-53.r5 SC-5 (2), NIST.800-53.R5 SI-13 (5)

Kategori: Lindungi > Perlindungan data > Perlindungan penghapusan data

Tingkat keparahan: Rendah

Jenis sumber daya: AWS::RDS::DBInstance

AWS Config aturan: [rds-instance-deletion-protection-enabled](#)

Jenis jadwal: Perubahan dipicu

Parameter:

- databaseEngines: mariadb,mysql,custom-oracle-ee,oracle-ee-cdb,oracle-se2-cdb,oracle-ee,oracle-se2,oracle-se1,oracle-se,postgres,sqlserver-ee,sqlserver-se,sqlserver-ex,sqlserver-web (tidak dapat disesuaikan)

Kontrol ini memeriksa apakah instans RDS DB Anda yang menggunakan salah satu mesin database yang terdaftar memiliki perlindungan penghapusan diaktifkan. Kontrol gagal jika instans RDS DB tidak mengaktifkan perlindungan penghapusan.

Mengaktifkan perlindungan penghapusan instance adalah lapisan perlindungan tambahan terhadap penghapusan atau penghapusan database yang tidak disengaja oleh entitas yang tidak sah.

Sementara perlindungan penghapusan diaktifkan, instans RDS DB tidak dapat dihapus. Sebelum permintaan penghapusan berhasil, perlindungan penghapusan harus dinonaktifkan.

Remediasi

Untuk mengaktifkan perlindungan penghapusan instans RDS DB, lihat [Memodifikasi instans Amazon RDS DB di Panduan Pengguna Amazon RDS](#). Untuk perlindungan penghapusan, pilih Aktifkan perlindungan penghapusan.

[RDS.9] Instans RDS DB harus menerbitkan log ke Log CloudWatch

Persyaratan terkait: NIST.800-53.r5 AC-2 (4), (26), NIST.800-53.r5 AC-4 (9), (10), NIST.800-53.r5 AC-6 (9) NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 Nist.800-53.R5 SI-3 NIST.800-53.r5 SC-7 (8), Nist.800-53.r5 SI-4 (20), NIST.800-53.R5 SI-7 (8), PCI DSS v4.0.1/10.2.1

Kategori: Identifikasi > Logging

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::RDS::DBInstance

AWS Config aturan: [rds-logging-enabled](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah instans Amazon RDS DB dikonfigurasi untuk mempublikasikan log berikut ke Amazon CloudWatch Logs. Kontrol gagal jika instance tidak dikonfigurasi untuk mempublikasikan log berikut ke CloudWatch Log:

- Oracle: Peringatan, Audit, Jejak, Pendengar
- PostgreSQL: Postgresql, Tingkatkan
- MySQL: Audit, Kesalahan, Umum, SlowQuery
- MariaDB: Audit, Kesalahan, Umum, SlowQuery
- SQL Server: Kesalahan, Agen
- Aurora: Audit, Kesalahan, Umum, SlowQuery
- Aurora-MySQL: Audit, Kesalahan, Umum, SlowQuery
- Aurora-PostgreSQL: Postgresql

Database RDS harus mengaktifkan log yang relevan. Database logging menyediakan catatan rinci permintaan yang dibuat untuk RDS. Log basis data dapat membantu audit keamanan dan akses dan dapat membantu mendiagnosis masalah ketersediaan.

Remediasi

Untuk informasi tentang memublikasikan log database RDS ke CloudWatch Log, lihat [Menentukan log yang akan dipublikasikan ke CloudWatch Log](#) di Panduan Pengguna Amazon RDS.

[RDS.10] Otentikasi IAM harus dikonfigurasi untuk instance RDS

Persyaratan terkait: NIST.800-53.r5 AC-2 (1) NIST.800-53.r5 AC-3,, NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-6

Kategori: Lindungi > Manajemen akses aman > Otentikasi tanpa kata sandi

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::RDS::DBInstance

AWS Config aturan: [rds-instance-iam-authentication-enabled](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah instans RDS DB memiliki otentikasi database IAM diaktifkan. Kontrol gagal jika otentikasi IAM tidak dikonfigurasi untuk instans RDS DB. Kontrol ini hanya mengevaluasi instans RDS dengan jenis mesin berikut:mysql,,, postgres auroraaurora-mysql, aurora-postgresql dan. mariadb Instance RDS juga harus berada di salah satu status berikut untuk menghasilkan temuan:available,, backing-upstorage-optimization, ataustorage-full.

Autentikasi basis data IAM memungkinkan otentikasi ke instance database dengan token otentikasi, bukan kata sandi. Lalu lintas jaringan ke dan dari database dienkripsi menggunakan SSL. Untuk informasi selengkapnya, lihat [otentikasi database IAM](#) di Panduan Pengguna Amazon Aurora.

Remediasi

Untuk mengaktifkan autentikasi database IAM pada instans RDS DB, lihat [Mengaktifkan dan menonaktifkan autentikasi database IAM](#) di Panduan Pengguna Amazon RDS.

[RDS.11] Instans RDS harus mengaktifkan pencadangan otomatis

Persyaratan terkait: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6, NIST.800-53.r5 CP-6(1), NIST.800-53.r5 CP-6(2), NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5 (2), NIST.800-53.R5 SI-12, NIST.800-53.R5 SI-13 (5)

Kategori: Pulih> Ketahanan > Cadangan diaktifkan

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::RDS::DBInstance

AWS Config aturan: [db-instance-backup-enabled](#)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
backupRetentionMinimum	Periode retensi cadangan minimum dalam beberapa hari	Bilangan Bulat	7 untuk 35	7
checkReadReplicas	Memeriksa apakah instans RDS DB memiliki cadangan yang diaktifkan untuk replika baca	Boolean	Tidak dapat disesuaikan	false

Kontrol ini memeriksa apakah instans Amazon Relational Database Service telah mengaktifkan pencadangan otomatis, dan periode retensi cadangan yang lebih besar dari atau sama dengan kerangka waktu yang ditentukan. Replika baca dikecualikan dari evaluasi. Kontrol gagal jika cadangan tidak diaktifkan untuk instance, atau jika periode retensi kurang dari kerangka waktu yang ditentukan. Kecuali Anda memberikan nilai parameter khusus untuk periode penyimpanan cadangan, Security Hub menggunakan nilai default 7 hari.

Pencadangan membantu Anda pulih lebih cepat dari insiden keamanan dan memperkuat ketahanan sistem Anda. Amazon RDS memungkinkan Anda mengonfigurasi snapshot volume instans penuh harian. Untuk informasi selengkapnya tentang pencadangan otomatis Amazon RDS, lihat [Bekerja dengan Pencadangan](#) di Panduan Pengguna Amazon RDS.

Remediasi

Untuk mengaktifkan pencadangan otomatis pada instans RDS DB, lihat [Mengaktifkan pencadangan otomatis](#) di Panduan Pengguna Amazon RDS.

[RDS.12] Otentikasi IAM harus dikonfigurasi untuk cluster RDS

Persyaratan terkait: NIST.800-53.r5 AC-2 (1) NIST.800-53.r5 AC-3,, NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-6

Kategori: Lindungi > Manajemen akses aman > Otentikasi tanpa kata sandi

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::RDS::DBCluster

AWS Config aturan: [rds-cluster-iam-authentication-enabled](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah kluster Amazon RDS DB memiliki otentikasi database IAM yang diaktifkan.

Autentikasi basis data IAM memungkinkan otentikasi bebas kata sandi ke instance database. Otentikasi menggunakan token otentikasi. Lalu lintas jaringan ke dan dari database dienkripsi menggunakan SSL. Untuk informasi selengkapnya, lihat [otentikasi database IAM](#) di Panduan Pengguna Amazon Aurora.

Remediasi

Untuk mengaktifkan autentikasi IAM untuk kluster DB, lihat [Mengaktifkan dan menonaktifkan autentikasi database IAM di](#) Panduan Pengguna Amazon Aurora.

[RDS.13] Peningkatan versi minor otomatis RDS harus diaktifkan

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v3.0.0/2.3.2, NIST.800-53.R5 SI-2, NIST.800-53.R5 SI-2 (2), Nist.800-53.R5 SI-2 (4), NIST.800-53.R5 SI-2 (5), PCI DSS v4.0.1/6.3.3

Kategori: Identifikasi > Kerentanan, tambalan, dan manajemen versi

Tingkat keparahan: Tinggi

Jenis sumber daya: AWS::RDS::DBInstance

AWS Config aturan: [rds-automatic-minor-version-upgrade-enabled](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah upgrade versi minor otomatis diaktifkan untuk instance database RDS.

Upgrade versi minor otomatis memperbarui database secara berkala ke versi mesin database terbaru. Namun, upgrade mungkin tidak selalu menyertakan versi mesin database terbaru. Jika Anda perlu menyimpan database Anda pada versi tertentu pada waktu tertentu, kami sarankan Anda meningkatkan secara manual ke versi database yang Anda butuhkan sesuai dengan jadwal yang Anda butuhkan. Dalam kasus masalah keamanan kritis atau ketika versi mencapai end-of-support tanggalnya, Amazon RDS mungkin menerapkan pemutakhiran versi minor meskipun Anda belum mengaktifkan opsi pemutakhiran versi minor Otomatis. Untuk informasi selengkapnya, lihat dokumentasi pemutakhiran Amazon RDS untuk mesin database spesifik Anda:

- [Upgrade versi minor otomatis untuk RDS untuk MariaDB](#)
- [Upgrade versi minor otomatis untuk RDS untuk MySQL](#)
- [Upgrade versi minor otomatis untuk RDS untuk PostgreSQL](#)
- [Db2 pada versi Amazon RDS](#)
- [Upgrade versi minor Oracle](#)
- [Peningkatan mesin Microsoft SQL Server DB](#)

Remediasi

Untuk mengaktifkan upgrade versi minor otomatis untuk instans DB yang ada, lihat [Memodifikasi instans Amazon RDS DB di Panduan](#) Pengguna Amazon RDS. Untuk upgrade versi minor otomatis, pilih Ya.

[RDS.14] Cluster Amazon Aurora seharusnya mengaktifkan backtracking

Persyaratan terkait: Nist.800-53.r5 CP-10, Nist.800-53.r5 CP-6, Nist.800-53.R5 CP-6 (1), Nist.800-53.r5 CP-6 (2), Nist.800-53.r5 CP-9, Nist.800-53.r5 SI-13 (5)

Kategori: Pulih> Ketahanan > Cadangan diaktifkan

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::RDS::DBCluster

AWS Config aturan: [aurora-mysql-backtracking-enabled](#)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub	
BacktrackWindowInHours	Jumlah jam untuk mundur cluster Aurora MySQL	Ganda	0.1 untuk 72	Tidak ada nilai default	

Kontrol ini memeriksa apakah klaster Amazon Aurora telah mengaktifkan backtracking. Kontrol gagal jika cluster tidak mengaktifkan backtracking. Jika Anda memberikan nilai kustom untuk BacktrackWindowInHours parameter, kontrol hanya akan diteruskan jika cluster mundur untuk jangka waktu yang ditentukan.

Cadangan membantu Anda pulih lebih cepat dari insiden keamanan. Mereka juga memperkuat ketahanan sistem Anda. Aurora backtracking mengurangi waktu untuk memulihkan database ke titik waktu. Hal ini tidak memerlukan database restore untuk melakukannya.

Remediasi

Untuk mengaktifkan backtracking Aurora, lihat [Mengonfigurasi backtracking di](#) Panduan Pengguna Amazon Aurora.

Perhatikan bahwa Anda tidak dapat mengaktifkan backtracking pada klaster yang ada. Sebagai gantinya, Anda dapat membuat klon yang mengaktifkan backtracking. Untuk informasi selengkapnya tentang batasan backtracking Aurora, lihat daftar batasan di [Ikhtisar](#) mundur.

[RDS.15] Cluster RDS DB harus dikonfigurasi untuk beberapa Availability Zone

Persyaratan terkait: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6(2), NIST.800-53.r5 SC-3 6, NIST.800-53.r5 SC-5 (2), NIST.800-53.R5 SI-13 (5)

Kategori: Pulihkan > Ketahanan > Ketersediaan tinggi

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::RDS::DBCluster

AWS Config aturan: [rds-cluster-multi-az-enabled](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah ketersediaan tinggi diaktifkan untuk kluster RDS DB Anda. Kontrol gagal jika kluster RDS DB tidak digunakan di beberapa Availability Zones (AZs).

Cluster RDS DB harus dikonfigurasi untuk beberapa AZs untuk memastikan ketersediaan data yang disimpan. Penerapan ke beberapa AZs memungkinkan failover otomatis jika terjadi masalah ketersediaan AZ dan selama acara pemeliharaan RDS reguler.

Remediasi

Untuk menerapkan cluster DB Anda dalam beberapa AZs, [Memodifikasi instans DB menjadi penerapan instans DB multi-AZ](#) di Panduan Pengguna Amazon RDS.

Langkah-langkah remediasi berbeda untuk database global Aurora. Untuk mengonfigurasi beberapa Availability Zone untuk database global Aurora, pilih cluster DB Anda. Kemudian, pilih Actions and Add reader, dan tentukan beberapa AZs. Untuk informasi selengkapnya, lihat [Menambahkan Replika Aurora ke cluster DB di Panduan](#) Pengguna Amazon Aurora.

[RDS.16] Cluster RDS DB harus dikonfigurasi untuk menyalin tag ke snapshot

Persyaratan terkait: NIST.800-53.r5 CA-9 (1), Nist.800-53.R5 CM-2, Nist.800-53.R5 CM-2 (2)

Kategori: Identifikasi > Persediaan

Tingkat keparahan: Rendah

Jenis sumber daya: AWS::RDS::DBCluster

AWS Config aturan: `rds-cluster-copy-tags-to-snapshots-enabled` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah cluster RDS DB dikonfigurasi untuk menyalin semua tag ke snapshot saat snapshot dibuat.

Identifikasi dan inventaris aset TI Anda adalah aspek penting dari tata kelola dan keamanan. Anda harus memiliki visibilitas semua cluster RDS DB Anda sehingga Anda dapat menilai postur keamanan mereka dan mengambil tindakan pada area kelemahan potensial. Snapshot harus ditandai dengan

cara yang sama seperti cluster database RDS induknya. Mengaktifkan pengaturan ini memastikan bahwa snapshot mewarisi tag cluster database induknya.

Remediasi

Untuk secara otomatis menyalin tag ke snapshot untuk klaster RDS DB, lihat [Memodifikasi cluster DB menggunakan konsol, CLI, dan API di Panduan Pengguna Amazon Aurora](#). Pilih Salin tag ke snapshot.

[RDS.17] Instans RDS DB harus dikonfigurasi untuk menyalin tag ke snapshot

Persyaratan terkait: NIST.800-53.r5 CA-9 (1), Nist.800-53.R5 CM-2, Nist.800-53.R5 CM-2 (2)

Kategori: Identifikasi > Persediaan

Tingkat keparahan: Rendah

Jenis sumber daya: AWS::RDS::DBInstance

AWS Config aturan: `rds-instance-copy-tags-to-snapshots-enabled` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah instance RDS DB dikonfigurasi untuk menyalin semua tag ke snapshot saat snapshot dibuat.

Identifikasi dan inventaris aset TI Anda adalah aspek penting dari tata kelola dan keamanan. Anda harus memiliki visibilitas semua instans RDS DB Anda sehingga Anda dapat menilai postur keamanan mereka dan mengambil tindakan pada area kelemahan potensial. Snapshot harus ditandai dengan cara yang sama seperti instance database RDS induknya. Mengaktifkan pengaturan ini memastikan bahwa snapshot mewarisi tag dari instance database induknya.

Remediasi

Untuk secara otomatis menyalin tag ke snapshot untuk instans RDS DB, lihat [Memodifikasi instans Amazon RDS DB di Panduan Pengguna Amazon RDS](#). Pilih Salin tag ke snapshot.

[RDS.18] Instans RDS harus digunakan di VPC

Kategori: Lindungi > Konfigurasi jaringan aman> Sumber daya dalam VPC

Tingkat keparahan: Tinggi

Jenis sumber daya: AWS::RDS::DBInstance

AWS Config aturan: `rds-deployed-in-vpc` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah instans Amazon RDS diterapkan pada -VPC. EC2

VPCs menyediakan sejumlah kontrol jaringan untuk mengamankan akses ke sumber daya RDS. Kontrol ini termasuk VPC Endpoint, jaringan ACLs, dan grup keamanan. Untuk memanfaatkan kontrol ini, kami sarankan Anda membuat instans RDS di -VPC. EC2

Remediasi

Untuk petunjuk cara memindahkan instans RDS ke VPC, lihat Memperbarui [VPC untuk instans DB di Panduan Pengguna Amazon RDS](#).

[RDS.19] Langganan pemberitahuan acara RDS yang ada harus dikonfigurasi untuk peristiwa klaster penting

Persyaratan terkait: NIST.800-53.r5 CA-7, NIST.800-53.R5 SI-2

Kategori: Deteksi > Layanan deteksi > Pemantauan aplikasi

Tingkat keparahan: Rendah

Jenis sumber daya: AWS::RDS::EventSubscription

AWS Config aturan: `rds-cluster-event-notifications-configured` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah langganan peristiwa Amazon RDS yang ada untuk kluster database telah mengaktifkan notifikasi untuk jenis sumber berikut dan pasangan nilai kunci kategori peristiwa:

```
DBCluster: ["maintenance","failure"]
```


Kontrol berlalu jika tidak ada langganan acara yang ada di akun Anda.

Pemberitahuan acara RDS menggunakan Amazon SNS untuk membuat Anda mengetahui perubahan ketersediaan atau konfigurasi sumber daya RDS Anda. Pemberitahuan ini memungkinkan respons cepat. Untuk informasi tambahan tentang pemberitahuan peristiwa RDS, lihat [Menggunakan pemberitahuan peristiwa Amazon RDS di Panduan](#) Pengguna Amazon RDS.

Remediasi

Untuk berlangganan notifikasi peristiwa klaster RDS, lihat [Berlangganan pemberitahuan acara Amazon RDS di Panduan](#) Pengguna Amazon RDS. Gunakan nilai berikut:

Bidang	Nilai
Jenis sumber	Klaster
Cluster untuk dimasukkan	Semua cluster
Kategori acara untuk disertakan	Pilih kategori acara tertentu atau Semua kategori acara

[RDS.20] Langganan pemberitahuan acara RDS yang ada harus dikonfigurasi untuk peristiwa instance basis data penting

Persyaratan terkait: NIST.800-53.r5 CA-7, NIST.800-53.R5 SI-2, PCI DSS v4.0.1/11.5.2

Kategori: Deteksi > Layanan deteksi > Pemantauan aplikasi

Tingkat keparahan: Rendah

Jenis sumber daya: AWS::RDS::EventSubscription

AWS Config aturan: rds-instance-event-notifications-configured (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah langganan peristiwa Amazon RDS yang ada untuk instans database telah mengaktifkan notifikasi untuk jenis sumber berikut dan pasangan nilai kunci kategori peristiwa:

```
DBInstance: ["maintenance","configuration change","failure"]
```

Kontrol berlalu jika tidak ada langganan acara yang ada di akun Anda.

Pemberitahuan peristiwa RDS menggunakan Amazon SNS untuk membuat Anda mengetahui perubahan ketersediaan atau konfigurasi sumber daya RDS Anda. Pemberitahuan ini memungkinkan respons cepat. Untuk informasi tambahan tentang pemberitahuan peristiwa RDS, lihat [Menggunakan pemberitahuan peristiwa Amazon RDS di Panduan](#) Pengguna Amazon RDS.

Remediasi

Untuk berlangganan notifikasi kejadian instans RDS, lihat [Berlangganan notifikasi peristiwa Amazon RDS di Panduan](#) Pengguna Amazon RDS. Gunakan nilai berikut:

Bidang	Nilai
Jenis sumber	Instans
Contoh untuk disertakan	Semua contoh
Kategori acara untuk disertakan	Pilih kategori acara tertentu atau Semua kategori acara

[RDS.21] Langganan pemberitahuan acara RDS harus dikonfigurasi untuk peristiwa grup parameter basis data penting

Persyaratan terkait: NIST.800-53.r5 CA-7, NIST.800-53.R5 SI-2, PCI DSS v4.0.1/11.5.2

Kategori: Deteksi > Layanan deteksi > Pemantauan aplikasi

Tingkat keparahan: Rendah

Jenis sumber daya: AWS::RDS::EventSubscription

AWS Config aturan: rds-pg-event-notifications-configured (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah langganan acara Amazon RDS ada dengan notifikasi diaktifkan untuk jenis sumber berikut, pasangan nilai kunci kategori peristiwa. Kontrol berlalu jika tidak ada langganan acara yang ada di akun Anda.

```
DBParameterGroup: ["configuration change"]
```

Pemberitahuan peristiwa RDS menggunakan Amazon SNS untuk membuat Anda mengetahui perubahan ketersediaan atau konfigurasi sumber daya RDS Anda. Pemberitahuan ini memungkinkan respons cepat. Untuk informasi tambahan tentang pemberitahuan peristiwa RDS, lihat [Menggunakan pemberitahuan peristiwa Amazon RDS di Panduan Pengguna Amazon RDS](#).

Remediasi

Untuk berlangganan pemberitahuan peristiwa grup parameter database RDS, lihat [Berlangganan pemberitahuan peristiwa Amazon RDS](#) di Panduan Pengguna Amazon RDS. Gunakan nilai berikut:

Bidang	Nilai
Jenis sumber	Grup parameter
Kelompok parameter untuk disertakan	Semua kelompok parameter
Kategori acara untuk disertakan	Pilih kategori acara tertentu atau Semua kategori acara

[RDS.22] Langganan pemberitahuan acara RDS harus dikonfigurasi untuk acara grup keamanan basis data penting

Persyaratan terkait: NIST.800-53.r5 CA-7, NIST.800-53.R5 SI-2, PCI DSS v4.0.1/11.5.2

Kategori: Deteksi > Layanan Deteksi > Pemantauan aplikasi

Tingkat keparahan: Rendah

Jenis sumber daya: AWS::RDS::EventSubscription

AWS Config aturan: rds-sg-event-notifications-configured (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah langganan acara Amazon RDS ada dengan notifikasi diaktifkan untuk jenis sumber berikut, pasangan nilai kunci kategori peristiwa. Kontrol berlalu jika tidak ada langganan acara yang ada di akun Anda.

```
DBSecurityGroup: ["configuration change","failure"]
```

Pemberitahuan peristiwa RDS menggunakan Amazon SNS untuk membuat Anda mengetahui perubahan ketersediaan atau konfigurasi sumber daya RDS Anda. Pemberitahuan ini memungkinkan respons yang cepat. Untuk informasi tambahan tentang pemberitahuan peristiwa RDS, lihat [Menggunakan pemberitahuan peristiwa Amazon RDS di Panduan Pengguna Amazon RDS](#).

Remediasi

Untuk berlangganan notifikasi kejadian instans RDS, lihat [Berlangganan notifikasi peristiwa Amazon RDS di Panduan Pengguna Amazon RDS](#). Gunakan nilai berikut:

Bidang	Nilai
Jenis sumber	Grup keamanan
Kelompok keamanan untuk memasukkan	Semua kelompok keamanan
Kategori acara untuk disertakan	Pilih kategori acara tertentu atau Semua kategori acara

[RDS.23] Instans RDS tidak boleh menggunakan port default mesin database

Persyaratan terkait: NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21) NIST.800-53.r5 SC-7,, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (5)

Kategori: Lindungi > Konfigurasi jaringan aman

Tingkat keparahan: Rendah

Jenis sumber daya: AWS::RDS::DBInstance

AWS Config aturan: rds-no-default-ports (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah cluster RDS atau instance menggunakan port selain port default mesin database. Kontrol gagal jika cluster atau instance RDS menggunakan port default. Kontrol ini tidak berlaku untuk instance RDS yang merupakan bagian dari cluster.

Jika Anda menggunakan port yang dikenal untuk menyebarkan cluster atau instance RDS, penyerang dapat menebak informasi tentang cluster atau instance. Penyerang dapat menggunakan informasi ini bersama dengan informasi lain untuk terhubung ke cluster atau instance RDS atau mendapatkan informasi tambahan tentang aplikasi Anda.

Ketika Anda mengubah port, Anda juga harus memperbarui string koneksi yang ada yang digunakan untuk terhubung ke port lama. Anda juga harus memeriksa grup keamanan instans DB untuk memastikan bahwa itu termasuk aturan masuk yang memungkinkan konektivitas pada port baru.

Remediasi

Untuk mengubah port default instans RDS DB yang ada, lihat [Memodifikasi instans Amazon RDS DB di Panduan](#) Pengguna Amazon RDS. Untuk mengubah port default kluster RDS DB yang ada, lihat [Memodifikasi cluster DB menggunakan konsol, CLI, dan API di](#) Panduan Pengguna Amazon Aurora. Untuk port Database, ubah nilai port ke nilai non-default.

[RDS.24] Kluster Database RDS harus menggunakan nama pengguna administrator khusus

Persyaratan terkait: NIST.800-53.r5 CA-9 (1), Nist.800-53.R5 CM-2, PCI DSS v4.0.1/2.2.2

Kategori: Identifikasi > Konfigurasi Sumber Daya

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::RDS::DBCluster

AWS Config aturan: [rds-cluster-default-admin-check](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah kluster database Amazon RDS telah mengubah nama pengguna admin dari nilai defaultnya. Kontrol tidak berlaku untuk mesin jenis neptunus (Neptunus DB) atau docdb (DocumentDB). Aturan ini akan gagal jika nama pengguna admin diatur ke nilai default.

Saat membuat database Amazon RDS, Anda harus mengubah nama pengguna admin default menjadi nilai unik. Nama pengguna default adalah pengetahuan publik dan harus diubah selama pembuatan database RDS. Mengubah nama pengguna default mengurangi risiko akses yang tidak diinginkan.

Remediasi

Untuk mengubah nama pengguna admin yang terkait dengan kluster database Amazon RDS, [buat kluster database RDS baru](#) dan ubah nama pengguna admin default saat membuat database.

[RDS.25] Instans database RDS harus menggunakan nama pengguna administrator khusus

Persyaratan terkait: NIST.800-53.r5 CA-9 (1), Nist.800-53.R5 CM-2, PCI DSS v4.0.1/2.2.2

Kategori: Identifikasi > Konfigurasi Sumber Daya

Tingkat keparahan: Sedang

Jenis sumber daya: AWS : : RDS : : DBInstance

AWS Config aturan: [rds-instance-default-admin-check](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah Anda telah mengubah nama pengguna administratif untuk instans database Amazon Relational Database Service (Amazon RDS) dari nilai default. Kontrol gagal jika nama pengguna administratif diatur ke nilai default. Kontrol tidak berlaku untuk mesin jenis neptunus (Neptunus DB) atau docdb (DocumentDB), dan untuk instance RDS yang merupakan bagian dari cluster.

Nama pengguna administratif default pada database Amazon RDS adalah pengetahuan publik. Saat membuat database Amazon RDS, Anda harus mengubah nama pengguna administratif default ke nilai unik untuk mengurangi risiko akses yang tidak diinginkan.

Remediasi

Untuk mengubah nama pengguna administratif yang terkait dengan instance database RDS, pertama [buat instance database RDS baru](#). Ubah nama pengguna administratif default saat membuat database.

[RDS.26] Instans RDS DB harus dilindungi oleh rencana cadangan

Kategori: Pulih> Ketahanan > Cadangan diaktifkan

Persyaratan terkait: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6, NIST.800-53.r5 CP-6(1), NIST.800-53.r5 CP-6(2), NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5 (2), NIST.800-53.R5 SI-12, NIST.800-53.R5 SI-13 (5)

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::RDS::DBInstance

AWS Config aturan: [rds-resources-protected-by-backup-plan](#)

Jenis jadwal: Periodik

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub	
backupVaultLockCheck	Kontrol menghasilkan PASSED temuan jika parameter disetel ke true dan sumber daya menggunakan AWS Backup Vault Lock.	Boolean	true atau false	Tidak ada nilai default	

Kontrol ini mengevaluasi jika instans Amazon RDS DB dicakup oleh paket cadangan. Kontrol ini gagal jika instans RDS DB tidak tercakup oleh rencana cadangan. Jika Anda menyetel backupVaultLockCheck parameter sama dengan true, kontrol hanya akan diteruskan jika instance dicadangkan di brankas yang AWS Backup terkunci.

AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya yang memusatkan dan mengotomatiskan pencadangan data di seluruh. Layanan AWS Dengan AWS Backup, Anda dapat membuat kebijakan cadangan yang disebut rencana cadangan. Anda dapat menggunakan paket ini untuk menentukan persyaratan pencadangan Anda, seperti seberapa sering mencadangkan data

Anda dan berapa lama untuk menyimpan cadangan tersebut. Menyertakan instans RDS DB dalam paket cadangan membantu Anda melindungi data Anda dari kehilangan atau penghapusan yang tidak diinginkan.

Remediasi

Untuk menambahkan instans RDS DB ke paket AWS Backup cadangan, lihat [Menetapkan sumber daya ke paket cadangan di Panduan AWS Backup](#) Pengembang.

[RDS.27] Cluster RDS DB harus dienkripsi saat istirahat

Persyaratan terkait: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-1 3, NIST.800-53.r5 SC-2 8, NIST.800-53.r5 SC-2 8 (1), NIST.800-53.r5 SC-7 (10), NIST.800-53.R5 SI-7 (6)

Kategori: Lindungi > Perlindungan Data > Enkripsi data-at-rest

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::RDS::DBCluster

AWS Config aturan: [rds-cluster-encrypted-at-rest](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah cluster RDS DB dienkripsi saat istirahat. Kontrol gagal jika cluster RDS DB tidak dienkripsi saat istirahat.

Data saat istirahat mengacu pada data apa pun yang disimpan dalam penyimpanan persisten dan tidak mudah menguap untuk durasi berapa pun. Enkripsi membantu Anda melindungi kerahasiaan data tersebut, mengurangi risiko bahwa pengguna yang tidak sah dapat mengaksesnya. Mengenkripsi kluster RDS DB Anda melindungi data dan metadata Anda terhadap akses yang tidak sah. Ini juga memenuhi persyaratan kepatuhan untuk data-at-rest enkripsi sistem file produksi.

Remediasi

Anda dapat mengaktifkan enkripsi saat istirahat saat Anda membuat cluster RDS DB. Anda tidak dapat mengubah pengaturan enkripsi setelah membuat cluster. Untuk informasi selengkapnya, lihat [Mengekripsi kluster Amazon Aurora DB](#) di Panduan Pengguna Amazon Aurora.

[RDS.28] Cluster RDS DB harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::RDS::DBCluster`

AWS Config aturan: `tagged-rds-dbccluster` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
<code>requiredTagKeys</code>	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS.	Tidak ada nilai default

Kontrol ini memeriksa apakah kluster Amazon RDS DB memiliki tag dengan kunci spesifik yang ditentukan dalam parameter `requiredTagKeys`. Kontrol gagal jika cluster DB tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter `requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika cluster DB tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke

AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat [Untuk apa ABAC? AWS](#) di Panduan Pengguna IAM.

Note

Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat [Menandai AWS sumber daya Anda](#) di Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke kluster RDS DB, lihat [Menandai sumber daya Amazon RDS di Panduan Pengguna Amazon RDS](#).

[RDS.29] Snapshot cluster RDS DB harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: AWS::RDS::DBClusterSnapshot

AWS Config aturan: tagged-rds-dbclustersnapshot (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
requiredTagKeys	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi	Tidak ada nilai default

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
			persyaratan AWS	

Kontrol ini memeriksa apakah snapshot kluster Amazon RDS DB memiliki tag dengan kunci spesifik yang ditentukan dalam parameter. `requiredTagKeys` Kontrol gagal jika snapshot cluster DB tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter `requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika snapshot cluster DB tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengkategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat [Untuk apa ABAC? AWS](#) di Panduan Pengguna IAM.

Note

Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat [Menandai AWS sumber daya Anda](#) di Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke snapshot klaster RDS DB, lihat [Menandai sumber daya Amazon RDS di Panduan Pengguna Amazon RDS](#).

[RDS.30] Instans RDS DB harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: AWS::RDS::DBInstance

AWS Config aturan: tagged-rds-dbinstance (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
<code>requiredTagKeys</code>	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS.	Tidak ada nilai default

Kontrol ini memeriksa apakah instans Amazon RDS DB memiliki tag dengan kunci spesifik yang ditentukan dalam parameter `requiredTagKeys`. Kontrol gagal jika instans DB tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter `requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika instance DB tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke

AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat [Untuk apa ABAC? AWS](#) di Panduan Pengguna IAM.

Note

Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat [Menandai AWS sumber daya Anda](#) di Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke instans RDS DB, lihat [Menandai sumber daya Amazon RDS di Panduan Pengguna Amazon RDS](#).

[RDS.31] Grup keamanan RDS DB harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: AWS::RDS::DBSecurityGroup

AWS Config aturan: tagged-rds-dbsecuritygroup (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
requiredTagKeys	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi	Tidak ada nilai default

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
			persyaratan AWS	

Kontrol ini memeriksa apakah grup keamanan Amazon RDS DB memiliki tag dengan kunci spesifik yang ditentukan dalam `parameterrequiredTagKeys`. Kontrol gagal jika grup keamanan DB tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam `parameterrequiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika grup keamanan DB tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat [Untuk apa ABAC? AWS](#) di Panduan Pengguna IAM.

Note

Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat [Menandai AWS sumber daya Anda](#) di Referensi Umum AWS.

Remediasi

Untuk menambahkan tag ke grup keamanan RDS DB, lihat [Menandai sumber daya Amazon RDS di Panduan Pengguna Amazon RDS](#).

[RDS.32] Snapshot RDS DB harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: AWS : : RDS : : DBSnapshot

AWS Config aturan: tagged-rds-dbsnapshot (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
<code>requiredTagKeys</code>	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS .	Tidak ada nilai default

Kontrol ini memeriksa apakah snapshot Amazon RDS DB memiliki tag dengan kunci tertentu yang ditentukan dalam parameter. `requiredTagKeys` Kontrol gagal jika snapshot DB tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter `requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika snapshot DB tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws :`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengkategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan

terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat [Untuk apa ABAC? AWS](#) di Panduan Pengguna IAM.

Note

Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat [Menandai AWS sumber daya Anda](#) di Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke snapshot RDS DB, lihat [Menandai sumber daya Amazon RDS di Panduan](#) Pengguna Amazon RDS.

[RDS.33] Grup subnet RDS DB harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: AWS::RDS::DBSubnetGroup

AWS Config aturan: tagged-rds-dbsubnetgroups (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
requiredTagKeys	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS .	Tidak ada nilai default

Kontrol ini memeriksa apakah grup subnet Amazon RDS DB memiliki tag dengan kunci spesifik yang ditentukan dalam parameter. `requiredTagKeys` Kontrol gagal jika grup subnet DB tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter `requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika grup subnet DB tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws :`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat [Untuk apa ABAC? AWS](#) di Panduan Pengguna IAM.

Note

Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat [Menandai AWS sumber daya Anda](#) di Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke grup subnet RDS DB, lihat [Menandai sumber daya Amazon RDS di Panduan Pengguna Amazon RDS](#).

[RDS.34] Kluster Aurora MySQL DB harus menerbitkan log audit ke Log CloudWatch

Persyaratan terkait: NIST.800-53.r5 AC-2 (4), (26), NIST.800-53.r5 AC-4 (9),, NIST.800-53.r5 AC-6 (9), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7 Nist.800-53.R5 SI-3 NIST.800-53.r5 SC-7 (8), Nist.800-53.r5 SI-4 (20), Nist.800-53.R5 SI-7 (8), PCI DSS v4.0.1/10.2.1

Kategori: Identifikasi > Logging

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::RDS::DBCluster

AWS Config aturan: [rds-aurora-mysql-audit-logging-enabled](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah kluster DB MySQL Amazon Aurora dikonfigurasi untuk mempublikasikan log audit ke Amazon Logs. CloudWatch Kontrol gagal jika klaster tidak dikonfigurasi untuk mempublikasikan log audit ke CloudWatch Log. Kontrol tidak menghasilkan temuan untuk cluster Aurora Serverless v1 DB.

Log audit menangkap catatan aktivitas database, termasuk upaya login, modifikasi data, perubahan skema, dan peristiwa lain yang dapat diaudit untuk tujuan keamanan dan kepatuhan. Saat mengonfigurasi klaster DB MySQL Aurora untuk mempublikasikan log audit ke grup log di Amazon Logs, Anda dapat melakukan analisis data CloudWatch log secara real-time. CloudWatch Log menyimpan log dalam penyimpanan yang sangat tahan lama. Anda juga dapat membuat alarm dan melihat metrik di CloudWatch

Note

Cara alternatif untuk mempublikasikan log audit ke CloudWatch Log adalah dengan mengaktifkan audit lanjutan dan menyetel parameter DB tingkat cluster ke. `server_audit_logs_upload 1` Default untuk `server_audit_logs_upload` parameter adalah `0`. Namun, kami sarankan Anda menggunakan instruksi remediasi berikut sebagai gantinya untuk melewati kontrol ini.

Remediasi

Untuk mempublikasikan log audit klaster MySQL DB Aurora ke Log, CloudWatch lihat Menerbitkan log [MySQL Amazon Aurora ke Log](#) Amazon di Panduan Pengguna Amazon Aurora. CloudWatch

[RDS.35] Cluster RDS DB harus mengaktifkan peningkatan versi minor otomatis

Persyaratan terkait: NIST.800-53.R5 SI-2, NIST.800-53.R5 SI-2 (2), NIST.800-53.R5 SI-2 (4), Nist.800-53.R5 SI-2 (5), PCI DSS v4.0.1/6.3.3

Kategori: Identifikasi > Kerentanan, tambalan, dan manajemen versi

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::RDS::DBCluster

AWS Config aturan: [rds-cluster-auto-minor-version-upgrade-enable](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah pemutakhiran versi minor otomatis diaktifkan untuk cluster DB Multi-AZ Amazon RDS. Kontrol gagal jika pemutakhiran versi minor otomatis tidak diaktifkan untuk cluster DB multi-AZ.

RDS menyediakan upgrade versi minor otomatis sehingga Anda dapat menjaga cluster DB multi-AZ Anda tetap up to date. Versi minor dapat memperkenalkan fitur perangkat lunak baru, perbaikan bug, patch keamanan, dan peningkatan kinerja. Dengan mengaktifkan upgrade versi minor otomatis pada cluster database RDS, cluster, bersama dengan instance di cluster, akan menerima pembaruan otomatis ke versi minor ketika versi baru tersedia. Pembaruan diterapkan secara otomatis selama jendela pemeliharaan.

Remediasi

Untuk mengaktifkan pemutakhiran versi minor otomatis pada klaster DB multi-AZ, lihat [Memodifikasi klaster DB Multi-AZ di Panduan Pengguna](#) Amazon RDS.

[RDS.36] RDS untuk instance PostgreSQL DB harus menerbitkan log ke Log CloudWatch

Persyaratan terkait: PCI DSS v4.0.1/10.4.2

Kategori: Identifikasi > Logging

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::RDS::DBInstance

AWS Config aturan: [rds-postgresql-logs-to-cloudwatch](#)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
logTypes	Daftar tipe log yang dipisahkan koma untuk dipublikasikan ke Log CloudWatch	StringList	Tidak dapat disesuaikan	postgresq l

Kontrol ini memeriksa apakah instans Amazon RDS for PostgreSQL DB dikonfigurasi untuk mempublikasikan log ke Amazon Logs. CloudWatch Kontrol gagal jika instance PostgreSQL DB tidak dikonfigurasi untuk mempublikasikan jenis log yang disebutkan dalam parameter ke Log. logTypes CloudWatch

Database logging menyediakan catatan rinci permintaan yang dibuat untuk instance RDS. PostgreSQL menghasilkan log peristiwa yang berisi informasi berguna bagi administrator. Menerbitkan log ini ke CloudWatch Log memusatkan manajemen log dan membantu Anda melakukan analisis data log secara real-time. CloudWatch Log menyimpan log dalam penyimpanan yang sangat tahan lama. Anda juga dapat membuat alarm dan melihat metrik di. CloudWatch

Remediasi

Untuk memublikasikan log instans PostgreSQL DB ke Log, lihat [Menerbitkan CloudWatch log PostgreSQL ke Log Amazon di Panduan Pengguna Amazon RDS](#). CloudWatch

[RDS.37] Cluster Aurora PostgreSQL DB harus menerbitkan log ke Log CloudWatch

Persyaratan terkait: PCI DSS v4.0.1/10.4.2

Kategori: Identifikasi > Logging

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::RDS::DBCluster

AWS Config aturan: [rds-aurora-postgresql-logs-to-cloudwatch](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah klaster DB PostgreSQL Amazon Aurora dikonfigurasi untuk mempublikasikan log ke Amazon Logs. CloudWatch Kontrol gagal jika klaster Aurora PostgreSQL DB tidak dikonfigurasi untuk mempublikasikan log PostgreSQL ke Log. CloudWatch

Database logging menyediakan catatan rinci permintaan yang dibuat untuk cluster RDS. Aurora PostgreSQL menghasilkan log peristiwa yang berisi informasi berguna bagi administrator. Menerbitkan log ini ke CloudWatch Log memusatkan manajemen log dan membantu Anda melakukan analisis data log secara real-time. CloudWatch Log menyimpan log dalam penyimpanan yang sangat tahan lama. Anda juga dapat membuat alarm dan melihat metrik di. CloudWatch

Remediasi

Untuk memublikasikan log klaster Aurora PostgreSQL DB ke Log, CloudWatch lihat Menerbitkan log [PostgreSQL](#) Aurora ke Log Amazon di Panduan Pengguna Amazon RDS. CloudWatch

[RDS.38] RDS untuk instance PostgreSQL DB harus dienkripsi saat transit

Kategori: Lindungi > Perlindungan Data > Enkripsi data-in-transit

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::RDS::DBInstance

AWS Config aturan: [rds-postgres-instance-encrypted-in-transit](#)

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah koneksi ke instance Amazon RDS for PostgreSQL database (DB) dienkripsi dalam perjalanan. Kontrol gagal jika `rds.force_ssl` parameter untuk grup parameter yang terkait dengan instance disetel ke 0 (off). Kontrol ini tidak mengevaluasi instans RDS DB yang merupakan bagian dari cluster DB.

Data dalam transit mengacu pada data yang berpindah dari satu lokasi ke lokasi lain, seperti antar node di cluster Anda atau antara klaster Anda dan aplikasi Anda. Data dapat bergerak di internet atau dalam jaringan pribadi. Mengenkripsi data dalam perjalanan mengurangi risiko bahwa pengguna yang tidak sah dapat menguping lalu lintas jaringan.

Remediasi

Untuk mewajibkan semua koneksi ke RDS agar instans PostgreSQL DB menggunakan SSL, lihat [Menggunakan SSL dengan instans PostgreSQL DB di Panduan](#) Pengguna Amazon RDS.

[RDS.39] RDS untuk instance MySQL DB harus dienkripsi saat transit

Kategori: Lindungi > Perlindungan Data > Enkripsi data-in-transit

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::RDS::DBInstance

AWS Config aturan: [rds-mysql-instance-encrypted-in-transit](#)

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah koneksi ke instance Amazon RDS for MySQL database (DB) dienkripsi dalam perjalanan. Kontrol gagal jika `rds.require_secure_transport` parameter untuk grup parameter yang terkait dengan instance disetel ke 0 (off). Kontrol ini tidak mengevaluasi instans RDS DB yang merupakan bagian dari cluster DB.

Data dalam transit mengacu pada data yang berpindah dari satu lokasi ke lokasi lain, seperti antar node di cluster Anda atau antara klaster Anda dan aplikasi Anda. Data dapat bergerak di internet atau dalam jaringan pribadi. Mengenkripsi data dalam perjalanan mengurangi risiko bahwa pengguna yang tidak sah dapat menguping lalu lintas jaringan.

Remediasi

Untuk mewajibkan semua koneksi ke RDS agar instans MySQL DB menggunakan SSL, lihat [dukungan SSL/TLS untuk instans MySQL DB di Amazon RDS di Panduan](#) Pengguna Amazon RDS.

[RDS.40] RDS untuk instance SQL Server DB harus menerbitkan log ke Log CloudWatch

Persyaratan terkait: NIST.800-53.r5 AC-2 (4), (26), NIST.800-53.r5 AC-4 (9), (10), NIST.800-53.r5 AC-6 (9) NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 Nist.800-53.R5 SI-3 NIST.800-53.r5 SC-7 (8), Nist.800-53.R5 SI-4 (20), NIST.800-53.R5 SI-7 (8)

Kategori: Identifikasi > Logging

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::RDS::DBInstance

AWS Config aturan: [rds-sql-server-logs-to-cloudwatch](#)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
logTypes	Daftar jenis log yang RDS untuk SQL Server DB instance harus dikonfigurasi untuk dipublikasikan ke CloudWatch Log. Kontrol ini gagal jika instans DB tidak dikonfigurasi untuk mempublikasikan jenis log yang ditentukan dalam daftar.	EnumList (maksimal 2 item)	agent, error	agent, error

Kontrol ini memeriksa apakah instans Amazon RDS for Microsoft SQL Server DB dikonfigurasi untuk mempublikasikan log ke Amazon Logs. CloudWatch Kontrol gagal jika RDS untuk instans SQL Server DB tidak dikonfigurasi untuk mempublikasikan log ke CloudWatch Log. Anda dapat secara opsional menentukan jenis log yang instans DB harus dikonfigurasi untuk diterbitkan.

Pencatatan basis data menyediakan catatan terperinci tentang permintaan yang dibuat ke instans Amazon RDS DB. Menerbitkan CloudWatch log ke Log memusatkan manajemen log dan membantu Anda melakukan analisis data log secara real-time. CloudWatch Log menyimpan log dalam penyimpanan yang sangat tahan lama. Selain itu, Anda dapat menggunakannya untuk membuat alarm untuk kesalahan tertentu yang dapat terjadi, seperti sering restart yang direkam dalam log kesalahan. Demikian pula, Anda dapat membuat alarm untuk kesalahan atau peringatan yang direkam dalam log agen SQL Server yang terkait dengan pekerjaan agen SQL.

Remediasi

Untuk informasi tentang mempublikasikan CloudWatch log ke Log untuk instans DB RDS for SQL Server, lihat file log [database Amazon RDS for Microsoft SQL Server](#) di Panduan Pengguna Layanan Amazon Relational Database Service.

[RDS.41] RDS untuk instance SQL Server DB harus dienkripsi saat transit

Kategori: Lindungi > Perlindungan Data > Enkripsi data-in-transit

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::RDS::DBInstance

AWS Config aturan: [rds-sqlserver-encrypted-in-transit](#)

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah koneksi ke Amazon RDS untuk instans Microsoft SQL Server DB dienkripsi dalam perjalanan. Kontrol gagal jika parameter grup `rds.force_ssl` parameter yang terkait dengan instans DB diatur ke `0` (`off`).

Data dalam transit mengacu pada data yang bergerak dari satu lokasi ke lokasi lain, seperti antara node dalam cluster DB atau antara cluster DB dan aplikasi klien. Data dapat bergerak di internet atau dalam jaringan pribadi. Mengenkripsi data dalam perjalanan mengurangi risiko pengguna yang tidak sah menguping lalu lintas jaringan.

Remediasi

Untuk informasi tentang mengaktifkan SSL/TLS koneksi ke instans Amazon RDS DB yang menjalankan Microsoft SQL Server, lihat [Menggunakan SSL dengan Instans DB Microsoft SQL Server](#) di Panduan Pengguna Layanan Amazon Relational Database Service.

[RDS.42] RDS untuk instance MariaDB DB harus menerbitkan log ke Log CloudWatch

Persyaratan terkait: NIST.800-53.r5 AC-2 (4), (26), NIST.800-53.r5 AC-4 (9),, NIST.800-53.r5 AC-6 (9), (10) NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 Nist.800-53.R5 SI-3 NIST.800-53.r5 SC-7 (8), Nist.800-53.R5 SI-4 (20), NIST.800-53.R5 SI-7 (8)

Kategori: Identifikasi > Logging

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::RDS::DBInstance

AWS Config aturan: [mariadb-publish-logs-to-cloudwatch-logs](#)

Jenis jadwal: Periodik

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
logTypes	Daftar jenis log yang instance MariaDB harus dikonfigurasi untuk dipublikasikan ke Log. CloudWatch Kontrol menghasilkan FAILED temuan jika instans DB tidak dikonfigurasi untuk mempublikasikan jenis log yang ditentukan dalam daftar.	EnumList (maksimal 4 item)	audit, error, general, slowquery	audit, error

Kontrol ini memeriksa apakah instans Amazon RDS for MariaDB DB dikonfigurasi untuk mempublikasikan jenis log tertentu ke Amazon Logs. CloudWatch Kontrol gagal jika instance MariaDB tidak dikonfigurasi untuk mempublikasikan log ke Log. CloudWatch Anda dapat secara opsional menentukan jenis log yang mana instance MariaDB DB harus dikonfigurasi untuk dipublikasikan.

Pencatatan basis data menyediakan catatan terperinci tentang permintaan yang dibuat ke Amazon RDS for MariaDB instans DB. Menerbitkan log ke Amazon CloudWatch Logs memusatkan manajemen log dan membantu Anda melakukan analisis data log secara real-time. Selain itu, CloudWatch Log menyimpan log dalam penyimpanan yang tahan lama, yang dapat mendukung ulasan dan audit keamanan, akses, dan ketersediaan. Dengan CloudWatch Log, Anda juga dapat membuat alarm dan meninjau metrik.

Remediasi

Untuk informasi tentang mengonfigurasi instans Amazon RDS for MariaDB untuk mempublikasikan log ke Log Amazon, lihat Menerbitkan log [MariaDB ke Log CloudWatch Amazon di CloudWatch Panduan Pengguna Layanan Amazon Relational Database Service](#).

[RDS.44] RDS untuk instance MariaDB DB harus dienkripsi saat transit

Kategori: Lindungi > Perlindungan Data > Enkripsi data-in-transit

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::RDS::DBInstance

AWS Config aturan: [rds-mariadb-instance-encrypted-in-transit](#)

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah koneksi ke instans Amazon RDS for MariaDB DB dienkripsi saat transit. Kontrol gagal jika grup parameter DB yang terkait dengan instans DB tidak sinkron, atau `require_secure_transport` parameter grup parameter tidak disetel ke ON.

Note

Kontrol ini tidak mengevaluasi instans Amazon RDS DB yang menggunakan versi MariaDB lebih awal dari versi 10.5. `require_secure_transport` Parameter hanya didukung untuk MariaDB versi 10.5 dan yang lebih baru.

Data dalam transit mengacu pada data yang bergerak dari satu lokasi ke lokasi lain, seperti antara node dalam cluster DB atau antara cluster DB dan aplikasi klien. Data dapat bergerak di internet atau dalam jaringan pribadi. Mengenkripsi data dalam perjalanan mengurangi risiko pengguna yang tidak sah menguping lalu lintas jaringan.

Remediasi

Untuk informasi tentang mengaktifkan koneksi ke instans Amazon RDS SSL/TLS for MariaDB DB, [SSL/TLS lihat Memerlukan semua koneksi ke instans DB MariaDB di Panduan Pengguna Layanan Amazon Relational Database Service](#).

Kontrol Security Hub untuk Amazon Redshift

AWS Security Hub Kontrol ini mengevaluasi layanan dan sumber daya Amazon Redshift. Kontrol mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat [Ketersediaan kontrol berdasarkan Wilayah](#).

[Redshift.1] Cluster Amazon Redshift harus melarang akses publik

Persyaratan terkait: NIST.800-53.r5 AC-2 1,, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-3,, (21),, NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (11), (16) NIST.800-53.r5 AC-6, (20) NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), (4), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SC-7 PCI DSS v3.2.1/1.2.1, NIST.800-53.r5 SC-7 PCI DSS v3.2.1/1.3.1, PCI DSS v3.2.1/1.3.2, PCI DSS v3.2.1/1.3.4, PCI DSS v3.2.1/1.3.6, PCI DSS v4.0.1/1.4.4 NIST.800-53.r5 SC-7

Kategori: Lindungi > Konfigurasi jaringan aman > Sumber daya tidak dapat diakses publik

Tingkat keparahan: Kritis

Jenis sumber daya: AWS::Redshift::Cluster

AWS Config aturan: [redshift-cluster-public-access-check](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah klaster Amazon Redshift dapat diakses publik. Ini mengevaluasi PubliclyAccessible bidang dalam item konfigurasi cluster.

PubliclyAccessibleAtribut konfigurasi klaster Amazon Redshift menunjukkan apakah klaster dapat diakses publik. Ketika cluster dikonfigurasi dengan PubliclyAccessible set to true, itu adalah instance yang menghadap Internet yang memiliki nama DNS yang dapat diselesaikan secara publik, yang diselesaikan ke alamat IP publik.

Ketika cluster tidak dapat diakses publik, itu adalah instance internal dengan nama DNS yang menyelesaikan ke alamat IP pribadi. Kecuali jika Anda bermaksud agar cluster Anda dapat diakses oleh publik, cluster tidak boleh dikonfigurasi dengan PubliclyAccessible set to true.

Remediasi

Untuk memperbarui klaster Amazon Redshift untuk menonaktifkan akses publik, lihat [Memodifikasi klaster di Panduan](#) Manajemen Pergeseran Merah Amazon. Setel Dapat diakses publik ke No.

[Redshift.2] Koneksi ke cluster Amazon Redshift harus dienkripsi saat transit

Persyaratan terkait: NIST.800-53.r5 AC-4, NIST.800-53.r5 SC-1 3, NIST.800-53.r5 SC-2 3, 3 (NIST.800-53.r5 SC-23), (4),, NIST.800-53.r5 SC-7 (1) NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 NIST.800-53.r5 SC-8 (2), PCI DSS v4.0.1/4.2.1

Kategori: Lindungi > Perlindungan Data > Enkripsi data-in-transit

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::Redshift::Cluster` `AWS::Redshift::ClusterParameterGroup`

AWS Config aturan: [redshift-require-tls-ssl](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah koneksi ke kluster Amazon Redshift diperlukan untuk menggunakan enkripsi dalam perjalanan. Pemeriksaan gagal jika parameter cluster Amazon Redshift `require_SSL` tidak disetel ke `True`

TLS dapat digunakan untuk membantu mencegah penyerang potensial menggunakan person-in-the-middle atau serangan serupa untuk menguping atau memanipulasi lalu lintas jaringan. Hanya koneksi terenkripsi melalui TLS yang diizinkan. Mengenkripsi data dalam perjalanan dapat memengaruhi kinerja. Anda harus menguji aplikasi Anda dengan fitur ini untuk memahami profil kinerja dan dampak TLS.

Remediasi

Untuk memperbarui grup parameter Amazon Redshift agar memerlukan enkripsi, lihat [Memodifikasi grup parameter](#) di Panduan Manajemen Pergeseran Merah Amazon. Setel `require_ssl` ke Benar.

[Redshift.3] Cluster Amazon Redshift harus mengaktifkan snapshot otomatis

Persyaratan terkait: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6, NIST.800-53.r5 CP-6(1), NIST.800-53.r5 CP-6(2), NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SC-7 (10), NIST.800-53.R5 SI-13 (5)

Kategori: Pulih> Ketahanan > Cadangan diaktifkan

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::Redshift::Cluster`

AWS Config aturan: [redshift-backup-enabled](#)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub	
MinRetentionPeriod	Periode retensi snapshot minimum dalam beberapa hari	Bilangan Bulat	7 untuk 35	7	

Kontrol ini memeriksa apakah klaster Amazon Redshift mengaktifkan snapshot otomatis, dan periode retensi yang lebih besar dari atau sama dengan kerangka waktu yang ditentukan. Kontrol gagal jika snapshot otomatis tidak diaktifkan untuk cluster, atau jika periode retensi kurang dari kerangka waktu yang ditentukan. Kecuali Anda memberikan nilai parameter khusus untuk periode retensi snapshot, Security Hub menggunakan nilai default 7 hari.

Cadangan membantu Anda pulih lebih cepat dari insiden keamanan. Mereka memperkuat ketahanan sistem Anda. Amazon Redshift mengambil snapshot periodik secara default. Kontrol ini memeriksa apakah snapshot otomatis diaktifkan dan dipertahankan setidaknya selama tujuh hari. Untuk detail selengkapnya tentang snapshot otomatis Amazon Redshift, lihat Snapshot [otomatis di Panduan Manajemen](#) Pergeseran Merah Amazon.

Remediasi

Untuk memperbarui periode retensi snapshot untuk klaster Amazon Redshift, [lihat Memodifikasi klaster di Panduan Manajemen](#) Pergeseran Merah Amazon. Untuk Backup, atur retensi Snapshot ke nilai 7 atau lebih tinggi.

[Redshift.4] Cluster Amazon Redshift harus mengaktifkan pencatatan audit

Persyaratan terkait: NIST.800-53.r5 AC-2 (4), (26), NIST.800-53.r5 AC-4 (9),, NIST.800-53.r5 AC-6 (9), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7 Nist.800-53.R5 SI-3 NIST.800-53.r5 SC-7 (8), Nist.800-53.r5 SI-4 (20), Nist.800-53.R5 SI-7 (8), PCI DSS v4.0.1/10.2.1

Kategori: Identifikasi > Logging

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::Redshift::Cluster`

AWS Config aturan: `redshift-cluster-audit-logging-enabled` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

- `loggingEnabled = true`(tidak dapat disesuaikan)

Kontrol ini memeriksa apakah klaster Amazon Redshift mengaktifkan pencatatan audit.

Pencatatan audit Amazon Redshift memberikan informasi tambahan tentang koneksi dan aktivitas pengguna di klaster Anda. Data ini dapat disimpan dan diamankan di Amazon S3 dan dapat membantu dalam audit dan investigasi keamanan. Untuk informasi selengkapnya, lihat [Pencatatan audit database](#) di Panduan Manajemen Pergeseran Merah Amazon.

Remediasi

Untuk mengonfigurasi pencatatan audit untuk klaster Amazon Redshift, lihat [Mengonfigurasi audit menggunakan konsol di Panduan Manajemen](#) Amazon Redshift.

[Redshift.6] Amazon Redshift harus mengaktifkan peningkatan otomatis ke versi utama

Persyaratan terkait: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5 (2), Nist.800-53.R5 SI-2, NIST.800-53.R5 SI-2 (2), Nist.800-53.R5 SI-2 (4), Nist.800-53.R5 SI-2 (5)

Kategori: Identifikasi > Kerentanan, tambalan, dan manajemen versi

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::Redshift::Cluster`

AWS Config aturan: [redshift-cluster-maintenancesettings-check](#)

Jenis jadwal: Perubahan dipicu

Parameter:

- `allowVersionUpgrade = true`(tidak dapat disesuaikan)

Kontrol ini memeriksa apakah pemutakhiran versi utama otomatis diaktifkan untuk klaster Amazon Redshift.

Mengaktifkan pemutakhiran versi utama otomatis memastikan bahwa pembaruan versi utama terbaru ke kluster Amazon Redshift diinstal selama jendela pemeliharaan. Pembaruan ini mungkin termasuk patch keamanan dan perbaikan bug. Tetap up to date dengan instalasi patch adalah langkah penting dalam mengamankan sistem.

Remediasi

Untuk mengatasi masalah ini dari AWS CLI, gunakan perintah Amazon `modify-cluster` Redshift, dan setel `--allow-version-upgrade` atribut. *clustername* adalah nama cluster Amazon Redshift Anda.

```
aws redshift modify-cluster --cluster-identifier clustername --allow-version-upgrade
```

[Redshift.7] Cluster Redshift harus menggunakan perutean VPC yang ditingkatkan

Persyaratan terkait: NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21) NIST.800-53.r5 SC-7,, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9)

Kategori: Lindungi > Konfigurasi jaringan aman > Akses pribadi API

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::Redshift::Cluster`

AWS Config aturan: [redshift-enhanced-vpc-routing-enabled](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah klaster Amazon Redshift telah `EnhancedVpcRouting` diaktifkan.

Perutean VPC yang disempurnakan memaksa semua COPY dan UNLOAD lalu lintas antara cluster dan repositori data untuk melewati VPC Anda. Anda kemudian dapat menggunakan fitur VPC seperti grup keamanan dan daftar kontrol akses jaringan untuk mengamankan lalu lintas jaringan. Anda juga dapat menggunakan VPC Flow Logs untuk memantau lalu lintas jaringan.

Remediasi

Untuk petunjuk remediasi terperinci, lihat [Mengaktifkan perutean VPC yang disempurnakan di Panduan Manajemen Pergeseran Merah Amazon](#).

[Redshift.8] Cluster Amazon Redshift tidak boleh menggunakan nama pengguna Admin default

Persyaratan terkait: NIST.800-53.r5 CA-9 (1), Nist.800-53.R5 CM-2

Kategori: Identifikasi > Konfigurasi Sumber Daya

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::Redshift::Cluster

AWS Config aturan: [redshift-default-admin-check](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah klaster Amazon Redshift telah mengubah nama pengguna admin dari nilai defaultnya. Kontrol ini akan gagal jika nama pengguna admin untuk cluster Redshift disetel ke. `awsuser`

Saat membuat klaster Redshift, Anda harus mengubah nama pengguna admin default menjadi nilai unik. Nama pengguna default adalah pengetahuan publik dan harus diubah pada konfigurasi. Mengubah nama pengguna default mengurangi risiko akses yang tidak diinginkan.

Remediasi

Anda tidak dapat mengubah nama pengguna admin untuk cluster Amazon Redshift Anda setelah membuatnya. Untuk membuat klaster baru dengan nama pengguna non-default, lihat [Langkah 1: Membuat contoh klaster Amazon Redshift](#) di Panduan Memulai Amazon Redshift.

[Redshift.9] Cluster Redshift tidak boleh menggunakan nama database default

Persyaratan terkait: NIST.800-53.r5 CA-9 (1), Nist.800-53.R5 CM-2

Kategori: Identifikasi > Konfigurasi Sumber Daya

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::Redshift::Cluster`

AWS Config aturan: [redshift-default-db-name-check](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah klaster Amazon Redshift telah mengubah nama database dari nilai defaultnya. Kontrol akan gagal jika nama database untuk cluster Redshift diatur ke. dev

Saat membuat cluster Redshift, Anda harus mengubah nama database default menjadi nilai unik. Nama default adalah pengetahuan publik dan harus diubah pada konfigurasi. Sebagai contoh, nama terkenal dapat menyebabkan akses yang tidak disengaja jika digunakan dalam kondisi kebijakan IAM.

Remediasi

Anda tidak dapat mengubah nama database untuk klaster Amazon Redshift setelah dibuat. Untuk petunjuk cara membuat klaster baru, lihat [Memulai Amazon Redshift](#) di Panduan Memulai Pergeseran Merah Amazon.

[Redshift.10] Cluster Redshift harus dienkripsi saat istirahat

Persyaratan terkait: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-1 3, NIST.800-53.r5 SC-2 8, NIST.800-53.r5 SC-2 8 (1), NIST.800-53.R5 SI-7 (6)

Kategori: Lindungi > Perlindungan Data > Enkripsi data-at-rest

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::Redshift::Cluster`

AWS Config aturan: [redshift-cluster-kms-enabled](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah cluster Amazon Redshift dienkripsi saat istirahat. Kontrol gagal jika klaster Redshift tidak dienkripsi saat istirahat atau jika kunci enkripsi berbeda dari kunci yang disediakan dalam parameter aturan.

Di Amazon Redshift, Anda dapat mengaktifkan enkripsi database untuk cluster Anda untuk membantu melindungi data saat istirahat. Saat Anda mengaktifkan enkripsi untuk cluster, blok data dan metadata sistem dienkripsi untuk cluster dan snapshot-nya. Enkripsi data saat istirahat adalah praktik terbaik yang disarankan karena menambahkan lapisan manajemen akses ke data Anda. Mengenkripsi cluster Redshift saat istirahat mengurangi risiko bahwa pengguna yang tidak sah dapat mengakses data yang disimpan pada disk.

Remediasi

Untuk memodifikasi klaster Redshift agar menggunakan enkripsi KMS, lihat [Mengubah enkripsi klaster di Panduan](#) Manajemen Pergeseran Merah Amazon.

[Redshift.11] Cluster Redshift harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::Redshift::Cluster`

AWS Config aturan: `tagged-redshift-cluster` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
<code>requiredTagKeys</code>	Daftar kunci tag non-sistem yang harus berisi sumber daya	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi	No default value

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
	yang dievaluasi. Kunci tag peka huruf besar dan kecil.		persyaratan AWS .	

Kontrol ini memeriksa apakah kluster Amazon Redshift memiliki tag dengan kunci spesifik yang ditentukan dalam parameter. `requiredTagKeys` Kontrol gagal jika cluster tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter `requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika cluster tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws :`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat [Untuk apa ABAC? AWS](#) di Panduan Pengguna IAM.

Note

Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat [Menandai AWS sumber daya Anda](#) di Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke kluster Redshift, lihat [Menandai sumber daya di Amazon Redshift di Panduan Manajemen Pergeseran Merah](#) Amazon.

[Redshift.12] Langganan pemberitahuan acara Redshift harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: AWS::Redshift::EventSubscription

AWS Config aturan: tagged-redshift-eventsubscription (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
<code>requiredTagKeys</code>	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS .	No default value

Kontrol ini memeriksa apakah snapshot klaster Amazon Redshift memiliki tag dengan kunci spesifik yang ditentukan dalam parameter. `requiredTagKeys` Kontrol gagal jika snapshot cluster tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter `requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika snapshot cluster tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke

AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat [Untuk apa ABAC? AWS](#) di Panduan Pengguna IAM.

Note

Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat [Menandai AWS sumber daya Anda](#) di Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke langganan notifikasi peristiwa Redshift, lihat [Menandai sumber daya di Amazon Redshift di Panduan Manajemen Pergeseran Merah](#) Amazon.

[Redshift.13] Snapshot cluster Redshift harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::Redshift::ClusterSnapshot`

AWS Config aturan: `tagged-redshift-clustersnapshot` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
<code>requiredTagKeys</code>	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi	No default value

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
			persyaratan AWS .	

Kontrol ini memeriksa apakah snapshot klaster Amazon Redshift memiliki tag dengan kunci spesifik yang ditentukan dalam parameter. `requiredTagKeys` Kontrol gagal jika snapshot cluster tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter `requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika snapshot cluster tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat [Untuk apa ABAC? AWS](#) di Panduan Pengguna IAM.

Note

Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat [Menandai AWS sumber daya Anda](#) di Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke snapshot klaster Redshift, lihat [Menandai sumber daya di Amazon Redshift](#) di Panduan Manajemen Pergeseran Merah Amazon.

[Redshift.14] Grup subnet cluster Redshift harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::Redshift::ClusterSubnetGroup`

AWS Config aturan: `tagged-redshift-cluster subnetgroup` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
<code>requiredTagKeys</code>	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS .	No default value

Kontrol ini memeriksa apakah grup subnet klaster Amazon Redshift memiliki tag dengan kunci spesifik yang ditentukan dalam parameter. `requiredTagKeys` Kontrol gagal jika grup subnet cluster tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter `requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika grup subnet cluster tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengkategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan

terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat [Untuk apa ABAC? AWS](#) di Panduan Pengguna IAM.

 Note

Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat [Menandai AWS sumber daya Anda](#) di Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke grup subnet klaster Redshift, lihat [Menandai sumber daya di Amazon Redshift](#) di Panduan Manajemen Pergeseran Merah Amazon.

[Redshift.15] Grup keamanan Redshift harus mengizinkan masuknya port cluster hanya dari asal yang dibatasi

Persyaratan terkait: PCI DSS v4.0.1/1.3.1

Kategori: Lindungi > Konfigurasi jaringan aman > Konfigurasi grup keamanan

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::Redshift::Cluster`

AWS Config aturan: [redshift-unrestricted-port-access](#)

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah grup keamanan yang terkait dengan klaster Amazon Redshift memiliki aturan masuk yang mengizinkan akses ke port cluster dari internet (0.0.0.0/0 atau :/0). Kontrol gagal jika aturan masuknya grup keamanan mengizinkan akses ke port cluster dari internet.

Mengizinkan akses masuk yang tidak terbatas ke port cluster Redshift (alamat IP dengan akhiran /0) dapat mengakibatkan akses atau insiden keamanan yang tidak sah. Kami merekomendasikan untuk menerapkan prinsip akses hak istimewa paling rendah saat membuat grup keamanan dan mengonfigurasi aturan masuk.

Remediasi

Untuk membatasi masuknya port klaster Redshift ke asal terbatas, lihat [Bekerja dengan aturan grup keamanan di Panduan Pengguna Amazon VPC](#). Perbarui aturan di mana rentang port cocok dengan port cluster Redshift dan rentang port IP adalah 0.0.0.0/0.

[Redshift.16] Grup subnet cluster Redshift harus memiliki subnet dari beberapa Availability Zone

Kategori: Pulihkan > Ketahanan > Ketersediaan tinggi

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::Redshift::ClusterSubnetGroup`

AWS Config aturan: [redshift-cluster-subnet-group-multi-az](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol memeriksa apakah grup subnet klaster Amazon Redshift memiliki subnet dari lebih dari satu Availability Zone (AZ). Kontrol gagal jika grup subnet cluster tidak memiliki subnet dari setidaknya dua subnet yang berbeda. AZs

Mengonfigurasi subnet di beberapa AZs bantuan memastikan bahwa gudang data Redshift Anda dapat terus beroperasi bahkan ketika peristiwa kegagalan terjadi.

Remediasi

Untuk mengubah grup subnet klaster Redshift menjadi rentang beberapa AZs, lihat [Memodifikasi grup subnet klaster di Panduan Manajemen Pergeseran Merah Amazon](#).

[Redshift.17] Grup parameter cluster Redshift harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::Redshift::ClusterParameterGroup`

AWS Config aturan: [redshift-cluster-parameter-group-tagged](#)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
<code>requiredKeyTags</code>	Daftar kunci tag non-sistem yang harus ditetapkan ke sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS .	Tidak ada nilai default

Kontrol ini memeriksa apakah grup parameter cluster Amazon Redshift memiliki kunci tag yang ditentukan oleh parameter. `requiredKeyTags` Kontrol gagal jika grup parameter tidak memiliki kunci tag, atau tidak memiliki semua kunci yang ditentukan oleh `requiredKeyTags` parameter. Jika Anda tidak menentukan nilai apa pun untuk `requiredKeyTags` parameter, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika grup parameter tidak memiliki kunci tag. Kontrol mengabaikan tag sistem, yang diterapkan secara otomatis dan memiliki `aws :` awalan.

Tag adalah label yang Anda buat dan tetapkan ke AWS sumber daya. Setiap tanda terdiri dari kunci tanda yang diperlukan dan nilai tanda opsional. Anda dapat menggunakan tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Mereka dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Mereka juga dapat membantu Anda melacak pemilik sumber daya untuk tindakan dan pemberitahuan. Anda juga dapat menggunakan tag untuk menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi. Untuk informasi selengkapnya tentang strategi ABAC, lihat [Menentukan izin berdasarkan atribut dengan otorisasi ABAC](#) di Panduan Pengguna IAM. Untuk informasi selengkapnya tentang tag, lihat [Panduan Pengguna AWS Sumber Daya Penandaan dan Editor Tag](#).

Note

Jangan menyimpan informasi pengenalan pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses dari banyak orang Layanan AWS. Mereka tidak dimaksudkan untuk digunakan untuk data pribadi atau sensitif.

Remediasi

Untuk informasi tentang menambahkan tag ke grup parameter klaster Amazon Redshift, lihat [Menandai sumber daya di Amazon Redshift di Panduan](#) Manajemen Pergeseran Merah Amazon.

Kontrol Security Hub untuk Amazon Redshift Serverless

AWS Security Hub Kontrol ini mengevaluasi layanan dan sumber daya Amazon Redshift Serverless. Kontrol mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat [Ketersediaan kontrol berdasarkan Wilayah](#).

[RedshiftServerless.1] Grup kerja Amazon Redshift Tanpa Server harus menggunakan perutean VPC yang disempurnakan

Kategori: Lindungi > Konfigurasi jaringan aman > Sumber daya dalam VPC

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::RedshiftServerless::Workgroup`

AWS Config aturan: [redshift-serverless-workgroup-routes-within-vpc](#)

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah perutean VPC yang disempurnakan diaktifkan untuk grup kerja Amazon Redshift Tanpa Server. Kontrol gagal jika perutean VPC yang ditingkatkan dinonaktifkan untuk grup kerja.

Jika perutean VPC yang disempurnakan dinonaktifkan untuk grup kerja Amazon Redshift Serverless, Amazon Redshift mengarahkan lalu lintas melalui internet, termasuk lalu lintas ke layanan lain dalam jaringan. AWS Jika Anda mengaktifkan perutean VPC yang disempurnakan untuk grup kerja, Amazon Redshift memaksa semua UNLOAD lalu lintas antara klaster Anda COPY dan repositori data Anda melalui virtual private cloud (VPC) Anda berdasarkan layanan Amazon VPC. Dengan perutean VPC yang disempurnakan, Anda dapat menggunakan fitur VPC standar untuk mengontrol aliran data antara cluster Amazon Redshift dan sumber daya lainnya. Ini termasuk fitur seperti grup keamanan VPC dan kebijakan titik akhir, daftar kontrol akses jaringan (ACLs), dan server Sistem Nama Domain (DNS). Anda juga dapat menggunakan log aliran VPC untuk memantau COPY dan UNLOAD lalu lintas.

Remediasi

Untuk informasi selengkapnya tentang perutean VPC yang disempurnakan dan cara mengaktifkannya untuk grup kerja, lihat [Mengontrol lalu lintas jaringan dengan perutean VPC yang disempurnakan Redshift](#) di Panduan Manajemen Amazon Redshift.

[RedshiftServerless.2] Koneksi ke grup kerja Redshift Serverless harus diperlukan untuk menggunakan SSL

Kategori: Lindungi > Perlindungan Data > Enkripsi data-in-transit

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::RedshiftServerless::Workgroup`

AWS Config aturan: [redshift-serverless-workgroup-encrypted-in-transit](#)

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah koneksi ke workgroup Amazon Redshift Tanpa Server diperlukan untuk mengenkripsi data dalam perjalanan. Kontrol gagal jika parameter `require_ssl` konfigurasi untuk workgroup diatur ke `false`.

Workgroup Amazon Redshift Tanpa Server adalah kumpulan sumber daya komputasi yang mengelompokkan sumber daya komputasi seperti, grup subnet RPU VPC, dan grup keamanan. Properti workgroup mencakup pengaturan jaringan dan keamanan. Pengaturan ini menentukan apakah koneksi ke workgroup harus diperlukan untuk menggunakan SSL untuk mengenkripsi data dalam perjalanan.

Remediasi

Untuk informasi tentang memperbarui setelan grup kerja Amazon Redshift Tanpa Server agar memerlukan koneksi SSL, lihat Menyambungkan ke [Amazon Redshift Tanpa Server di Panduan Manajemen Amazon Redshift](#).

[RedshiftServerless.3] Kelompok kerja Redshift Tanpa Server harus melarang akses publik

Kategori: Lindungi > Konfigurasi jaringan aman > Sumber daya tidak dapat diakses publik

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::RedshiftServerless::Workgroup`

AWS Config aturan: [redshift-serverless-workgroup-no-public-access](#)

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah akses publik dinonaktifkan untuk grup kerja Amazon Redshift Tanpa Server. Ini mengevaluasi `publiclyAccessible` properti grup kerja Redshift Serverless. Kontrol gagal jika akses publik diaktifkan (`true`) untuk workgroup.

Pengaturan public access (`publiclyAccessible`) untuk workgroup Amazon Redshift Serverless menentukan apakah workgroup dapat diakses dari jaringan publik. Jika akses publik diaktifkan (`true`) untuk grup kerja, Amazon Redshift akan membuat alamat IP Elastis yang membuat grup kerja dapat diakses publik dari luar VPC. Jika Anda tidak ingin grup kerja dapat diakses publik, nonaktifkan akses publik untuk itu.

Remediasi

Untuk informasi tentang mengubah setelan akses publik untuk grup kerja Amazon Redshift Tanpa Server, lihat [Melihat properti untuk grup kerja di](#) Panduan Manajemen Amazon Redshift.

[RedshiftServerless.4] Ruang nama Redshift Tanpa Server harus dienkripsi dengan pengelolaan pelanggan AWS KMS keys

Persyaratan terkait: NIST.800-53.r5 AU-9, NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SC-1 2 (2), NIST.800-53.r5 SC-1 3, 8, NIST.800-53.r5 SC-2 NIST.800-53.r5 SC-2 8 (1), Nist.800-53.R5 SI-7 (6)

Kategori: Lindungi > Perlindungan Data > Enkripsi data-at-rest

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::RedshiftServerless::Namespace`

AWS Config aturan: [redshift-serverless-namespace-cmk-encryption](#)

Jenis jadwal: Periodik

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
kmsKeyArns	Daftar Nama Sumber Daya Amazon (ARNs) AWS KMS keys untuk disertakan dalam evaluasi. Kontrol menghasilkan FAILED temuan jika namespace Redshift Tanpa Server tidak dienkripsi dengan kunci KMS dalam daftar.	StringList (maksimal 3 item)	1—3 kunci ARNs KMS yang ada. Sebagai contoh: arn:aws:kms:us-west-2:11112223333:key/1234abcd-12ab-34cd-56ef-1234567890ab	Tidak ada nilai default

Kontrol ini memeriksa apakah namespace Amazon Redshift Tanpa Server dienkripsi saat istirahat dengan pelanggan yang dikelola. AWS KMS key Kontrol gagal jika namespace Redshift Tanpa Server tidak dienkripsi dengan kunci KMS yang dikelola pelanggan. Anda dapat secara opsional menentukan daftar kunci KMS untuk kontrol untuk disertakan dalam evaluasi.

Di Amazon Redshift Tanpa Server, namespace mendefinisikan wadah logis untuk objek database. Kontrol ini secara berkala memeriksa apakah pengaturan enkripsi untuk namespace menentukan pelanggan yang dikelola AWS KMS key, bukan kunci KMS yang AWS dikelola, untuk enkripsi data di namespace. Dengan kunci KMS yang dikelola pelanggan, Anda memiliki kendali penuh atas kunci tersebut. Ini termasuk mendefinisikan dan memelihara kebijakan kunci, mengelola hibah, memutar materi kriptografi, menetapkan tag, membuat alias, dan mengaktifkan dan menonaktifkan kunci.

Remediasi

Untuk informasi tentang memperbarui setelan enkripsi untuk namespace Amazon Redshift Tanpa Server dan menentukan pelanggan yang dikelola AWS KMS key, lihat [Mengubah AWS KMS key namespace di](#) Panduan Manajemen Amazon Redshift.

[RedshiftServerless.5] Ruang nama Redshift Tanpa Server tidak boleh menggunakan nama pengguna admin default

Kategori: Identifikasi > Konfigurasi sumber daya

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::RedshiftServerless::Namespace

AWS Config aturan: [redshift-serverless-default-admin-check](#)

Jenis jadwal: Periodik

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
validAdminUserNames	Daftar nama pengguna admin yang harus digunakan ruang nama Redshift Tanpa Server. Kontrol menghasilkan FAILED temuan jika namespace menggunakan nama pengguna admin yang tidak ada dalam daftar. Daftar tidak dapat menentukan nilai default,admin.	StringList (maksimal 6 item)	1—6 nama pengguna admin yang valid untuk ruang nama Redshift Tanpa Server.	Tidak ada nilai default

Kontrol ini memeriksa apakah nama pengguna admin untuk namespace Amazon Redshift Tanpa Server adalah nama pengguna admin default. admin Kontrol gagal jika nama pengguna admin untuk namespace Redshift Serverless adalah. admin Anda dapat secara opsional menentukan daftar nama pengguna admin untuk kontrol yang akan disertakan dalam evaluasi.

Saat membuat namespace Amazon Redshift Tanpa Server, Anda harus menentukan nama pengguna admin khusus untuk namespace. Nama pengguna admin default adalah pengetahuan publik. Dengan menentukan nama pengguna admin kustom, Anda dapat, misalnya, membantu mengurangi risiko atau efektivitas serangan brute force terhadap namespace.

Remediasi

Anda dapat mengubah nama pengguna admin untuk namespace Amazon Redshift Tanpa Server dengan menggunakan konsol Amazon Redshift Serverless atau API. Untuk mengubahnya dengan menggunakan konsol, pilih konfigurasi namespace, lalu pilih Edit kredensi admin di menu Tindakan. Untuk mengubahnya secara terprogram, gunakan [UpdateNamespace](#) operasi atau, jika Anda menggunakan AWS CLI, jalankan perintah [update-namespace](#). Jika Anda mengubah nama pengguna admin, Anda juga harus mengubah kata sandi admin secara bersamaan.

[RedshiftServerless.6] Ruang nama Redshift Tanpa Server harus mengekspor log ke Log CloudWatch

Kategori: Identifikasi > Logging

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::RedshiftServerless::Namespace

AWS Config aturan: [redshift-serverless-publish-logs-to-cloudwatch](#)

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah namespace Amazon Redshift Tanpa Server dikonfigurasi untuk mengekspor koneksi dan log pengguna ke Amazon Logs. CloudWatch Kontrol gagal jika namespace Redshift Tanpa Server tidak dikonfigurasi untuk mengekspor log ke Log. CloudWatch

Jika Anda mengonfigurasi Amazon Redshift Tanpa Server untuk mengekspor data log koneksi (connectionlog) dan log pengguna (userlog) ke grup log di Amazon CloudWatch Logs, Anda dapat mengumpulkan dan menyimpan catatan log Anda dalam penyimpanan tahan lama, yang dapat mendukung ulasan dan audit keamanan, akses, dan ketersediaan. Dengan CloudWatch Log, Anda

dapat melakukan analisis data log secara waktu nyata dan menggunakannya CloudWatch untuk membuat alarm dan meninjau metrik.

Remediasi

Untuk mengeksport data log untuk namespace Amazon Redshift Tanpa Server ke Amazon CloudWatch Logs, masing-masing log harus dipilih untuk diekspor dalam setelan konfigurasi pencatatan audit untuk namespace. Untuk informasi tentang memperbarui setelan ini, lihat [Mengedit keamanan dan enkripsi](#) di Panduan Manajemen Amazon Redshift.

[RedshiftServerless.7] Ruang nama Redshift Tanpa Server seharusnya tidak menggunakan nama database default

Persyaratan terkait: NIST.800-53.r5 CA-9 (1), Nist.800-53.R5 CM-2

Kategori: Identifikasi > Konfigurasi sumber daya

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::RedshiftServerless::Namespace

AWS Config aturan: [redshift-serverless-default-db-name-check](#)

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah namespace Amazon Redshift Tanpa Server menggunakan nama database default,. dev Kontrol gagal jika namespace Redshift Serverless menggunakan nama database default,. dev

Saat membuat namespace Amazon Redshift Tanpa Server, Anda harus menentukan nilai khusus yang unik untuk nama database dan tidak menggunakan nama database default, yaitu. dev Nama database default adalah pengetahuan publik. Dengan menentukan nama database yang berbeda, Anda dapat mengurangi risiko seperti pengguna yang tidak sah secara tidak sengaja mendapatkan akses ke data di namespace.

Remediasi

Anda tidak dapat mengubah nama instans Amazon Redshift Server setelah membuat namespace. Namun, Anda dapat menentukan nama database kustom untuk namespace Redshift Tanpa Server saat Anda membuat namespace. Untuk informasi tentang membuat namespace, lihat [Workgroups dan namespace di](#) Panduan Manajemen Amazon Redshift.

Kontrol Security Hub untuk Route 53

AWS Security Hub Kontrol ini mengevaluasi layanan dan sumber daya Amazon Route 53.

Kontrol ini mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat [Ketersediaan kontrol berdasarkan Wilayah](#).

[Route53.1] Pemeriksaan kesehatan rute 53 harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: AWS::Route53::HealthCheck

AWS Config aturan: tagged-route53-healthcheck (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
<code>requiredTagKeys</code>	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS .	Tidak ada nilai default

Kontrol ini memeriksa apakah pemeriksaan kesehatan Amazon Route 53 memiliki tag dengan kunci spesifik yang ditentukan dalam parameter `requiredTagKeys`. Kontrol gagal jika pemeriksaan kesehatan tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter `requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika pemeriksaan kesehatan tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengkategorikan sumber daya berdasarkan tujuan, pemilik,

lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat [Untuk apa ABAC? AWS](#) di Panduan Pengguna IAM.

Note

Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat [Menandai AWS sumber daya Anda](#) di Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke pemeriksaan kesehatan Route 53, lihat [Penamaan dan penandaan pemeriksaan kesehatan](#) di Panduan Pengembang Amazon Route 53.

[Route53.2] Route 53 zona yang dihosting publik harus mencatat kueri DNS

Persyaratan terkait: NIST.800-53.r5 AC-2 (4), (26), NIST.800-53.r5 AC-4 (9),, NIST.800-53.r5 AC-6 (9), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7 Nist.800-53.R5 SI-3 NIST.800-53.r5 SC-7 (8), Nist.800-53.R5 SI-4 (20), Nist.800-53.R5 SI-7 (8), PCI DSS v4.0.1/10.4.2

Kategori: Identifikasi > Logging

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::Route53::HostedZone

AWS Config aturan: [route53-query-logging-enabled](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah pencatatan kueri DNS diaktifkan untuk zona host publik Amazon Route 53. Kontrol gagal jika pencatatan kueri DNS tidak diaktifkan untuk zona host publik Route 53.

Mencatat kueri DNS untuk zona yang dihosting Route 53 memenuhi persyaratan keamanan dan kepatuhan DNS dan memberikan visibilitas. Log mencakup informasi seperti domain atau subdomain yang ditanyakan, tanggal dan waktu kueri, jenis catatan DNS (misalnya, A atau AAAA), dan kode respons DNS (misalnya, atau). NoError ServFail Saat pencatatan kueri DNS diaktifkan, Route 53 menerbitkan file log ke Amazon CloudWatch Logs.

Remediasi

Untuk mencatat kueri DNS untuk zona host publik Route 53, lihat [Mengonfigurasi pencatatan untuk kueri DNS](#) di Panduan Pengembang Amazon Route 53.

Kontrol Security Hub untuk Amazon S3

AWS Security Hub Kontrol ini mengevaluasi layanan dan sumber daya Amazon Simple Storage Service (Amazon S3). Kontrol mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat [Ketersediaan kontrol berdasarkan Wilayah](#).

[S3.1] Bucket tujuan umum S3 harus mengaktifkan pengaturan akses publik blok

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v3.0.0/2.1.4, Tolok Ukur AWS Yayasan CIS v1.4.0/2.1.5, NIST.800-53.r5 AC-2 1,, NIST.800-53.r5 AC-3 (7),, (21),,, (11), (16) NIST.800-53.r5 AC-3, (20), (21) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (3), (4) NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (9) NIST.800-53.r5 SC-7, PCI DSS v3.2.1/1.2.1, NIST.800-53.r5 SC-7 PCI DSS v3.2.1/1.3.1, NIST.800-53.r5 SC-7 PCI DSS v3.2.1/1.3.2, NIST.800-53.r5 SC-7 PCI DSS v3.2.1/1.3.4, PCI DSS v3.2.1/1.3.6, PCI DSS v4.0.1/1.4.4 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7

Kategori: Lindungi > Konfigurasi jaringan aman

Tingkat keparahan: Sedang

Jenis sumber daya: AWS :: : Account

AWS Config aturan: [s3-account-level-public-access-blocks-periodic](#)

Jenis jadwal: Periodik

Parameter:

- `ignorePublicAcls: true` (tidak dapat disesuaikan)
- `blockPublicPolicy: true` (tidak dapat disesuaikan)
- `blockPublicAcls: true` (tidak dapat disesuaikan)
- `restrictPublicBuckets: true` (tidak dapat disesuaikan)

Kontrol ini memeriksa apakah setelan akses publik blok Amazon S3 sebelumnya dikonfigurasi pada tingkat akun untuk bucket tujuan umum S3. Kontrol gagal jika satu atau lebih pengaturan akses publik blok diatur ke `false`.

Kontrol gagal jika salah satu pengaturan diatur ke `false`, atau jika salah satu pengaturan tidak dikonfigurasi.

Blok akses publik Amazon S3 dirancang untuk menyediakan kontrol di seluruh Akun AWS atau pada tingkat bucket S3 individual untuk memastikan bahwa objek tidak pernah memiliki akses publik. Akses publik diberikan ke bucket dan objek melalui daftar kontrol akses (ACLs), kebijakan bucket, atau keduanya.

Kecuali jika Anda bermaksud agar bucket S3 Anda dapat diakses publik, Anda harus mengonfigurasi fitur Amazon S3 Block Public Access level akun.

Untuk mempelajari selengkapnya, lihat [Menggunakan Amazon S3 Blokir Akses Publik](#) di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

Remediasi

Untuk mengaktifkan Amazon S3 Blokir Akses Publik untuk Anda Akun AWS, lihat [Mengonfigurasi setelan blokir akses publik untuk akun Anda](#) di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

[S3.2] Bucket tujuan umum S3 harus memblokir akses baca publik

Persyaratan terkait: PCI DSS v3.2.1/1.2.1, PCI DSS v3.2.1/1.3.1, PCI DSS v3.2.1/1.3.2, PCI DSS v3.2.1/1.3.6, PCI DSS v3.2.1/7.2.1, NIST.800-53.r5 AC-2 1,, NIST.800-53.r5 AC-3 (7),, (21),,, (11), (16), (20), (21), (3), (4) NIST.800-53.r5 AC-3, (9) NIST.800-53.r5 AC-4 NIST.800-53.r5 AC-4 NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7

Kategori: Lindungi > Konfigurasi jaringan aman

Tingkat keparahan: Kritis

Jenis sumber daya: AWS::S3::Bucket

AWS Config aturan: [s3-bucket-public-read-prohibited](#)

Jenis jadwal: Berkala dan perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah bucket tujuan umum Amazon S3 mengizinkan akses baca publik. Ini mengevaluasi pengaturan blokir akses publik, kebijakan bucket, dan daftar kontrol akses bucket (ACL). Kontrol gagal jika bucket mengizinkan akses baca publik.

Note

Jika bucket S3 memiliki kebijakan bucket, kontrol ini tidak mengevaluasi kondisi kebijakan yang menggunakan karakter atau variabel wildcard. Untuk menghasilkan PASSED temuan, kondisi dalam kebijakan bucket hanya boleh menggunakan nilai tetap, yaitu nilai yang tidak mengandung karakter wildcard atau variabel kebijakan. Untuk informasi tentang variabel kebijakan, lihat [Variabel dan tag](#) di Panduan AWS Identity and Access Management Pengguna.

Beberapa kasus penggunaan mungkin mengharuskan semua orang di internet dapat membaca dari bucket S3 Anda. Namun, situasi itu jarang terjadi. Untuk memastikan integritas dan keamanan data Anda, bucket S3 Anda tidak boleh dibaca publik.

Remediasi

Untuk memblokir akses baca publik di bucket Amazon S3, lihat [Mengonfigurasi blokir setelan akses publik untuk bucket S3 Anda di](#) Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

[S3.3] Bucket tujuan umum S3 harus memblokir akses tulis publik

Persyaratan terkait: PCI DSS v3.2.1/1.2.1, PCI DSS v3.2.1/1.3.1, PCI DSS v3.2.1/1.3.2, PCI DSS v3.2.1/1.3.4, PCI DSS v3.2.1/1.3.6, PCI DSS v3.2.1/7.2.1, 1,, (7),, (21),,, (11), (16), (16), (20), (21), (3), (4), (9) NIST.800-53.r5 AC-2 NIST.800-53.r5 AC-3 NIST.800-53.r5 AC-3 NIST.800-53.r5 AC-4 NIST.800-53.r5 AC-4 NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7

Kategori: Lindungi > Konfigurasi jaringan aman

Tingkat keparahan: Kritis

Jenis sumber daya: AWS::S3::Bucket

AWS Config aturan: [s3-bucket-public-write-prohibited](#)

Jenis jadwal: Berkala dan perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah bucket tujuan umum Amazon S3 mengizinkan akses tulis publik. Ini mengevaluasi pengaturan blokir akses publik, kebijakan bucket, dan daftar kontrol akses bucket (ACL). Kontrol gagal jika bucket mengizinkan akses tulis publik.

 Note

Jika bucket S3 memiliki kebijakan bucket, kontrol ini tidak mengevaluasi kondisi kebijakan yang menggunakan karakter atau variabel wildcard. Untuk menghasilkan PASSED temuan, kondisi dalam kebijakan bucket hanya boleh menggunakan nilai tetap, yaitu nilai yang tidak mengandung karakter wildcard atau variabel kebijakan. Untuk informasi tentang variabel kebijakan, lihat [Variabel dan tag](#) di Panduan AWS Identity and Access Management Pengguna.

Beberapa kasus penggunaan mengharuskan semua orang di internet dapat menulis ke bucket S3 Anda. Namun, situasi itu jarang terjadi. Untuk memastikan integritas dan keamanan data Anda, bucket S3 Anda tidak boleh ditulis secara publik.

Remediasi

Untuk memblokir akses tulis publik di bucket Amazon S3, lihat [Mengonfigurasi setelan blokir akses publik untuk bucket S3 Anda di](#) Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

[S3.5] Bucket tujuan umum S3 harus memerlukan permintaan untuk menggunakan SSL

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v3.0.0/2.1.1, Tolok Ukur AWS Yayasan CIS v1.4.0/2.1.2, 7 (2), (1), 2 (3), 3, 3, 3 (3), (4), (1), NIST.800-53.r5 IA-5 (2) NIST.800-53.r5 AC-4, Nist.800-53.r5 NIST.800-53.r5 AC-1 SI-7 (6), NIST.800-53.r5 SC-1 NIST.800-53.r5 SC-1

Nist.800-171.r2 3.13.8, NIST.800-53.r5 SC-2 Nist.800-171.r2 3.13.8 NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 Nist.800-800-171.r2 3.13.15, NIST.800-53.r5 SC-8 PCI DSS v3.2.1/4.1, PCI DSS v4.0.1/4.2.1 NIST.800-53.r5 SC-2 NIST.800-53.r5 SC-7

Kategori: Lindungi > Manajemen akses yang aman

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::S3::Bucket

AWS Config aturan: [s3-bucket-ssl-requests-only](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah bucket tujuan umum Amazon S3 memiliki kebijakan yang mengharuskan permintaan untuk menggunakan SSL. Kontrol gagal jika kebijakan bucket tidak memerlukan permintaan untuk menggunakan SSL.

Bucket S3 harus memiliki kebijakan yang mengharuskan semua permintaan (Action: S3:*) hanya menerima transmisi data melalui HTTPS dalam kebijakan sumber daya S3, yang ditunjukkan oleh kunci kondisi. `aws:SecureTransport`

Remediasi

Untuk memperbarui kebijakan bucket Amazon S3 untuk menolak transportasi yang tidak aman, lihat [Menambahkan kebijakan bucket menggunakan konsol Amazon S3 di](#) Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

Tambahkan pernyataan kebijakan yang mirip dengan yang ada di kebijakan berikut. Ganti `amzn-s3-demo-bucket` dengan nama bucket yang Anda modifikasi.

```
{
  "Id": "ExamplePolicy",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowSSLRequestsOnly",
      "Action": "s3:*",
      "Effect": "Deny",
      "Resource": [
```



```

        "arn:aws:s3:::amzn-s3-demo-bucket",
        "arn:aws:s3:::amzn-s3-demo-bucket/*"
    ],
    "Condition": {
        "Bool": {
            "aws:SecureTransport": "false"
        }
    },
    "Principal": "*"
}
]
}

```

Untuk informasi selengkapnya, lihat [Kebijakan bucket S3 apa yang harus saya gunakan untuk mematuhi AWS Config aturan s3-? bucket-ssl-requests-only](#) di Pusat Pengetahuan AWS Resmi.

[S3.6] Kebijakan bucket tujuan umum S3 harus membatasi akses ke yang lain Akun AWS

Persyaratan terkait: NIST.800-53.r5 CA-9 (1), Nist.800-53.r5 CM-2, Nist.800-171.r2 3.13.4

Kategori: Lindungi > Manajemen akses aman > Tindakan operasi API sensitif dibatasi

Tingkat keparahan: Tinggi

Jenis sumber daya: AWS::S3::Bucket

AWS Configaturan: [s3-bucket-blacklisted-actions-prohibited](#)

Jenis jadwal: Perubahan dipicu

Parameter:

- `blacklistedactionpatterns`: `s3:DeleteBucketPolicy`, `s3:PutBucketAcl`, `s3:PutBucketPolicy`, `s3:PutEncryptionConfiguration`, `s3:PutObjectAcl` (tidak dapat disesuaikan)

Kontrol ini memeriksa apakah kebijakan bucket tujuan umum Amazon S3 mencegah prinsipal dari pihak lain Akun AWS melakukan tindakan yang ditolak pada sumber daya di bucket S3. Kontrol gagal jika kebijakan bucket mengizinkan satu atau beberapa tindakan sebelumnya untuk prinsipal di tempat lain. Akun AWS

Menerapkan akses hak istimewa paling sedikit sangat penting untuk mengurangi risiko keamanan dan dampak kesalahan atau niat jahat. Jika kebijakan bucket S3 mengizinkan akses dari akun eksternal, hal itu dapat mengakibatkan eksfiltrasi data oleh ancaman orang dalam atau penyerang.

`blacklistedactionpatterns` Parameter ini memungkinkan evaluasi aturan yang berhasil untuk ember S3. Parameter memberikan akses ke akun eksternal untuk pola tindakan yang tidak termasuk dalam `blacklistedactionpatterns` daftar.

Remediasi

Untuk memperbarui kebijakan bucket Amazon S3 guna menghapus izin, lihat. [Menambahkan kebijakan bucket dengan menggunakan konsol Amazon S3](#) di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

Pada halaman Edit kebijakan bucket, di kotak teks pengeditan kebijakan, lakukan salah satu tindakan berikut:

- Hapus pernyataan yang memberikan Akun AWS akses lain ke tindakan yang ditolak.
- Hapus tindakan yang ditolak yang diizinkan dari pernyataan.

[S3.7] Ember tujuan umum S3 harus menggunakan replikasi lintas wilayah

Persyaratan terkait: PCI DSS v3.2.1/2.2, NIST.800-53.r5 AU-9(2), NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6, NIST.800-53.r5 CP-6(1), NIST.800-53.r5 CP-6(2), NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-3 6 (2), (2), NIST.800-53.R5 NIST.800-53.r5 SC-5 SI-13 (5)

Kategori: Lindungi > Manajemen akses yang aman

Tingkat keparahan: Rendah

Jenis sumber daya: AWS :: S3 :: Bucket

AWS Config aturan: [s3-bucket-cross-region-replication-enabled](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah bucket tujuan umum Amazon S3 mengaktifkan replikasi lintas wilayah. Kontrol gagal jika bucket tidak mengaktifkan replikasi lintas wilayah.

Replikasi adalah penyalinan objek secara otomatis dan asinkron di seluruh ember dalam hal yang sama atau berbeda. Wilayah AWS Replikasi menyalin objek dan pembaruan objek yang baru dibuat dari bucket sumber ke bucket atau bucket tujuan. AWS praktik terbaik merekomendasikan replikasi untuk ember sumber dan tujuan yang dimiliki oleh yang sama. Akun AWS Selain ketersediaan, Anda harus mempertimbangkan pengaturan pengerasan sistem lainnya.

Kontrol ini menghasilkan FAILED temuan untuk bucket tujuan replikasi jika replikasi lintas wilayah tidak diaktifkan. Jika ada alasan sah bahwa bucket tujuan tidak memerlukan replikasi lintas wilayah untuk diaktifkan, Anda dapat menekan temuan untuk bucket ini.

Remediasi

Untuk mengaktifkan Replikasi Lintas Wilayah pada bucket S3, lihat [Mengonfigurasi replikasi untuk bucket sumber dan tujuan yang dimiliki oleh akun yang sama di](#) Panduan Pengguna Layanan Penyimpanan Sederhana Amazon. Untuk bucket Source, pilih Apply to all objects in the bucket.

[S3.8] Bucket tujuan umum S3 harus memblokir akses publik

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v3.0.0/2.1.4, Tolok Ukur AWS Yayasan CIS v1.4.0/2.1.5, NIST.800-53.r5 AC-2 1,, NIST.800-53.r5 AC-3 (7),, (21) NIST.800-53.r5 AC-3,,, (11) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (16), (20) NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), (4), NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SC-7 PCI DSS v4.0.1/1.4.4 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7

Kategori: Lindungi > Manajemen akses yang aman > Kontrol akses

Tingkat keparahan: Tinggi

Jenis sumber daya: AWS :: S3 :: Bucket

AWS Config aturan: [s3-bucket-level-public-access-prohibited](#)

Jenis jadwal: Perubahan dipicu

Parameter:

- `excludedPublicBuckets`(tidak dapat disesuaikan) - Daftar terpisah koma dari nama bucket S3 publik yang diizinkan yang diketahui

Kontrol ini memeriksa apakah bucket tujuan umum Amazon S3 memblokir akses publik di tingkat bucket. Kontrol gagal jika salah satu pengaturan berikut diatur ke `false`:

- `ignorePublicAcls`
- `blockPublicPolicy`
- `blockPublicAcls`
- `restrictPublicBuckets`

Blokir Akses Publik pada tingkat bucket S3 menyediakan kontrol untuk memastikan bahwa objek tidak pernah memiliki akses publik. Akses publik diberikan ke bucket dan objek melalui daftar kontrol akses (ACLs), kebijakan bucket, atau keduanya.

Kecuali jika Anda bermaksud agar bucket S3 dapat diakses publik, Anda harus mengonfigurasi fitur Amazon S3 Block Public Access level bucket.

Remediasi

Untuk informasi tentang cara menghapus akses publik pada tingkat bucket, lihat [Memblokir akses publik ke penyimpanan Amazon S3 Anda di Panduan](#) Pengguna Amazon S3.

[S3.9] Bucket tujuan umum S3 harus mengaktifkan pencatatan akses server

Persyaratan terkait: NIST.800-53.r5 AC-2 (4), (26), NIST.800-53.r5 AC-4 (9),, NIST.800-53.r5 AC-6 (9), Nist.800-53.r5 SI-3 NIST.800-53.r5 SC-7 (8) NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, Nist.800-53.r5 SI-4 (20), Nist.800-53.r5 SI-7 (8), Nist.800-171.r2 3.3.8, PCI DSS v4.0.1/10.2.1

Kategori: Identifikasi > Logging

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::S3::Bucket

AWS Config aturan: [s3-bucket-logging-enabled](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah pencatatan akses server diaktifkan untuk bucket tujuan umum Amazon S3. Kontrol gagal jika pencatatan akses server tidak diaktifkan. Saat logging diaktifkan, Amazon S3 mengirimkan log akses untuk bucket sumber ke bucket target yang dipilih. Bucket target harus

Wilayah AWS sama dengan bucket sumber dan tidak boleh memiliki periode retensi default yang dikonfigurasi. Bucket logging target tidak perlu mengaktifkan pencatatan akses server, dan Anda harus menekan temuan untuk bucket ini.

Pencatatan akses server menyediakan catatan terperinci tentang permintaan yang dibuat ke ember. Log akses server dapat membantu dalam audit keamanan dan akses. Untuk informasi selengkapnya, lihat [Praktik Terbaik Keamanan untuk Amazon S3: Aktifkan pencatatan akses server Amazon S3](#).

Remediasi

Untuk mengaktifkan pencatatan akses server Amazon S3, lihat [Mengaktifkan pencatatan akses server Amazon S3 di](#) Panduan Pengguna Amazon S3.

[S3.10] Bucket tujuan umum S3 dengan versi diaktifkan harus memiliki konfigurasi Siklus Hidup

Persyaratan terkait: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6(2), NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5 (2), NIST.800-53.R5 SI-13 (5)

Kategori: Identifikasi > Logging

Tingkat keparahan: Sedang

Jenis sumber daya: AWS :: S3 :: Bucket

AWS Config aturan: [s3-version-lifecycle-policy-check](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah bucket berversi tujuan umum Amazon S3 memiliki konfigurasi Siklus Hidup. Kontrol gagal jika bucket tidak memiliki konfigurasi Siklus Hidup.

Sebaiknya buat konfigurasi Siklus Hidup untuk bucket S3 untuk membantu menentukan tindakan yang ingin dilakukan Amazon S3 selama masa pakai objek.

Remediasi

[Untuk informasi selengkapnya tentang mengonfigurasi siklus hidup di bucket Amazon S3, lihat Menyetel konfigurasi siklus hidup pada bucket dan Mengelola siklus hidup penyimpanan Anda.](#)

[S3.11] Bucket tujuan umum S3 harus mengaktifkan pemberitahuan acara

Persyaratan terkait: NIST.800-53.r5 CA-7, NIST.800-53.R5 SI-3 (8), NIST.800-53.R5 SI-4, NIST.800-53.R5 SI-4 (4), Nist.800-171.R2 3.3.8

Kategori: Identifikasi > Logging

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::S3::Bucket

AWS Config aturan: [s3-event-notifications-enabled](#)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
eventTypes	Daftar jenis acara S3 pilihan	EnumList (maksimal 28 item)	s3:IntelligentTiering, s3:LifecycleExpiration:*, s3:LifecycleExpiration:Delete, s3:LifecycleExpiration:DeleteMarkerCreated, s3:LifecycleTransition,	Tidak ada nilai default

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
			s3:Object Acl:Put, s3:Object Created:* , s3:Object Created:CompleteMulti partUp load, s3:Object Created:Copy, s3:Object Created:Post, s3:Object Created:Put, s3:Object Removed:* , s3:Object Removed:Delete, s3:Object Removed:DeleteMark erCreated , s3:Object Restore:*	

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
			, s3:ObjectRestore:Completed, s3:ObjectRestore:Delete, s3:ObjectRestore:Post, s3:ObjectTagging:* , s3:ObjectTagging:Delete, s3:ObjectTagging:Put, s3:ReducedRedundancyLostObject, s3:Replication:*, s3:Replication:OperationFailedReplication, s3:Replication:Ope	

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
			<code>rationMissedThreshold,</code> <code>s3:Replication:OperationNotTracked,</code> <code>s3:Replication:OperationReplicatedAfterThreshold,</code> <code>s3:TestEvent</code>	

Kontrol ini memeriksa apakah Pemberitahuan Peristiwa S3 diaktifkan pada bucket tujuan umum Amazon S3. Kontrol gagal jika Pemberitahuan Acara S3 tidak diaktifkan di bucket. Jika Anda memberikan nilai kustom untuk `eventTypes` parameter, kontrol hanya akan diteruskan jika pemberitahuan peristiwa diaktifkan untuk jenis peristiwa yang ditentukan.

Saat mengaktifkan Pemberitahuan Acara S3, Anda menerima peringatan saat peristiwa tertentu terjadi yang memengaruhi bucket S3 Anda. Misalnya, Anda dapat diberi tahu tentang pembuatan objek, penghapusan objek, dan restorasi objek. Pemberitahuan ini dapat mengingatkan tim terkait untuk modifikasi yang tidak disengaja atau disengaja yang dapat menyebabkan akses data yang tidak sah.

Remediasi

Untuk informasi tentang mendeteksi perubahan pada bucket dan objek S3, lihat [Pemberitahuan Acara Amazon S3 di Panduan Pengguna Amazon S3](#).

[S3.12] tidak ACLs boleh digunakan untuk mengelola akses pengguna ke bucket tujuan umum S3

Persyaratan terkait: NIST.800-53.r5 AC-2 (1) NIST.800-53.r5 AC-3,, NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-6

Kategori: Lindungi > Manajemen akses yang aman > Kontrol akses

Tingkat keparahan: Sedang

Jenis sumber daya: AWS : : S3 : : Bucket

AWS Config aturan: [s3-bucket-acl-prohibited](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah bucket tujuan umum Amazon S3 menyediakan izin pengguna dengan daftar kontrol akses (ACL). Kontrol gagal jika ACL dikonfigurasi untuk mengelola akses pengguna di bucket.

ACLs adalah mekanisme kontrol akses lama yang mendahului IAM. Sebagai gantinya ACLs, sebaiknya gunakan kebijakan bucket S3 atau kebijakan AWS Identity and Access Management (IAM) untuk mengelola akses ke bucket S3 Anda.

Remediasi

Untuk melewati kontrol ini, Anda harus menonaktifkan ACLs bucket S3 Anda. Untuk petunjuknya, lihat [Mengontrol kepemilikan objek dan menonaktifkan ACLs bucket Anda](#) di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

Untuk membuat kebijakan bucket S3, lihat [Menambahkan kebijakan bucket menggunakan konsol Amazon S3](#). Untuk membuat kebijakan pengguna IAM di bucket S3, lihat [Mengontrol akses ke bucket dengan kebijakan pengguna](#).

[S3.13] Bucket tujuan umum S3 harus memiliki konfigurasi Siklus Hidup

Persyaratan terkait: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6(2), NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5 (2), NIST.800-53.R5 SI-13 (5)

Kategori: Lindungi > Perlindungan data

Tingkat keparahan: Rendah

Jenis sumber daya: AWS::S3::Bucket

AWS Config aturan: [s3-lifecycle-policy-check](#)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
targetTransitionDays	Jumlah hari setelah pembuatan objek ketika objek dialihkan ke kelas penyimpanan tertentu	Bilangan Bulat	1 untuk 36500	Tidak ada nilai default
targetExpirationDays	Jumlah hari setelah pembuatan objek saat objek dihapus	Bilangan Bulat	1 untuk 36500	Tidak ada nilai default
targetTransitionStorageClasses	Jenis kelas penyimpanan S3 tujuan	Enum	STANDARD_IA, INTELLIGENT_TIERING, ONEZONE_IA, GLACIER, GLACIER_IR, DEEP_ARCHIVE	Tidak ada nilai default

Kontrol ini memeriksa apakah bucket tujuan umum Amazon S3 memiliki konfigurasi Siklus Hidup. Kontrol gagal jika bucket tidak memiliki konfigurasi Siklus Hidup. Jika Anda memberikan nilai kustom

untuk satu atau beberapa parameter sebelumnya, kontrol hanya akan diteruskan jika kebijakan menyertakan kelas penyimpanan, waktu penghapusan, atau waktu transisi yang ditentukan.

Membuat konfigurasi Siklus Hidup untuk bucket S3 menentukan tindakan yang ingin dilakukan Amazon S3 selama masa pakai objek. Misalnya, Anda dapat mentransisikan objek ke kelas penyimpanan lain, mengarsipkannya, atau menghapusnya setelah jangka waktu tertentu.

Remediasi

Untuk informasi tentang mengonfigurasi kebijakan siklus hidup di bucket Amazon S3, lihat [Menyetel konfigurasi siklus hidup di bucket dan lihat Mengelola siklus hidup penyimpanan di](#) Panduan Pengguna Amazon S3.

[S3.14] Bucket tujuan umum S3 harus mengaktifkan versi

Kategori: Lindungi > Perlindungan data > Perlindungan penghapusan data

Persyaratan terkait: NIST.800-53.r5 AU-9(2), NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6, NIST.800-53.r5 CP-6(1), NIST.800-53.r5 CP-6(2), NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5 (2), Nist.800-53.R5 SI-12, NIST.800-53.R5 SI-13 (5), Nist.800-171.R2 3.3.8

Tingkat keparahan: Rendah

Jenis sumber daya: AWS : : S3 : : Bucket

AWS Config aturan: [s3-bucket-versioning-enabled](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah bucket tujuan umum Amazon S3 mengaktifkan versi. Kontrol gagal jika pembuatan versi ditangguhkan untuk bucket.

Pembuatan versi menyimpan beberapa varian objek dalam bucket S3 yang sama. Anda dapat menggunakan pembuatan versi untuk mempertahankan, mengambil, dan memulihkan versi sebelumnya dari objek yang disimpan di bucket S3 Anda. Pembuatan versi membantu Anda pulih dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

Tip

Karena jumlah objek bertambah dalam bucket karena pembuatan versi, Anda dapat mengatur konfigurasi Siklus Hidup untuk mengarsipkan atau menghapus objek berversi

secara otomatis berdasarkan aturan. Untuk informasi selengkapnya, lihat [Manajemen Siklus Hidup Amazon S3](#) untuk Objek Berversi.

Remediasi

Untuk menggunakan pembuatan versi pada bucket S3, lihat [Mengaktifkan pembuatan versi pada bucket di Panduan Pengguna](#) Amazon S3.

[S3.15] Bucket tujuan umum S3 harus mengaktifkan Object Lock

Kategori: Lindungi > Perlindungan data > Perlindungan penghapusan data

Persyaratan terkait: Nist.800-53.r5 CP-6 (2), PCI DSS v4.0.1/10.5.1

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::S3::Bucket

AWS Config aturan: [s3-bucket-default-lock-enabled](#)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
mode	Mode retensi Kunci Objek S3	Enum	GOVERNANCE , COMPLIANCE	Tidak ada nilai default

Kontrol ini memeriksa apakah bucket tujuan umum Amazon S3 mengaktifkan Object Lock. Kontrol gagal jika Object Lock tidak diaktifkan untuk bucket. Jika Anda memberikan nilai kustom untuk mode parameter, kontrol hanya akan diteruskan jika S3 Object Lock menggunakan mode retensi yang ditentukan.

Anda dapat menggunakan S3 Object Lock untuk menyimpan objek menggunakan model write-once-read-many (WORM). Object Lock dapat membantu mencegah objek di bucket S3 dihapus atau ditimpa untuk jangka waktu tertentu atau tanpa batas waktu. Anda dapat menggunakan S3 Object Lock untuk memenuhi persyaratan peraturan yang memerlukan penyimpanan WORM, atau menambahkan lapisan perlindungan tambahan terhadap perubahan dan penghapusan objek.

Remediasi

Untuk mengonfigurasi Object Lock untuk bucket S3 baru dan yang sudah ada, lihat [Mengonfigurasi Kunci Objek S3 di Panduan Pengguna](#) Amazon S3.

[S3.17] Ember tujuan umum S3 harus dienkripsi saat istirahat AWS KMS keys

Kategori: Lindungi > Perlindungan Data > Enkripsi data-at-rest

Persyaratan terkait: NIST.800-53.r5 SC-1 2 (2), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-1 3, 8, NIST.800-53.r5 SC-2 8 (1), (10), (1), Nist.800-53.r5 SI-7 NIST.800-53.r5 SC-7 (6), Nist.800-53.r5 NIST.800-53.r5 SC-2 AU-9, Nist.800-171.r2 3.8.9, Nist.800-171.r2 3.13.11, Nist.800-171.r2 3.13.16, PCI DCI SS v4.0.1/3.5.1 NIST.800-53.r5 CA-9

Tingkat keparahan: Sedang

Jenis sumber daya: AWS : : S3 : : Bucket

AWS Config aturan: [s3-default-encryption-kms](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah bucket tujuan umum Amazon S3 dienkripsi dengan (SSE-KMS atau AWS KMS key DSSE-KMS). Kontrol gagal jika bucket dienkripsi dengan enkripsi default (SSE-S3).

Server-side encryption (SSE) adalah enkripsi data di tujuannya oleh aplikasi atau layanan yang menerimanya. Kecuali Anda menentukan sebaliknya, bucket S3 menggunakan kunci terkelola Amazon S3 (SSE-S3) secara default untuk enkripsi sisi server. Namun, untuk kontrol tambahan, Anda dapat memilih untuk mengonfigurasi bucket untuk menggunakan enkripsi sisi server dengan AWS KMS keys (SSE-KMS atau DSSE-KMS) sebagai gantinya. Amazon S3 mengenkripsi data Anda pada tingkat objek saat menulisnya ke disk di pusat AWS data dan mendekripsi untuk Anda saat Anda mengaksesnya.

Remediasi

Untuk mengenkripsi bucket S3 menggunakan SSE-KMS, lihat [Menentukan enkripsi sisi server dengan \(SSE-KMS\) di Panduan Pengguna Amazon AWS KMS S3](#). Untuk mengenkripsi bucket S3 menggunakan DSSE-KMS, lihat [Menentukan enkripsi sisi server dua lapis dengan \(AWS KMS keys DSSE-KMS\)](#) di Panduan Pengguna Amazon S3.

[S3.19] Titik akses S3 harus mengaktifkan pengaturan akses publik blok

Persyaratan terkait: NIST.800-53.r5 AC-2 1, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21),, NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (9), PCI DSS v4.0.1/1.4.4

Kategori: Lindungi > Manajemen akses aman > Sumber daya tidak dapat diakses publik

Tingkat keparahan: Kritis

Jenis sumber daya: AWS::S3::AccessPoint

AWS Config aturan: [s3-access-point-public-access-blocks](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah titik akses Amazon S3 telah mengaktifkan pengaturan akses publik blok. Kontrol gagal jika blokir pengaturan akses publik tidak diaktifkan untuk titik akses.

Fitur Akses Publik Blok Amazon S3 membantu Anda mengelola akses ke sumber daya S3 di tiga tingkatan: tingkat akun, bucket, dan titik akses. Pengaturan di setiap level dapat dikonfigurasi secara independen, memungkinkan Anda memiliki tingkat pembatasan akses publik yang berbeda untuk data Anda. Pengaturan titik akses tidak dapat secara individual mengganti pengaturan yang lebih ketat di tingkat yang lebih tinggi (tingkat akun atau bucket yang ditetapkan ke titik akses). Sebaliknya, pengaturan pada tingkat titik akses bersifat aditif, yang berarti mereka melengkapi dan bekerja bersama pengaturan di tingkat lain. Kecuali jika Anda bermaksud jalur akses S3 dapat diakses publik, Anda harus mengaktifkan blokir pengaturan akses publik.

Remediasi

Saat ini, Amazon S3 tidak mendukung perubahan pengaturan akses publik blokir titik akses setelah titik akses dibuat. Semua pengaturan akses publik blok diaktifkan secara default saat Anda membuat titik akses baru. Kami menyarankan Anda tetap mengaktifkan semua pengaturan kecuali Anda tahu bahwa Anda memiliki kebutuhan khusus untuk menonaktifkan salah satu pengaturan tersebut. Untuk informasi selengkapnya, lihat [Mengelola akses publik ke titik akses](#) di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

[S3.20] Bucket tujuan umum S3 harus mengaktifkan penghapusan MFA

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v3.0.0/2.1.2, Tolok Ukur AWS Yayasan CIS v1.4.0/2.1.3, (1), (2) NIST.800-53.r5 CA-9 NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2(2), NIST.800-53.r5 CM-3, NIST.800-53.r5 SC-5

Kategori: Lindungi > Perlindungan data > Perlindungan penghapusan data

Tingkat keparahan: Rendah

Jenis sumber daya: AWS::S3::Bucket

AWS Config aturan: [s3-bucket-mfa-delete-enabled](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah penghapusan autentikasi multi-faktor (MFA) diaktifkan untuk bucket tujuan umum Amazon S3. Kontrol gagal jika penghapusan MFA tidak diaktifkan untuk bucket. Kontrol tidak menghasilkan temuan untuk bucket yang memiliki konfigurasi siklus hidup.

Jika Anda mengaktifkan pembuatan versi untuk bucket tujuan umum S3, Anda dapat menambahkan lapisan keamanan lain secara opsional dengan mengonfigurasi penghapusan MFA untuk bucket. Jika Anda melakukan ini, pemilik bucket harus menyertakan dua bentuk otentikasi dalam permintaan apa pun untuk menghapus versi objek di bucket atau mengubah status pembuatan versi bucket. MFA delete memberikan keamanan tambahan jika, misalnya, kredensi keamanan pemilik bucket dikompromikan. Penghapusan MFA juga dapat membantu mencegah penghapusan bucket yang tidak disengaja dengan mengharuskan pengguna yang memulai tindakan penghapusan untuk membuktikan kepemilikan fisik perangkat MFA dengan kode MFA, yang menambahkan lapisan gesekan dan keamanan ekstra pada tindakan penghapusan.

 Note

Kontrol ini menghasilkan PASSED temuan hanya jika penghapusan MFA diaktifkan untuk bucket tujuan umum S3. Untuk mengaktifkan penghapusan MFA untuk bucket, pembuatan versi juga harus diaktifkan untuk bucket. Bucket versioning adalah metode menyimpan beberapa variasi objek S3 dalam bucket yang sama. Selain itu, hanya pemilik bucket yang masuk sebagai pengguna root yang dapat mengaktifkan penghapusan MFA dan melakukan tindakan penghapusan pada bucket. Anda tidak dapat menggunakan penghapusan MFA dengan bucket yang memiliki konfigurasi siklus hidup.

Remediasi

Untuk informasi tentang mengaktifkan versi dan mengonfigurasi penghapusan MFA untuk bucket S3, lihat Mengonfigurasi penghapusan [MFA di Panduan Pengguna](#) Layanan Penyimpanan Sederhana Amazon.

[S3.22] Bucket tujuan umum S3 harus mencatat peristiwa penulisan tingkat objek

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v3.0.0/3.8, PCI DSS v4.0.1/10.2.1

Kategori: Identifikasi > Logging

Tingkat keparahan: Sedang

Jenis sumber daya: AWS :: : Account

AWS Config aturan: [cloudtrail-all-write-s3-data-event-check](#)

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah Akun AWS memiliki setidaknya satu jejak AWS CloudTrail Multi-wilayah yang mencatat semua peristiwa data tulis untuk bucket Amazon S3. Kontrol gagal jika akun tidak memiliki jejak Multi-wilayah yang mencatat peristiwa data tulis untuk bucket S3.

Operasi tingkat objek S3, seperti, `GetObject`, dan `DeleteObjectPutObject`, disebut peristiwa data. Secara default, CloudTrail tidak mencatat peristiwa data, tetapi Anda dapat mengonfigurasi jejak untuk mencatat peristiwa data untuk bucket S3. Saat mengaktifkan pencatatan tingkat objek

untuk peristiwa data tulis, Anda dapat mencatat setiap akses objek (file) individual dalam bucket S3. Mengaktifkan pencatatan tingkat objek dapat membantu Anda memenuhi persyaratan kepatuhan data, melakukan analisis keamanan komprehensif, memantau pola perilaku pengguna tertentu dalam diri Anda Akun AWS, dan mengambil tindakan pada aktivitas API tingkat objek dalam bucket S3 Anda dengan menggunakan Amazon Events. CloudWatch Kontrol ini menghasilkan PASSED temuan jika Anda mengonfigurasi jejak Multi-wilayah yang mencatat hanya penulisan atau semua jenis peristiwa data untuk semua bucket S3.

Remediasi

Untuk mengaktifkan pencatatan tingkat objek untuk bucket S3, lihat [Mengaktifkan pencatatan CloudTrail peristiwa untuk bucket dan objek S3](#) di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

[S3.23] Bucket tujuan umum S3 harus mencatat peristiwa pembacaan tingkat objek

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v3.0.0/3.9, PCI DSS v4.0.1/10.2.1

Kategori: Identifikasi > Logging

Tingkat keparahan: Sedang

Jenis sumber daya: AWS :: : Account

AWS Config aturan: [cloudtrail-all-read-s3-data-event-check](#)

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah an Akun AWS memiliki setidaknya satu jejak AWS CloudTrail Multi-wilayah yang mencatat semua peristiwa data baca untuk bucket Amazon S3. Kontrol gagal jika akun tidak memiliki jejak Multi-wilayah yang mencatat peristiwa data baca untuk bucket S3.

Operasi tingkat objek S3, seperti, `GetObject`, dan `DeleteObjectPutObject`, disebut peristiwa data. Secara default, CloudTrail tidak mencatat peristiwa data, tetapi Anda dapat mengonfigurasi jejak untuk mencatat peristiwa data untuk bucket S3. Saat mengaktifkan pencatatan tingkat objek untuk peristiwa data baca, Anda dapat mencatat setiap akses objek (file) individual dalam bucket S3. Mengaktifkan pencatatan tingkat objek dapat membantu Anda memenuhi persyaratan kepatuhan data, melakukan analisis keamanan komprehensif, memantau pola perilaku pengguna tertentu dalam

diri Anda Akun AWS, dan mengambil tindakan pada aktivitas API tingkat objek dalam bucket S3 Anda dengan menggunakan Amazon Events. CloudWatch Kontrol ini menghasilkan PASSED temuan jika Anda mengonfigurasi jejak Multi-wilayah yang mencatat read-only atau semua jenis peristiwa data untuk semua bucket S3.

Remediasi

Untuk mengaktifkan pencatatan tingkat objek untuk bucket S3, lihat [Mengaktifkan pencatatan CloudTrail peristiwa untuk bucket dan objek S3](#) di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

[S3.24] Poin Akses Multi-Wilayah S3 harus mengaktifkan pengaturan akses publik blok

Persyaratan terkait: PCI DSS v4.0.1/1.4.4

Kategori: Lindungi > Konfigurasi jaringan aman > Sumber daya tidak dapat diakses publik

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::S3::MultiRegionAccessPoint`

AWS Config aturan: `s3-mrap-public-access-blocked` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah Titik Akses Multi-Wilayah Amazon S3 telah mengaktifkan pengaturan akses publik blokir. Kontrol gagal ketika Titik Akses Multi-Wilayah tidak mengaktifkan pengaturan akses publik blok.

Sumber daya yang dapat diakses publik dapat menyebabkan akses yang tidak sah, pelanggaran data, atau eksploitasi kerentanan. Membatasi akses melalui tindakan otentikasi dan otorisasi membantu melindungi informasi sensitif dan menjaga integritas sumber daya Anda.

Remediasi

Secara default, semua pengaturan Blokir Akses Publik diaktifkan untuk Titik Akses Multi-Wilayah S3. Untuk informasi selengkapnya, lihat [Memblokir akses publik dengan Titik Akses Multi-Wilayah Amazon S3](#) di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon. Anda tidak dapat mengubah pengaturan Blokir Akses Publik untuk Titik Akses Multi-Wilayah setelah dibuat.

Kontrol Security Hub untuk SageMaker AI

AWS Security Hub Kontrol ini mengevaluasi layanan dan sumber daya Amazon SageMaker AI. Kontrol mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat [Ketersediaan kontrol berdasarkan Wilayah](#).

[SageMaker.1] Instans SageMaker notebook Amazon seharusnya tidak memiliki akses internet langsung

Persyaratan terkait: NIST.800-53.r5 AC-2 1,, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-3,, (21),, NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (11), (16) NIST.800-53.r5 AC-6, (20) NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), (4), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SC-7 PCI DSS v3.2.1/1.2.1, NIST.800-53.r5 SC-7 PCI DSS v3.2.1/1.3.1, PCI DSS v3.2.1/1.3.2, PCI DSS v3.2.1/1.3.4, PCI DSS v3.2.1/1.3.6, PCI DSS v4.0.1/1.4.4 NIST.800-53.r5 SC-7

Kategori: Lindungi > Konfigurasi jaringan aman

Tingkat keparahan: Tinggi

Jenis sumber daya: AWS::SageMaker::NotebookInstance

AWS Config aturan: [sagemaker-notebook-no-direct-internet-access](#)

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah akses internet langsung dinonaktifkan untuk instance notebook SageMaker AI. Kontrol gagal jika DirectInternetAccess bidang diaktifkan untuk instance notebook.

Jika Anda mengonfigurasi instans SageMaker AI tanpa VPC, maka secara default akses internet langsung diaktifkan pada instans Anda. Anda harus mengonfigurasi instans Anda dengan VPC dan mengubah pengaturan default menjadi Nonaktifkan — Akses internet melalui VPC. Untuk melatih atau meng-host model dari notebook, Anda memerlukan akses internet. Untuk mengaktifkan akses internet, VPC Anda harus memiliki antarmuka endpoint (AWS PrivateLink) atau gateway NAT dan grup keamanan yang memungkinkan koneksi keluar. Untuk mempelajari lebih lanjut tentang cara menghubungkan instans notebook ke sumber daya di VPC, lihat [Menyambungkan instans notebook ke sumber daya di VPC di](#) Panduan Pengembang Amazon SageMaker AI. Anda juga harus memastikan bahwa akses ke konfigurasi SageMaker AI Anda terbatas hanya untuk pengguna

yang berwenang. Batasi izin IAM yang memungkinkan pengguna mengubah pengaturan dan sumber daya SageMaker AI.

Remediasi

Anda tidak dapat mengubah setelan akses internet setelah membuat instance notebook. Sebagai gantinya, Anda dapat menghentikan, menghapus, dan membuat ulang instance dengan akses internet yang diblokir. Untuk menghapus instance notebook yang mengizinkan akses internet langsung, lihat [Menggunakan instance notebook untuk membuat model: Bersihkan di Panduan Pengembang Amazon SageMaker AI](#). Untuk membuat ulang instance notebook yang menolak akses internet, lihat [Membuat instance notebook](#). Untuk Jaringan, akses internet langsung, pilih Nonaktifkan — Akses internet melalui VPC.

[SageMaker.2] instance SageMaker notebook harus diluncurkan dalam VPC khusus

Persyaratan terkait: NIST.800-53.r5 AC-2 1 NIST.800-53.r5 AC-3,, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-4,, NIST.800-53.r5 AC-4 (21) NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7,, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9)

Kategori: Lindungi > Konfigurasi jaringan aman> Sumber daya dalam VPC

Tingkat keparahan: Tinggi

Jenis sumber daya: AWS::SageMaker::NotebookInstance

AWS Config aturan: [sagemaker-notebook-instance-inside-vpc](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah instans notebook Amazon SageMaker AI diluncurkan dalam cloud pribadi virtual kustom (VPC). Kontrol ini gagal jika instance notebook SageMaker AI tidak diluncurkan dalam VPC khusus atau jika diluncurkan di VPC layanan SageMaker AI.

Subnet adalah berbagai alamat IP dalam VPC. Sebaiknya simpan sumber daya Anda di dalam VPC kustom bila memungkinkan untuk memastikan perlindungan jaringan yang aman dari infrastruktur Anda. VPC Amazon adalah jaringan virtual yang didedikasikan untuk Anda. Akun AWS Dengan Amazon VPC, Anda dapat mengontrol akses jaringan dan konektivitas internet SageMaker AI Studio dan instance notebook Anda.

Remediasi

Anda tidak dapat mengubah pengaturan VPC setelah membuat instance notebook. Sebagai gantinya, Anda dapat menghentikan, menghapus, dan membuat ulang instance. Untuk petunjuknya, lihat [Menggunakan instance notebook untuk membuat model: Bersihkan](#) di Panduan Pengembang Amazon SageMaker AI.

[SageMaker.3] Pengguna seharusnya tidak memiliki akses root ke instance SageMaker notebook

Persyaratan terkait: NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-6, NIST.800-53.r5 AC-6 (10), NIST.800-53.r5 AC-6 (2)

Kategori: Lindungi > Manajemen akses aman > Pembatasan akses pengguna root

Tingkat keparahan: Tinggi

Jenis sumber daya: AWS::SageMaker::NotebookInstance

AWS Config aturan: [sagemaker-notebook-instance-root-access-check](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah akses root diaktifkan untuk instance notebook Amazon SageMaker AI. Kontrol gagal jika akses root diaktifkan untuk instance notebook SageMaker AI.

Sesuai dengan prinsip hak istimewa terkecil, ini adalah praktik terbaik keamanan yang disarankan untuk membatasi akses root ke sumber daya instans untuk menghindari izin penyediaan secara tidak sengaja.

Remediasi

Untuk membatasi akses root ke instance notebook SageMaker AI, lihat [Kontrol akses root ke instans notebook SageMaker AI di Panduan](#) Pengembang Amazon SageMaker AI.

[SageMaker.4] varian produksi SageMaker titik akhir harus memiliki jumlah instance awal yang lebih besar dari 1

Persyaratan terkait: NIST.800-53.r5 CP-10, NIST.800-53.r5 SC-5, NIST.800-53.r5 SC-3 6, NIST.800-53.r5 SA-1 3

Kategori: Pulihkan > Ketahanan > Ketersediaan tinggi

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::SageMaker::EndpointConfig`

AWS Config aturan: [sagemaker-endpoint-config-prod-instance-count](#)

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah varian produksi titik akhir Amazon SageMaker AI memiliki jumlah instans awal lebih besar dari 1. Kontrol gagal jika varian produksi titik akhir hanya memiliki 1 instance awal.

Varian produksi yang berjalan dengan jumlah instans lebih dari 1 memungkinkan redundansi instans multi-AZ yang dikelola oleh AI. SageMaker Menyebarkan sumber daya di beberapa Availability Zone adalah praktik AWS terbaik untuk menyediakan ketersediaan tinggi dalam arsitektur Anda. Ketersediaan tinggi membantu Anda pulih dari insiden keamanan.

 Note

Kontrol ini hanya berlaku untuk konfigurasi endpoint berbasis instance.

Remediasi

Untuk informasi selengkapnya tentang parameter konfigurasi titik akhir, lihat [Membuat konfigurasi titik akhir di Panduan](#) Pengembang Amazon SageMaker AI.

[SageMaker.5] SageMaker model harus memblokir lalu lintas masuk

Kategori: Lindungi > Konfigurasi jaringan aman > Sumber daya tidak dapat diakses publik

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::SageMaker::Model`

AWS Config aturan: [sagemaker-model-isolation-enabled](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah model yang dihosting Amazon SageMaker AI memblokir lalu lintas jaringan masuk. Kontrol gagal jika `EnableNetworkIsolation` parameter untuk model yang dihosting disetel ke `False`.

SageMaker Pelatihan AI dan wadah inferensi yang diterapkan diaktifkan internet secara default. Jika Anda tidak ingin SageMaker AI menyediakan akses jaringan eksternal ke wadah pelatihan atau inferensi, Anda dapat mengaktifkan isolasi jaringan. Jika Anda mengaktifkan isolasi jaringan, kontainer tidak dapat melakukan panggilan jaringan keluar, bahkan ke yang lain Layanan AWS. Selain itu, tidak ada AWS kredensial yang tersedia untuk lingkungan runtime container. Mengaktifkan isolasi jaringan membantu mencegah akses yang tidak diinginkan ke sumber daya SageMaker AI Anda dari internet.

Remediasi

Untuk informasi selengkapnya tentang isolasi jaringan untuk model SageMaker AI, lihat [Menjalankan pelatihan dan wadah inferensi dalam mode bebas internet di Panduan](#) Pengembang Amazon SageMaker AI. Anda dapat mengaktifkan isolasi jaringan saat membuat pekerjaan atau model pelatihan dengan menyetel nilai `EnableNetworkIsolation` parameter `True`.

[SageMaker.6] konfigurasi gambar SageMaker aplikasi harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::SageMaker::AppImageConfig`

AWS Config aturan: [sagemaker-app-image-config-tagged](#)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
<code>requiredKeyTags</code>	Daftar kunci tag non-sistem yang harus ditetapkan ke sumber daya yang dievaluasi	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi	Tidak ada nilai default

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
	i. Kunci tag peka huruf besar dan kecil.		persyaratan AWS .	

Kontrol ini memeriksa apakah konfigurasi gambar aplikasi Amazon SageMaker AI (AppImageConfig) memiliki kunci tag yang ditentukan oleh `requiredKeyTags` parameter. Kontrol gagal jika konfigurasi gambar aplikasi tidak memiliki kunci tag, atau tidak memiliki semua kunci yang ditentukan oleh `requiredKeyTags` parameter. Jika Anda tidak menentukan nilai apa pun untuk `requiredKeyTags` parameter, kontrol hanya akan memeriksa keberadaan kunci tag dan gagal jika konfigurasi gambar aplikasi tidak memiliki kunci tag. Kontrol mengabaikan tag sistem, yang diterapkan secara otomatis dan memiliki `aws :` awalan.

Tag adalah label yang Anda buat dan tetapkan ke AWS sumber daya. Setiap tanda terdiri dari kunci tanda yang diperlukan dan nilai tanda opsional. Anda dapat menggunakan tag untuk mengkategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Mereka dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Mereka juga dapat membantu Anda melacak pemilik sumber daya untuk tindakan dan pemberitahuan. Anda juga dapat menggunakan tag untuk menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi. Untuk informasi selengkapnya tentang strategi ABAC, lihat [Menentukan izin berdasarkan atribut dengan otorisasi ABAC](#) di Panduan Pengguna IAM. Untuk informasi selengkapnya tentang tag, lihat [Panduan Pengguna AWS Sumber Daya Penandaan dan Editor Tag](#).

Note

Jangan menyimpan informasi pengenalan pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses dari banyak orang Layanan AWS. Mereka tidak dimaksudkan untuk digunakan untuk data pribadi atau sensitif.

Remediasi

Untuk menambahkan tag ke konfigurasi gambar aplikasi Amazon SageMaker AI (AppImageConfig), Anda dapat menggunakan [AddTags](#) pengoperasian SageMaker AI API atau, jika Anda menggunakan AWS CLI, jalankan perintah [add-tag](#).

[SageMaker.7] SageMaker gambar harus diberi tag

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: AWS :: SageMaker :: Image

AWS Config aturan: [sagemaker-image-tagged](#)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
<code>requiredKeyTags</code>	Daftar kunci tag non-sistem yang harus ditetapkan ke sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS .	Tidak ada nilai default

Kontrol ini memeriksa apakah gambar Amazon SageMaker AI memiliki kunci tag yang ditentukan oleh `requiredKeyTags` parameter. Kontrol gagal jika gambar tidak memiliki kunci tag, atau tidak memiliki semua kunci yang ditentukan oleh `requiredKeyTags` parameter. Jika Anda tidak menentukan nilai apa pun untuk `requiredKeyTags` parameter, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika gambar tidak memiliki kunci tag. Kontrol mengabaikan tag sistem, yang diterapkan secara otomatis dan memiliki `aws :` awalan.

Tag adalah label yang Anda buat dan tetapkan ke AWS sumber daya. Setiap tanda terdiri dari kunci tanda yang diperlukan dan nilai tanda opsional. Anda dapat menggunakan tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Mereka dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Mereka juga dapat membantu Anda melacak pemilik sumber daya untuk tindakan dan pemberitahuan. Anda juga dapat menggunakan tag untuk menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi. Untuk informasi selengkapnya tentang strategi ABAC, lihat [Menentukan izin berdasarkan](#)

[atribut dengan otorisasi ABAC](#) di Panduan Pengguna IAM. Untuk informasi selengkapnya tentang tag, lihat [Panduan Pengguna AWS Sumber Daya Penandaan dan Editor Tag](#).

 Note

Jangan menyimpan informasi pengenalan pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses dari banyak orang Layanan AWS. Mereka tidak dimaksudkan untuk digunakan untuk data pribadi atau sensitif.

Remediasi

Untuk menambahkan tag ke image Amazon SageMaker AI, Anda dapat menggunakan [AddTags](#) pengoperasian SageMaker AI API atau, jika Anda menggunakan AWS CLI, jalankan perintah [add-tag](#).

[SageMaker.8] instance SageMaker notebook harus berjalan pada platform yang didukung

Kategori: Deteksi > Kerentanan, tambalan, dan manajemen versi

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::SageMaker::NotebookInstance

AWS Config aturan: [sagemaker-notebook-instance-platform-version](#)

Jenis jadwal: Periodik

Parameter:

- supportedPlatformIdentifierVersions: notebook-al2-v1, notebook-al2-v2, notebook-al2-v3 (tidak dapat disesuaikan)

Kontrol ini memeriksa apakah instance notebook Amazon SageMaker AI dikonfigurasi untuk berjalan pada platform yang didukung, berdasarkan pengenalan platform yang ditentukan untuk instance notebook. Kontrol gagal jika instance notebook dikonfigurasi untuk berjalan pada platform yang tidak lagi didukung.

Jika platform untuk instans notebook Amazon SageMaker AI tidak lagi didukung, platform tersebut mungkin tidak menerima patch keamanan, perbaikan bug, atau jenis pembaruan lainnya.

Instans notebook mungkin terus berfungsi, tetapi mereka tidak akan menerima pembaruan keamanan SageMaker AI atau perbaikan bug penting. Anda menanggung risiko yang terkait dengan penggunaan platform yang tidak didukung. Untuk informasi selengkapnya, lihat [JupyterLab pembuatan versi](#) di Panduan Pengembang Amazon SageMaker AI.

Remediasi

Untuk informasi tentang platform yang didukung Amazon SageMaker AI saat ini dan cara bermigrasi ke platform tersebut, lihat [Instans notebook Amazon Linux 2 di Panduan](#) Pengembang Amazon SageMaker AI.

Kontrol Security Hub untuk Secrets Manager

AWS Security Hub Kontrol ini mengevaluasi AWS Secrets Manager layanan dan sumber daya.

Kontrol ini mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat [Ketersediaan kontrol berdasarkan Wilayah](#).

[SecretsManager.1] Rahasia Secrets Manager harus mengaktifkan rotasi otomatis

Persyaratan terkait: NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3 (15), PCI DSS v4.0.1/8.6.3, PCI DSS v4.0.1/8.3.9

Kategori: Lindungi > Pengembangan aman

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::SecretsManager::Secret

AWS Config aturan: [secretsmanager-rotation-enabled-check](#)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
maximumAllowedRotation	Jumlah hari maksimum yang diizinkan untuk frekuensi rotasi rahasia	Bilangan Bulat	1 untuk 365	Tidak ada nilai default

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub

tionFrequency

Kontrol ini memeriksa apakah rahasia yang disimpan AWS Secrets Manager dikonfigurasi dengan rotasi otomatis. Kontrol gagal jika rahasia tidak dikonfigurasi dengan rotasi otomatis. Jika Anda memberikan nilai khusus untuk `maximumAllowedRotationFrequency` parameter, kontrol hanya akan berlalu jika rahasia diputar secara otomatis dalam jendela waktu yang ditentukan.

Secrets Manager membantu Anda meningkatkan postur keamanan organisasi Anda. Rahasia mencakup kredensi basis data, kata sandi, dan kunci API pihak ketiga. Anda dapat menggunakan Secrets Manager untuk menyimpan rahasia secara terpusat, mengenkripsi rahasia secara otomatis, mengontrol akses ke rahasia, dan memutar rahasia dengan aman dan otomatis.

Secrets Manager dapat memutar rahasia. Anda dapat menggunakan rotasi untuk mengganti rahasia jangka panjang dengan rahasia jangka pendek. Memutar rahasia Anda membatasi berapa lama pengguna yang tidak sah dapat menggunakan rahasia yang disusupi. Untuk alasan ini, Anda harus sering memutar rahasia Anda. Untuk mempelajari lebih lanjut tentang rotasi, lihat [Memutar AWS Secrets Manager rahasia Anda](#) di Panduan AWS Secrets Manager Pengguna.

Remediasi

Untuk mengaktifkan rotasi otomatis rahasia Secrets Manager, lihat [Mengatur rotasi otomatis untuk AWS Secrets Manager rahasia menggunakan konsol](#) di Panduan AWS Secrets Manager Pengguna. Anda harus memilih dan mengkonfigurasi AWS Lambda fungsi untuk rotasi.

[SecretsManager.2] Rahasia Secrets Manager yang dikonfigurasi dengan rotasi otomatis harus berhasil diputar

Persyaratan terkait: NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3 (15), PCI DSS v4.0.1/8.6.3, PCI DSS v4.0.1/8.3.9

Kategori: Lindungi > Pengembangan aman

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::SecretsManager::Secret`

AWS Config aturan: [secretsmanager-scheduled-rotation-success-check](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah AWS Secrets Manager rahasia berhasil diputar berdasarkan jadwal rotasi. Kontrol gagal jika `RotationOccurringAsScheduled` adalah `false`. Kontrol hanya mengevaluasi rahasia yang telah dihidupkan rotasi.

Secrets Manager membantu Anda meningkatkan postur keamanan organisasi Anda. Rahasia mencakup kredensi basis data, kata sandi, dan kunci API pihak ketiga. Anda dapat menggunakan Secrets Manager untuk menyimpan rahasia secara terpusat, mengenkripsi rahasia secara otomatis, mengontrol akses ke rahasia, dan memutar rahasia dengan aman dan otomatis.

Secrets Manager dapat memutar rahasia. Anda dapat menggunakan rotasi untuk mengganti rahasia jangka panjang dengan rahasia jangka pendek. Memutar rahasia Anda membatasi berapa lama pengguna yang tidak sah dapat menggunakan rahasia yang disusupi. Untuk alasan ini, Anda harus sering memutar rahasia Anda.

Selain mengonfigurasi rahasia untuk diputar secara otomatis, Anda harus memastikan bahwa rahasia tersebut berhasil diputar berdasarkan jadwal rotasi.

Untuk mempelajari lebih lanjut tentang rotasi, lihat [Memutar AWS Secrets Manager rahasia Anda](#) di Panduan AWS Secrets Manager Pengguna.

Remediasi

Jika rotasi otomatis gagal, maka Secrets Manager mungkin mengalami kesalahan dengan konfigurasi. Untuk memutar rahasia di Secrets Manager, Anda menggunakan fungsi Lambda yang mendefinisikan cara berinteraksi dengan database atau layanan yang memiliki rahasia.

Untuk bantuan mendiagnosis dan memperbaiki kesalahan umum yang terkait dengan rotasi rahasia, lihat [Memecahkan masalah AWS Secrets Manager rotasi rahasia di Panduan Pengguna](#). AWS Secrets Manager

[SecretsManager.3] Hapus rahasia Secrets Manager yang tidak digunakan

Persyaratan terkait: NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3 (15)

Kategori: Lindungi > Manajemen akses yang aman

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::SecretsManager::Secret`

AWS Config aturan: [secretsmanager-secret-unused](#)

Jenis jadwal: Periodik

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
<code>unusedForDays</code>	Jumlah hari maksimum yang rahasia dapat tetap tidak digunakan	Bilangan Bulat	1 untuk 365	90

Kontrol ini memeriksa apakah AWS Secrets Manager rahasia telah diakses dalam jangka waktu yang ditentukan. Kontrol gagal jika rahasia tidak digunakan di luar kerangka waktu yang ditentukan. Kecuali Anda memberikan nilai parameter khusus untuk periode akses, Security Hub menggunakan nilai default 90 hari.

Menghapus rahasia yang tidak digunakan sama pentingnya dengan memutar rahasia. Rahasia yang tidak digunakan dapat disalahgunakan oleh mantan pengguna mereka, yang tidak lagi membutuhkan akses ke rahasia ini. Selain itu, karena semakin banyak pengguna mendapatkan akses ke rahasia, seseorang mungkin salah menangani dan membocorkannya ke entitas yang tidak sah, yang meningkatkan risiko penyalahgunaan. Menghapus rahasia yang tidak digunakan membantu mencabut akses rahasia dari pengguna yang tidak lagi membutuhkannya. Ini juga membantu mengurangi biaya penggunaan Secrets Manager. Oleh karena itu, penting untuk secara rutin menghapus rahasia yang tidak digunakan.

Remediasi

Untuk menghapus rahasia Secrets Manager yang tidak aktif, lihat [Menghapus AWS Secrets Manager rahasia](#) di Panduan AWS Secrets Manager Pengguna.

[SecretsManager.4] Rahasia Secrets Manager harus diputar dalam jumlah hari tertentu

Persyaratan terkait: NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3 (15), PCI DSS v4.0.1/8.6.3, PCI DSS v4.0.1/8.3.9

Kategori: Lindungi > Manajemen akses yang aman

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::SecretsManager::Secret

AWS Config aturan: [secretsmanager-secret-periodic-rotation](#)

Jenis jadwal: Periodik

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
maxDaysSinceRotation	Jumlah hari maksimum yang rahasia dapat tetap tidak berubah	Bilangan Bulat	1 untuk 180	90

Kontrol ini memeriksa apakah sebuah AWS Secrets Manager rahasia diputar setidaknya sekali dalam jangka waktu yang ditentukan. Kontrol gagal jika rahasia tidak diputar setidaknya ini sering. Kecuali Anda memberikan nilai parameter khusus untuk periode rotasi, Security Hub menggunakan nilai default 90 hari.

Rahasia berputar dapat membantu Anda mengurangi risiko penggunaan rahasia Anda yang tidak sah dalam diri Anda. Akun AWS Contohnya termasuk kredensi basis data, kata sandi, kunci API pihak ketiga, dan bahkan teks arbitrer. Jika Anda tidak mengubah rahasia Anda untuk jangka waktu yang lama, rahasianya lebih mungkin dikompromikan.

Karena semakin banyak pengguna mendapatkan akses ke rahasia, kemungkinan besar seseorang salah menangani dan membocorkannya ke entitas yang tidak sah. Rahasia dapat bocor melalui log dan data cache. Mereka dapat dibagikan untuk tujuan debugging dan tidak diubah atau dicabut setelah debugging selesai. Untuk semua alasan ini, rahasia harus sering diputar.

Anda dapat mengonfigurasi rotasi otomatis untuk rahasia di AWS Secrets Manager. Dengan rotasi otomatis, Anda dapat mengganti rahasia jangka panjang dengan rahasia jangka pendek, secara signifikan mengurangi risiko kompromi. Kami menyarankan Anda mengonfigurasi rotasi otomatis untuk rahasia Secrets Manager Anda. Untuk informasi selengkapnya, lihat [Memutar rahasia AWS Secrets Manager Anda](#) di Panduan Pengguna AWS Secrets Manager .

Remediasi

Untuk mengaktifkan rotasi otomatis rahasia Secrets Manager, lihat [Mengatur rotasi otomatis untuk AWS Secrets Manager rahasia menggunakan konsol](#) di Panduan AWS Secrets Manager Pengguna. Anda harus memilih dan mengkonfigurasi AWS Lambda fungsi untuk rotasi.

[SecretsManager.5] Rahasia Secrets Manager harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::SecretsManager::Secret`

AWS Config aturan: `tagged-secretsmanager-secret` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
<code>requiredTagKeys</code>	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS .	No default value

Kontrol ini memeriksa apakah AWS Secrets Manager rahasia memiliki tag dengan kunci tertentu yang ditentukan dalam parameter `requiredTagKeys`. Kontrol gagal jika rahasia tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter `requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika rahasia tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengkategorikan sumber daya berdasarkan tujuan, pemilik,

lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat [Untuk apa ABAC? AWS](#) di Panduan Pengguna IAM.

Note

Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat [Menandai AWS sumber daya Anda](#) di Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke rahasia Secrets Manager, lihat [Menandai AWS Secrets Manager rahasia](#) di Panduan AWS Secrets Manager Pengguna.

Kontrol Security Hub untuk Service Catalog

AWS Security Hub Kontrol ini mengevaluasi AWS Service Catalog layanan dan sumber daya.

Kontrol ini mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat [Ketersediaan kontrol berdasarkan Wilayah](#).

[ServiceCatalog.1] Portofolio Service Catalog harus dibagikan hanya dalam suatu organisasi AWS

Persyaratan terkait: NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-6, NIST.800-53.r5 CM-8, NIST.800-53.r5 SC-7

Kategori: Lindungi > Manajemen akses yang aman

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::ServiceCatalog::Portfolio`

AWS Config aturan: [service-catalog-shared-within-organization](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah AWS Service Catalog berbagi portofolio dalam organisasi saat integrasi dengan AWS Organizations diaktifkan. Kontrol gagal jika portofolio tidak dibagikan dalam suatu organisasi.

Berbagi portofolio hanya dalam Organizations membantu memastikan bahwa portofolio tidak dibagikan dengan salah Akun AWS. Untuk membagikan portofolio Service Catalog dengan akun di organisasi, Security Hub merekomendasikan penggunaan `ORGANIZATION_MEMBER_ACCOUNT` sebagai gantinya `ACCOUNT`. Ini menyederhanakan administrasi dengan mengatur akses yang diberikan ke akun di seluruh organisasi. [Jika Anda memiliki kebutuhan bisnis untuk berbagi portofolio Service Catalog dengan akun eksternal, Anda dapat secara otomatis menekan temuan dari kontrol ini atau menonaktifkannya.](#)

Remediasi

Untuk mengaktifkan berbagi portofolio dengan Organizations, lihat [Berbagi dengan AWS Organizations](#) di Panduan Administrator Service Catalog

Kontrol Security Hub untuk Amazon SES

AWS Security Hub Kontrol ini mengevaluasi layanan dan sumber daya Amazon Simple Email Service (Amazon SES).

Kontrol ini mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat [Ketersediaan kontrol berdasarkan Wilayah](#).

[SES.1] Daftar kontak SES harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::SES::ContactList`

AWS Config aturan: `tagged-ses-contactlist` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
<code>requiredTagKeys</code>	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS.	Tidak ada nilai default

Kontrol ini memeriksa apakah daftar kontak Amazon SES memiliki tag dengan kunci tertentu yang ditentukan dalam parameter `requiredTagKeys`. Kontrol gagal jika daftar kontak tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter `requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika daftar kontak tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat [Untuk apa ABAC? AWS](#) di Panduan Pengguna IAM.

Note

Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS

Billing. Untuk praktik terbaik penandaan lainnya, lihat [Menandai AWS sumber daya Anda](#) di Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke daftar kontak Amazon SES, lihat [TagResource](#) di Referensi Amazon SES API v2.

[SES.2] Set konfigurasi SES harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: AWS::SES::ConfigurationSet

AWS Config aturan: tagged-ses-configurationset (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
<code>requiredTagKeys</code>	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS .	Tidak ada nilai default

Kontrol ini memeriksa apakah set konfigurasi Amazon SES memiliki tag dengan kunci spesifik yang ditentukan dalam parameter `requiredTagKeys`. Kontrol gagal jika set konfigurasi tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter `requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika set konfigurasi tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat [Untuk apa ABAC? AWS](#) di Panduan Pengguna IAM.

Note

Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat [Menandai AWS sumber daya Anda](#) di Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke set konfigurasi Amazon SES, lihat [TagResource](#) di Referensi Amazon SES API v2.

Kontrol Security Hub untuk Amazon SNS

AWS Security Hub Kontrol ini mengevaluasi layanan dan sumber daya Amazon Simple Notification Service (Amazon SNS). Kontrol mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat [Ketersediaan kontrol berdasarkan Wilayah](#).

[SNS.1] Topik SNS harus dienkripsi saat istirahat menggunakan AWS KMS

Persyaratan terkait: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-1 3, 8, NIST.800-53.r5 SC-2 8 (1), (10), Nist.800-53.r5 SI-7 NIST.800-53.r5 SC-7 (NIST.800-53.r5 SC-26), Nist.800-171.r2 3.13.11, Nist.800-171.r2 3.13.16

Kategori: Lindungi > Perlindungan Data > Enkripsi data-at-rest

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::SNS::Topic

AWS Config aturan: [sns-encrypted-kms](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah topik Amazon SNS dienkripsi saat istirahat menggunakan kunci yang dikelola di (). AWS Key Management Service AWS KMS Kontrol gagal jika topik SNS tidak menggunakan kunci KMS untuk enkripsi sisi server (SSE). Secara default, SNS menyimpan pesan dan file menggunakan enkripsi disk. Untuk melewati kontrol ini, Anda harus memilih untuk menggunakan kunci KMS untuk enkripsi sebagai gantinya. Ini menambahkan lapisan keamanan tambahan dan memberikan lebih banyak fleksibilitas kontrol akses.

Mengenkripsi data saat istirahat mengurangi risiko data yang disimpan pada disk diakses oleh pengguna yang tidak diautentikasi. AWS Izin API diperlukan untuk mendekripsi data sebelum dapat dibaca. Kami merekomendasikan mengenkripsi topik SNS dengan kunci KMS untuk lapisan keamanan tambahan.

Remediasi

Untuk mengaktifkan SSE untuk topik SNS, lihat [Mengaktifkan enkripsi sisi server \(SSE\) untuk topik Amazon SNS di Panduan Pengembang Layanan Pemberitahuan Sederhana Amazon](#). Sebelum Anda dapat menggunakan SSE, Anda juga harus mengonfigurasi AWS KMS key kebijakan untuk mengizinkan enkripsi topik dan enkripsi dan dekripsi pesan. Untuk informasi selengkapnya, lihat [Mengonfigurasi AWS KMS izin di Panduan](#) Pengembang Layanan Pemberitahuan Sederhana Amazon.

[SNS.2] Pencatatan status pengiriman harus diaktifkan untuk pesan notifikasi yang dikirim ke suatu topik

Important

Security Hub menghentikan kontrol ini pada April 2024. Untuk informasi selengkapnya, lihat [Ubah log untuk kontrol CSPM Security Hub](#).

Persyaratan terkait: Nist.800-53.r5 AU-12, Nist.800-53.r5 AU-2

Kategori: Identifikasi > Logging

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::SNS::Topic

AWS Config aturan: [sns-topic-message-delivery-notification-enabled](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah pencatatan diaktifkan untuk status pengiriman pesan notifikasi yang dikirim ke topik Amazon SNS untuk titik akhir. Kontrol ini gagal jika pemberitahuan status pengiriman pesan tidak diaktifkan.

Logging adalah bagian penting dalam menjaga keandalan, ketersediaan, dan kinerja layanan.

Mencatat status pengiriman pesan membantu memberikan wawasan operasional, seperti berikut ini:

- Mengetahui apakah pesan dikirim ke titik akhir Amazon SNS.
- Mengidentifikasi respon yang dikirim dari titik akhir Amazon SNS ke Amazon SNS.
- Menentukan waktu tinggal pesan (waktu antara stempel waktu publikasi dan penyerahan ke titik akhir Amazon SNS).

Remediasi

Untuk mengonfigurasi pencatatan status pengiriman untuk suatu topik, lihat [Status pengiriman pesan Amazon SNS di Panduan](#) Pengembang Layanan Pemberitahuan Sederhana Amazon.

[SNS.3] Topik SNS harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: AWS::SNS::Topic

AWS Config aturan: tagged-sns-topic (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
<code>requiredTagKeys</code>	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS.	No default value

Kontrol ini memeriksa apakah topik Amazon SNS memiliki tag dengan kunci tertentu yang ditentukan dalam parameter. `requiredTagKeys` Kontrol gagal jika topik tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter `requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika topik tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat [Untuk apa ABAC? AWS](#) di Panduan Pengguna IAM.

Note

Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS

Billing. Untuk praktik terbaik penandaan lainnya, lihat [Menandai AWS sumber daya Anda](#) di Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke topik SNS, lihat [Mengonfigurasi tag topik Amazon SNS](#) di Panduan Pengembang Layanan Pemberitahuan Sederhana Amazon.

[SNS.4] Kebijakan akses topik SNS seharusnya tidak mengizinkan akses publik

Kategori: Lindungi > Konfigurasi jaringan aman > Sumber daya tidak dapat diakses publik

Tingkat keparahan: Tinggi

Jenis sumber daya: AWS::SNS::Topic

AWS Config aturan: [sns-topic-no-public-access](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah kebijakan akses topik Amazon SNS memungkinkan akses publik. Kontrol ini gagal jika kebijakan akses topik SNS mengizinkan akses publik.

Anda menggunakan kebijakan akses Amazon SNS dengan topik tertentu untuk membatasi siapa yang dapat bekerja dengan topik tersebut (misalnya, siapa yang dapat mempublikasikan pesan ke topik tersebut atau siapa yang dapat berlangganan). Kebijakan SNS dapat memberikan akses ke orang lain Akun AWS, atau ke pengguna di dalam milik Akun AWS Anda. Menyediakan wildcard (*) di Principal bidang kebijakan topik dan kurangnya kondisi untuk membatasi kebijakan topik dapat mengakibatkan eksfiltrasi data, penolakan layanan, atau injeksi pesan yang tidak diinginkan ke layanan Anda oleh penyerang.

Note

Kontrol ini tidak mengevaluasi kondisi kebijakan yang menggunakan karakter atau variabel wildcard. Untuk menghasilkan PASSED temuan, kondisi dalam kebijakan akses Amazon SNS untuk suatu topik hanya boleh menggunakan nilai tetap, yaitu nilai yang tidak berisi karakter

wildcard atau variabel kebijakan. Untuk informasi tentang variabel kebijakan, lihat [Variabel dan tag](#) di Panduan AWS Identity and Access Management Pengguna.

Remediasi

Untuk memperbarui kebijakan akses untuk topik SNS, lihat [Ikhtisar mengelola akses di Amazon SNS di](#) Panduan Pengembang Layanan Pemberitahuan Sederhana Amazon.

Kontrol Security Hub untuk Amazon SQS

AWS Security Hub Kontrol ini mengevaluasi layanan dan sumber daya Amazon Simple Queue Service (Amazon SQS). Kontrol mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat [Ketersediaan kontrol berdasarkan Wilayah](#).

[SQS.1] Antrian Amazon SQS harus dienkrpsi saat istirahat

Persyaratan terkait: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-1 3, NIST.800-53.r5 SC-2 8, NIST.800-53.r5 SC-2 8 (1), NIST.800-53.r5 SC-7 (10), NIST.800-53.R5 SI-7 (6)

Kategori: Lindungi > Perlindungan Data > Enkripsi data-at-rest

Tingkat keparahan: Sedang

Jenis sumber daya: AWS : : SQS : : Queue

AWS Config aturan: sqs-queue-encrypted (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah antrian Amazon SQS dienkrpsi saat istirahat. Kontrol gagal jika antrian tidak dienkrpsi dengan kunci yang dikelola SQS (SSE-SQS) atau kunci () (SSE-KMS). AWS Key Management Service AWS KMS

Mengenkrpsi data saat istirahat mengurangi risiko pengguna yang tidak sah mengakses data yang disimpan di disk. Enkripsi sisi server (SSE) melindungi isi pesan dalam antrian SQS menggunakan kunci enkripsi yang dikelola SQS (SSE-SQS) atau kunci (SSE-KMS). AWS KMS

Remediasi

Untuk mengonfigurasi SSE untuk antrian SQS, lihat [Mengonfigurasi enkripsi sisi server \(SSE\) untuk antrian \(konsol\) di Panduan Pengembang Layanan Antrian Sederhana Amazon](#).

[SQS.2] Antrian SQS harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: AWS : : SQS : : Queue

AWS Config aturan: tagged-sqs-queue (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
requiredTagKeys	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS .	No default value

Kontrol ini memeriksa apakah antrian Amazon SQS memiliki tag dengan kunci tertentu yang ditentukan dalam parameter. `requiredTagKeys` Kontrol gagal jika antrian tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter `requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika antrian tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws :`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengkategorikan sumber daya berdasarkan tujuan, pemilik,

lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat [Untuk apa ABAC? AWS](#) di Panduan Pengguna IAM.

Note

Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat [Menandai AWS sumber daya Anda](#) di Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke antrean yang ada menggunakan konsol Amazon SQS, [lihat Mengonfigurasi tag alokasi biaya untuk antrean \(konsol\) Amazon SQS di Panduan Pengembangan Layanan Antrian](#) Sederhana Amazon.

[SQS.3] Kebijakan akses antrian SQS seharusnya tidak mengizinkan akses publik

Kategori: Lindungi > Manajemen akses aman > Sumber daya tidak dapat diakses publik

Tingkat keparahan: Tinggi

Jenis sumber daya: AWS : : SQS : : Queue

AWS Config aturan: [sqs-queue-no-public-access](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah kebijakan akses Amazon SQS memungkinkan akses publik ke antrean SQS. Kontrol gagal jika kebijakan akses SQS mengizinkan akses publik ke antrian.

Kebijakan akses Amazon SQS dapat mengizinkan akses publik ke antrian SQS, yang memungkinkan pengguna anonim atau identitas AWS IAM yang diautentikasi untuk mengakses antrian. Kebijakan akses SQS biasanya menyediakan akses ini dengan menentukan karakter wildcard (*) dalam Principal elemen kebijakan, tidak menggunakan kondisi yang tepat untuk membatasi akses ke antrian, atau keduanya. Jika kebijakan akses SQS mengizinkan akses publik, pihak ketiga mungkin dapat melakukan tugas seperti menerima pesan dari antrian, mengirim pesan ke antrian, atau mengubah kebijakan akses untuk antrian. Hal ini dapat mengakibatkan peristiwa seperti eksfiltrasi data, penolakan layanan, atau injeksi pesan ke dalam antrian oleh aktor ancaman.

Note

Kontrol ini tidak mengevaluasi kondisi kebijakan yang menggunakan karakter atau variabel wildcard. Untuk menghasilkan PASSED temuan, kondisi dalam kebijakan akses Amazon SQS untuk antrian hanya boleh menggunakan nilai tetap, yaitu nilai yang tidak berisi karakter wildcard atau variabel kebijakan. Untuk informasi tentang variabel kebijakan, lihat [Variabel dan tag](#) di Panduan AWS Identity and Access Management Pengguna.

Remediasi

Untuk informasi tentang mengonfigurasi kebijakan akses SQS untuk antrian SQS, lihat [Menggunakan kebijakan khusus dengan Bahasa Kebijakan Akses Amazon SQS di Panduan Pengembang Layanan](#) Antrian Sederhana Amazon.

Kontrol Security Hub untuk Step Functions

AWS Security Hub Kontrol ini mengevaluasi AWS Step Functions layanan dan sumber daya.

Kontrol ini mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat [Ketersediaan kontrol berdasarkan Wilayah](#).

[StepFunctions.1] Mesin status Step Functions seharusnya mengaktifkan logging

Persyaratan terkait: PCI DSS v4.0.1/10.4.2

Kategori: Identifikasi > Logging

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::StepFunctions::StateMachine`

AWS Config aturan: [step-functions-state-machine-logging-enabled](#)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
LogLevel	Tingkat logging minimum	Enum	ALL, ERROR, FATAL	Tidak ada nilai default

Kontrol ini memeriksa apakah mesin AWS Step Functions status telah mengaktifkan pencatatan. Kontrol gagal jika mesin status tidak mengaktifkan logging. Jika Anda memberikan nilai khusus untuk LogLevel parameter, kontrol hanya akan diteruskan jika mesin status mengaktifkan level logging yang ditentukan.

Pemantauan membantu Anda menjaga keandalan, ketersediaan, dan kinerja Step Functions. Anda harus mengumpulkan sebanyak mungkin data pemantauan dari Layanan AWS yang Anda gunakan sehingga Anda dapat lebih mudah men-debug kegagalan multi-titik. Memiliki konfigurasi logging yang ditentukan untuk mesin status Step Functions memungkinkan Anda melacak riwayat eksekusi dan hasil di Amazon CloudWatch Logs. Secara opsional, Anda hanya dapat melacak kesalahan atau peristiwa fatal.

Remediasi

Untuk mengaktifkan logging untuk mesin status Step Functions, lihat [Mengkonfigurasi logging](#) di Panduan AWS Step Functions Pengembang.

[StepFunctions.2] Aktivitas Step Functions harus diberi tag

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: AWS::StepFunctions::Activity

AWS Config aturan: tagged-stepfunctions-activity (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
<code>requiredTagKeys</code>	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS.	Tidak ada nilai default

Kontrol ini memeriksa apakah AWS Step Functions aktivitas memiliki tag dengan kunci tertentu yang ditentukan dalam `parameterrequiredTagKeys`. Kontrol gagal jika aktivitas tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam `parameterrequiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika aktivitas tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws :`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat [Untuk apa ABAC? AWS](#) di Panduan Pengguna IAM.

Note

Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS

Billing. Untuk praktik terbaik penandaan lainnya, lihat [Menandai AWS sumber daya Anda](#) di Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke aktivitas Step Functions, lihat [Menandai di Step Functions](#) di Panduan AWS Step Functions Pengembang.

Kontrol Security Hub untuk Systems Manager

AWS Security Hub Kontrol ini mengevaluasi layanan dan sumber daya AWS Systems Manager (SSM). Kontrol mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat [Ketersediaan kontrol berdasarkan Wilayah](#).

[SSM.1] EC2 Instans Amazon harus dikelola oleh AWS Systems Manager

Persyaratan terkait: PCI DSS v3.2.1/2.4, NIST.800-53.r5 CA-9 (1), 5 (2), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2(2), NIST.800-53.r5 CM-8, NIST.800-53.r5 CM-8(1), NIST.800-53.r5 CM-8(2), NIST.800-53.r5 CM-8(3), NIST.800-53.r5 SA-1 5 (8),, NIST.800-53.r5 SA-1 NIST.800-53.R5 SI-2 (3) NIST.800-53.r5 SA-3

Kategori: Identifikasi > Persediaan

Tingkat keparahan: Sedang

Sumber daya yang dievaluasi: AWS::EC2::Instance

Sumber daya AWS Config perekaman yang diperlukan: AWS::EC2::Instance, AWS::SSM::ManagedInstanceInventory

AWS Config aturan: [ec2-instance-managed-by-systems-manager](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah EC2 instans yang berhenti dan berjalan di akun Anda dikelola oleh AWS Systems Manager. Systems Manager adalah sebuah Layanan AWS yang dapat Anda gunakan untuk melihat dan mengontrol AWS infrastruktur Anda.

Untuk membantu Anda menjaga keamanan dan kepatuhan, Systems Manager memindai instans terkelola yang berhenti dan berjalan. Instans terkelola adalah mesin yang dikonfigurasi untuk digunakan dengan Systems Manager. Systems Manager kemudian melaporkan atau mengambil tindakan korektif atas setiap pelanggaran kebijakan yang terdeteksi. Systems Manager juga membantu Anda mengonfigurasi dan mempertahankan instans terkelola Anda.

Untuk mempelajari lebih lanjut, lihat [Panduan AWS Systems Manager Pengguna](#).

Tindakan Perbaikan

Untuk mengelola EC2 instans dengan Systems Manager, lihat [Manajemen EC2 host Amazon](#) di Panduan AWS Systems Manager Pengguna. Di bagian Opsi konfigurasi, Anda dapat menyimpan pilihan default atau mengubahnya seperlunya untuk konfigurasi pilihan Anda.

[SSM.2] EC2 Instans Amazon yang dikelola oleh Systems Manager harus memiliki status kepatuhan patch COMPLIANT setelah instalasi patch

Persyaratan terkait: NIST.800-53.R5 CM-8 (3), NIST.800-53.R5 SI-2, NIST.800-53.R5 SI-2 (2), Nist.800-53.R5 SI-2 (3), Nist.800-53.R5 SI-2 (4), Nist.800-53.r5 SI-2 (5), NIST.800-53.R5 SI-2 (5), Nist.800-171.r2 3.7.1, PCI DSS v3.2.1/6.2, PCI DSS v4.0.1/2.2.1, PCI DSS v4.0.1/6.3.3

Kategori: Deteksi > Layanan deteksi

Tingkat keparahan: Tinggi

Jenis sumber daya: AWS::SSM::PatchCompliance

AWS Config aturan: [ec2-managedinstance-patch-compliance-status-check](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah status kepatuhan kepatuhan patch Systems Manager COMPLIANT atau NON_COMPLIANT setelah penginstalan tambalan pada instance. Kontrol gagal jika status kepatuhanNON_COMPLIANT. Kontrol hanya memeriksa instance yang dikelola oleh Systems Manager Patch Manager.

Menambal EC2 instance Anda seperti yang dipersyaratkan oleh organisasi Anda mengurangi permukaan serangan Anda. Akun AWS

Tindakan Perbaikan

Systems Manager merekomendasikan penggunaan [kebijakan tambalan](#) untuk mengonfigurasi patching untuk instance terkelola Anda. Anda juga dapat menggunakan [dokumen Systems Manager](#), seperti yang dijelaskan di prosedur berikut ini, untuk menambal instans.

Untuk memulihkan tambalan yang tidak sesuai

1. Buka AWS Systems Manager konsol di <https://console.aws.amazon.com/systems-manager/>.
2. Untuk Node Management, pilih Run Command, lalu pilih Run command.
3. Pilih opsi untuk AWS- RunPatchBaseline.
4. Ubah Operasi untuk Menginstal.
5. Pilih instance secara manual, lalu pilih instans yang tidak sesuai.
6. Pilih Jalankan.
7. Setelah perintah selesai, untuk memantau status kepatuhan baru dari instance yang ditambah, pilih Kepatuhan di panel navigasi.

[SSM.3] EC2 Instans Amazon yang dikelola oleh Systems Manager harus memiliki status kepatuhan asosiasi COMPLIANT

Persyaratan terkait: NIST.800-53.r5 CA-9 (1), NIST.800-53.R5 CM-2, NIST.800-53.R5 CM-2 (2), Nist.800-53.r5 CM-8, Nist.800-53.r5 CM-8 (1), Nist.800-53.R5 CM-8 (3), Nist.800-53.r5 SI-2 (3), PCI DSS v3.2.1/2.4, PCI DSS v4.0.1/2.2.1, PCI DSS v4.0.1/6.3.3

Kategori: Deteksi > Layanan deteksi

Tingkat keparahan: Rendah

Jenis sumber daya: AWS::SSM::AssociationCompliance

AWS Config aturan: [ec2-managedinstance-association-compliance-status-check](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah status kepatuhan AWS Systems Manager asosiasi COMPLIANT atau NON_COMPLIANT setelah asosiasi dijalankan pada sebuah instance. Kontrol gagal jika status kepatuhan asosiasiNON_COMPLIANT.

Asosiasi State Manager adalah konfigurasi yang ditetapkan untuk instans terkelola Anda. Konfigurasi mendefinisikan status yang ingin Anda pertahankan pada instans Anda. Sebagai contoh, suatu asosiasi dapat menentukan bahwa perangkat lunak antivirus harus diinstal dan berjalan pada instans Anda atau bahwa port tertentu harus ditutup.

Setelah Anda membuat satu atau beberapa asosiasi State Manager, informasi status kepatuhan segera tersedia untuk Anda. Anda dapat melihat status kepatuhan di konsol atau sebagai respons terhadap AWS CLI perintah atau tindakan API Systems Manager yang sesuai. Untuk asosiasi, Kepatuhan Konfigurasi menunjukkan status kepatuhan (Compliant atau Non-compliant). Ini juga menunjukkan tingkat keparahan yang ditetapkan untuk asosiasi, seperti Critical atau Medium.

Untuk mempelajari lebih lanjut tentang kepatuhan asosiasi Manajer [Negara](#), lihat [Tentang kepatuhan asosiasi Manajer Negara](#) di Panduan AWS Systems Manager Pengguna.

Tindakan Perbaikan

Asosiasi yang gagal dapat dikaitkan dengan hal-hal yang berbeda, termasuk target dan nama dokumen Systems Manager. Untuk mengatasi masalah ini, Anda harus terlebih dahulu mengidentifikasi dan menyelidiki asosiasi dengan melihat riwayat asosiasi. Untuk petunjuk tentang melihat riwayat asosiasi, lihat [Melihat riwayat asosiasi](#) di Panduan AWS Systems Manager Pengguna.

Setelah menyelidiki, Anda dapat mengedit asosiasi untuk memperbaiki masalah yang diidentifikasi. Anda dapat mengedit asosiasi untuk menentukan nama baru, jadwal, tingkat keparahan, atau target. Setelah Anda mengedit asosiasi, AWS Systems Manager buat versi baru. Untuk petunjuk tentang mengedit asosiasi, lihat [Mengedit dan membuat versi baru asosiasi](#) di Panduan AWS Systems Manager Pengguna.

[SSM.4] Dokumen SSM seharusnya tidak bersifat publik

Persyaratan terkait: NIST.800-53.r5 AC-2 1 NIST.800-53.r5 AC-3,, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-4,, NIST.800-53.r5 AC-4 (21) NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7,, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9)

Kategori: Lindungi > Konfigurasi jaringan aman > Sumber daya tidak dapat diakses publik

Tingkat keparahan: Kritis

Jenis sumber daya: AWS : : SSM : : Document

AWS Config aturan: [ssm-document-not-public](#)

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah AWS Systems Manager dokumen yang dimiliki oleh akun bersifat publik. Kontrol ini gagal jika dokumen Systems Manager dengan pemiliknya `Self` bersifat publik.

Dokumen Systems Manager yang bersifat publik mungkin memungkinkan akses yang tidak diinginkan ke dokumen Anda. Dokumen Systems Manager publik dapat mengekspos informasi berharga tentang akun, sumber daya, dan proses internal Anda.

Kecuali kasus penggunaan Anda mengharuskan berbagi publik, sebaiknya blokir pengaturan berbagi publik untuk dokumen Systems Manager yang dimiliki oleh `Systems ManagerSelf`.

Tindakan Perbaikan

Untuk memblokir berbagi publik untuk dokumen Systems Manager, lihat [Memblokir berbagi publik untuk dokumen SSM](#) di Panduan AWS Systems Manager Pengguna.

[SSM.5] Dokumen SSM harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::SSM::Document`

AWS Config aturan: [ssm-document-tagged](#)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
<code>requiredKeyTags</code>	Daftar kunci tag non-sistem yang harus ditetapkan ke sumber daya yang dievaluasi	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi	Tidak ada nilai default

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
	i. Kunci tag peka huruf besar dan kecil.		persyaratan AWS .	

Kontrol ini memeriksa apakah AWS Systems Manager dokumen memiliki kunci tag yang ditentukan oleh `requiredKeyTags` parameter. Kontrol gagal jika dokumen tidak memiliki kunci tag, atau tidak memiliki semua kunci yang ditentukan oleh `requiredKeyTags` parameter. Jika Anda tidak menentukan nilai apa pun untuk `requiredKeyTags` parameter, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika dokumen tidak memiliki kunci tag. Kontrol mengabaikan tag sistem, yang diterapkan secara otomatis dan memiliki `aws :` awalan. Kontrol tidak mengevaluasi dokumen Systems Manager yang dimiliki oleh Amazon.

Tag adalah sebuah label yang Anda buat dan tetapkan ke sebuah AWS sumber daya. Setiap tanda terdiri dari kunci tanda yang diperlukan dan nilai tanda opsional. Anda dapat menggunakan tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Mereka dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Mereka juga dapat membantu Anda melacak pemilik sumber daya untuk tindakan dan pemberitahuan. Anda juga dapat menggunakan tag untuk menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi. Untuk informasi selengkapnya tentang strategi ABAC, lihat [Menentukan izin berdasarkan atribut dengan otorisasi ABAC](#) di Panduan Pengguna IAM. Untuk informasi selengkapnya tentang penandaan, lihat [Panduan Pengguna Tagging AWS Resources dan Tag Editor](#).

Note

Jangan menyimpan informasi pengenalan pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses dari banyak orang Layanan AWS. Mereka tidak dimaksudkan untuk digunakan untuk data privat atau sensitif.

Tindakan Perbaikan

Untuk menambahkan tag ke AWS Systems Manager dokumen, Anda dapat menggunakan [AddTagsToResource](#) operasi AWS Systems Manager API atau, jika Anda menggunakan AWS CLI,

jalankan [add-tags-to-resource](#) perintah. Anda juga dapat menggunakan AWS Systems Manager konsol.

Kontrol Security Hub untuk AWS Transfer Family

AWS Security Hub Kontrol ini mengevaluasi AWS Transfer Family layanan dan sumber daya. Kontrol mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat [Ketersediaan kontrol berdasarkan Wilayah](#).

[Transfer.1] AWS Transfer Family alur kerja harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::Transfer::Workflow`

AWS Config aturan: `tagged-transfer-workflow` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
<code>requiredTagKeys</code>	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS .	No default value

Kontrol ini memeriksa apakah AWS Transfer Family alur kerja memiliki tag dengan kunci tertentu yang ditentukan dalam parameter `requiredTagKeys`. Kontrol gagal jika alur kerja tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter `requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika alur kerja tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan `aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat [Untuk apa ABAC? AWS](#) di Panduan Pengguna IAM.

Note

Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat [Menandai AWS sumber daya Anda](#) di Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke alur kerja Transfer Family (konsol)

1. Buka AWS Transfer Family konsol.
2. Di panel navigasi, pilih Alur Kerja. Kemudian, pilih alur kerja yang ingin Anda tag.
3. Pilih Kelola tag, lalu tambahkan tag.

[Transfer.2] Server Transfer Family tidak boleh menggunakan protokol FTP untuk koneksi titik akhir

Persyaratan terkait: NIST.800-53.r5 CM-7, NIST.800-53.r5 IA-5, NIST.800-53.r5 SC-8, PCI DSS v4.0.1/4.2.1

Kategori: Lindungi > Perlindungan Data > Enkripsi data-in-transit

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::Transfer::Server

AWS Config aturan: [transfer-family-server-no-ftp](#)

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah AWS Transfer Family server menggunakan protokol selain FTP untuk koneksi endpoint. Kontrol gagal jika server menggunakan protokol FTP untuk klien untuk terhubung ke endpoint server.

FTP (File Transfer Protocol) menetapkan koneksi titik akhir melalui saluran yang tidak terenkripsi, meninggalkan data yang dikirim melalui saluran ini rentan terhadap intersepsi. Menggunakan SFTP (SSH File Transfer Protocol), FTPS (File Transfer Protocol Secure), atau AS2 (Applicability Statement 2) menawarkan lapisan keamanan ekstra dengan mengenkripsi data Anda dalam perjalanan dan dapat digunakan untuk membantu mencegah penyerang potensial menggunakan person-in-the-middle atau serangan serupa untuk menguping atau memanipulasi lalu lintas jaringan.

Remediasi

Untuk mengubah protokol server Transfer Family, lihat [Mengedit protokol transfer file](#) di AWS Transfer Family Panduan Pengguna.

[Transfer.3] Konektor Transfer Family seharusnya mengaktifkan logging

Persyaratan terkait: NIST.800-53.r5 AC-2 (12), (4), NIST.800-53.r5 AC-2 (26), (9),, NIST.800-53.r5 AC-4 (9), NIST.800-53.r5 AC-6 Nist.800-53.R5 SI-3 NIST.800-53.r5 SC-7 (8) NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 AU-9(7), NIST.800-53.r5 CA-7, Nist.800-53.R5 SI-4, Nist.800-53.R5 SI-4 (20), NIST.800-53.R5 SI-7 (8)

Kategori: Identifikasi > Logging

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::Transfer::Connector

AWS Config aturan: [transfer-connector-logging-enabled](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah CloudWatch pencatatan Amazon diaktifkan untuk AWS Transfer Family konektor. Kontrol gagal jika CloudWatch logging tidak diaktifkan untuk konektor.

Amazon CloudWatch adalah layanan pemantauan dan observabilitas yang memberikan visibilitas ke AWS sumber daya Anda, termasuk AWS Transfer Family sumber daya. Untuk Transfer Family, CloudWatch menyediakan audit dan pencatatan terkonsolidasi untuk kemajuan dan hasil alur kerja. Ini mencakup beberapa metrik yang didefinisikan Transfer Family untuk alur kerja. Anda dapat mengonfigurasi Transfer Family untuk secara otomatis mencatat peristiwa konektor CloudWatch. Untuk melakukan ini, Anda menentukan peran logging untuk konektor. Untuk peran logging, Anda membuat peran IAM dan kebijakan IAM berbasis sumber daya yang menentukan izin untuk peran tersebut.

Remediasi

Untuk informasi tentang mengaktifkan CloudWatch logging untuk konektor Transfer Family, lihat [Amazon CloudWatch logging untuk AWS Transfer Family server](#) di Panduan AWS Transfer Family Pengguna.

[Transfer.4] Perjanjian Transfer Family harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: AWS::Transfer::Agreement

AWS Config aturan: [transfer-agreement-tagged](#)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
requiredKeyTags	Daftar kunci tag non-sistem yang harus ditetapkan ke sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS .	Tidak ada nilai default

Kontrol ini memeriksa apakah AWS Transfer Family perjanjian memiliki kunci tag yang ditentukan oleh `requiredKeyTags` parameter. Kontrol gagal jika perjanjian tidak memiliki kunci tag, atau tidak memiliki semua kunci yang ditentukan oleh `requiredKeyTags` parameter. Jika Anda tidak menentukan nilai apa pun untuk `requiredKeyTags` parameter, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika perjanjian tidak memiliki kunci tag. Kontrol mengabaikan tag sistem, yang diterapkan secara otomatis dan memiliki `aws :` awalan.

Tag adalah label yang Anda buat dan tetapkan ke AWS sumber daya. Setiap tanda terdiri dari kunci tanda yang diperlukan dan nilai tanda opsional. Anda dapat menggunakan tag untuk mengkategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Mereka dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Mereka juga dapat membantu Anda melacak pemilik sumber daya untuk tindakan dan pemberitahuan. Anda juga dapat menggunakan tag untuk menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi. Untuk informasi selengkapnya tentang strategi ABAC, lihat [Menentukan izin berdasarkan atribut dengan otorisasi ABAC](#) di Panduan Pengguna IAM. Untuk informasi selengkapnya tentang tag, lihat [Panduan Pengguna AWS Sumber Daya Penandaan dan Editor Tag](#).

Note

Jangan menyimpan informasi pengenalan pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses dari banyak orang Layanan AWS. Mereka tidak dimaksudkan untuk digunakan untuk data pribadi atau sensitif.

Remediasi

Untuk informasi tentang menambahkan tag ke AWS Transfer Family perjanjian, lihat [Metode penandaan sumber daya](#) di Panduan Pengguna AWS Sumber Daya Penandaan dan Editor Tag.

[Transfer.5] Sertifikat Transfer Family harus diberi tag

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::Transfer::Certificate`

AWS Config aturan: [transfer-certificate-tagged](#)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
<code>requiredKeyTags</code>	Daftar kunci tag non-sistem yang harus ditetapkan ke sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS .	Tidak ada nilai default

Kontrol ini memeriksa apakah AWS Transfer Family sertifikat memiliki kunci tag yang ditentukan oleh `requiredKeyTags` parameter. Kontrol gagal jika sertifikat tidak memiliki kunci tag, atau tidak memiliki semua kunci yang ditentukan oleh `requiredKeyTags` parameter. Jika Anda tidak menentukan nilai apa pun untuk `requiredKeyTags` parameter, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika sertifikat tidak memiliki kunci tag. Kontrol mengabaikan tag sistem, yang diterapkan secara otomatis dan memiliki `aws :` awalan.

Tag adalah label yang Anda buat dan tetapkan ke AWS sumber daya. Setiap tanda terdiri dari kunci tanda yang diperlukan dan nilai tanda opsional. Anda dapat menggunakan tag untuk mengkategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Mereka dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Mereka juga dapat membantu Anda melacak pemilik sumber daya untuk tindakan dan pemberitahuan. Anda juga dapat menggunakan tag untuk menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi. Untuk informasi selengkapnya tentang strategi ABAC, lihat [Menentukan izin berdasarkan atribut dengan otorisasi ABAC](#) di Panduan Pengguna IAM. Untuk informasi selengkapnya tentang tag, lihat [Panduan Pengguna AWS Sumber Daya Penandaan dan Editor Tag](#).

 Note

Jangan menyimpan informasi pengenalan pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses dari banyak orang Layanan AWS. Mereka tidak dimaksudkan untuk digunakan untuk data pribadi atau sensitif.

Remediasi

Untuk informasi tentang menambahkan tag ke AWS Transfer Family sertifikat, lihat [Metode penandaan sumber daya](#) di Panduan Pengguna AWS Sumber Daya Penandaan dan Editor Tag.

[Transfer.6] Konektor Transfer Family harus diberi tag

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::Transfer::Connector`

AWS Config aturan: [transfer-connector-tagged](#)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
<code>requiredKeyTags</code>	Daftar kunci tag non-sistem yang harus ditetapkan ke sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS .	Tidak ada nilai default

Kontrol ini memeriksa apakah AWS Transfer Family konektor memiliki kunci tag yang ditentukan oleh `requiredKeyTags` parameter. Kontrol gagal jika konektor tidak memiliki kunci tag, atau tidak memiliki semua kunci yang ditentukan oleh `requiredKeyTags` parameter. Jika Anda tidak menentukan nilai apa pun untuk `requiredKeyTags` parameter, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika konektor tidak memiliki kunci tag. Kontrol mengabaikan tag sistem, yang diterapkan secara otomatis dan memiliki `aws:` awalan.

Tag adalah label yang Anda buat dan tetapkan ke AWS sumber daya. Setiap tanda terdiri dari kunci tanda yang diperlukan dan nilai tanda opsional. Anda dapat menggunakan tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Mereka dapat membantu

Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Mereka juga dapat membantu Anda melacak pemilik sumber daya untuk tindakan dan pemberitahuan. Anda juga dapat menggunakan tag untuk menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi. Untuk informasi selengkapnya tentang strategi ABAC, lihat [Menentukan izin berdasarkan atribut dengan otorisasi ABAC](#) di Panduan Pengguna IAM. Untuk informasi selengkapnya tentang tag, lihat [Panduan Pengguna AWS Sumber Daya Penandaan dan Editor Tag](#).

Note

Jangan menyimpan informasi pengenalan pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses dari banyak orang Layanan AWS. Mereka tidak dimaksudkan untuk digunakan untuk data pribadi atau sensitif.

Remediasi

Untuk informasi tentang menambahkan tag ke AWS Transfer Family konektor, lihat [Metode penandaan sumber daya](#) di Panduan Pengguna AWS Sumber Daya Penandaan dan Editor Tag.

[Transfer.7] Profil Transfer Family harus diberi tag

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::Transfer::Profile`

AWS Config aturan: [transfer-profile-tagged](#)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
<code>requiredKeyTags</code>	Daftar kunci tag non-sistem yang harus ditetapkan ke sumber daya yang dievaluasi	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi	Tidak ada nilai default

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default Security Hub
	i. Kunci tag peka huruf besar dan kecil.		persyaratan AWS .	

Kontrol ini memeriksa apakah AWS Transfer Family profil memiliki kunci tag yang ditentukan oleh `requiredKeyTags` parameter. Kontrol gagal jika profil tidak memiliki kunci tag, atau tidak memiliki semua kunci yang ditentukan oleh `requiredKeyTags` parameter. Jika Anda tidak menentukan nilai apa pun untuk `requiredKeyTags` parameter, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika profil tidak memiliki kunci tag. Kontrol mengabaikan tag sistem, yang diterapkan secara otomatis dan memiliki `aws:` awalan. Kontrol mengevaluasi profil lokal dan profil mitra.

Tag adalah label yang Anda buat dan tetapkan ke AWS sumber daya. Setiap tanda terdiri dari kunci tanda yang diperlukan dan nilai tanda opsional. Anda dapat menggunakan tag untuk mengkategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Mereka dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Mereka juga dapat membantu Anda melacak pemilik sumber daya untuk tindakan dan pemberitahuan. Anda juga dapat menggunakan tag untuk menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi. Untuk informasi selengkapnya tentang strategi ABAC, lihat [Menentukan izin berdasarkan atribut dengan otorisasi ABAC](#) di Panduan Pengguna IAM. Untuk informasi selengkapnya tentang tag, lihat [Panduan Pengguna AWS Sumber Daya Penandaan dan Editor Tag](#).

Note

Jangan menyimpan informasi pengenalan pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses dari banyak orang Layanan AWS. Mereka tidak dimaksudkan untuk digunakan untuk data pribadi atau sensitif.

Remediasi

Untuk informasi tentang menambahkan tag ke AWS Transfer Family profil, lihat [Metode penandaan sumber daya](#) di Panduan Pengguna AWS Sumber Daya Tag dan Editor Tag.

Kontrol Security Hub untuk AWS WAF

AWS Security Hub Kontrol ini mengevaluasi AWS WAF layanan dan sumber daya. Kontrol mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat [Ketersediaan kontrol berdasarkan Wilayah](#).

[WAF.1] Pencatatan ACL Web Global AWS WAF Klasik harus diaktifkan

Persyaratan terkait: NIST.800-53.r5 AC-4 (26),, NIST.800-53.r5 SC-7 (9) NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, NIST.800-53.R5 SI-7 (8), PCI DSS v4.0.1/10.4.2

Kategori: Identifikasi > Logging

Tingkat keparahan: Sedang

Jenis sumber daya: AWS : :WAF : :WebACL

AWS Config aturan: [waf-classic-logging-enabled](#)

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah logging diaktifkan untuk ACL web AWS WAF global. Kontrol ini gagal jika logging tidak diaktifkan untuk ACL web.

Pencatatan adalah bagian penting dari pemeliharaan keandalan, ketersediaan, dan performa AWS WAF global. Ini adalah persyaratan bisnis dan kepatuhan di banyak organisasi, dan memungkinkan Anda memecahkan masalah perilaku aplikasi. Ini juga memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web yang dilampirkan AWS WAF.

Tindakan Perbaikan

Untuk mengaktifkan pencatatan untuk ACL AWS WAF web, lihat [Mencatat informasi lalu lintas ACL web](#) di Panduan AWS WAF Pengembang.

[WAF.2] Aturan Regional AWS WAF Klasik harus memiliki setidaknya satu syarat

Persyaratan terkait: NIST.800-53.r5 AC-4 (21) NIST.800-53.r5 SC-7,, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (21)

Kategori: Lindungi > Konfigurasi jaringan aman

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::WAFRegional::Rule`

AWS Config aturan: [waf-regional-rule-not-empty](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah aturan AWS WAF Regional memiliki setidaknya satu syarat. Kontrol gagal jika tidak ada kondisi dalam suatu aturan.

Aturan Regional WAF dapat berisi beberapa kondisi. Ketentuan aturan memungkinkan inspeksi lalu lintas dan mengambil tindakan yang ditentukan (izinkan, blokir, atau hitung). Tanpa kondisi apa pun, lalu lintas berlalu tanpa inspeksi. Aturan Regional WAF tanpa kondisi, tetapi dengan nama atau tag yang menyarankan izinkan, blokir, atau hitung, dapat menyebabkan asumsi yang salah bahwa salah satu tindakan tersebut terjadi.

Tindakan Perbaikan

Untuk menambahkan kondisi ke aturan kosong, lihat [Menambahkan dan menghapus kondisi dalam aturan](#) di Panduan AWS WAF Pengembang.

[WAF.3] Kelompok aturan Regional AWS WAF Klasik harus memiliki setidaknya satu aturan

Persyaratan terkait: NIST.800-53.r5 AC-4 (21) NIST.800-53.r5 SC-7,, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (21)

Kategori: Lindungi > Konfigurasi jaringan aman

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::WAFRegional::RuleGroup`

AWS Config aturan: [waf-regional-rulegroup-not-empty](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah kelompok aturan AWS WAF Regional memiliki setidaknya satu aturan. Kontrol gagal jika tidak ada aturan dalam kelompok aturan.

Grup aturan Regional WAF dapat berisi beberapa aturan. Ketentuan aturan memungkinkan inspeksi lalu lintas dan mengambil tindakan yang ditentukan (izinkan, blokir, atau hitung). Tanpa aturan apa pun, lalu lintas berlalu tanpa inspeksi. Kelompok aturan Regional WAF tanpa aturan, tetapi dengan nama atau tag yang menyarankan izinkan, blokir, atau hitung, dapat menyebabkan asumsi yang salah bahwa salah satu tindakan tersebut terjadi.

Tindakan Perbaikan

Untuk menambahkan aturan dan ketentuan aturan ke grup aturan kosong, lihat [Menambahkan dan menghapus aturan dari grup aturan AWS WAF Klasik](#) serta [Menambahkan dan menghapus kondisi dalam aturan](#) di Panduan AWS WAF Pengembang.

[WAF.4] Web Regional AWS WAF Klasik ACLs harus memiliki setidaknya satu aturan atau kelompok aturan

Persyaratan terkait: NIST.800-53.r5 CA-9 (1), Nist.800-53.R5 CM-2

Kategori: Lindungi > Konfigurasi jaringan aman

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::WAFRegional::WebACL

AWS Config aturan: [waf-regional-webacl-not-empty](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah ACL AWS WAF Classic Regional web berisi aturan WAF atau grup aturan WAF. Kontrol ini gagal jika ACL web tidak berisi aturan WAF atau grup aturan.

ACL web Regional WAF dapat berisi kumpulan aturan dan kelompok aturan yang memeriksa dan mengendalikan permintaan web. Jika ACL web kosong, lalu lintas web dapat lewat tanpa terdeteksi atau ditindaklanjuti oleh WAF tergantung pada tindakan default.

Tindakan Perbaikan

Untuk menambahkan aturan atau grup aturan ke ACL web Regional AWS WAF Klasik kosong, lihat [Mengedit ACL Web di Panduan AWS WAF](#) Pengembang.

[WAF.6] Aturan global AWS WAF klasik harus memiliki setidaknya satu syarat

Persyaratan terkait: NIST.800-53.r5 CA-9 (1), Nist.800-53.R5 CM-2

Kategori: Lindungi > Konfigurasi jaringan aman

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::WAF::Rule

AWS Config aturan: [waf-global-rule-not-empty](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah aturan AWS WAF global berisi kondisi apa pun. Kontrol gagal jika tidak ada kondisi dalam suatu aturan.

Aturan global WAF dapat berisi beberapa kondisi. Kondisi aturan memungkinkan inspeksi lalu lintas dan mengambil tindakan yang ditentukan (izinkan, blokir, atau hitung). Tanpa kondisi apa pun, lalu lintas berlalu tanpa inspeksi. Aturan global WAF tanpa kondisi, tetapi dengan nama atau tag yang menyarankan izinkan, blokir, atau hitung, dapat menyebabkan asumsi yang salah bahwa salah satu tindakan tersebut terjadi.

Tindakan Perbaikan

Untuk petunjuk cara membuat aturan dan menambahkan kondisi, lihat [Membuat aturan dan menambahkan kondisi](#) di Panduan AWS WAF Pengembang.

[WAF.7] Kelompok aturan global AWS WAF klasik harus memiliki setidaknya satu aturan

Persyaratan terkait: NIST.800-53.r5 CA-9 (1), Nist.800-53.R5 CM-2

Kategori: Lindungi > Konfigurasi jaringan aman

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::WAF::RuleGroup

AWS Config aturan: [waf-global-rulegroup-not-empty](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah grup aturan AWS WAF global memiliki setidaknya satu aturan. Kontrol gagal jika tidak ada aturan dalam kelompok aturan.

Grup aturan global WAF dapat berisi beberapa aturan. Ketentuan aturan memungkinkan inspeksi lalu lintas dan mengambil tindakan yang ditentukan (izinkan, blokir, atau hitung). Tanpa aturan apa pun, lalu lintas berlalu tanpa inspeksi. Grup aturan global WAF tanpa aturan, tetapi dengan nama atau tag yang menyarankan izinkan, blokir, atau hitung, dapat menyebabkan asumsi yang salah bahwa salah satu tindakan tersebut terjadi.

Tindakan Perbaikan

Untuk petunjuk cara menambahkan aturan ke grup aturan, lihat [Membuat grup aturan AWS WAF Klasik](#) di Panduan AWS WAF Pengembang.

[WAF.8] Web global AWS WAF klasik ACLs harus memiliki setidaknya satu aturan atau kelompok aturan

Persyaratan terkait: NIST.800-53.r5 AC-4 (21) NIST.800-53.r5 SC-7,, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (21)

Kategori: Lindungi > Konfigurasi jaringan aman

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::WAF::WebACL

AWS Config aturan: [waf-global-webacl-not-empty](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah ACL web AWS WAF global berisi setidaknya satu aturan WAF atau grup aturan WAF. Kontrol gagal jika ACL web tidak berisi aturan WAF atau grup aturan.

ACL web global WAF dapat berisi kumpulan aturan dan kelompok aturan yang memeriksa dan mengendalikan permintaan web. Jika ACL web kosong, lalu lintas web dapat lewat tanpa terdeteksi atau ditindaklanjuti oleh WAF tergantung pada tindakan default.

Tindakan Perbaikan

Untuk menambahkan aturan atau grup aturan ke ACL web AWS WAF global yang kosong, lihat [Mengedit ACL web di Panduan AWS WAF](#) Pengembang. Untuk Filter, pilih Global (CloudFront).

[WAF.10] AWS WAF web ACLs harus memiliki setidaknya satu aturan atau kelompok aturan

Persyaratan terkait: NIST.800-53.r5 CA-9 (1), Nist.800-53.R5 CM-2

Kategori: Lindungi > Konfigurasi jaringan aman

Tingkat keparahan: Sedang

Jenis sumber daya: AWS : :WAFv2 : :WebACL

AWS Config aturan: [wafv2-webacl-not-empty](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah daftar kontrol akses web AWS WAF V2 (web ACL) berisi setidaknya satu aturan atau grup aturan. Kontrol gagal jika ACL web tidak berisi aturan atau grup aturan apa pun.

ACL web memberi Anda kontrol halus atas semua permintaan web HTTP (S) yang ditanggapi oleh sumber daya Anda yang dilindungi. ACL web harus berisi kumpulan aturan dan kelompok aturan yang memeriksa dan mengendalikan permintaan web. Jika ACL web kosong, lalu lintas web dapat lewat tanpa terdeteksi atau ditindaklanjuti dengan AWS WAF tergantung pada tindakan default.

Tindakan Perbaikan

Untuk menambahkan aturan atau grup aturan ke ACL WAFV2 web kosong, lihat [Mengedit ACL Web di Panduan AWS WAF](#) Pengembang.

[WAF.11] pencatatan ACL AWS WAF web harus diaktifkan

Persyaratan terkait: NIST.800-53.r5 AC-4 (26),, (10) NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (9), NIST.800-53.R5 SI-7 NIST.800-53.r5 SC-7 (8), PCI DSS v4.0.1/10.4.2

Kategori: Identifikasi > Logging

Tingkat keparahan: Rendah

Jenis sumber daya: AWS : :WAFv2 : :WebACL

AWS Config aturan: [wafv2-logging-enabled](#)

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah pencatatan diaktifkan untuk daftar kontrol akses web AWS WAF V2 (web ACL). Kontrol ini gagal jika pencatatan dinonaktifkan untuk ACL web.

Note

Kontrol ini tidak memeriksa apakah pencatatan ACL AWS WAF web diaktifkan untuk akun melalui Amazon Security Lake.

Pencatatan menjaga keandalan, ketersediaan, dan performa AWS WAF. Selain itu, penebangan adalah persyaratan bisnis dan kepatuhan di banyak organisasi. Dengan mencatat lalu lintas yang dianalisis oleh ACL web Anda, Anda dapat memecahkan masalah perilaku aplikasi.

Tindakan Perbaikan

Untuk mengaktifkan logging untuk ACL AWS WAF web, lihat [Mengelola logging untuk ACL web di Panduan AWS WAF](#) Pengembang.

AWS WAF Aturan [WAF.12] harus mengaktifkan metrik CloudWatch

Persyaratan terkait: NIST.800-53.r5 AC-4 (26),, (10), NIST.800-53.r5 SC-7 (9) NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3),

NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, Nist.800-53.R5 SI-7 NIST.800-53.r5 SC-7 (8), Nist.800-171.R2 3.14.6, Nist.800-171.R2 3.14.7

Kategori: Identifikasi > Logging

Tingkat keparahan: Sedang

Jenis sumber daya: AWS : :WAFv2 : :RuleGroup

AWS Config aturan: [wafv2-rulegroup-logging-enabled](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah AWS WAF aturan atau grup aturan mengaktifkan CloudWatch metrik Amazon. Kontrol gagal jika aturan atau grup aturan tidak mengaktifkan CloudWatch metrik.

Mengkonfigurasi CloudWatch metrik pada AWS WAF aturan dan grup aturan memberikan visibilitas ke arus lalu lintas. Anda dapat melihat aturan ACL mana yang dipicu dan permintaan mana yang diterima dan diblokir. Visibilitas ini dapat membantu Anda mengidentifikasi aktivitas berbahaya pada sumber daya terkait.

Tindakan Perbaikan

Untuk mengaktifkan CloudWatch metrik pada grup AWS WAF aturan, panggil API.

[UpdateRuleGroup](#) Untuk mengaktifkan CloudWatch metrik pada AWS WAF aturan, panggil [UpdateWebACL](#) API. Atur CloudWatchMetricsEnabled bidang ke true. Saat Anda menggunakan AWS WAF konsol untuk membuat aturan atau grup aturan, CloudWatch metrik diaktifkan secara otomatis.

Kontrol Security Hub untuk WorkSpaces

AWS Security Hub Kontrol ini mengevaluasi WorkSpaces layanan dan sumber daya Amazon.

Kontrol ini mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat [Ketersediaan kontrol berdasarkan Wilayah](#).

[WorkSpaces.1] volume WorkSpaces pengguna harus dienkripsi saat istirahat

Kategori: Lindungi > Perlindungan Data > Enkripsi data-at-rest

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::WorkSpaces::Workspace

AWS Config aturan: [workspaces-user-volume-encryption-enabled](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah volume pengguna di Amazon WorkSpaces Workspace dienkripsi saat istirahat. Kontrol gagal jika volume Workspace pengguna tidak dienkripsi saat istirahat.

Data saat istirahat mengacu pada data yang disimpan dalam penyimpanan persisten dan tidak mudah menguap untuk durasi berapa pun. Mengenkripsi data saat istirahat membantu Anda melindungi kerahasiaannya, yang mengurangi risiko bahwa pengguna yang tidak sah dapat mengaksesnya.

Remediasi

Untuk mengenkripsi volume WorkSpaces pengguna, lihat [Mengekripsi Workspace](#) di Panduan WorkSpaces Administrasi Amazon.

[WorkSpaces.2] volume WorkSpaces root harus dienkripsi saat istirahat

Kategori: Lindungi > Perlindungan Data > Enkripsi data-at-rest

Tingkat keparahan: Sedang

Jenis sumber daya: AWS::WorkSpaces::Workspace

AWS Config aturan: [workspaces-root-volume-encryption-enabled](#)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah volume root di Amazon WorkSpaces Workspace dienkripsi saat istirahat. Kontrol gagal jika volume Workspace root tidak dienkripsi saat istirahat.

Data saat istirahat mengacu pada data yang disimpan dalam penyimpanan persisten dan tidak mudah menguap untuk durasi berapa pun. Mengenkripsi data saat istirahat membantu Anda

melindungi kerahasiaannya, yang mengurangi risiko bahwa pengguna yang tidak sah dapat mengaksesnya.

Remediasi

Untuk mengenkripsi volume WorkSpaces root, lihat [Mengenkripsi a Workspace di Panduan WorkSpaces](#) Administrasi Amazon.

Izin yang diperlukan untuk mengonfigurasi kontrol di Security Hub CSPM

Untuk melihat informasi tentang kontrol keamanan dan mengaktifkan serta menonaktifkan kontrol keamanan dalam standar, peran AWS Identity and Access Management (IAM) yang Anda gunakan untuk mengakses AWS Security Hub Cloud Security Posture Management (CSPM) memerlukan izin untuk memanggil operasi CSPM API Security Hub berikut ini.

Untuk mendapatkan izin yang diperlukan, Anda dapat menggunakan kebijakan terkelola [CSPM Security Hub](#). Atau, Anda dapat memperbarui kebijakan IAM khusus untuk menyertakan izin untuk tindakan ini.

- [BatchGetSecurityControls](#)— Mengembalikan informasi tentang sekumpulan kontrol keamanan untuk akun saat ini dan Wilayah AWS.
- [ListSecurityControlDefinitions](#)— Mengembalikan informasi tentang kontrol keamanan yang berlaku untuk standar tertentu.
- [ListStandardsControlAssociations](#)— Mengidentifikasi apakah kontrol keamanan saat ini diaktifkan atau dinonaktifkan dari setiap standar yang diaktifkan di akun.
- [BatchGetStandardsControlAssociations](#)— Untuk sekumpulan kontrol keamanan, identifikasi apakah setiap kontrol saat ini diaktifkan atau dinonaktifkan dari standar yang ditentukan.
- [BatchUpdateStandardsControlAssociations](#)— Digunakan untuk mengaktifkan kontrol keamanan dalam standar yang mencakup kontrol, atau untuk menonaktifkan kontrol dalam standar. Ini adalah pengganti batch untuk [UpdateStandardsControl](#) operasi yang ada.
- [BatchUpdateStandardsControlAssociations](#)— Digunakan untuk mengaktifkan atau menonaktifkan sekumpulan kontrol keamanan dalam standar yang mencakup kontrol. Ini adalah pengganti batch untuk [UpdateStandardsControl](#) operasi yang ada.
- [UpdateStandardsControl](#)— Digunakan untuk mengaktifkan atau menonaktifkan kontrol keamanan tunggal dalam standar yang mencakup kontrol

- [DescribeStandardsControl](#)— Mengembalikan rincian tentang kontrol keamanan tertentu.

Selain yang sebelumnya APIs, Anda harus menambahkan izin untuk menelepon `BatchGetControlEvaluations` ke peran IAM Anda. Izin ini diperlukan untuk melihat status pemberdayaan dan kepatuhan kontrol, jumlah temuan untuk kontrol, dan skor keamanan keseluruhan untuk kontrol pada konsol CSPM Security Hub. Karena hanya panggilan `BatchGetControlEvaluations`, izin ini tidak secara langsung sesuai dengan CSPM APIs atau perintah Security Hub yang didokumentasikan secara publik. AWS CLI

Mengaktifkan kontrol di Security Hub CSPM

Dalam AWS Security Hub Cloud Security Posture Management (CSPM), kontrol adalah perlindungan dalam standar keamanan yang membantu organisasi melindungi kerahasiaan, integritas, dan ketersediaan informasinya. Setiap kontrol CSPM Security Hub terkait dengan sumber daya tertentu AWS . Ketika Anda mengaktifkan kontrol, Security Hub CSPM mulai menjalankan pemeriksaan keamanan untuk kontrol dan menghasilkan temuan untuk itu. Security Hub CSPM juga mempertimbangkan semua kontrol yang diaktifkan saat menghitung skor keamanan.

Anda dapat memilih untuk mengaktifkan kontrol di semua standar keamanan yang berlaku. Atau, Anda dapat mengonfigurasi status pemberdayaan secara berbeda dalam standar yang berbeda. Kami merekomendasikan opsi sebelumnya, di mana status pemberdayaan kontrol disejajarkan di semua standar yang Anda aktifkan. Untuk petunjuk tentang mengaktifkan kontrol di semua standar yang diterapkan, lihat [Mengaktifkan kontrol lintas standar](#). Untuk petunjuk tentang mengaktifkan kontrol dalam standar tertentu, lihat [Mengaktifkan kontrol dalam standar tertentu](#).

Jika Anda mengaktifkan agregasi lintas wilayah dan masuk ke Wilayah agregasi, konsol CSPM Security Hub menampilkan kontrol yang tersedia di setidaknya satu Wilayah tertaut. Jika kontrol tersedia di Wilayah tertaut tetapi tidak di Wilayah agregasi, Anda tidak dapat mengaktifkan atau menonaktifkan kontrol tersebut dari Wilayah agregasi.

Anda dapat mengaktifkan dan menonaktifkan kontrol di setiap Wilayah dengan menggunakan konsol CSPM Security Hub, Security Hub CSPM API, atau. AWS CLI

[Petunjuk untuk mengaktifkan dan menonaktifkan kontrol bervariasi berdasarkan apakah Anda menggunakan konfigurasi pusat atau tidak.](#) Topik ini menjelaskan perbedaannya. Konfigurasi pusat tersedia untuk pengguna yang mengintegrasikan Security Hub CSPM dan. AWS Organizations. Sebaiknya gunakan konfigurasi pusat untuk menyederhanakan proses mengaktifkan dan menonaktifkan kontrol di lingkungan multi-akun dan Multi-wilayah. Jika Anda menggunakan

konfigurasi pusat, Anda dapat mengaktifkan kontrol di beberapa akun dan Wilayah melalui penggunaan kebijakan konfigurasi. Jika Anda tidak menggunakan konfigurasi pusat, Anda harus mengaktifkan kontrol secara terpisah di setiap Wilayah dan akun.

Mengaktifkan kontrol lintas standar

Kami merekomendasikan untuk mengaktifkan kontrol AWS Security Hub Cloud Security Posture Management (CSPM) di semua standar yang berlaku untuk kontrol tersebut. Jika Anda mengaktifkan temuan kontrol konsolidasi, Anda menerima satu temuan per pemeriksaan kontrol bahkan jika kontrol milik lebih dari satu standar.

Pemberdayaan lintas standar di lingkungan multi-akun, Multi-wilayah

[Untuk mengaktifkan kontrol keamanan di beberapa Akun AWS dan Wilayah AWS, Anda harus masuk ke akun administrator CSPM Security Hub yang didelegasikan dan menggunakan konfigurasi pusat.](#)

Di bawah konfigurasi pusat, administrator yang didelegasikan dapat membuat kebijakan konfigurasi CSPM Security Hub yang mengaktifkan kontrol tertentu di seluruh standar yang diaktifkan. Anda kemudian dapat mengaitkan kebijakan konfigurasi dengan akun tertentu dan unit organisasi (OUs) atau root. Kebijakan konfigurasi berlaku di Wilayah asal Anda (juga disebut Wilayah agregasi) dan semua Wilayah yang ditautkan.

Kebijakan konfigurasi menawarkan kustomisasi. Misalnya, Anda dapat memilih untuk mengaktifkan semua kontrol dalam satu OU, dan Anda dapat memilih untuk mengaktifkan hanya kontrol Amazon Elastic Compute Cloud (EC2) di OU lain. Tingkat perincian tergantung pada tujuan yang Anda maksudkan untuk cakupan keamanan di organisasi Anda. Untuk petunjuk cara membuat kebijakan konfigurasi yang memungkinkan kontrol tertentu di seluruh standar, lihat [Membuat dan mengaitkan kebijakan konfigurasi](#).

Note

Administrator yang didelegasikan dapat membuat kebijakan konfigurasi untuk mengelola kontrol di semua standar kecuali Standar [yang Dikelola Layanan](#). AWS Control Tower Kontrol untuk standar ini harus dikonfigurasi dalam AWS Control Tower layanan.

Jika Anda ingin beberapa akun mengonfigurasi kontrolnya sendiri daripada administrator yang didelegasikan, administrator yang didelegasikan dapat menetapkan akun tersebut sebagai dikelola sendiri. Akun yang dikelola sendiri harus mengonfigurasi kontrol secara terpisah di setiap Wilayah.

Pemberdayaan lintas standar dalam satu akun dan Wilayah

Jika Anda tidak menggunakan konfigurasi pusat atau akun yang dikelola sendiri, Anda tidak dapat menggunakan kebijakan konfigurasi untuk mengaktifkan kontrol secara terpusat di beberapa akun dan Wilayah. Namun, Anda dapat menggunakan langkah-langkah berikut untuk mengaktifkan kontrol dalam satu akun dan Wilayah.

Security Hub CSPM console

Untuk mengaktifkan kontrol lintas standar dalam satu akun dan Wilayah

1. Buka konsol AWS Security Hub Cloud Security Posture Management (CSPM) di <https://console.aws.amazon.com/securityhub/>
2. Pilih Kontrol dari panel navigasi.
3. Pilih tab Dinonaktifkan.
4. Pilih opsi di sebelah kontrol.
5. Pilih Aktifkan Kontrol (opsi ini tidak muncul untuk kontrol yang sudah diaktifkan).
6. Ulangi di setiap Wilayah di mana Anda ingin mengaktifkan kontrol.

Security Hub CSPM API

Untuk mengaktifkan kontrol lintas standar dalam satu akun dan Wilayah

1. Memanggil [ListStandardsControlAssociations](#) API. Berikan ID kontrol keamanan.

Contoh permintaan:

```
{
  "SecurityControlId": "IAM.1"
}
```

2. Memanggil [BatchUpdateStandardsControlAssociations](#) API. Berikan Nama Sumber Daya Amazon (ARN) dari standar apa pun yang kontrol tidak diaktifkan. Untuk mendapatkan standar ARNs, jalankan [DescribeStandards](#).
3. Atur `AssociationStatus` parameter sama dengan `ENABLED`. Jika Anda mengikuti langkah-langkah ini untuk kontrol yang sudah diaktifkan, API akan mengembalikan respons kode status HTTP 200.

Contoh permintaan:

```
{
  "StandardsControlAssociationUpdates": [{"SecurityControlId": "IAM.1",
    "StandardsArn": "arn:aws:securityhub::ruleset/cis-aws-foundations-benchmark/v/1.2.0", "AssociationStatus": "ENABLED"}, {"SecurityControlId": "IAM.1",
    "StandardsArn": "arn:aws:securityhub::standards/aws-foundational-security-best-practices/v/1.0.0", "AssociationStatus": "ENABLED"}]
}
```

4. Ulangi di setiap Wilayah di mana Anda ingin mengaktifkan kontrol.

AWS CLI

Untuk mengaktifkan kontrol lintas standar dalam satu akun dan Wilayah

1. Jalankan perintah [list-standards-control-associations](#). Berikan ID kontrol keamanan.

```
aws securityhub --region us-east-1 list-standards-control-associations --
security-control-id CloudTrail.1
```

2. Jalankan perintah [batch-update-standards-control-associations](#). Berikan Nama Sumber Daya Amazon (ARN) dari standar apa pun yang kontrol tidak diaktifkan. Untuk mendapatkan standar ARNs, jalankan `describe-standards` perintah.
3. Atur `AssociationStatus` parameter sama dengan `ENABLED`. Jika Anda mengikuti langkah-langkah ini untuk kontrol yang sudah diaktifkan, perintah akan mengembalikan respons kode status HTTP 200.

```
aws securityhub --region us-east-1 batch-update-standards-control-associations
--standards-control-association-updates '[{"SecurityControlId": "CloudTrail.1",
"StandardsArn": "arn:aws:securityhub::ruleset/cis-aws-foundations-benchmark/v/1.2.0", "AssociationStatus": "ENABLED"}, {"SecurityControlId": "CloudTrail.1",
"StandardsArn": "arn:aws:securityhub::standards/cis-aws-foundations-benchmark/v/1.4.0", "AssociationStatus": "ENABLED"}]'
```

4. Ulangi di setiap Wilayah di mana Anda ingin mengaktifkan kontrol.

Mengaktifkan kontrol dalam standar tertentu

Saat Anda mengaktifkan standar di AWS Security Hub Cloud Security Posture Management (CSPM), semua kontrol yang berlaku akan diaktifkan secara otomatis dalam standar tersebut (pengecualian untuk ini adalah standar yang dikelola layanan). Anda kemudian dapat menonaktifkan dan mengaktifkan kembali kontrol tertentu dalam standar. Namun, kami menyarankan untuk menyelaraskan status pemberdayaan kontrol di semua standar yang Anda aktifkan. Untuk petunjuk tentang mengaktifkan kontrol di semua standar, lihat [Mengaktifkan kontrol lintas standar](#).

Halaman detail untuk standar berisi daftar kontrol yang berlaku untuk standar, dan informasi tentang kontrol mana yang saat ini diaktifkan dan dinonaktifkan dalam standar tersebut.

Pada halaman detail standar, Anda juga dapat mengaktifkan kontrol dalam standar tertentu. Anda harus mengaktifkan kontrol dalam standar tertentu secara terpisah di masing-masing Akun AWS dan Wilayah AWS. Ketika Anda mengaktifkan kontrol dalam standar tertentu, itu hanya memengaruhi akun saat ini dan Wilayah.

Untuk mengaktifkan kontrol dalam standar, Anda harus terlebih dahulu mengaktifkan setidaknya satu standar yang berlaku kontrol. Untuk petunjuk tentang mengaktifkan standar, lihat [Mengaktifkan standar keamanan](#). Ketika Anda mengaktifkan kontrol dalam satu atau beberapa standar, Security Hub CSPM mulai menghasilkan temuan untuk kontrol tersebut. Security Hub CSPM mencakup [status kontrol](#) dalam perhitungan skor keamanan keseluruhan dan skor keamanan standar. Bahkan jika Anda mengaktifkan kontrol dalam beberapa standar, Anda akan menerima satu temuan per pemeriksaan keamanan di seluruh standar jika Anda mengaktifkan temuan kontrol konsolidasi. Untuk informasi lebih lanjut, lihat [Temuan kontrol konsolidasi](#).

Untuk mengaktifkan kontrol dalam standar, kontrol harus tersedia di Wilayah Anda saat ini. Untuk informasi selengkapnya, lihat [Ketersediaan kontrol menurut Wilayah](#).

Ikuti langkah-langkah ini untuk mengaktifkan kontrol CSPM Security Hub dalam standar tertentu. Sebagai pengganti langkah-langkah berikut, Anda juga dapat menggunakan tindakan [UpdateStandardsControl](#) API untuk mengaktifkan kontrol dalam standar tertentu. Untuk petunjuk tentang mengaktifkan kontrol di semua standar, lihat [Pemberdayaan lintas standar dalam satu akun dan Wilayah](#).

Security Hub CSPM console

Untuk mengaktifkan kontrol dalam standar tertentu

1. Buka konsol AWS Security Hub Cloud Security Posture Management (CSPM) di <https://console.aws.amazon.com/securityhub/>
2. Pilih Standar keamanan dari panel navigasi.
3. Pilih Lihat hasil untuk standar yang relevan.
4. Pilih kontrol.
5. Pilih Aktifkan Kontrol (opsi ini tidak muncul untuk kontrol yang sudah diaktifkan). Konfirmasikan dengan memilih Aktifkan.

Security Hub CSPM API

Untuk mengaktifkan kontrol dalam standar tertentu

1. Jalankan [ListSecurityControlDefinitions](#), dan berikan ARN standar untuk mendapatkan daftar kontrol yang tersedia untuk standar tertentu. Untuk mendapatkan ARN standar, jalankan [DescribeStandards](#) API ini mengembalikan kontrol keamanan agnostik standar, bukan kontrol IDs khusus standar. IDs

Contoh permintaan:

```
{
  "StandardsArn": "arn:aws:securityhub:::standards/aws-foundational-security-best-practices/v/1.0.0"
}
```

2. Jalankan [ListStandardsControlAssociations](#), dan berikan ID kontrol khusus untuk mengembalikan status pengaktifan kontrol saat ini di setiap standar.

Contoh permintaan:

```
{
  "SecurityControlId": "IAM.1"
}
```

3. Jalankan [BatchUpdateStandardsControlAssociations](#). Berikan ARN standar yang ingin Anda aktifkan kontrolnya.

4. Atur `AssociationStatus` parameter sama dengan `ENABLED`.

Contoh permintaan:

```
{
  "StandardsControlAssociationUpdates": [{"SecurityControlId": "IAM.1",
    "StandardsArn": "arn:aws:securityhub::ruleset/cis-aws-foundations-benchmark/v/1.2.0", "AssociationStatus": "ENABLED"}]
}
```

AWS CLI

Untuk mengaktifkan kontrol dalam standar tertentu

1. Jalankan [list-security-control-definitions](#) perintah, dan berikan ARN standar untuk mendapatkan daftar kontrol yang tersedia untuk standar tertentu. Untuk mendapatkan ARN standar, jalankan `describe-standards` Perintah ini mengembalikan kontrol keamanan agnostik standar, bukan kontrol IDs khusus standar. IDs

```
aws securityhub --region us-east-1 list-security-control-definitions --
standards-arn "arn:aws:securityhub:us-east-1::standards/aws-foundational-
security-best-practices/v/1.0.0"
```

2. Jalankan [list-standards-control-associations](#) perintah, dan berikan ID kontrol khusus untuk mengembalikan status pengaktifan kontrol saat ini di setiap standar.

```
aws securityhub --region us-east-1 list-standards-control-associations --
security-control-id CloudTrail.1
```

3. Jalankan perintah [batch-update-standards-control-associations](#). Berikan ARN standar yang ingin Anda aktifkan kontrolnya.
4. Atur `AssociationStatus` parameter sama dengan `ENABLED`.

```
aws securityhub --region us-east-1 batch-update-standards-control-associations
--standards-control-association-updates '[{"SecurityControlId": "CloudTrail.1",
  "StandardsArn": "arn:aws:securityhub:us-east-1::standards/aws-foundational-
security-best-practices/v/1.0.0", "AssociationStatus": "ENABLED"}]'
```


Mengaktifkan kontrol baru dalam standar yang diaktifkan secara otomatis

AWS Security Hub Cloud Security Posture Management (CSPM) secara teratur merilis kontrol baru dan menambahkannya ke satu atau lebih standar. Anda dapat memilih apakah akan mengaktifkan kontrol baru secara otomatis dalam standar yang diaktifkan.

Sebaiknya gunakan konfigurasi pusat CSPM Security Hub untuk mengaktifkan kontrol keamanan baru secara otomatis. Anda dapat membuat kebijakan konfigurasi yang menyertakan daftar kontrol yang akan dinonaktifkan di seluruh standar. Semua kontrol lainnya, termasuk yang baru dirilis, diaktifkan secara default. Atau, Anda dapat membuat kebijakan yang menyertakan daftar kontrol yang akan diaktifkan di seluruh standar. Semua kontrol lainnya, termasuk yang baru dirilis, dinonaktifkan secara default. Untuk informasi selengkapnya, lihat [Memahami konfigurasi pusat di Security Hub CSPM](#).

Security Hub CSPM tidak mengaktifkan kontrol baru saat ditambahkan ke standar yang belum Anda aktifkan.

Petunjuk berikut hanya berlaku jika Anda tidak menggunakan konfigurasi pusat.

Pilih metode akses pilihan Anda, dan ikuti langkah-langkah untuk mengaktifkan kontrol baru secara otomatis dalam standar yang diaktifkan.

Note

Saat Anda mengaktifkan kontrol baru secara otomatis menggunakan petunjuk berikut, Anda dapat berinteraksi dengan kontrol di konsol dan secara terprogram segera setelah rilis. Namun, kontrol yang diaktifkan secara otomatis memiliki status default sementara Dinonaktifkan. Diperlukan waktu hingga beberapa hari untuk Security Hub CSPM untuk memproses rilis kontrol dan menetapkan kontrol sebagai Diaktifkan di akun Anda. Selama periode pemrosesan, Anda dapat mengaktifkan atau menonaktifkan kontrol secara manual, dan Security Hub CSPM akan mempertahankan penunjukan itu terlepas dari apakah Anda mengaktifkan kontrol otomatis diaktifkan.

Security Hub CSPM console

Untuk mengaktifkan kontrol baru secara otomatis

1. Buka konsol AWS Security Hub Cloud Security Posture Management (CSPM) di. <https://console.aws.amazon.com/securityhub/>

2. Di panel navigasi, pilih Pengaturan, lalu pilih tab Umum.
3. Di bawah Kontrol, pilih Edit.
4. Aktifkan Aktifkan otomatis kontrol baru dalam standar yang diaktifkan.
5. Pilih Simpan.

Security Hub CSPM API

Untuk mengaktifkan kontrol baru secara otomatis

1. Jalankan [UpdateSecurityHubConfiguration](#).
2. Untuk mengaktifkan kontrol baru secara otomatis untuk standar yang diaktifkan, setel `AutoEnableControls` ke `true`. Jika Anda tidak ingin mengaktifkan kontrol baru secara otomatis, setel `AutoEnableControls` ke `false`.

AWS CLI

Untuk mengaktifkan kontrol baru secara otomatis

1. Jalankan perintah [update-security-hub-configuration](#).
2. Untuk mengaktifkan kontrol baru secara otomatis untuk standar yang diaktifkan, tentukan `--auto-enable-controls`. Jika Anda tidak ingin mengaktifkan kontrol baru secara otomatis, tentukan `--no-auto-enable-controls`.

```
aws securityhub update-security-hub-configuration --auto-enable-controls | --no-auto-enable-controls
```

Contoh perintah

```
aws securityhub update-security-hub-configuration --auto-enable-controls
```

Jika Anda tidak secara otomatis mengaktifkan kontrol baru, maka Anda harus mengaktifkannya secara manual. Untuk petunjuk, lihat [Mengaktifkan kontrol di Security Hub CSPM](#).

Menonaktifkan kontrol di Security Hub CSPM

Untuk mengurangi kebisingan temuan, akan sangat membantu untuk menonaktifkan kontrol yang tidak relevan dengan lingkungan Anda. Di AWS Security Hub Cloud Security Posture Management (CSPM), Anda dapat menonaktifkan kontrol di semua standar keamanan atau hanya untuk standar tertentu.

Jika Anda menonaktifkan kontrol di semua standar, hal berikut terjadi:

- Pemeriksaan keamanan untuk kontrol tidak lagi dilakukan.
- Tidak ada temuan tambahan yang dihasilkan untuk kontrol.
- Temuan yang ada untuk kontrol diarsipkan secara otomatis, biasanya dalam 3-5 hari dengan upaya terbaik.
- Security Hub CSPM menghapus AWS Config aturan terkait yang dibuat untuk kontrol.

Jika Anda menonaktifkan kontrol hanya untuk standar tertentu, Security Hub CSPM berhenti menjalankan pemeriksaan keamanan untuk kontrol hanya untuk standar tersebut. Ini juga menghilangkan kontrol [dari perhitungan skor keamanan](#) untuk masing-masing standar tersebut. Jika kontrol diaktifkan dalam standar lain, Security Hub CSPM mempertahankan AWS Config aturan terkait, jika berlaku, dan terus menjalankan pemeriksaan keamanan untuk kontrol untuk standar lainnya. Security Hub CSPM juga menyertakan kontrol saat menghitung skor keamanan untuk masing-masing standar lainnya, yang memengaruhi skor keamanan ringkasan Anda.

Jika Anda menonaktifkan standar, semua kontrol yang berlaku untuk standar dinonaktifkan secara otomatis untuk standar itu. Namun, kontrol mungkin terus diaktifkan dalam standar lain. Saat Anda menonaktifkan standar, Security Hub CSPM tidak melacak kontrol mana yang dinonaktifkan untuk standar tersebut. Akibatnya, jika nanti Anda mengaktifkan kembali standar yang sama, semua kontrol yang berlaku padanya diaktifkan secara otomatis. Untuk informasi tentang menonaktifkan standar, lihat [Menonaktifkan standar](#).

Menonaktifkan kontrol bukanlah tindakan permanen. Misalkan Anda menonaktifkan kontrol, dan kemudian mengaktifkan standar yang mencakup kontrol. Kontrol kemudian diaktifkan untuk standar itu. Saat Anda mengaktifkan standar di Security Hub CSPM, semua kontrol yang berlaku untuk standar tersebut akan diaktifkan secara otomatis. Untuk informasi tentang mengaktifkan standar, lihat [Mengaktifkan standar](#).

Topik

- [Menonaktifkan kontrol lintas standar](#)
- [Menonaktifkan kontrol dalam standar tertentu](#)
- [Kontrol yang disarankan untuk dinonaktifkan di CSPM Security Hub](#)

Menonaktifkan kontrol lintas standar

Sebaiknya nonaktifkan kontrol AWS Security Hub Cloud Security Posture Management (CSPM) di seluruh standar untuk menjaga keselarasan di seluruh organisasi Anda. Jika Anda menonaktifkan kontrol hanya dalam standar tertentu, Anda terus menerima temuan untuk kontrol jika diaktifkan dalam standar lain.

Penonaktifan lintas standar di beberapa akun dan Wilayah

Untuk menonaktifkan kontrol keamanan di beberapa Akun AWS dan Wilayah AWS, Anda harus menggunakan [konfigurasi pusat](#).

Bila Anda menggunakan konfigurasi pusat, administrator yang didelegasikan dapat membuat kebijakan konfigurasi CSPM Security Hub yang menonaktifkan kontrol tertentu di seluruh standar yang diaktifkan. Anda kemudian dapat mengaitkan kebijakan konfigurasi dengan akun tertentu OUs,, atau root. Kebijakan konfigurasi berlaku di Wilayah asal Anda (juga disebut Wilayah agregasi) dan semua Wilayah yang ditautkan.

Kebijakan konfigurasi menawarkan kustomisasi. Misalnya, Anda dapat memilih untuk menonaktifkan semua AWS CloudTrail kontrol dalam satu OU, dan Anda dapat memilih untuk menonaktifkan semua kontrol IAM di OU lain. Tingkat perincian tergantung pada tujuan yang Anda maksudkan untuk cakupan keamanan di organisasi Anda. Untuk petunjuk cara membuat kebijakan konfigurasi yang menonaktifkan kontrol tertentu di seluruh standar, lihat [Membuat dan mengaitkan kebijakan konfigurasi](#).

Note

Administrator yang didelegasikan dapat membuat kebijakan konfigurasi untuk mengelola kontrol di semua standar kecuali Standar [yang Dikelola Layanan](#):. AWS Control Tower Kontrol untuk standar ini harus dikonfigurasi dalam AWS Control Tower layanan.

Jika Anda ingin beberapa akun mengonfigurasi kontrolnya sendiri daripada administrator yang didelegasikan, administrator yang didelegasikan dapat menetapkan akun tersebut sebagai dikelola sendiri. Akun yang dikelola sendiri harus mengonfigurasi kontrol secara terpisah di setiap Wilayah.

Penonaktifan lintas standar dalam satu akun dan Wilayah

Jika Anda tidak menggunakan konfigurasi pusat atau akun yang dikelola sendiri, Anda tidak dapat menggunakan kebijakan konfigurasi untuk menonaktifkan kontrol secara terpusat di beberapa akun dan Wilayah. Namun, Anda dapat menonaktifkan kontrol dalam satu akun dan Wilayah.

Security Hub CSPM console

Untuk menonaktifkan kontrol di seluruh standar dalam satu akun dan Wilayah

1. Buka konsol AWS Security Hub Cloud Security Posture Management (CSPM) di <https://console.aws.amazon.com/securityhub/>
2. Pilih Kontrol dari panel navigasi.
3. Pilih opsi di sebelah kontrol.
4. Pilih Nonaktifkan Kontrol. Opsi ini tidak muncul untuk kontrol yang sudah dinonaktifkan.
5. Pilih alasan untuk menonaktifkan kontrol, dan konfirmasi dengan memilih Nonaktifkan.
6. Ulangi di setiap Wilayah di mana Anda ingin menonaktifkan kontrol.

Security Hub CSPM API

Untuk menonaktifkan kontrol di seluruh standar dalam satu akun dan Wilayah

1. Memanggil [ListStandardsControlAssociations](#) API. Berikan ID kontrol keamanan.

Contoh permintaan:

```
{
  "SecurityControlId": "IAM.1"
}
```

2. Memanggil [BatchUpdateStandardsControlAssociations](#) API. Berikan ARN dari standar apa pun tempat kontrol diaktifkan. Untuk mendapatkan standar ARNs, jalankan [DescribeStandards](#).

3. Atur `AssociationStatus` parameter sama dengan `DISABLED`. Jika Anda mengikuti langkah-langkah ini untuk kontrol yang sudah dinonaktifkan, API akan mengembalikan respons kode status HTTP 200.

Contoh permintaan:

```
{
  "StandardsControlAssociationUpdates": [{
    "SecurityControlId": "IAM.1",
    "StandardsArn": "arn:aws:securityhub::ruleset/cis-aws-foundations-benchmark/v/1.2.0",
    "AssociationStatus": "DISABLED",
    "UpdatedReason": "Not applicable to environment"
  }, {
    "SecurityControlId": "IAM.1",
    "StandardsArn": "arn:aws:securityhub::standards/aws-foundational-security-best-practices/v/1.0.0",
    "AssociationStatus": "DISABLED",
    "UpdatedReason": "Not applicable to environment"
  }]
}
```

4. Ulangi di setiap Wilayah di mana Anda ingin menonaktifkan kontrol.

AWS CLI

Untuk menonaktifkan kontrol di seluruh standar dalam satu akun dan Wilayah

1. Jalankan perintah [list-standards-control-associations](#). Berikan ID kontrol keamanan.

```
aws securityhub --region us-east-1 list-standards-control-associations --
security-control-id CloudTrail.1
```

2. Jalankan perintah [batch-update-standards-control-associations](#). Berikan ARN dari standar apa pun tempat kontrol diaktifkan. Untuk mendapatkan standar ARNs, jalankan `describe-standards` perintah.
3. Atur `AssociationStatus` parameter sama dengan `DISABLED`. Jika Anda mengikuti langkah-langkah ini untuk kontrol yang sudah dinonaktifkan, perintah akan mengembalikan respons kode status HTTP 200.

```
aws securityhub --region us-east-1 batch-update-standards-control-associations
--standards-control-association-updates '[{"SecurityControlId": "CloudTrail.1",
"StandardsArn": "arn:aws:securityhub::ruleset/cis-aws-foundations-benchmark/
v/1.2.0", "AssociationStatus": "DISABLED", "UpdatedReason": "Not applicable
to environment"}, {"SecurityControlId": "CloudTrail.1", "StandardsArn":
"arn:aws:securityhub::standards/cis-aws-foundations-benchmark/v/1.4.0",
```

```
"AssociationStatus": "DISABLED", "UpdatedReason": "Not applicable to environment"]}]'
```

4. Ulangi di setiap Wilayah di mana Anda ingin menonaktifkan kontrol.

Menonaktifkan kontrol dalam standar tertentu

Anda dapat menonaktifkan kontrol hanya dalam standar keamanan tertentu, bukan di semua standar. Jika kontrol berlaku untuk standar lain yang diaktifkan, AWS Security Hub Cloud Security Posture Management (CSPM) terus menjalankan pemeriksaan keamanan untuk kontrol dan Anda terus menerima temuan untuk kontrol.

Kami merekomendasikan untuk menyelaraskan status pemberdayaan kontrol di semua standar yang diaktifkan yang berlaku untuk kontrol. Untuk informasi tentang menonaktifkan kontrol di semua standar yang berlaku, lihat [Menonaktifkan kontrol lintas standar](#)

Pada halaman detail standar, Anda juga dapat menonaktifkan kontrol dalam standar tertentu. Anda harus menonaktifkan kontrol dalam standar tertentu secara terpisah di masing-masing Akun AWS dan Wilayah AWS. Ketika Anda menonaktifkan kontrol dalam standar tertentu, itu hanya memengaruhi akun saat ini dan Wilayah.

Pilih metode pilihan Anda, dan ikuti langkah-langkah ini untuk menonaktifkan kontrol dalam satu atau lebih standar spesifik.

Security Hub CSPM console

Untuk menonaktifkan kontrol dalam standar tertentu

1. Buka konsol AWS Security Hub Cloud Security Posture Management (CSPM) di <https://console.aws.amazon.com/securityhub/>
2. Pilih Standar keamanan dari panel navigasi. Pilih Lihat hasil untuk standar yang relevan.
3. Pilih kontrol.
4. Pilih Nonaktifkan Kontrol. Opsi ini tidak muncul untuk kontrol yang sudah dinonaktifkan.
5. Berikan alasan untuk menonaktifkan kontrol, dan konfirmasi dengan memilih Nonaktifkan.

Security Hub CSPM API

Untuk menonaktifkan kontrol dalam standar tertentu

1. Jalankan [ListSecurityControlDefinitions](#), dan berikan ARN standar untuk mendapatkan daftar kontrol yang tersedia untuk standar tertentu. Untuk mendapatkan ARN standar, jalankan [DescribeStandards](#) API ini mengembalikan kontrol keamanan agnostik standar, bukan kontrol IDs khusus standar. IDs

Contoh permintaan:

```
{
  "StandardsArn": "arn:aws:securityhub::standards/aws-foundational-security-best-practices/v/1.0.0"
}
```

2. Jalankan [ListStandardsControlAssociations](#), dan berikan ID kontrol khusus untuk mengembalikan status pengaktifan kontrol saat ini di setiap standar.

Contoh permintaan:

```
{
  "SecurityControlId": "IAM.1"
}
```

3. Jalankan [BatchUpdateStandardsControlAssociations](#). Berikan ARN standar di mana Anda ingin menonaktifkan kontrol.
4. Atur AssociationStatus parameter sama dengan DISABLED. Jika Anda mengikuti langkah-langkah ini untuk kontrol yang sudah dinonaktifkan, API akan mengembalikan respons kode status HTTP 200.

Contoh permintaan:

```
{
  "StandardsControlAssociationUpdates": [{"SecurityControlId": "IAM.1",
    "StandardsArn": "arn:aws:securityhub::ruleset/cis-aws-foundations-benchmark/v/1.2.0", "AssociationStatus": "DISABLED", "UpdatedReason": "Not applicable to environment"}]
}
```


AWS CLI

Untuk menonaktifkan kontrol dalam standar tertentu

1. Jalankan [list-security-control-definitions](#) perintah, dan berikan ARN standar untuk mendapatkan daftar kontrol yang tersedia untuk standar tertentu. Untuk mendapatkan ARN standar, jalankan. `describe-standards` Perintah ini mengembalikan kontrol keamanan agnostik standar, bukan kontrol IDs khusus standar. IDs

```
aws securityhub --region us-east-1 list-security-control-definitions --  
standards-arn "arn:aws:securityhub:us-east-1::standards/aws-foundational-  
security-best-practices/v/1.0.0"
```

2. Jalankan [list-standards-control-associations](#) perintah, dan berikan ID kontrol khusus untuk mengembalikan status pengaktifan kontrol saat ini di setiap standar.

```
aws securityhub --region us-east-1 list-standards-control-associations --  
security-control-id CloudTrail.1
```

3. Jalankan perintah [batch-update-standards-control-associations](#). Berikan ARN standar di mana Anda ingin menonaktifkan kontrol.
4. Atur `AssociationStatus` parameter sama dengan `DISABLED`. Jika Anda mengikuti langkah-langkah ini untuk kontrol yang sudah diaktifkan, perintah akan mengembalikan respons kode status HTTP 200.

```
aws securityhub --region us-east-1 batch-update-standards-control-  
associations --standards-control-association-updates '[{"SecurityControlId":  
"CloudTrail.1", "StandardsArn": "arn:aws:securityhub:us-east-1::standards/aws-  
foundational-security-best-practices/v/1.0.0", "AssociationStatus": "DISABLED",  
"UpdatedReason": "Not applicable to environment"}]'
```

Kontrol yang disarankan untuk dinonaktifkan di CSPM Security Hub

Kami merekomendasikan untuk menonaktifkan beberapa kontrol AWS Security Hub Cloud Security Posture Management (CSPM) Security Hub untuk mengurangi kebisingan dan biaya penggunaan.

Kontrol yang menggunakan sumber daya global

Beberapa Layanan AWS mendukung sumber daya global, yang berarti Anda dapat mengakses sumber daya dari mana pun Wilayah AWS. Untuk menghemat biaya AWS Config, Anda dapat menonaktifkan perekaman sumber daya global di semua kecuali satu Wilayah. Namun, setelah Anda melakukan ini, Security Hub CSPM masih menjalankan pemeriksaan keamanan di semua Wilayah di mana kontrol diaktifkan dan menagih Anda berdasarkan jumlah cek per akun per Wilayah. Dengan demikian, untuk mengurangi kebisingan dan menghemat biaya CSPM Security Hub, Anda juga harus menonaktifkan kontrol yang melibatkan sumber daya global di semua Wilayah kecuali Wilayah yang mencatat sumber daya global.

Jika kontrol melibatkan sumber daya global tetapi hanya tersedia di satu Wilayah, menonaktifkannya di Wilayah tersebut mencegah Anda mendapatkan temuan apa pun untuk sumber daya yang mendasarinya. Dalam hal ini, kami sarankan untuk tetap mengaktifkan kontrol. Saat menggunakan agregasi lintas wilayah, Wilayah di mana kontrol tersedia harus merupakan Wilayah agregasi atau salah satu Wilayah yang ditautkan. Kontrol berikut melibatkan sumber daya global tetapi hanya tersedia di satu Wilayah:

- Semua CloudFront kontrol - Hanya tersedia di Wilayah AS Timur (Virginia N.)
- GlobalAccelerator.1 — Hanya tersedia di Wilayah AS Barat (Oregon)
- Route53.2 - Hanya tersedia di Wilayah AS Timur (Virginia N.)
- WAF.1, WAF.6, WAF.7, WAF.8 - Hanya tersedia di Wilayah AS Timur (Virginia N.)

Note

Jika Anda menggunakan konfigurasi pusat, Security Hub CSPM secara otomatis menonaktifkan kontrol yang melibatkan sumber daya global di semua Wilayah kecuali Wilayah asal. Kontrol lain yang Anda pilih untuk diaktifkan meskipun kebijakan konfigurasi diaktifkan di semua Wilayah yang tersedia. Untuk membatasi temuan untuk kontrol ini hanya pada satu Wilayah, Anda dapat memperbarui pengaturan AWS Config perekam dan menonaktifkan perekaman sumber daya global di semua Wilayah kecuali Wilayah asal. Jika kontrol yang diaktifkan yang melibatkan sumber daya global tidak didukung di Wilayah asal, CSPM Security Hub mencoba mengaktifkan kontrol di satu Wilayah tertaut di mana kontrol didukung. Dengan konfigurasi pusat, Anda tidak memiliki cakupan untuk kontrol yang tidak tersedia di Wilayah asal atau Wilayah yang ditautkan.

Untuk informasi selengkapnya tentang konfigurasi pusat, lihat [Memahami konfigurasi pusat di Security Hub CSPM](#).

Untuk kontrol yang memiliki jenis jadwal periodik, menonaktifkannya di Security Hub CSPM diperlukan untuk mencegah penagihan. Menyetel AWS Config parameter `includeGlobalResourceTypes` ke `false` tidak memengaruhi kontrol CSPM Security Hub berkala.

Kontrol CSPM Security Hub berikut menggunakan sumber daya global:

- [\[Akun.1\] Informasi kontak keamanan harus disediakan untuk Akun AWS](#)
- [\[Akun.2\] Akun AWS harus menjadi bagian dari organisasi AWS Organizations](#)
- [\[CloudFront.1\] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi](#)
- [\[CloudFront.3\] CloudFront distribusi harus memerlukan enkripsi dalam perjalanan](#)
- [\[CloudFront.4\] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi](#)
- [\[CloudFront.5\] CloudFront distribusi seharusnya mengaktifkan logging](#)
- [\[CloudFront.6\] CloudFront distribusi harus mengaktifkan WAF](#)
- [\[CloudFront.7\] CloudFront distribusi harus menggunakan sertifikat SSL/TLS khusus](#)
- [\[CloudFront.8\] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS](#)
- [\[CloudFront.9\] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus](#)
- [\[CloudFront.10\] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal kustom](#)
- [\[CloudFront.12\] CloudFront distribusi seharusnya tidak menunjukkan asal S3 yang tidak ada](#)
- [\[CloudFront.13\] CloudFront distribusi harus menggunakan kontrol akses asal](#)
- [\[GlobalAccelerator.1\] Akselerator Akselerator Global harus diberi tag](#)
- [\[IAM.1\] Kebijakan IAM seharusnya tidak mengizinkan hak administratif “*” penuh](#)
- [\[IAM.2\] Pengguna IAM seharusnya tidak memiliki kebijakan IAM yang dilampirkan](#)
- [\[IAM.3\] Kunci akses pengguna IAM harus diputar setiap 90 hari atau kurang](#)
- [\[IAM.4\] Kunci akses pengguna root IAM seharusnya tidak ada](#)
- [\[IAM.5\] MFA harus diaktifkan untuk semua pengguna IAM yang memiliki kata sandi konsol](#)
- [\[IAM.6\] MFA perangkat keras harus diaktifkan untuk pengguna root](#)

- [\[IAM.7\] Kebijakan kata sandi untuk pengguna IAM harus memiliki konfigurasi yang kuat](#)
- [\[IAM.8\] Kredensi pengguna IAM yang tidak digunakan harus dihapus](#)
- [\[IAM.9\] MFA harus diaktifkan untuk pengguna root](#)
- [\[IAM.10\] Kebijakan kata sandi untuk pengguna IAM harus memiliki konfigurasi yang kuat](#)
- [\[IAM.11\] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu huruf besar](#)
- [\[IAM.12\] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu huruf kecil](#)
- [\[IAM.13\] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu simbol](#)
- [\[IAM.14\] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu nomor](#)
- [\[IAM.15\] Pastikan kebijakan kata sandi IAM membutuhkan panjang kata sandi minimum 14 atau lebih](#)
- [\[IAM.16\] Pastikan kebijakan kata sandi IAM mencegah penggunaan kembali kata sandi](#)
- [\[IAM.17\] Pastikan kebijakan kata sandi IAM kedaluwarsa kata sandi dalam waktu 90 hari atau kurang](#)
- [\[IAM.18\] Memastikan peran dukungan telah dibuat untuk mengelola insiden dengan AWS Dukungan](#)
- [\[IAM.19\] MFA harus diaktifkan untuk semua pengguna IAM](#)
- [\[IAM.21\] Kebijakan terkelola pelanggan IAM yang Anda buat seharusnya tidak mengizinkan tindakan wildcard untuk layanan](#)
- [\[IAM.22\] Kredensi pengguna IAM yang tidak digunakan selama 45 hari harus dihapus](#)
- [\[IAM.24\] Peran IAM harus ditandai](#)
- [\[IAM.25\] Pengguna IAM harus diberi tag](#)
- [\[IAM.26\] Sertifikat SSL/TLS kedaluwarsa yang dikelola di IAM harus dihapus](#)
- [\[IAM.27\] Identitas IAM seharusnya tidak memiliki kebijakan yang dilampirkan AWSCloudShellFullAccess](#)
- [\[KMS.1\] Kebijakan yang dikelola pelanggan IAM tidak boleh mengizinkan tindakan dekripsi pada semua kunci KMS](#)
- [\[KMS.2\] Prinsipal IAM tidak boleh memiliki kebijakan inline IAM yang memungkinkan tindakan dekripsi pada semua kunci KMS](#)
- [\[Route53.2\] Route 53 zona yang dihosting publik harus mencatat kueri DNS](#)
- [\[WAF.1\] Pencatatan ACL Web Global AWS WAF Klasik harus diaktifkan](#)

- [\[WAF.6\] Aturan global AWS WAF klasik harus memiliki setidaknya satu syarat](#)
- [\[WAF.7\] Kelompok aturan global AWS WAF klasik harus memiliki setidaknya satu aturan](#)
- [\[WAF.8\] Web global AWS WAF klasik ACLs harus memiliki setidaknya satu aturan atau kelompok aturan](#)

CloudTrail kontrol logging

Kontrol ini berkaitan dengan penggunaan AWS Key Management Service (AWS KMS) untuk mengenkripsi log AWS CloudTrail jejak. Jika Anda mencatat jejak ini di akun logging terpusat, Anda harus mengaktifkan kontrol ini hanya di akun dan Wilayah tempat pencatatan terpusat berlangsung.

Note

Jika Anda menggunakan [konfigurasi pusat](#), status pengaktifan kontrol disejajarkan di seluruh Wilayah beranda dan Wilayah yang ditautkan. Anda tidak dapat menonaktifkan kontrol di beberapa Wilayah dan mengaktifkannya di wilayah lain. Dalam hal ini, tekan temuan dari kontrol berikut untuk mengurangi kebisingan temuan.

- [\[CloudTrail.2\] CloudTrail harus mengaktifkan enkripsi saat istirahat](#)

CloudWatch kontrol alarm

Jika Anda lebih suka menggunakan Amazon GuardDuty untuk deteksi anomali daripada CloudWatch alarm Amazon, Anda dapat menonaktifkan kontrol berikut, yang berfokus pada alarm: CloudWatch

- [\[CloudWatch.1\] Filter metrik log dan alarm harus ada untuk penggunaan pengguna “root”](#)
- [\[CloudWatch.2\] Pastikan filter metrik log dan alarm ada untuk panggilan API yang tidak sah](#)
- [\[CloudWatch.3\] Pastikan filter metrik log dan alarm ada untuk login Konsol Manajemen tanpa MFA](#)
- [\[CloudWatch.4\] Pastikan filter metrik log dan alarm ada untuk perubahan kebijakan IAM](#)
- [\[CloudWatch.5\] Pastikan filter metrik log dan alarm ada untuk perubahan CloudTrail konfigurasi](#)
- [\[CloudWatch.6\] Pastikan filter metrik log dan alarm ada untuk kegagalan AWS Management Console otentikasi](#)
- [\[CloudWatch.7\] Pastikan filter metrik log dan alarm ada untuk menonaktifkan atau menjadwalkan penghapusan kunci yang dikelola pelanggan](#)

- [\[CloudWatch.8\]](#) Pastikan filter metrik log dan alarm ada untuk perubahan kebijakan bucket S3
- [\[CloudWatch.9\]](#) Pastikan filter metrik log dan alarm ada untuk perubahan AWS Config konfigurasi
- [\[CloudWatch.10\]](#) Pastikan filter metrik log dan alarm ada untuk perubahan grup keamanan
- [\[CloudWatch.11\]](#) Pastikan filter metrik log dan alarm ada untuk perubahan pada Daftar Kontrol Akses Jaringan (NACL)
- [\[CloudWatch.12\]](#) Pastikan filter metrik log dan alarm ada untuk perubahan pada gateway jaringan
- [\[CloudWatch.13\]](#) Pastikan filter metrik log dan alarm ada untuk perubahan tabel rute
- [\[CloudWatch.14\]](#) Pastikan filter metrik log dan alarm ada untuk perubahan VPC

Memahami pemeriksaan dan skor keamanan di Security Hub CSPM

Untuk setiap kontrol yang Anda aktifkan, AWS Security Hub Cloud Security Posture Management (CSPM) menjalankan pemeriksaan keamanan. Pemeriksaan keamanan menghasilkan temuan yang memberi tahu Anda apakah AWS sumber daya tertentu sesuai dengan aturan yang termasuk dalam kontrol.

Beberapa pemeriksaan berjalan pada jadwal berkala. Pemeriksaan lain hanya berjalan ketika ada perubahan pada status sumber daya. Untuk informasi selengkapnya, lihat [Jadwal untuk menjalankan pemeriksaan keamanan](#).

Banyak pemeriksaan keamanan menggunakan aturan AWS Config terkelola atau kustom untuk menetapkan persyaratan kepatuhan. Untuk menjalankan pemeriksaan ini, Anda harus mengatur AWS Config dan mengaktifkan perekaman sumber daya untuk sumber daya yang diperlukan. Untuk informasi lebih lanjut tentang pengaturan AWS Config, lihat [Mengaktifkan dan mengonfigurasi AWS Config untuk Security Hub CSPM](#). Untuk daftar AWS Config sumber daya yang harus Anda rekam untuk setiap standar, lihat [AWS Config Sumber daya yang diperlukan untuk temuan kontrol](#). Kontrol lain menggunakan fungsi Lambda khusus, yang dikelola oleh Security Hub CSPM dan tidak memerlukan prasyarat apa pun.

Karena Security Hub CSPM menjalankan pemeriksaan keamanan, CSPM menghasilkan temuan dan memberi mereka status kepatuhan. Untuk informasi selengkapnya tentang status kepatuhan, lihat [Mengevaluasi status kepatuhan temuan CSPM Security Hub](#).

Security Hub CSPM menggunakan status kepatuhan temuan kontrol untuk menentukan status kontrol secara keseluruhan. Berdasarkan status kontrol, Security Hub CSPM juga menghitung

skor keamanan di semua kontrol yang diaktifkan dan untuk standar tertentu. Untuk informasi selengkapnya, lihat [the section called “Status kepatuhan dan status kontrol”](#) dan [the section called “Menghitung skor keamanan”](#).

Jika Anda mengaktifkan temuan kontrol konsolidasi, Security Hub CSPM menghasilkan satu temuan bahkan ketika kontrol dikaitkan dengan lebih dari satu standar. Lihat informasi yang lebih lengkap di [Temuan kontrol terkonsolidasi](#).

Topik

- [AWS Config Sumber daya yang diperlukan untuk temuan kontrol](#)
- [Jadwal untuk menjalankan pemeriksaan keamanan](#)
- [Menghasilkan dan memperbarui temuan kontrol](#)
- [Mengevaluasi status kepatuhan dan status kontrol](#)
- [Menghitung skor keamanan](#)

AWS Config Sumber daya yang diperlukan untuk temuan kontrol

Di AWS Security Hub Cloud Security Posture Management (CSPM), beberapa kontrol menggunakan AWS Config aturan terkait layanan yang mendeteksi perubahan konfigurasi dalam sumber daya Anda. AWS Agar CSPM Security Hub menghasilkan temuan akurat untuk kontrol ini, Anda harus mengaktifkan AWS Config dan mengaktifkan perekaman sumber daya. AWS Config Untuk informasi tentang cara Security Hub CSPM menggunakan AWS Config aturan dan cara mengaktifkan dan mengonfigurasi AWS Config, lihat. [Mengaktifkan dan mengonfigurasi AWS Config untuk Security Hub CSPM](#) Untuk informasi rinci tentang perekaman sumber daya, lihat [Bekerja dengan perekam konfigurasi](#) di Panduan AWS Config Pengembang.

Untuk menerima temuan kontrol yang akurat, Anda harus mengaktifkan perekaman AWS Config sumber daya untuk kontrol yang diaktifkan dengan jenis jadwal yang dipicu perubahan. Beberapa kontrol dengan jenis jadwal periodik juga memerlukan perekaman sumber daya. Halaman ini mencantumkan sumber daya yang diperlukan untuk kontrol CSPM Security Hub ini.

Kontrol CSPM Security Hub dapat mengandalkan AWS Config aturan terkelola atau aturan CSPM Security Hub kustom. Pastikan tidak ada kebijakan AWS Identity and Access Management (IAM) atau kebijakan AWS Organizations terkelola yang AWS Config mencegah izin untuk merekam sumber daya Anda. Kontrol CSPM Security Hub mengevaluasi konfigurasi sumber daya secara langsung dan tidak memperhitungkan AWS Organizations kebijakan.

Note

Di Wilayah AWS mana kontrol tidak tersedia, sumber daya yang sesuai tidak tersedia di AWS Config. Untuk daftar batasan ini, lihat [Batas regional pada kontrol CSPM Security Hub](#).

Topik

- [Sumber daya yang diperlukan untuk semua kontrol CSPM Security Hub](#)
- [Sumber daya yang diperlukan untuk standar Praktik Terbaik Keamanan AWS Dasar](#)
- [Sumber daya yang dibutuhkan untuk Tolok Ukur AWS Yayasan CIS](#)
- [Sumber daya yang diperlukan untuk standar NIST SP 800-53 Revisi 5](#)
- [Sumber daya yang diperlukan untuk standar NIST SP 800-171 Revisi 2](#)
- [Sumber daya yang dibutuhkan untuk PCI DSS v3.2.1](#)
- [Sumber daya yang diperlukan untuk standar Penandaan AWS Sumber Daya](#)
- [Sumber daya yang diperlukan untuk standar yang AWS Control Tower dikelola layanan](#)

Sumber daya yang diperlukan untuk semua kontrol CSPM Security Hub

Agar CSPM Security Hub menghasilkan temuan untuk kontrol yang dipicu perubahan yang diaktifkan dan menggunakan AWS Config aturan, Anda harus mencatat jenis sumber daya berikut. AWS Config Tabel ini juga menunjukkan kontrol mana yang mengevaluasi jenis sumber daya tertentu. Sebuah kontrol tunggal dapat mengevaluasi lebih dari satu jenis sumber daya.

Layanan AWS	Jenis sumber daya	Kontrol terkait
AWS Amplify	AWS::Amplify::App	Amplify.1
	AWS::Amplify::Branch	Amplify.2
Amazon API Gateway	AWS::ApiGateway::Stage	APIGateway.1
		APIGateway.2
		APIGateway.3

Layanan AWS	Jenis sumber daya	Kontrol terkait
		APIGateway.4
		APIGateway.5
	AWS::ApiGatewayV2::Stage	APIGateway.1
		APIGateway.9
AWS AppConfig	AWS::AppConfig::Application	AppConfig.1
	AWS::AppConfig::ConfigurationProfile	AppConfig.2
	AWS::AppConfig::Environment	AppConfig.3
	AWS::AppConfig::ExtensionAssociation	AppConfig.4
Amazon AppFlow	AWS::AppFlow::Flow	AppFlow.1
AWS App Runner	AWS::AppRunner::Service	AppRunner.1
	AWS::AppRunner::VpcConnector	AppRunner.2

Layanan AWS	Jenis sumber daya	Kontrol terkait
AWS AppSync	AWS::AppSync::GraphQLApi	AppSync.2 AppSync.4 AppSync.5
	AWS::AppSync::ApiCache	AppSync.1 AppSync.6
AWS Backup	AWS::Backup::BackupPlan	Cadangan.5
	AWS::Backup::BackupVault	Cadangan.3
	AWS::Backup::RecoveryPoint	Backup.1 Backup.2
	AWS::Backup::ReportPlan	Cadangan.4
AWS Batch	AWS::Batch::ComputeEnvironment	Batch.3 Batch.4
	AWS::Batch::JobQueue	Batch.1
	AWS::Batch::SchedulingPolicy	Batch.2

Layanan AWS	Jenis sumber daya	Kontrol terkait
AWS Certificate Manager (ACM)	AWS::ACM::Certificate	ACM.1
		ACM.2
		ACM.3
Amazon Athena	AWS::Athena::DataCatalog	Athena.2
	AWS::Athena::WorkGroup	Athena.3 Athena.4
AWS CloudFormation	AWS::CloudFormation::Stack	CloudFormation.2
Amazon CloudFront	AWS::CloudFront::Distribution	CloudFront.1
		CloudFront.3
		CloudFront.4
		CloudFront.5
		CloudFront.6
		CloudFront.7
		CloudFront.8
		CloudFront.9
		CloudFront.10
		CloudFront.13
		CloudFront.14

Layanan AWS	Jenis sumber daya	Kontrol terkait
AWS CloudTrail	AWS::CloudTrail::Trail	CloudTrail.9
Amazon CloudWatch	AWS::CloudWatch::Alarm	CloudWatch.15 CloudWatch.17
AWS CodeArtifact	AWS::CodeArtifact::Repository	CodeArtifact.1
AWS CodeBuild	AWS::CodeBuild::Project	CodeBuild.1 CodeBuild.2 CodeBuild.3 CodeBuild.4
	AWS::CodeBuild::ReportGroup	CodeBuild.7
Amazon CodeGuru Profiler	AWS::CodeGuruProfiler::ProfilingGroup	CodeGuruProfiler.1
CodeGuru Peninjau Amazon	AWS::CodeGuruReviewer::RepositoryAssociation	CodeGuruReviewer.1
Amazon Cognito	AWS::Cognito::UserPool	Kognito.1

Layanan AWS	Jenis sumber daya	Kontrol terkait
Amazon Connect	AWS::CustomerProfiles::ObjectType	Hubungkan.1
	AWS::Connect::Instance	Hubungkan.2
AWS DataSync	AWS::DataSync::Task	DataSync.1 DataSync.2
Amazon Detective	AWS::Detective::Graph	Detektif.1
AWS Database Migration Service (AWS DMS)	AWS::DMS::Certificate	DMS.2
	AWS::DMS::Endpoint	DMS.9
		DMS.10
		DMS.11
		DMS.12
	AWS::DMS::EventSubscription	DMS.3
	AWS::DMS::ReplicationInstance	DMS.4
		DMS.6
	AWS::DMS::ReplicationSubnetGroup	DMS.5

Layanan AWS	Jenis sumber daya	Kontrol terkait
	AWS::DMS: :ReplicationTask	DMS.7 DMS.8
Amazon DynamoDB	AWS::DynamoDB::Table	DynamoDB.1 DynamoDB.2 DynamoDB.5 DynamoDb.6
Amazon Elastic Compute Cloud () EC2	AWS::EC2: :ClientVpnEndpoint	EC2.51
	AWS::EC2: :CustomerGateway	EC2.36
	AWS::EC2: :DHCPOptions	EC2.174
	AWS::EC2::EIP	EC2.12 EC2.37
		EC2.48

Layanan AWS	Jenis sumber daya	Kontrol terkait
	AWS::EC2: :Instance	EC2.4 EC2.8 EC2.9 EC2.17 EC2.24 EC2.38 EMR.1 SSM.1
	AWS::EC2: :Internet Gateway	EC2.39
	AWS::EC2: :LaunchTe mplate	EC2.25 EC2.170 EC2.175
	AWS::EC2: :NatGateway	EC2.40
	AWS::EC2: :NetworkAcl	EC2.16 EC2.21 EC2.41
	AWS::EC2: :NetworkI nterface	EC2.22 EC2.35

Layanan AWS	Jenis sumber daya	Kontrol terkait
	AWS::EC2: :PrefixList	EC2.176
	AWS::EC2: :RouteTable	EC2.42
	AWS::EC2: :SecurityGroup	EC2.2
		EC2.13
		EC2.14
		EC2.18
		EC2.19
		EC2.43
	AWS::EC2: :SpotFleet	EC2.173
	AWS::EC2: :Subnet	EC2.15
		EC2.44
		ElastiCache.7
	AWS::EC2: :TrafficMirrorFilter	EC2.178
	AWS::EC2: :TrafficMirrorSession	EC2.177
	AWS::EC2: :TrafficMirrorTarget	EC2.179

Layanan AWS	Jenis sumber daya	Kontrol terkait
	AWS::EC2: :TransitG ateway	EC2.23 EC2.52
	AWS::EC2: :TransitG atewayAtt achment	EC2.33
	AWS::EC2: :TransitG atewayRou teTable	EC2.34
	AWS::EC2: :Volume	EC2.3 EC2.45
	AWS::EC2::VPC	EC2.6 EC2.46
	AWS::EC2: :VPCBlock PublicAcc essOptions	EC2.172
	AWS::EC2: :VPCEndpo intService	EC2.47
	AWS::EC2: :VPCPeeri ngConnection	EC2.49

Layanan AWS	Jenis sumber daya	Kontrol terkait
	AWS::EC2: :VPNConnection	EC2.20 EC2.171
	AWS::EC2: :VPNGateway	EC2.50
EC2 Auto Scaling Amazon	AWS::Auto Scaling:: AutoScali ngGroup	AutoScaling.1 AutoScaling.2 AutoScaling.6 AutoScaling.9 AutoScaling.10
	AWS::Auto Scaling:: LaunchCon figuration	AutoScaling.3 Penskalaan otomatis.5
Amazon EC2 Systems Manager (SSM)	AWS::SSM: :Associat ionCompliance	SSM.3
	AWS::SSM: :ManagedI nstanceIn ventory	SSM.1
	AWS::SSM: :PatchCom pliance	SSM.2
Amazon Elastic Container Registry (Amazon ECR)	AWS::ECR: :PublicRe pository	ECR.4

Layanan AWS	Jenis sumber daya	Kontrol terkait
	AWS::ECR: :Repository	ECR.2
		ECR.3
		ECR.5
Amazon Elastic Container Service (Amazon ECS)	AWS::ECS: :Cluster	ECS.12
		ECS.14
	AWS::ECS: :Service	ECS.2
		ECS.10
		ECS.13
	AWS::ECS: :TaskDefinition	ECS.1
		ECS.3
		ECS.4
		DLS.5
		ECS.8
		ECS.9
		ECS.15
	AWS::ECS: :TaskSet	ECS.16
Amazon Elastic File System (Amazon EFS)	AWS::EFS: :AccessPoint	EFS.3
		EFS.4
		EFS.5

Layanan AWS	Jenis sumber daya	Kontrol terkait
	AWS::EFS: :FileSystem	EFS.7 EFS.8
Amazon Elastic Kubernetes Service (Amazon EKS)	AWS::EKS: :Cluster	EKS.2 EKS.6 EKS.8
AWS Elastic Beanstalk	AWS::ElasticBeanstalk::Environment	EKS.7
Penyeimbang Beban Elastis	AWS::ElasticLoadBalancing::LoadBalancer	ElasticBeanstalk.1 ElasticBeanstalk.2 ElasticBeanstalk.3
	AWS::ElasticLoadBalancingV2::Listener	ELB.2 ELB.3 ELB.5 ELB.7 ELB.8 ELB.9 ELB.10 ELB.14
		ELB.17

Layanan AWS	Jenis sumber daya	Kontrol terkait
	AWS::ElasticLoadBalancingV2::LoadBalancer	ELB.1 ELB.4 ELB.5 ELB.6 ELB.12 ELB.13 ELB.16
ElasticSearch	AWS::Elasticsearch::Domain	ES.3 ES.4 ES.5 ES.6 ES.7 ES.8 ES.9
Amazon EMR	AWS::EMR::SecurityConfiguration	EMR.3 EMR.4
Amazon EventBridge	AWS::Events::EventBus	EventBridge.2 EventBridge.3
	AWS::Events::Endpoint	EventBridge.4

Layanan AWS	Jenis sumber daya	Kontrol terkait
Amazon Fraud Detector	AWS::FraudDetector::EntityType	FraudDetector.1
	AWS::FraudDetector::Label	FraudDetector.2
	AWS::FraudDetector::Outcome	FraudDetector.3
	AWS::FraudDetector::Variable	FraudDetector.4
AWS Global Accelerator	AWS::GlobalAccelerator::Accelerator	GlobalAccelerator.1
AWS Glue	AWS::Glue::Job	Lem. 1 Lem.4
	AWS::Glue::MLTransform	Lem.3
Amazon GuardDuty	AWS::GuardDuty::Detector	GuardDuty.4
	AWS::GuardDuty::Filter	GuardDuty.2
	AWS::GuardDuty::IPSet	GuardDuty.3

Layanan AWS	Jenis sumber daya	Kontrol terkait
AWS Identity and Access Management (IAM)	AWS::IAM::Group	IAM.27 KMS.2
	AWS::IAM::Policy	IAM.1 IAM.21 KMS.1
	AWS::IAM::Role	IAM.24 IAM.27 KMS.2
	AWS::IAM::User	IAM.2 IAM.3 IAM.5 IAM.8 IAM.19 IAM.22 IAM.25 IAM.27 KMS.2
AWS Identity and Access Management Access Analyzer	AWS::AccessAnalyzer::Analyzer	IAM.23

Layanan AWS	Jenis sumber daya	Kontrol terkait
Amazon Interactive Video Service (Amazon IVS)	AWS::IVS: :Playback KeyPair	IVS.1
	AWS::IVS: :Recording Configuration	IVS.2
	AWS::IVS: :Channel	IVS.3
AWS IoT	AWS::IoT: :Authorizer	IoT.4
	AWS::IoT: :Dimension	IoT.3
	AWS::IoT: :Mitigation Action	IoT.2
	AWS::IoT: :Policy	IoT.6
	AWS::IoT: :RoleAlias	IoT.5
	AWS::IoT: :Security Profile	IoT.1
AWS IoT Events	AWS::IoTEvents: :AlarmModel	IoTEvents.3

Layanan AWS	Jenis sumber daya	Kontrol terkait
	AWS::IoTEvents::DetectorModel	IoTEvents .2
	AWS::IoTEvents::Input	IoTEvents .1
AWS IoT SiteWise	AWS::IoTSiteWise::AssetModel	IoTSite Bijak.1
	AWS::IoTSiteWise::Dashboard	IoTSite Bijak.2
	AWS::IoTSiteWise::Gateway	IoTSite Bijak.3
	AWS::IoTSiteWise::Portal	IoTSite Bijak.4
	AWS::IoTSiteWise::Project	IoTSite Bijak.5
AWS IoT TwinMaker	AWS::IoTTwinMaker::Entity	TTwinPembuat IoT.4
	AWS::IoTTwinMaker::Scene	TTwinPembuat IoT.3

Layanan AWS	Jenis sumber daya	Kontrol terkait
	AWS::IoT winMaker: :SyncJob	TTwinPembuat Io. 1
	AWS::IoT winMaker: :Workspace	TTwinPembuat Io.2
AWS IoT Wireless	AWS::IoT Wireless:: MulticastGroup	Io TWireless .1
	AWS::IoT Wireless:: ServiceProfile	Io TWireless .2
	AWS::IoT Wireless:: FirmwareTask	Io TWireless .3
Amazon Keyspaces (untuk Apache Cassandra)	AWS::Cass andra::Ke yspace	Ruang kunci.1
Amazon Kinesis	AWS::Kine sis::Stream	Kinesis.1
		Kinesis.2
		Kinesis.3
AWS Key Management Service (AWS KMS)	AWS::KMS::Alias	S3.17
	AWS::KMS::Key	KMS.3
		KMS.5
		S3.17

Layanan AWS	Jenis sumber daya	Kontrol terkait
AWS Lambda	AWS::Lambda::Function	Lambda.1
		Lambda.2
		Lambda.3
		Lambda.5
		Lambda.6
Amazon MSK	AWS::MSK::Cluster	MSK.1
		MSK.2
	AWS::KafkaConnect::Connector	MSK.3
Amazon MQ	AWS::AmazonMQ::Broker	MQ.2
		MQ.3
		MQ.4
		MQ.5
		MQ.6
AWS Network Firewall	AWS::NetworkFirewall::Firewall	NetworkFirewall.1
		NetworkFirewall.7
		NetworkFirewall.9
		NetworkFirewall.10

Layanan AWS	Jenis sumber daya	Kontrol terkait
	AWS::NetworkFirewall::FirewallPolicy	NetworkFirewall.3 NetworkFirewall.4 NetworkFirewall.5 NetworkFirewall.8
	AWS::NetworkFirewall::RuleGroup	NetworkFirewall.6
OpenSearch Layanan Amazon	AWS::OpenSearch::Domain	Opensearch.1 Opensearch.2 Opensearch.3 Opensearch.4 Opensearch.5 Opensearch.6 Opensearch.7 Opensearch.8 Opensearch.9 Opensearch.10 Opensearch.11
AWS Private CA	AWS::ACMPCA::CertificateAuthority	PCA.2

Layanan AWS	Jenis sumber daya	Kontrol terkait
Amazon Relational Database Service (Amazon RDS)	AWS::RDS::DBCluster	DokumenDB.1
		DokumenDB.2
		DokumenDB.4
		DokumenDB.5
		Neptunus.1
		Neptunus.2
		Neptunus.4
		Neptunus.5
		Neptunus.7
		Neptunus.8
		Neptunus.9
		RDS.7
		RDS.12
		RDS.14
		RDS.15
		RDS.16
		RDS.24
		RDS.27
		RDS.28
		RDS.34
		RDS.35

Layanan AWS	Jenis sumber daya	Kontrol terkait
		RDS.37
	AWS::RDS: :DBClusterSnapshot	DokumenDB.3
		Neptunus.3
		Neptunus.6
		RDS.1
		RDS.4
		RDS.29

Layanan AWS	Jenis sumber daya	Kontrol terkait
	AWS::RDS: DBInstance	RDS.2
		RDS.3
		RDS.5
		RDS.6
		RDS.8
		RDS.9
		RDS.10
		RDS.11
		RDS.13
		RDS.17
		RDS.18
		RDS.23
		RDS.25
		RDS.30
		RDS.36
		RDS.40
	AWS::RDS: DBSecurityGroup	RDS.31

Layanan AWS	Jenis sumber daya	Kontrol terkait
	AWS::RDS: :DBSnapshot	RDS.1
		RDS.4
		RDS.32
	AWS::RDS: :DBSubnetGroup	RDS.33
	AWS::RDS: :EventSubscription	RDS.19
		RDS.20
		RDS.21
		RDS.22
Amazon Redshift	AWS::Redshift::Cluster	Pergeseran merah.1 Pergeseran merah.2 Pergeseran merah.3 Pergeseran merah.4 Pergeseran Merah.6 Pergeseran Merah.7 Pergeseran Merah.8 Pergeseran Merah.9 Pergeseran Merah.10 Pergeseran Merah.11

Layanan AWS	Jenis sumber daya	Kontrol terkait
	AWS::Redshift::ClusterParameterGroup	Pergeseran merah.2 Pergeseran Merah.17
	AWS::Redshift::ClusterSnapshot	Pergeseran Merah.13
	AWS::Redshift::ClusterSubnetGroup	Pergeseran Merah.14 Pergeseran Merah.16
	AWS::Redshift::EventSubscription	Pergeseran Merah.12
Amazon Route 53	AWS::Route53::HostedZone	Route53.2
	AWS::Route53::HealthCheck	Route53.1
Amazon Simple Storage Service (Amazon S3)	AWS::S3::AccessPoint	S3.19
	AWS::S3::AccountPublicAccessBlock	S3.2 S3.3

Layanan AWS	Jenis sumber daya	Kontrol terkait
	AWS::S3::Bucket	CloudTrail.6
		CloudTrail.7
		S3.2
		S3.3
		S3.5
		S3.6
		S3.7
		S3.8
		S3.9
		S3.10
		S3.11
		S3.12
		S3.13
		S3.14
		S3.15
		S3.17
		S3.20
	AWS::S3::MultiRegionAccessPoint	S3.24

Layanan AWS	Jenis sumber daya	Kontrol terkait
Amazon SageMaker AI	AWS::SageMaker::AppImageConfig	SageMaker.6
	AWS::SageMaker::Image	SageMaker.7
	AWS::SageMaker::Model	SageMaker.5
	AWS::SageMaker::NotebookInstance	SageMaker.2 SageMaker.3
AWS Secrets Manager	AWS::SecretsManager::Secret	SecretsManager.1
		SecretsManager.2
		SecretsManager.5
AWS Service Catalog	AWS::ServiceCatalog::Portfolio	ServiceCatalog.1
Amazon Simple Email Service (Amazon SES)	AWS::SES::ConfigurationSet	SES.2
	AWS::SES::ContactList	SES.1
Amazon Simple Notification Service (Amazon SNS)	AWS::SNS::Topic	SNS.1
		SNS.3
		SNS.4

Layanan AWS	Jenis sumber daya	Kontrol terkait
Amazon Simple Queue Service (Amazon SQS)	AWS::SQS::Queue	SQS.1
		SQS.2
		SQS.3
AWS Step Functions	AWS::Step Functions::StateMachine	StepFunctions.1
	AWS::Step Functions::Activity	StepFunctions.2
AWS Systems Manager (SSM)	AWS::SSM::Document	SSM.5
AWS Transfer Family	AWS::Transfer::Agreement	Transfer.4
	AWS::Transfer::Certificate	Transfer.5
	AWS::Transfer::Connector	Transfer.3 Transfer.6
	AWS::Transfer::Profile	Transfer.7
	AWS::Transfer::Workflow	Transfer.1
AWS WAF	AWS::WAF::Rule	WAF.6

Layanan AWS	Jenis sumber daya	Kontrol terkait
	AWS::WAF: :RuleGroup	WAF.7
	AWS::WAF: :WebACL	WAF.1 WAF.8
	AWS::WAFRegional::Rule	WAF.2
	AWS::WAFRegional::RuleGroup	WAF.3
	AWS::WAFRegional::WebACL	WAF.4
	AWS::WAFV2::RuleGroup	WAF.12
	AWS::WAFV2::WebACL	WAF.10 WAF.11
Amazon WorkSpaces	AWS::WorkSpaces::Workspace	WorkSpaces.1 WorkSpaces.2

Sumber daya yang diperlukan untuk standar Praktik Terbaik Keamanan AWS Dasar

Agar CSPM Security Hub melaporkan temuan secara akurat untuk kontrol yang dipicu perubahan yang berlaku pada standar Praktik Terbaik Keamanan AWS Dasar (v.1.0.0), diaktifkan, dan menggunakan AWS Config aturan, Anda harus mencatat jenis sumber daya berikut ini. AWS Config Untuk informasi tentang standar ini, lihat [AWS Standar Praktik Terbaik Keamanan Dasar di Security Hub CSPM](#).

Layanan AWS	Jenis sumber daya
Amazon API Gateway	AWS::ApiGateway::Stage , AWS::ApiGatewayV2::Stage
AWS AppSync	AWS::AppSync::ApiCache , AWS::AppSync::GraphQLApi
AWS Backup	AWS::Backup::RecoveryPoint
AWS Certificate Manager (ACM)	AWS::ACM::Certificate
AWS CloudFormation	AWS::CloudFormation::Stack
Amazon CloudFront	AWS::CloudFront::Distribution
AWS CodeBuild	AWS::CodeBuild::Project , AWS::CodeBuild::ReportGroup
Amazon Cognito	AWS::Cognito::UserPool
Amazon Connect	AWS::Connect::Instance
AWS DataSync	AWS::DataSync::Task
AWS Database Migration Service (AWS DMS)	AWS::DMS::Endpoint , AWS::DMS::ReplicationInstance , AWS::DMS::ReplicationTask
Amazon DynamoDB	AWS::DynamoDB::Table
Amazon EC2 Systems Manager (SSM)	AWS::SSM::AssociationCompliance , AWS::SSM::ManagedInstanceInventory , AWS::SSM::PatchCompliance
Amazon Elastic Compute Cloud (Amazon EC2)	AWS::EC2::ClientVpnEndpoint , AWS::EC2::Instance , AWS::EC2::LaunchTemplate , AWS::EC2::NetworkAcl , AWS::EC2::NetworkI

Layanan AWS	Jenis sumber daya
	Interface , AWS::EC2::SecurityGroup , AWS::EC2::SpotFleet , AWS::EC2::Subnet , AWS::EC2::TransitGateway , AWS::EC2::VPCElasticNetworkOptions , AWS::EC2::VPNConnection , AWS::EC2::Volume
EC2 Auto Scaling Amazon	AWS::AutoScaling::AutoScalingGroup , AWS::AutoScaling::LaunchConfiguration
Amazon Elastic Container Registry (Amazon ECR)	AWS::ECR::Repository
Amazon Elastic Container Service (Amazon ECS)	AWS::ECS::Cluster , AWS::ECS::Service , AWS::ECS::TaskDefinition , AWS::ECS::TaskSet
Amazon Elastic File System (Amazon EFS)	AWS::EFS::AccessPoint , AWS::EFS::FileSystem
Amazon Elastic Kubernetes Service (Amazon EKS)	AWS::EKS::Cluster
AWS Elastic Beanstalk	AWS::ElasticBeanstalk::Environment
Penyeimbang Beban Elastis	AWS::ElasticLoadBalancing::LoadBalancer , AWS::ElasticLoadBalancingV2::Listener , AWS::ElasticLoadBalancingV2::LoadBalancer
ElasticSearch	AWS::Elasticsearch::Domain
Amazon EMR	AWS::EMR::SecurityConfiguration

Layanan AWS	Jenis sumber daya
AWS Glue	AWS::Glue::Job , AWS::Glue::MLTransform
AWS Identity and Access Management (IAM)	AWS::IAM::Group , AWS::IAM::Policy , AWS::IAM::Role , AWS::IAM::User
Amazon Kinesis	AWS::Kinesis::Stream
AWS Key Management Service (AWS KMS)	AWS::KMS::Key
AWS Lambda	AWS::Lambda::Function
Amazon Managed Streaming for Apache Kafka (Amazon MSK)	AWS::MSK::Cluster , AWS::KafkaConnect::Connector
AWS Network Firewall	AWS::NetworkFirewall::Firewall , AWS::NetworkFirewall::FirewallPolicy , AWS::NetworkFirewall::RuleGroup
OpenSearch Layanan Amazon	AWS::OpenSearch::Domain
Amazon Relational Database Service (Amazon RDS)	AWS::RDS::DBCluster , AWS::RDS::DBClusterSnapshot , AWS::RDS::DBInstance , AWS::RDS::DBProxy , AWS::RDS::DBSnapshot , AWS::RDS::EventSubscription
Amazon Redshift	AWS::Redshift::Cluster , AWS::Redshift::ClusterSubnetGroup
Amazon Redshift Tanpa Server	AWS::RedshiftServerless::Workgroup
Amazon Route 53	AWS::Route53::HostedZone

Layanan AWS	Jenis sumber daya
Amazon Simple Storage Service (Amazon S3)	AWS::S3::AccessPoint , AWS::S3::AccountPublicAccessBlock , AWS::S3::Bucket , AWS::S3::MultiRegionAccessPoint
Amazon SageMaker AI	AWS::SageMaker::Model , AWS::SageMaker::NotebookInstance
Amazon Simple Notification Service (Amazon SNS)	AWS::SNS::Topic
Amazon Simple Queue Service (Amazon SQS)	AWS::SQS::Queue
AWS Secrets Manager	AWS::SecretsManager::Secret
AWS Step Functions	AWS::StepFunctions::StateMachine
AWS Transfer Family	AWS::Transfer::Connector
AWS WAF	AWS::WAF::Rule , AWS::WAF::RuleGroup , AWS::WAF::WebACL , AWS::WAFRegional::Rule , AWS::WAFRegional::RuleGroup , AWS::WAFRegional::WebACL , AWS::WAFv2::RuleGroup , AWS::WAFv2::WebACL
Amazon WorkSpaces	AWS::WorkSpaces::Workspace

Sumber daya yang dibutuhkan untuk Tolok Ukur AWS Yayasan CIS

Untuk menjalankan pemeriksaan keamanan untuk kontrol yang diaktifkan yang berlaku untuk Tolok Ukur AWS Yayasan Center for Internet Security (CIS), Security Hub CSPM berjalan melalui langkah-langkah audit yang tepat yang ditentukan untuk pemeriksaan atau menggunakan aturan terkelola tertentu. AWS Config Untuk informasi tentang standar ini di Security Hub CSPM, lihat. [Tolok Ukur AWS Yayasan CIS di Security Hub CSPM](#)

Sumber daya yang diperlukan untuk CIS v3.0.0

Agar CSPM Security Hub melaporkan temuan secara akurat untuk kontrol yang dipicu perubahan CIS v3.0.0 yang diaktifkan yang menggunakan AWS Config aturan, Anda harus mencatat jenis sumber daya berikut. AWS Config

Layanan AWS	Jenis sumber daya
Amazon Elastic Compute Cloud (Amazon EC2)	AWS::EC2::Instance , AWS::EC2::NetworkAcl , AWS::EC2::SecurityGroup
AWS Identity and Access Management (IAM)	AWS::IAM::Group , AWS::IAM::User , AWS::IAM::Role
Amazon Relational Database Service (Amazon RDS)	AWS::RDS::DBInstance
Amazon Simple Storage Service (Amazon S3)	AWS::S3::Bucket

Sumber daya yang dibutuhkan untuk CIS v1.4.0

Agar CSPM Security Hub melaporkan temuan secara akurat untuk kontrol yang dipicu perubahan CIS v1.4.0 yang diaktifkan yang menggunakan AWS Config aturan, Anda harus mencatat jenis sumber daya berikut. AWS Config

Layanan AWS	Jenis sumber daya
Amazon Elastic Compute Cloud (Amazon EC2)	AWS::EC2::NetworkAcl , AWS::EC2::SecurityGroup
AWS Identity and Access Management (IAM)	AWS::IAM::Policy , AWS::IAM::User
Amazon Relational Database Service (Amazon RDS)	AWS::RDS::DBInstance
Amazon Simple Storage Service (Amazon S3)	AWS::S3::Bucket

Sumber daya yang diperlukan untuk CIS v1.2.0

Agar CSPM Security Hub melaporkan temuan secara akurat untuk kontrol yang dipicu perubahan CIS v1.2.0 yang diaktifkan yang menggunakan AWS Config aturan, Anda harus mencatat jenis sumber daya berikut. AWS Config

Layanan AWS	Jenis sumber daya
Amazon Elastic Compute Cloud (Amazon EC2)	AWS::EC2::SecurityGroup
AWS Identity and Access Management (IAM)	AWS::IAM::Policy , AWS::IAM::User

Sumber daya yang diperlukan untuk standar NIST SP 800-53 Revisi 5

Agar CSPM Security Hub melaporkan temuan secara akurat untuk kontrol yang dipicu perubahan yang berlaku pada standar NIST SP 800-53 Revisi 5, diaktifkan, dan menggunakan AWS Config aturan, Anda harus mencatat jenis sumber daya berikut. AWS Config Untuk informasi tentang standar ini, lihat [NIST SP 800-53 Revisi 5 di Security Hub CSPM](#).

Layanan AWS	Jenis sumber daya
Amazon API Gateway	AWS::ApiGateway::Stage , AWS::ApiGatewayV2::Stage
AWS AppSync	AWS::AppSync::GraphQLApi
AWS Backup	AWS::Backup::RecoveryPoint
AWS Certificate Manager (ACM)	AWS::ACM::Certificate
AWS CloudFormation	AWS::CloudFormation::Stack
Amazon CloudFront	AWS::CloudFront::Distribution
Amazon CloudWatch	AWS::CloudWatch::Alarm
AWS CodeBuild	AWS::CodeBuild::Project

Layanan AWS	Jenis sumber daya
AWS Database Migration Service (AWS DMS)	AWS::DMS::Endpoint , AWS::DMS::ReplicationInstance , AWS::DMS::ReplicationTask
Amazon DynamoDB	AWS::DynamoDB::Table
Amazon Elastic Compute Cloud (Amazon EC2)	AWS::EC2::ClientVpnEndpoint , AWS::EC2::EIP , AWS::EC2::Instance , AWS::EC2::LaunchTemplate , AWS::EC2::NetworkAcl , AWS::EC2::NetworkInterface , AWS::EC2::SecurityGroup , AWS::EC2::Subnet , AWS::EC2::TransitGateway , AWS::EC2::VPNConnection , AWS::EC2::Volume
EC2 Auto Scaling Amazon	AWS::AutoScaling::AutoScalingGroup , AWS::AutoScaling::LaunchConfiguration
Amazon Elastic Container Registry (Amazon ECR)	AWS::ECR::Repository
Amazon Elastic Container Service (Amazon ECS)	AWS::ECS::Cluster , AWS::ECS::Service , AWS::ECS::TaskDefinition
Amazon Elastic File System (Amazon EFS)	AWS::EFS::AccessPoint
Amazon Elastic Kubernetes Service (Amazon EKS)	AWS::EKS::Cluster
AWS Elastic Beanstalk	AWS::ElasticBeanstalk::Environment

Layanan AWS	Jenis sumber daya
Penyeimbang Beban Elastis	<code>AWS::ElasticLoadBalancing::LoadBalancer</code> , <code>AWS::ElasticLoadBalancingV2::Listener</code> , <code>AWS::ElasticLoadBalancingV2::LoadBalancer</code>
Amazon ElasticSearch	<code>AWS::Elasticsearch::Domain</code>
Amazon EMR	<code>AWS::EMR::SecurityConfiguration</code>
Amazon EventBridge	<code>AWS::Events::Endpoint</code> , <code>AWS::Events::EventBus</code>
AWS Glue	<code>AWS::Glue::Job</code>
AWS Identity and Access Management (IAM)	<code>AWS::IAM::Group</code> , <code>AWS::IAM::Policy</code> , <code>AWS::IAM::Role</code> , <code>AWS::IAM::User</code>
AWS Key Management Service (AWS KMS)	<code>AWS::KMS::Alias</code> , <code>AWS::KMS::Key</code>
Amazon Kinesis	<code>AWS::Kinesis::Stream</code>
AWS Lambda	<code>AWS::Lambda::Function</code>
Amazon Managed Streaming for Apache Kafka (Amazon MSK)	<code>AWS::MSK::Cluster</code>
Amazon MQ	<code>AWS::AmazonMQ::Broker</code>
AWS Network Firewall	<code>AWS::NetworkFirewall::Firewall</code> , <code>AWS::NetworkFirewall::FirewallPolicy</code> , <code>AWS::NetworkFirewall::RuleGroup</code>
OpenSearch Layanan Amazon	<code>AWS::OpenSearch::Domain</code>

Layanan AWS	Jenis sumber daya
Amazon Relational Database Service (Amazon RDS)	<code>AWS::RDS::DBCluster</code> , <code>AWS::RDS::DBClusterSnapshot</code> , <code>AWS::RDS::DBInstance</code> , <code>AWS::RDS::DBSnapshot</code> , <code>AWS::RDS::EventSubscription</code>
Amazon Redshift	<code>AWS::Redshift::Cluster</code> , <code>AWS::Redshift::ClusterSubnetGroup</code>
Amazon Route 53	<code>AWS::Route53::HostedZone</code>
Amazon Simple Storage Service (Amazon S3)	<code>AWS::S3::AccessPoint</code> , <code>AWS::S3::AccountPublicAccessBlock</code> , <code>AWS::S3::Bucket</code>
AWS Service Catalog	<code>AWS::ServiceCatalog::Portfolio</code>
Amazon Simple Notification Service (Amazon SNS)	<code>AWS::SNS::Topic</code>
Amazon Simple Queue Service (Amazon SQS)	<code>AWS::SQS::Queue</code>
Amazon EC2 Systems Manager (SSM)	<code>AWS::SSM::AssociationCompliance</code> , <code>AWS::SSM::ManagedInstanceInventory</code> , <code>AWS::SSM::PatchCompliance</code>
Amazon SageMaker AI	<code>AWS::SageMaker::NotebookInstance</code>
AWS Secrets Manager	<code>AWS::SecretsManager::Secret</code>
AWS Transfer Family	<code>AWS::Transfer::Connector</code>

Layanan AWS	Jenis sumber daya
AWS WAF	AWS::WAF::Rule , AWS::WAF::RuleGroup , AWS::WAF::WebACL , AWS::WAFRegional::Rule , AWS::WAFRegional::RuleGroup , AWS::WAFRegional::WebACL , AWS::WAFv2::RuleGroup , AWS::WAFv2::WebACL

Sumber daya yang diperlukan untuk standar NIST SP 800-171 Revisi 2

Agar CSPM Security Hub melaporkan temuan secara akurat untuk kontrol yang dipicu perubahan yang berlaku pada standar NIST SP 800-171 Revisi 2, diaktifkan, dan menggunakan AWS Config aturan, Anda harus mencatat jenis sumber daya berikut. AWS Config Untuk informasi tentang standar ini, lihat [NIST SP 800-171 Revisi 2 di Security Hub CSPM](#).

Layanan AWS	Jenis sumber daya
AWS Certificate Manager(ACM)	AWS::ACM::Certificate
Amazon API Gateway	AWS::ApiGateway::Stage
Amazon CloudFront	AWS::CloudFront::Distribution
Amazon CloudWatch	AWS::CloudWatch::Alarm
Amazon Elastic Compute Cloud (Amazon EC2)	AWS::EC2::ClientVpnEndpoint , AWS::EC2::NetworkAcl , AWS::EC2::SecurityGroup , AWS::EC2::VPC , AWS::EC2::VPNConnection
Penyeimbang Beban Elastis	AWS::ElasticLoadBalancing::LoadBalancer
AWS Identity and Access Management(IAM)	AWS::IAM::Policy , AWS::IAM::User
AWS Key Management Service (AWS KMS)	AWS::KMS::Alias , AWS::KMS::Key

Layanan AWS	Jenis sumber daya
AWS Network Firewall	AWS::NetworkFirewall::FirewallPolicy , AWS::NetworkFirewall::RuleGroup
Layanan Penyimpanan Sederhana Amazon (Amazon S3)	AWS::S3::Bucket
Layanan Pemberitahuan Sederhana Amazon (Amazon SNS)	AWS::SNS::Topic
AWS Systems Manager(SSM)	AWS::SSM::PatchCompliance
AWS WAF	AWS::WAFv2::RuleGroup

Sumber daya yang dibutuhkan untuk PCI DSS v3.2.1

Agar CSPM Security Hub melaporkan temuan secara akurat untuk kontrol yang berlaku untuk v3.2.1 Standar Keamanan Data Industri Kartu Pembayaran (PCI DSS), diaktifkan, dan menggunakan AWS Config aturan, Anda harus mencatat jenis sumber daya berikut di AWS Config Untuk informasi tentang standar ini, lihat [PCI DSS di Security Hub CSPM](#).

Layanan AWS	Jenis sumber daya
AWS CodeBuild	AWS::CodeBuild::Project
Amazon Elastic Compute Cloud (Amazon EC2)	AWS::EC2::EIP , AWS::EC2::Instance , AWS::EC2::SecurityGroup
EC2 Auto Scaling Amazon	AWS::AutoScaling::AutoScalingGroup
AWS Identity and Access Management (IAM)	AWS::IAM::Policy , AWS::IAM::User
AWS Lambda	AWS::Lambda::Function
OpenSearch Layanan Amazon	AWS::OpenSearch::Domain

Layanan AWS	Jenis sumber daya
Amazon Relational Database Service (Amazon RDS)	AWS::RDS::DBClusterSnapshot , AWS::RDS::DBInstance , AWS::RDS::DBSnapshot
Amazon Redshift	AWS::Redshift::Cluster
Amazon Simple Storage Service (Amazon S3)	AWS::S3::AccountPublicAccessBlock , AWS::S3::Bucket
Amazon EC2 Systems Manager (SSM)	AWS::SSM::AssociationCompliance , AWS::SSM::ManagedInstanceInventory , AWS::SSM::PatchCompliance

Sumber daya yang diperlukan untuk standar Penandaan AWS Sumber Daya

Semua kontrol yang berlaku untuk standar AWS Resource Tagging dipicu perubahan dan menggunakan AWS Config aturan. Agar CSPM Security Hub melaporkan temuan untuk kontrol ini secara akurat, Anda harus mencatat jenis sumber daya berikut. AWS Config Untuk informasi tentang standar ini, lihat [AWS Standar Penandaan Sumber Daya di Security Hub CSPM](#).

Layanan AWS	Jenis sumber daya
AWS Amplify	AWS::Amplify::App , AWS::Amplify::Branch
Amazon AppFlow	AWS::AppFlow::Flow
AWS App Runner	AWS::AppRunner::Service , AWS::AppRunner::VpcConnector
AWS AppConfig	AWS::AppConfig::Application , AWS::AppConfig::ConfigurationProfile , AWS::AppConfig::Environment , AWS::AppConfig::ExtensionAssociation

Layanan AWS	Jenis sumber daya
AWS AppSync	<code>AWS::AppSync::GraphQLApi</code>
Amazon Athena	<code>AWS::Athena::DataCatalog</code> , <code>AWS::Athena::WorkGroup</code>
AWS Backup	<code>AWS::Backup::BackupPlan</code> , <code>AWS::Backup::BackupVault</code> , <code>AWS::Backup::RecoveryPlan</code> , <code>AWS::Backup::ReportPlan</code>
AWS Batch	<code>AWS::Batch::ComputeEnvironment</code> , <code>AWS::Batch::JobQueue</code> , <code>AWS::Batch::SchedulingPolicy</code>
AWS Certificate Manager (ACM)	<code>AWS::ACM::Certificate</code>
AWS CloudFormation	<code>AWS::CloudFormation::Stack</code>
Amazon CloudFront	<code>AWS::CloudFront::Distribution</code>
AWS CloudTrail	<code>AWS::CloudTrail::Trail</code>
AWS CodeArtifact	<code>AWS::CodeArtifact::Repository</code>
Amazon CodeGuru	<code>AWS::CodeGuruProfiler::ProfilingGroup</code> , <code>AWS::CodeGuruReviewer::RepositoryAssociation</code>
Amazon Connect	<code>AWS::CustomerProfiles::ObjectType</code>
AWS Database Migration Service (AWS DMS)	<code>AWS::DMS::Certificate</code> , <code>AWS::DMS::EventSubscription</code> <code>AWS::DMS::ReplicationInstance</code> , <code>AWS::DMS::ReplicationSubnetGroup</code>
AWS DataSync	<code>AWS::DataSync::Task</code>

Layanan AWS	Jenis sumber daya
Amazon Detective	AWS::Detective::Graph
Amazon DynamoDB	AWS::DynamoDB::Trail
Amazon Elastic Compute Cloud () EC2	AWS::EC2::CustomerGateway , AWS::EC2::DHCPOptions , AWS::EC2: :EIP , AWS::EC2::FlowLog , AWS::EC2: :Instance , AWS::EC2::Internet Gateway , AWS::EC2::LaunchTe mplate , AWS::EC2::NatGateway , AWS::EC2::NetworkAcl , AWS::EC2: :NetworkInterface , AWS::EC2: :PrefixList , AWS::EC2::RouteTab le , AWS::EC2::SecurityGroup , AWS::EC2::Subnet , AWS::EC2: :TrafficMirrorFilter , AWS::EC2: :TrafficMirrorSession , AWS::EC2: :TrafficMirrorTarget , AWS::EC2: :TransitGateway , AWS::EC2: :TransitGatewayAttachment , AWS::EC2::TransitGatewayRou teTable , AWS::EC2::Volume , AWS::EC2::VPC , AWS::EC2::VPCEndpo intService , AWS::EC2::VPCPeeri ngConnection , AWS::EC2::VPNGatew ay
EC2 Auto Scaling Amazon	AWS::AutoScaling::AutoScali ngGroup
Amazon Elastic Container Registry (Amazon ECR)	AWS::ECR::PublicRepository

Layanan AWS	Jenis sumber daya
Amazon Elastic Container Service (Amazon ECS)	<code>AWS::ECS::Cluster</code> , <code>AWS::ECS::Service</code> , <code>AWS::ECS::TaskDefinition</code>
Amazon Elastic File System (Amazon EFS)	<code>AWS::EFS::AccessPoint</code>
Amazon Elastic Kubernetes Service (Amazon EKS)	<code>AWS::EKS::Cluster</code> , <code>AWS::EKS::IdentityProviderConfig</code>
AWS Elastic Beanstalk	<code>AWS::ElasticBeanstalk::Environment</code>
ElasticSearch	<code>AWS::Elasticsearch::Domain</code>
Amazon EventBridge	<code>AWS::Events::EventBus</code>
Amazon Fraud Detector	<code>AWS::FraudDetector::EntityType</code> , <code>AWS::FraudDetector::Label</code> <code>AWS::FraudDetector::Outcome</code> , <code>AWS::FraudDetector::Variable</code>
AWS Global Accelerator	<code>AWS::GlobalAccelerator::Accelerator</code>
AWS Glue	<code>AWS::Glue::Job</code>
Amazon GuardDuty	<code>AWS::GuardDuty::Detector</code> , <code>AWS::GuardDuty::Filter</code> , <code>AWS::GuardDuty::IPSet</code>
AWS Identity and Access Management (IAM)	<code>AWS::IAM::Role</code> , <code>AWS::IAM::User</code>
AWS Identity and Access Management Access Analyzer (Penganalisis Akses IAM)	<code>AWS::AccessAnalyzer::Analyzer</code>

Layanan AWS	Jenis sumber daya
AWS IoT	<code>AWS::IoT::Authorizer</code> , <code>AWS::IoT::Dimension</code> , <code>AWS::IoT::MitigationAction</code> , <code>AWS::IoT::Policy</code> , <code>AWS::IoT::RoleAlias</code> , <code>AWS::IoT::SecurityProfile</code>
AWS IoT Acara	<code>AWS::IoTEvents::AlarmModel</code> , <code>AWS::IoTEvents::DetectorModel</code> , <code>AWS::IoTEvents::Input</code>
AWS IoT SiteWise	<code>AWS::IoTSiteWise::Dashboard</code> , <code>AWS::IoTSiteWise::Gateway</code> , <code>AWS::IoTSiteWise::Portal</code> , <code>AWS::IoTSiteWise::Project</code>
AWS IoT TwinMaker	<code>AWS::IoTTwinMaker::Entity</code> , <code>AWS::IoTTwinMaker::Scene</code> , <code>AWS::IoTTwinMaker::SyncJob</code> , <code>AWS::IoTTwinMaker::Workspace</code>
AWS IoT Nirkabel	<code>AWS::IoTWireless::FirmwareTask</code> , <code>AWS::IoTWireless::MulticastGroup</code> , <code>AWS::IoTWireless::ServiceProfile</code>
Amazon Interactive Video Service (Amazon IVS)	<code>AWS::IVS::Channel</code> , <code>AWS::IVS::PlaybackKeyPair</code> , <code>AWS::IVS::RecordingConfiguration</code>
Amazon Keyspaces (untuk Apache Cassandra)	<code>AWS::Cassandra::Keyspace</code>
Amazon Kinesis	<code>AWS::Kinesis::Stream</code>
AWS Lambda	<code>AWS::Lambda::Function</code>
Amazon MQ	<code>AWS::AmazonMQ::Broker</code>

Layanan AWS	Jenis sumber daya
AWS Network Firewall	AWS::NetworkFirewall::Firewall , AWS::NetworkFirewall::FirewallPolicy
OpenSearch Layanan Amazon	AWS::OpenSearch::Domain
AWS Private Certificate Authority	AWS::ACMPCA::CertificateAuthority
Amazon Relational Database Service	AWS::RDS::DBCluster , AWS::RDS::DBClusterSnapshot , AWS::RDS::DBInstance , AWS::RDS::DBSecurityGroup , AWS::RDS::DBSnapshot , AWS::RDS::DBSubnetGroup
Amazon Redshift	AWS::Redshift::Cluster , AWS::Redshift::ClusterParameterGroup , AWS::Redshift::ClusterSnapshot , AWS::Redshift::ClusterSubnetGroup , AWS::Redshift::EventSubscription
Amazon Route 53	AWS::Route53::HealthCheck
Amazon SageMaker AI	AWS::SageMaker::AppImageConfig , AWS::SageMaker::Image
AWS Secrets Manager	AWS::SecretsManager::Secret
Amazon Simple Email Service (Amazon SES)	AWS::SES::ConfigurationSet , AWS::SES::ContactList
Amazon Simple Notification Service (Amazon SNS)	AWS::SNS::Topic
Amazon Simple Queue Service (Amazon SQS)	AWS::SQS::Queue

Layanan AWS	Jenis sumber daya
AWS Step Functions	<code>AWS::StepFunctions::Activity</code>
AWS Systems Manager (SSM)	<code>AWS::SSM::Document</code>
AWS Transfer Family	<code>AWS::Transfer::Agreement</code> , <code>AWS::Transfer::Certificate</code> , <code>AWS::Transfer::Connector</code> , <code>AWS::Transfer::Profile</code> , <code>AWS::Transfer::Workflow</code>

Sumber daya yang diperlukan untuk standar yang AWS Control Tower dikelola layanan

Agar CSPM Security Hub melaporkan temuan secara akurat untuk kontrol yang dipicu perubahan yang berlaku pada standar yang AWS Control Tower dikelola layanan, diaktifkan, dan menggunakan AWS Config aturan, Anda harus mencatat jenis sumber daya berikut. AWS Config Untuk informasi tentang standar ini, lihat [Standar yang Dikelola Layanan: AWS Control Tower](#).

Layanan AWS	Jenis sumber daya
Amazon API Gateway	<code>AWS::ApiGateway::Stage</code> <code>AWS::ApiGatewayV2::Stage</code>
AWS Certificate Manager (ACM)	<code>AWS::ACM::Certificate</code>
AWS CodeBuild	<code>AWS::CodeBuild::Project</code>
Amazon DynamoDB	<code>AWS::DynamoDB::Table</code>
Amazon Elastic Compute Cloud () EC2	<code>AWS::EC2::Instance</code> <code>AWS::EC2::NetworkAcl</code> <code>AWS::EC2::NetworkInterface</code> <code>AWS::EC2::SecurityGroup</code>

Layanan AWS	Jenis sumber daya
	AWS::EC2::Subnet
	AWS::EC2::VPNConnection
	AWS::EC2::Volume
EC2 Auto Scaling Amazon	AWS::AutoScaling::AutoScalingGroup
	AWS::AutoScaling::LaunchConfiguration
Amazon Elastic Container Registry (Amazon ECR)	AWS::ECR::Repository
Amazon Elastic Container Service (Amazon ECS)	AWS::ECS::Cluster
	AWS::ECS::Service
	AWS::ECS::TaskDefinition
Amazon Elastic File System (Amazon EFS)	AWS::EFS::AccessPoint
Amazon EKS	AWS::EKS::Cluster
ElasticBeanstalk	AWS::ElasticBeanstalk::Environment
Penyeimbang Beban Elastis	AWS::ElasticLoadBalancing::LoadBalancer
	AWS::ElasticLoadBalancingV2::LoadBalancer
ElasticSearch	AWS::Elasticsearch::Domain

Layanan AWS	Jenis sumber daya
AWS Identity and Access Management (IAM)	AWS::IAM::Group AWS::IAM::Policy AWS::IAM::Role AWS::IAM::User
AWS Key Management Service (AWS KMS)	AWS::KMS::Alias AWS::KMS::Key
Amazon Kinesis	AWS::Kinesis::Stream
AWS Lambda	AWS::Lambda::Function
AWS Network Firewall	AWS::NetworkFirewall::FirewallPolicy AWS::NetworkFirewall::RuleGroup
OpenSearch Layanan Amazon	AWS::OpenSearch::Domain
Amazon Relational Database Service (Amazon RDS)	AWS::RDS::DBCluster AWS::RDS::DBClusterSnapshot AWS::RDS::DBInstance AWS::RDS::DBSnapshot AWS::RDS::EventSubscription
Amazon Redshift	AWS::Redshift::Cluster
Amazon Simple Storage Service (Amazon S3)	AWS::S3::AccountPublicAccessBlock AWS::S3::Bucket

Layanan AWS	Jenis sumber daya
Amazon Simple Notification Service (Amazon SNS)	AWS::SNS::Topic
Amazon Simple Queue Service (Amazon SQS)	AWS::SQS::Queue
AWS Secrets Manager	AWS::SecretsManager::Secret
Amazon EC2 Systems Manager (SSM)	AWS::SSM::AssociationCompliance AWS::SSM::ManagedInstanceInventory AWS::SSM::PatchCompliance
AWS WAF	AWS::WAFRegional::Rule AWS::WAFRegional::RuleGroup AWS::WAFRegional::WebACL AWS::WAFv2::WebACL

Jadwal untuk menjalankan pemeriksaan keamanan

Setelah Anda mengaktifkan standar keamanan, AWS Security Hub Cloud Security Posture Management (CSPM) mulai menjalankan semua pemeriksaan dalam waktu dua jam. Sebagian besar pemeriksaan mulai berjalan dalam waktu 25 menit. Security Hub CSPM menjalankan pemeriksaan dengan mengevaluasi aturan yang mendasari kontrol. Sampai kontrol menyelesaikan pemeriksaan pertamanya, statusnya adalah Tidak ada data.

Saat Anda mengaktifkan standar baru, CSPM Security Hub mungkin memerlukan waktu hingga 24 jam untuk menghasilkan temuan untuk kontrol yang menggunakan aturan AWS Config terkait layanan dasar yang sama dengan kontrol yang diaktifkan dari standar lain yang diaktifkan. Misalnya, jika Anda mengaktifkan kontrol [Lambda.1](#) dalam standar Praktik Terbaik Keamanan AWS Dasar (FSBP), Security Hub CSPM akan membuat aturan terkait layanan dan biasanya menghasilkan temuan dalam hitungan menit. Setelah ini, jika Anda mengaktifkan kontrol Lambda.1 di Standar Keamanan Data Industri Kartu Pembayaran (PCI DSS), mungkin diperlukan waktu hingga 24 jam

untuk Security Hub CSPM untuk menghasilkan temuan untuk kontrol karena menggunakan aturan terkait layanan yang sama.

Setelah pemeriksaan awal, jadwal untuk setiap kontrol dapat berupa periodik atau perubahan yang dipicu. Untuk kontrol yang didasarkan pada AWS Config aturan terkelola, deskripsi kontrol menyertakan tautan ke deskripsi aturan di Panduan AWS Config Pengembang. Deskripsi itu menentukan apakah aturan tersebut dipicu perubahan atau periodik.

Pemeriksaan keamanan berkala

Pemeriksaan keamanan berkala berjalan secara otomatis dalam waktu 12 atau 24 jam setelah proses terbaru. Security Hub CSPM menentukan periodisitas, dan Anda tidak dapat mengubahnya. Kontrol periodik mencerminkan evaluasi pada saat pemeriksaan berjalan.

Jika Anda memperbarui status alur kerja dari temuan kontrol berkala, dan kemudian pada pemeriksaan berikutnya status kepatuhan temuan tetap sama, status alur kerja tetap dalam status yang diubah. Misalnya, jika Anda memiliki temuan gagal untuk kontrol [KMS.4](#) (AWS KMS key rotasi harus diaktifkan), dan kemudian memulihkan temuan, Security Hub CSPM mengubah status alur kerja dari ke. NEW RESOLVED Jika Anda menonaktifkan rotasi kunci KMS sebelum pemeriksaan berkala berikutnya, status alur kerja temuan tetap ada. RESOLVED

Pemeriksaan yang menggunakan fungsi Lambda kustom Security Hub CSPM bersifat periodik.

Pemeriksaan keamanan yang dipicu perubahan

Pemeriksaan keamanan yang dipicu perubahan berjalan saat sumber daya terkait mengubah status. AWS Config memungkinkan Anda memilih antara perekaman terus menerus dari perubahan status sumber daya dan perekaman harian. Jika Anda memilih perekaman harian, AWS Config mengirimkan data konfigurasi sumber daya pada akhir setiap periode 24 jam jika ada perubahan status sumber daya. Jika tidak ada perubahan, tidak ada data yang dikirimkan. Hal ini dapat menunda pembuatan temuan CSPM Security Hub hingga periode 24 jam selesai. Terlepas dari periode perekaman yang Anda pilih, Security Hub CSPM memeriksa setiap 18 jam untuk memastikan tidak ada pembaruan sumber daya yang AWS Config lewatkan.

Secara umum, Security Hub CSPM menggunakan aturan yang dipicu perubahan bila memungkinkan. Agar sumber daya menggunakan aturan yang dipicu perubahan, ia harus mendukung item AWS Config konfigurasi.

Menghasilkan dan memperbarui temuan kontrol

AWS Security Hub Cloud Security Posture Management (CSPM) menghasilkan temuan kontrol saat menjalankan pemeriksaan terhadap kontrol keamanan. Temuan kontrol menggunakan [AWS Security Finding Format \(ASFF\)](#).

Security Hub CSPM biasanya mengenakan biaya untuk setiap pemeriksaan keamanan untuk kontrol. Namun, jika beberapa kontrol menggunakan AWS Config aturan yang sama, CSPM Security Hub hanya mengenakan biaya sekali untuk setiap pemeriksaan terhadap aturan. Misalnya, AWS Config `iam-password-policy` aturan ini digunakan oleh beberapa kontrol dalam standar Tolok Ukur AWS Yayasan CIS dan standar Praktik Terbaik Keamanan AWS Dasar. Setiap kali Security Hub CSPM menjalankan pemeriksaan terhadap aturan itu, itu menghasilkan temuan kontrol terpisah untuk setiap kontrol terkait, tetapi hanya mengenakan biaya sekali untuk pemeriksaan.

Jika ukuran temuan kontrol melebihi maksimum 240 KB, Security Hub CSPM menghapus `Resource.Details` objek dari temuan. Untuk kontrol yang didukung oleh AWS Config sumber daya, Anda dapat meninjau detail sumber daya menggunakan AWS Config konsol.

Topik

- [Temuan kontrol terkonsolidasi](#)
- [Menghasilkan, memperbarui, dan mengarsipkan temuan kontrol](#)
- [Otomatisasi dan penindasan temuan kontrol](#)
- [Detail kepatuhan untuk temuan kontrol](#)
- [ProductFields rincian untuk temuan kontrol](#)
- [Tingkat keparahan untuk temuan kontrol](#)

Temuan kontrol terkonsolidasi

Jika temuan kontrol konsolidasi diaktifkan untuk akun Anda, Security Hub CSPM menghasilkan satu temuan baru atau menemukan pembaruan untuk setiap pemeriksaan keamanan kontrol, bahkan jika kontrol berlaku untuk beberapa standar yang diaktifkan. Untuk daftar kontrol dan standar yang mereka terapkan, lihat [Referensi kontrol untuk Security Hub CSPM](#). Kami merekomendasikan untuk mengaktifkan temuan kontrol terkonsolidasi untuk mengurangi kebisingan temuan.

Jika Anda mengaktifkan CSPM Security Hub Akun AWS sebelum 23 Februari 2023, Anda dapat mengaktifkan temuan kontrol konsolidasi dengan mengikuti petunjuk nanti di bagian ini. Jika Anda

mengaktifkan CSPM Security Hub pada atau setelah 23 Februari 2023, temuan kontrol konsolidasi diaktifkan secara otomatis untuk akun Anda.

Jika Anda menggunakan [integrasi CSPM Security Hub dengan AWS Organizations](#) atau akun anggota yang diundang melalui [proses undangan manual](#), temuan kontrol konsolidasi diaktifkan untuk akun anggota hanya jika diaktifkan untuk akun administrator. Jika fitur dinonaktifkan untuk akun administrator, itu dinonaktifkan untuk akun anggota. Perilaku ini berlaku untuk akun anggota baru dan yang sudah ada. Selain itu, jika administrator menggunakan [konfigurasi pusat](#) untuk mengelola CSPM Security Hub untuk beberapa akun, mereka tidak dapat menggunakan kebijakan konfigurasi pusat untuk mengaktifkan atau menonaktifkan temuan kontrol konsolidasi untuk akun.

Jika Anda menonaktifkan temuan kontrol konsolidasi untuk akun Anda, Security Hub CSPM akan menghasilkan temuan kontrol terpisah untuk setiap pemeriksaan keamanan dan setiap standar yang diaktifkan yang menyertakan kontrol. Misalnya, jika Anda mengaktifkan empat standar yang berbagi kontrol, Anda menerima empat temuan terpisah setelah pemeriksaan keamanan untuk kontrol. Jika Anda mengaktifkan temuan kontrol terkonsolidasi, Anda hanya menerima satu temuan.

Saat Anda mengaktifkan temuan kontrol terkonsolidasi, Security Hub CSPM menciptakan temuan agnostik standar baru dan mengarsipkan temuan berbasis standar asli. Beberapa bidang dan nilai pencarian kontrol akan berubah, yang mungkin memengaruhi alur kerja Anda yang ada. Untuk informasi tentang perubahan ini, lihat [Temuan kontrol konsolidasi - perubahan ASFF](#). Mengaktifkan temuan kontrol konsolidasi juga dapat memengaruhi temuan yang diterima produk pihak ketiga terintegrasi dari Security Hub CSPM. Jika Anda menggunakan [Respons Keamanan Otomatis pada solusi AWS v2.0.0](#), perhatikan bahwa solusi ini mendukung temuan kontrol terkonsolidasi.

Untuk mengaktifkan atau menonaktifkan temuan kontrol konsolidasi, Anda harus masuk ke akun administrator atau akun mandiri.

Note

Setelah Anda mengaktifkan temuan kontrol terkonsolidasi, dibutuhkan waktu hingga 24 jam untuk CSPM Security Hub untuk menghasilkan temuan baru yang terkonsolidasi dan mengarsipkan temuan asli berbasis standar. Demikian pula, setelah menonaktifkan temuan kontrol konsolidasi, dibutuhkan waktu hingga 24 jam bagi Security Hub CSPM untuk menghasilkan temuan baru berbasis standar dan mengarsipkan temuan konsolidasi. Selama masa-masa ini, Anda mungkin melihat campuran temuan agnostik standar dan berbasis standar di akun Anda.

Security Hub CSPM console

Untuk mengaktifkan atau menonaktifkan temuan kontrol terkonsolidasi

1. Buka konsol AWS Security Hub Cloud Security Posture Management (CSPM) di <https://console.aws.amazon.com/securityhub/>
2. Di panel navigasi, pada Pengaturan, pilih Umum.
3. Di bagian Kontrol, pilih Edit.
4. Gunakan sakelar temuan kontrol Konsolidasi untuk mengaktifkan atau menonaktifkan temuan kontrol terkonsolidasi.
5. Pilih Simpan.

Security Hub CSPM API

Untuk mengaktifkan atau menonaktifkan temuan kontrol terkonsolidasi secara terprogram, gunakan [UpdateSecurityHubConfiguration](#) pengoperasian Security Hub CSPM API. Atau, jika Anda menggunakan AWS CLI, jalankan [update-security-hub-configuration](#) perintah.

Untuk `control-finding-generator` parameter, tentukan `SECURITY_CONTROL` untuk mengaktifkan temuan kontrol terkonsolidasi. Untuk menonaktifkan temuan kontrol konsolidasi, tentukan `STANDARD_CONTROL`.

Misalnya, AWS CLI perintah berikut memungkinkan temuan kontrol terkonsolidasi.

```
$ aws securityhub --region us-east-1 update-security-hub-configuration --control-finding-generator SECURITY_CONTROL
```

AWS CLI Perintah berikut menonaktifkan temuan kontrol konsolidasi.

```
$ aws securityhub --region us-east-1 update-security-hub-configuration --control-finding-generator STANDARD_CONTROL
```

Menghasilkan, memperbarui, dan mengarsipkan temuan kontrol

[Security Hub CSPM menjalankan pemeriksaan keamanan sesuai jadwal.](#) Pemeriksaan berikutnya terhadap kontrol yang diberikan dapat menghasilkan hasil baru. Misalnya, status kontrol dapat berubah dari FAILED ke PASSED. Dalam hal ini, Security Hub CSPM menghasilkan temuan baru yang

berisi hasil terbaru. Jika pemeriksaan berikutnya terhadap kontrol yang diberikan menghasilkan hasil yang identik dengan hasil saat ini, Security Hub CSPM memperbarui temuan yang ada. Tidak ada temuan baru yang dihasilkan.

Selain menghasilkan dan memperbarui temuan kontrol, Security Hub CSPM secara otomatis mengarsipkan temuan kontrol yang memenuhi kriteria tertentu. Security Hub CSPM mengarsipkan temuan jika kontrol dinonaktifkan, sumber daya yang ditentukan dihapus, atau sumber daya yang ditentukan tidak ada lagi. Sumber daya mungkin tidak ada lagi karena layanan terkait tidak lagi digunakan. Lebih khusus lagi, Security Hub CSPM secara otomatis mengarsipkan temuan kontrol jika temuan tersebut memenuhi salah satu kriteria berikut:

- Temuan ini belum diperbarui selama 3-5 hari. Perhatikan bahwa arsip berdasarkan kerangka waktu ini adalah upaya terbaik dan tidak dijamin.
- AWS Config Evaluasi terkait dikembalikan NOT_APPLICABLE untuk status kepatuhan sumber daya yang ditentukan.

Untuk menentukan apakah suatu temuan diarsipkan, Anda dapat merujuk ke bidang record state (RecordState) dari temuan tersebut. Jika temuan diarsipkan, nilai untuk bidang ini adalah ARCHIVED.

Security Hub CSPM menyimpan temuan kontrol yang diarsipkan selama 30 hari. Setelah 30 hari, temuan berakhir dan Security Hub CSPM menghapusnya secara permanen. Untuk menentukan apakah temuan kontrol yang diarsipkan telah kedaluwarsa, Security Hub CSPM mendasarkan perhitungannya pada nilai untuk UpdatedAt bidang temuan.

Untuk menyimpan temuan kontrol yang diarsipkan selama lebih dari 30 hari, Anda dapat mengekspor temuan ke ember S3. Anda dapat melakukan ini dengan menggunakan tindakan kustom dengan EventBridge aturan Amazon. Untuk informasi selengkapnya, lihat [Menggunakan EventBridge untuk respon otomatis dan remediasi](#).

Otomatisasi dan penindasan temuan kontrol

Anda dapat menggunakan aturan otomatisasi CSPM Security Hub untuk memperbarui atau menekan temuan kontrol tertentu. Jika Anda menekan temuan, Anda dapat terus mengaksesnya di akun Anda. Namun, penindasan menunjukkan keyakinan Anda bahwa tidak ada tindakan yang diperlukan untuk mengatasi temuan tersebut.

Dengan menekan temuan, Anda dapat mengurangi kebisingan temuan. Misalnya, Anda mungkin menekan temuan kontrol yang dihasilkan di akun pengujian. Atau, Anda mungkin menekan temuan

yang terkait dengan sumber daya tertentu. Untuk mempelajari lebih lanjut tentang memperbarui atau menekan temuan secara otomatis, lihat [Memahami aturan otomatisasi di Security Hub CSPM](#).

Aturan otomatisasi sesuai ketika Anda ingin memperbarui atau menekan temuan kontrol tertentu. Namun, jika kontrol tidak relevan dengan organisasi atau kasus penggunaan Anda, sebaiknya [nonaktifkan](#) kontrol. Saat Anda menonaktifkan kontrol, Security Hub CSPM tidak menjalankan pemeriksaan keamanan di dalamnya, dan Anda tidak dikenakan biaya untuk itu.

Detail kepatuhan untuk temuan kontrol

Dalam temuan yang dihasilkan oleh pemeriksaan keamanan untuk kontrol, [Compliance](#) objek dan bidang dalam AWS Security Finding Format (ASFF) memberikan rincian kepatuhan untuk sumber daya individu yang diperiksa kontrol. Ini termasuk informasi berikut:

- **AssociatedStandards**— Standar yang diaktifkan di mana kontrol diaktifkan.
- **RelatedRequirements**— Persyaratan terkait untuk kontrol di semua standar yang diaktifkan. Persyaratan ini berasal dari kerangka keamanan pihak ketiga untuk kontrol, seperti Standar Keamanan Data Industri Kartu Pembayaran (PCI DSS) atau standar NIST SP 800-171 Revisi 2.
- **SecurityControlId**— Pengidentifikasi untuk kontrol di seluruh standar yang didukung Security Hub CSPM.
- **Status**— Hasil pemeriksaan terbaru bahwa Security Hub CSPM berjalan untuk kontrol. Hasil pemeriksaan sebelumnya disimpan dalam keadaan diarsipkan.
- **StatusReasons**— Array yang mencantumkan alasan untuk nilai yang ditentukan oleh Status bidang. Untuk setiap alasan, ini termasuk kode alasan dan deskripsi.

Tabel berikut mencantumkan kode alasan dan deskripsi bahwa temuan mungkin termasuk dalam StatusReasons array. Langkah-langkah remediasi bervariasi berdasarkan kontrol mana yang menghasilkan temuan dengan kode alasan tertentu. Untuk meninjau panduan remediasi untuk kontrol, lihat [Referensi kontrol untuk Security Hub CSPM](#)

Kode alasan	Status kepatuhan	Deskripsi
CLOUDTRAIL_METRIC_FILTER_NOT_VALID	FAILED	CloudTrail Jejak Multi-wilayah tidak memiliki filter metrik yang valid.

Kode alasan	Status kepatuhan	Deskripsi
CLOUDTRAIL_METRIC_FILTERS_NOT_PRESENT	FAILED	Filter metrik tidak ada untuk CloudTrail jejak Multi-wilayah.
CLOUDTRAIL_MULTI_REGION_NOT_PRESENT	FAILED	Akun tidak memiliki CloudTrail jejak Multi-wilayah dengan konfigurasi yang diperlukan.
CLOUDTRAIL_REGION_INVALID	WARNING	CloudTrail Jalur Multi-Region tidak berada di Wilayah saat ini.
CLOUDWATCH_ALARM_ACTIONS_NOT_VALID	FAILED	Tidak ada tindakan alarm yang valid.
CLOUDWATCH_ALARMS_NOT_PRESENT	FAILED	CloudWatch alarm tidak ada di akun.
CONFIG_ACCESS_DENIED	NOT_AVAILABLE AWS Config Status adalah ConfigError	AWS Config akses ditolak. Verifikasi bahwa AWS Config diaktifkan dan telah diberikan izin yang cukup.
CONFIG_EVALUATIONS_EMPTY	PASSED	AWS Config mengevaluasi sumber daya Anda berdasarkan aturan. Aturan tidak berlaku untuk AWS sumber daya dalam ruang lingkungannya, sumber daya yang ditentukan dihapus, atau hasil evaluasi dihapus.

Kode alasan	Status kepatuhan	Deskripsi
CONFIG_RECORDER_CUSTOM_ROLE	FAILED(untuk Config.1)	AWS Config Perekam menggunakan peran IAM khusus alih-alih peran AWS Config terkait layanan, dan parameter <code>includeConfigServiceLinkedRoleCheck</code> khusus untuk Config.1 tidak disetel ke <code>false</code>
CONFIG_RECORDER_DISABLED	FAILED(untuk Config.1)	AWS Config tidak diaktifkan dengan perekam konfigurasi dihidupkan.
CONFIG_RECORDER_MISSING_REQUIRED_RESOURCE_TYPES	FAILED(untuk Config.1)	AWS Config tidak merekam semua jenis sumber daya yang sesuai dengan kontrol CSPM Security Hub yang diaktifkan. Aktifkan perekaman untuk sumber daya berikut: <i>Resources that aren't being recorded.</i>

Kode alasan	Status kepatuhan	Deskripsi
CONFIG_RETURNS_NOT_APPLICABLE	NOT_AVAILABLE	Status kepatuhan adalah NOT_AVAILABLE karena AWS Config mengembalikan status Tidak Berlaku. AWS Config tidak memberikan alasan untuk status tersebut. Berikut adalah beberapa kemungkinan alasan untuk status Tidak Berlaku: • Sumber daya telah dihapus dari ruang lingkup AWS Config aturan. • AWS Config Aturan itu dihapus. • Sumber daya telah dihapus. • Logika AWS Config aturan dapat menghasilkan status Tidak Berlaku.

Kode alasan	Status kepatuhan	Deskripsi
CONFIG_RULE_EVALUATION_ERROR	NOT_AVAILABLE AWS Config Status adalah ConfigError	Kode alasan ini digunakan untuk beberapa jenis kesalahan evaluasi. Deskripsi memberikan informasi alasan spesifik. Jenis kesalahan dapat berupa salah satu dari yang berikut: • Ketidakmampuan untuk melakukan evaluasi karena kurangnya izin. Deskripsi memberikan izin khusus yang hilang. • Nilai yang hilang atau tidak valid untuk parameter. Deskripsi memberikan parameter dan persyaratan untuk nilai parameter. • Kesalahan membaca dari ember S3. Deskripsi mengidentifikasi ember dan memberikan kesalahan spesifik. • AWS Langganan yang hilang. • Batas waktu umum pada evaluasi. • Akun yang ditangguhkan.
CONFIG_RULE_NOT_FOUND	NOT_AVAILABLE AWS Config Status adalah ConfigError	AWS Config Aturannya sedang dalam proses diciptakan.
INTERNAL_SERVICE_ERROR	NOT_AVAILABLE	Terjadi kesalahan yang tidak diketahui.

Kode alasan	Status kepatuhan	Deskripsi
LAMBDA_CUSTOM_RUNTIME_DETAILS_NOT_AVAILABLE	FAILED	Security Hub CSPM tidak dapat melakukan pemeriksaan terhadap runtime Lambda kustom.
S3_BUCKET_CROSS_ACCOUNT_CROSS_REGION	WARNING	Temuan ini dalam WARNING keadaan karena bucket S3 yang dikaitkan dengan aturan ini berada di Wilayah atau akun yang berbeda. Aturan ini tidak mendukung pemeriksaan lintas wilayah atau lintas akun. Disarankan agar Anda menonaktifkan kontrol ini di Wilayah atau akun ini. Jalankan saja di Wilayah atau akun tempat sumber daya berada.
SNS_SUBSCRIPTION_NOTIFICATION_PRESENT	FAILED	Filter metrik CloudWatch Log tidak memiliki langganan Amazon SNS yang valid.
SNS_TOPIC_CROSS_ACCOUNT	WARNING	Temuan itu dalam WARNING keadaan. Topik SNS yang terkait dengan aturan ini dimiliki oleh akun yang berbeda. Akun saat ini tidak dapat memperoleh informasi berlangganan. Akun yang memiliki topik SNS harus memberikan <code>sns:ListSubscriptionsByTopic</code> izin kepada akun saat ini untuk topik SNS.

Kode alasan	Status kepatuhan	Deskripsi
SNS_TOPIC_CROSS_ACCOUNT_CROSS_REGION	WARNING	Temuan ini dalam WARNING keadaan karena topik SNS yang terkait dengan aturan ini berada di Wilayah atau akun yang berbeda. Aturan ini tidak mendukung pemeriksaan lintas wilayah atau lintas akun. Disarankan agar Anda menonaktifkan kontrol ini di Wilayah atau akun ini. Jalankan saja di Wilayah atau akun tempat sumber daya berada.
SNS_TOPIC_INVALID	FAILED	Topik SNS yang terkait dengan aturan ini tidak valid.
THROTTLING_ERROR	NOT_AVAILABLE	Operasi API yang relevan melebihi tarif yang diizinkan.

ProductFields rincian untuk temuan kontrol

Saat Security Hub CSPM menjalankan pemeriksaan keamanan dan menghasilkan temuan kontrol, [ProductFields](#) atribut di ASFF menyertakan bidang-bidang berikut:

`ArchivalReasons:0/Description`

Menjelaskan mengapa Security Hub CSPM telah mengarsipkan temuan yang ada.

Misalnya, Security Hub CSPM mengarsipkan temuan yang ada saat Anda menonaktifkan kontrol atau standar dan saat Anda mengaktifkan atau menonaktifkan [temuan kontrol konsolidasi](#).

`ArchivalReasons:0/ReasonCode`

Memberikan alasan mengapa Security Hub CSPM telah mengarsipkan temuan yang ada.

Misalnya, Security Hub CSPM mengarsipkan temuan yang ada saat Anda menonaktifkan kontrol atau standar dan saat Anda mengaktifkan atau menonaktifkan [temuan kontrol konsolidasi](#).

`StandardsGuideArn` atau `StandardsArn`

ARN dari standar yang terkait dengan kontrol.

Untuk standar CIS AWS Foundations Benchmark, bidangnya adalah `StandardsGuideArn`

Untuk standar PCI DSS dan AWS Foundational Security Best Practices, bidangnya adalah `StandardsArn`

Bidang ini dihapus demi `Compliance.AssociatedStandards` jika Anda mengaktifkan [temuan kontrol terkonsolidasi](#).

`StandardsGuideSubscriptionArn` atau `StandardsSubscriptionArn`

ARN berlangganan akun ke standar.

Untuk standar CIS AWS Foundations Benchmark, bidangnya adalah `StandardsGuideSubscriptionArn`

Untuk standar PCI DSS dan AWS Foundational Security Best Practices, bidangnya adalah `StandardsSubscriptionArn`

Bidang ini akan dihapus jika Anda mengaktifkan [temuan kontrol terkonsolidasi](#).

`RuleId` atau `ControlId`

Pengidentifikasi kontrol.

Untuk standar CIS AWS Foundations Benchmark, bidangnya adalah `RuleId`

Untuk standar lain, bidangnya `ControlId`.

Bidang ini dihapus demi `Compliance.SecurityControlId` jika Anda mengaktifkan [temuan kontrol terkonsolidasi](#).

`RecommendationUrl`

URL ke informasi remediasi untuk kontrol. Bidang ini dihapus demi `Remediation.Recommendation.Url` jika Anda mengaktifkan [temuan kontrol terkonsolidasi](#).

`RelatedAWSResources:0/name`

Nama sumber daya yang terkait dengan temuan.

`RelatedAWSResource:0/type`

Jenis sumber daya yang terkait dengan kontrol.

`StandardsControlArn`

ARN dari kontrol. Bidang ini dihapus jika Anda mengaktifkan [temuan kontrol konsolidasi](#).

`aws/securityhub/ProductName`

Untuk temuan berbasis kontrol, nama produknya adalah Security Hub CSPM.

`aws/securityhub/CompanyName`

Untuk temuan berbasis kontrol, nama perusahaan adalah. AWS

`aws/securityhub/annotation`

Deskripsi masalah yang ditemukan oleh kontrol.

`aws/securityhub/FindingId`

Pengidentifikasi temuan. Bidang ini tidak mereferensikan standar jika Anda mengaktifkan [temuan kontrol terkonsolidasi](#).

Tingkat keparahan untuk temuan kontrol

Tingkat keparahan yang ditetapkan ke kontrol CSPM Security Hub mengidentifikasi pentingnya kontrol. Tingkat keparahan kontrol menentukan label keparahan yang ditetapkan untuk temuan kontrol.

Kriteria keparahan

Tingkat keparahan kontrol ditentukan berdasarkan penilaian kriteria berikut:

- Seberapa sulit bagi aktor ancaman untuk memanfaatkan kelemahan konfigurasi yang terkait dengan kontrol?

Kesulitan ditentukan oleh jumlah kecanggihan atau kompleksitas yang diperlukan untuk menggunakan kelemahan untuk melakukan skenario ancaman.

- Seberapa besar kemungkinan kelemahan itu akan mengarah pada kompromi terhadap sumber daya Anda Akun AWS atau sumber daya?

Kompromi terhadap sumber daya Anda Akun AWS berarti kerahasiaan, integritas, atau ketersediaan data atau AWS infrastruktur Anda rusak dalam beberapa cara.

Kemungkinan kompromi menunjukkan seberapa besar kemungkinan skenario ancaman akan mengakibatkan gangguan atau pelanggaran AWS layanan atau sumber daya Anda.

Sebagai contoh, pertimbangkan kelemahan konfigurasi berikut:

- Kunci akses pengguna tidak dirotasi setiap 90 hari.
- Kunci pengguna root IAM ada.

Kedua kelemahan sama-sama sulit untuk dimanfaatkan oleh musuh. Dalam kedua kasus, musuh dapat menggunakan pencurian kredensial atau metode lain untuk memperoleh kunci pengguna. Mereka kemudian dapat menggunakannya untuk mengakses sumber daya Anda dengan cara yang tidak sah.

Namun, kemungkinan kompromi jauh lebih tinggi jika aktor ancaman memperoleh kunci akses pengguna root karena ini memberi mereka akses yang lebih besar. Akibatnya, kelemahan kunci pengguna root memiliki tingkat keparahan yang lebih tinggi.

Tingkat keparahannya tidak memperhitungkan kekritisannya sumber daya yang mendasarinya. Kritikalitas adalah tingkat pentingnya sumber daya yang terkait dengan temuan tersebut. Misalnya, sumber daya yang terkait dengan aplikasi kritis misi lebih penting daripada sumber daya yang terkait dengan pengujian nonproduksi. Untuk menangkap informasi kekritisannya sumber daya, gunakan *Criticality* bidang AWS Security Finding Format (ASFF).

Tabel berikut memetakan kesulitan untuk mengeksploitasi dan kemungkinan kompromi dengan label keamanan.

	Kompromi sangat mungkin	Kemungkinan kompromi	Kompromi tidak mungkin	Kompromi sangat tidak mungkin
Sangat mudah untuk dieksplo- tasi	Kritis	Kritis	Tinggi	Sedang

Agak mudah untuk dieksploitasi	Kritis	Tinggi	Sedang	Sedang
Agak sulit untuk dieksploitasi	Tinggi	Sedang	Sedang	Rendah
Sangat sulit untuk dieksploitasi	Sedang	Sedang	Rendah	Rendah

Definisi keparahan

Label keparahan didefinisikan sebagai berikut.

Kritis — Masalah ini harus segera diperbaiki untuk menghindari eskalasi.

Misalnya, bucket S3 terbuka dianggap sebagai temuan tingkat keparahan kritis. Karena begitu banyak pelaku ancaman memindai bucket S3 terbuka, data dalam bucket S3 yang terbuka kemungkinan akan ditemukan dan diakses oleh orang lain.

Secara umum, sumber daya yang dapat diakses publik dianggap sebagai masalah keamanan kritis. Anda harus memperlakukan temuan kritis dengan sangat mendesak. Anda juga harus mempertimbangkan kekritisannya sumber daya.

Tinggi — Masalah ini harus ditangani sebagai prioritas jangka pendek.

Misalnya, jika grup keamanan VPC default terbuka untuk lalu lintas masuk dan keluar, itu dianggap tingkat keparahan tinggi. Agak mudah bagi aktor ancaman untuk mengkompromikan VPC menggunakan metode ini. Kemungkinan juga aktor ancaman akan dapat mengganggu atau mengeksfiltrasi sumber daya begitu mereka berada di VPC.

Security Hub CSPM merekomendasikan agar Anda memperlakukan temuan tingkat keparahan tinggi sebagai prioritas jangka pendek. Anda harus segera mengambil langkah-langkah remediasi. Anda juga harus mempertimbangkan kekritisannya sumber daya.

Medium — Masalah ini harus ditangani sebagai prioritas jangka menengah.

Misalnya, kurangnya enkripsi untuk data dalam perjalanan dianggap sebagai temuan tingkat keparahan sedang. Dibutuhkan man-in-the-middle serangan canggih untuk memanfaatkan

kelemahan ini. Dengan kata lain, ini agak sulit. Kemungkinan beberapa data akan dikompromikan jika skenario ancaman berhasil.

Security Hub CSPM merekomendasikan agar Anda menyelidiki sumber daya yang terlibat pada kenyamanan Anda paling awal. Anda juga harus mempertimbangkan kekritisannya sumber daya.

Rendah — Masalah ini tidak memerlukan tindakan sendiri.

Misalnya, kegagalan untuk mengumpulkan informasi forensik dianggap tingkat keparahan rendah. Kontrol ini dapat membantu mencegah kompromi di masa depan, tetapi tidak adanya forensik tidak mengarah langsung pada kompromi.

Anda tidak perlu mengambil tindakan segera pada temuan tingkat keparahan rendah, tetapi mereka dapat memberikan konteks ketika Anda menghubungkannya dengan masalah lain.

Informasi - Tidak ada kelemahan konfigurasi yang ditemukan.

Dengan kata lain, statusnya adalah `PASSED`, `WARNING`, atau `NOT AVAILABLE`.

Tidak ada tindakan yang disarankan. Temuan informasi membantu pelanggan untuk menunjukkan bahwa mereka berada dalam keadaan patuh.

Mengevaluasi status kepatuhan dan status kontrol

`Compliance.Status` Bidang Format Pencarian AWS Keamanan menjelaskan hasil temuan kontrol. AWS Security Hub Cloud Security Posture Management (CSPM) menggunakan status kepatuhan temuan kontrol untuk menentukan status kontrol secara keseluruhan. Status kontrol ditampilkan pada halaman detail kontrol pada konsol CSPM Security Hub.

Mengevaluasi status kepatuhan temuan CSPM Security Hub

Status kepatuhan untuk setiap temuan diberikan salah satu dari nilai berikut:

- **PASSED**— Menunjukkan bahwa kontrol melewati pemeriksaan keamanan untuk temuan tersebut. Ini secara otomatis mengatur `CSPM Workflow.Status` Security Hub ke `RESOLVED`
- **FAILED**— Menunjukkan bahwa kontrol tidak lulus pemeriksaan keamanan untuk temuan tersebut.
- **WARNING**— Menunjukkan bahwa Security Hub CSPM tidak dapat menentukan apakah sumber daya berada dalam status `PASSED` atau `FAILED` tidak. Misalnya, [perekaman AWS Config sumber daya](#) tidak diaktifkan untuk jenis sumber daya yang sesuai.
- **NOT_AVAILABLE**— Menunjukkan bahwa pemeriksaan tidak dapat diselesaikan karena server gagal, sumber daya dihapus, atau hasil AWS Config evaluasi `NOT_APPLICABLE`. Jika hasil AWS

Config evaluasi itu `NOT_APPLICABLE`, Security Hub CSPM secara otomatis mengarsipkan temuan tersebut.

Jika status kepatuhan untuk temuan berubah dari `PASSED` menjadi `FAILED`, `WARNING`, dan `Workflow.Status` merupakan salah satu `NOTIFIED` atau `NOT_AVAILABLE`, `RESOLVED`, CSPM Security Hub secara otomatis berubah `Workflow.Status` menjadi `NEW`.

Jika Anda tidak memiliki sumber daya yang sesuai dengan kontrol, Security Hub CSPM menghasilkan `PASSED` temuan di tingkat akun. Jika Anda memiliki sumber daya yang sesuai dengan kontrol tetapi kemudian menghapus sumber daya, Security Hub CSPM membuat `NOT_AVAILABLE` temuan dan mengarsipkannya segera. Setelah 18 jam, Anda menerima `PASSED` temuan karena Anda tidak lagi memiliki sumber daya yang sesuai dengan kontrol.

Mendapatkan status kontrol dari status kepatuhan

Security Hub CSPM memperoleh status kontrol keseluruhan dari status kepatuhan temuan kontrol. Saat menentukan status kontrol, Security Hub CSPM mengabaikan temuan yang memiliki `RecordState` of `ARCHIVED` dan temuan yang memiliki `Workflow.Status` `SUPPRESSED`.

Status kontrol diberikan salah satu nilai berikut:

- **Lulus** — Menunjukkan bahwa semua temuan memiliki status kepatuhan `PASSED`.
- **Gagal** - Menunjukkan bahwa setidaknya satu temuan memiliki status kepatuhan `FAILED`.
- **Tidak diketahui** - Menunjukkan bahwa setidaknya satu temuan memiliki status kepatuhan `WARNING` atau `NOT_AVAILABLE`. Tidak ada temuan yang memiliki status kepatuhan `FAILED`.
- **Tidak ada data** — Menunjukkan bahwa tidak ada temuan untuk kontrol. Misalnya, kontrol yang baru diaktifkan memiliki status ini sampai Security Hub CSPM mulai menghasilkan temuan untuk itu. Kontrol juga memiliki status ini jika semua temuannya `SUPPRESSED` atau tidak tersedia saat ini Wilayah AWS.
- **Dinonaktifkan** - Menunjukkan bahwa kontrol dinonaktifkan di akun saat ini dan Wilayah. Saat ini tidak ada pemeriksaan keamanan yang dilakukan untuk kontrol ini di akun saat ini dan Wilayah. Namun, temuan kontrol yang dinonaktifkan mungkin memiliki nilai untuk status kepatuhan hingga 24 jam setelah penonaktifan.

Untuk akun administrator, status kontrol mencerminkan status kontrol untuk akun administrator dan akun anggota. Secara khusus, status keseluruhan kontrol muncul sebagai **Gagal** jika kontrol memiliki

satu atau lebih temuan gagal di akun administrator atau salah satu akun anggota. Jika Anda telah menetapkan Wilayah agregasi, status kontrol di Wilayah agregasi mencerminkan status kontrol di Wilayah agregasi dan Wilayah yang ditautkan. Secara khusus, status keseluruhan kontrol muncul sebagai Gagal jika kontrol memiliki satu atau lebih temuan gagal di Wilayah agregasi atau salah satu Wilayah terkait.

Security Hub CSPM biasanya menghasilkan status kontrol awal dalam waktu 30 menit setelah kunjungan pertama Anda ke halaman Ringkasan atau halaman standar Keamanan di konsol CSPM Security Hub. Anda harus memiliki [perekaman AWS Config sumber daya](#) yang dikonfigurasi agar status kontrol muncul. Setelah status kontrol dibuat untuk pertama kalinya, Security Hub CSPM memperbarui status kontrol setiap 24 jam berdasarkan temuan dari 24 jam sebelumnya. Stempel waktu pada halaman detail kontrol menunjukkan kapan status kontrol terakhir diperbarui.

Note

Setelah mengaktifkan kontrol untuk pertama kalinya, diperlukan waktu hingga 24 jam untuk status kontrol yang akan dihasilkan di Wilayah Tiongkok dan. AWS GovCloud (US) Region

Menghitung skor keamanan

Pada konsol AWS Security Hub Cloud Security Posture Management (CSPM), halaman Ringkasan dan halaman Kontrol menampilkan skor keamanan ringkasan di semua standar yang diaktifkan. Pada halaman standar Keamanan, Security Hub CSPM juga menampilkan skor keamanan dari 0-100 persen untuk setiap standar yang diaktifkan.

Saat pertama kali mengaktifkan Security Hub CSPM, Security Hub CSPM menghitung skor keamanan ringkasan dan skor keamanan standar dalam waktu 30 menit sejak kunjungan pertama Anda ke halaman Ringkasan atau Standar Keamanan di konsol. Skor dihasilkan hanya untuk standar yang diaktifkan saat Anda mengunjungi halaman tersebut di konsol. Selain itu, perekaman AWS Config sumber daya harus dikonfigurasi agar skor muncul. Skor keamanan ringkasan adalah rata-rata skor keamanan standar. Untuk meninjau daftar standar yang saat ini diaktifkan, Anda dapat menggunakan [GetEnabledStandards](#) pengoperasian Security Hub CSPM API.

Setelah menghasilkan skor pertama kali, Security Hub CSPM memperbarui skor keamanan setiap 24 jam. Security Hub CSPM menampilkan stempel waktu untuk menunjukkan kapan skor keamanan terakhir diperbarui. Perhatikan bahwa diperlukan waktu hingga 24 jam untuk skor keamanan pertama kali dihasilkan di Wilayah Tiongkok dan. AWS GovCloud (US) Regions

Jika Anda mengaktifkan [temuan kontrol konsolidasi](#), diperlukan waktu hingga 24 jam agar skor keamanan Anda diperbarui. Selain itu, mengaktifkan Wilayah agregasi baru atau memperbarui Wilayah tertaut akan me-reset skor keamanan yang ada. Diperlukan waktu hingga 24 jam untuk Security Hub CSPM untuk menghasilkan skor keamanan baru yang mencakup data dari Wilayah yang diperbarui.

Metode penghitungan skor keamanan

Skor keamanan mewakili proporsi kontrol Lulus ke kontrol yang diaktifkan. Skor ditampilkan sebagai persentase yang dibulatkan ke atas atau ke bawah ke bilangan bulat terdekat.

Security Hub CSPM menghitung skor keamanan ringkasan di semua standar yang Anda aktifkan. Security Hub CSPM juga menghitung skor keamanan untuk setiap standar yang diaktifkan. Untuk tujuan perhitungan skor, kontrol yang diaktifkan menyertakan kontrol dengan status Lulus, Gagal, dan Tidak Diketahui. Kontrol dengan status Tidak ada data dikecualikan dari perhitungan skor.

Security Hub CSPM mengabaikan temuan yang diarsipkan dan ditekan saat menghitung status kontrol. Ini dapat memengaruhi skor keamanan. Misalnya, jika Anda menekan semua temuan yang gagal untuk kontrol, statusnya menjadi Lulus, yang pada gilirannya dapat meningkatkan skor keamanan Anda. Untuk informasi selengkapnya tentang status kontrol, lihat [Mengevaluasi status kepatuhan dan status kontrol](#).

Contoh penilaian:

Standar	Kontrol yang lulus	Kontrol gagal	Kontrol tidak diketahui	Skor standar
AWS Praktik Terbaik Keamanan Dasar v1.0.0	168	22	0	88%
Tolok Ukur AWS Yayasan CIS v1.4.0	8	29	0	22%
Tolok Ukur AWS Yayasan CIS v1.2.0	6	35	0	15%

Standar	Kontrol yang lulus	Kontrol gagal	Kontrol tidak diketahui	Skor standar
Publikasi Khusus NIST 800-53 Revisi 5	159	56	0	74%
PCI DSS v3.2.1	28	17	0	62%

Saat menghitung skor keamanan ringkasan, Security Hub CSPM menghitung setiap kontrol hanya sekali di seluruh standar. Misalnya, jika Anda telah mengaktifkan kontrol yang berlaku untuk tiga standar yang diaktifkan, itu hanya dihitung sebagai satu kontrol yang diaktifkan untuk tujuan penilaian.

Dalam contoh ini, meskipun jumlah total kontrol yang diaktifkan di seluruh standar yang diaktifkan adalah 528, Security Hub CSPM menghitung setiap kontrol unik hanya sekali untuk tujuan penilaian. Jumlah kontrol unik yang diaktifkan kemungkinan lebih rendah dari 528. Jika kita menganggap jumlah kontrol unik yang diaktifkan adalah 515, dan jumlah kontrol unik yang dilewati adalah 357, skor ringkasan adalah 69%. Skor ini dihitung dengan membagi jumlah kontrol unik yang dilewatkan dengan jumlah kontrol unik yang diaktifkan.

Anda mungkin memiliki skor ringkasan yang berbeda dari skor keamanan standar, meskipun Anda hanya mengaktifkan satu standar di akun Anda di Wilayah saat ini. Hal ini dapat terjadi jika Anda masuk ke akun administrator dan akun anggota memiliki standar tambahan atau standar yang berbeda diaktifkan. Hal ini juga dapat terjadi jika Anda melihat skor dari Wilayah agregasi dan standar tambahan atau standar yang berbeda diaktifkan di Wilayah tertaut.

Skor keamanan untuk akun administrator

Jika Anda masuk ke akun administrator, skor keamanan ringkasan dan skor standar akun untuk status kontrol di akun administrator dan semua akun anggota.

Jika status kontrol Gagal bahkan di satu akun anggota, statusnya Gagal di akun administrator dan berdampak pada skor akun administrator.

Jika Anda masuk ke akun administrator dan melihat skor di Wilayah agregasi, skor keamanan akan memperhitungkan status kontrol di semua akun anggota dan semua Wilayah yang ditautkan.

Skor keamanan jika Anda telah menetapkan Wilayah agregasi

Jika Anda telah menetapkan agregasi Wilayah AWS, skor keamanan ringkasan dan skor standar memperhitungkan status kontrol di semua Wilayah terkait.

Jika status kontrol Gagal bahkan di satu Wilayah yang ditautkan, statusnya Gagal di Wilayah agregasi dan berdampak pada skor Wilayah agregasi.

Jika Anda masuk ke akun administrator dan melihat skor di Wilayah agregasi, skor keamanan akan memperhitungkan status kontrol di semua akun anggota dan semua Wilayah yang ditautkan.

Kategori kontrol di Security Hub CSPM

Setiap kontrol diberi kategori. Kategori untuk kontrol mencerminkan fungsi keamanan yang berlaku untuk kontrol.

Nilai kategori berisi kategori, subkategori dalam kategori, dan, secara opsional, pengklasifikasi dalam subkategori. Misalnya:

- Identifikasi > Inventaris
- Lindungi > Perlindungan data > Enkripsi data dalam perjalanan

Berikut adalah deskripsi dari kategori, subkategori, dan pengklasifikasi yang tersedia.

Identifikasi

Mengembangkan pemahaman organisasi untuk mengelola risiko keamanan siber terhadap sistem, aset, data, dan kemampuan.

Inventaris

Sudahkah layanan menerapkan strategi penandaan sumber daya yang benar? Apakah strategi penandaan termasuk pemilik sumber daya?

Sumber daya apa yang digunakan layanan ini? Apakah mereka menyetujui sumber daya untuk layanan ini?

Apakah Anda memiliki visibilitas ke inventaris yang disetujui? Misalnya, apakah Anda menggunakan layanan seperti Amazon EC2 Systems Manager dan Service Catalog?

Pencatatan log

Sudahkah Anda mengaktifkan semua pencatatan yang relevan untuk layanan ini dengan aman?
Contoh file log meliputi yang berikut ini:

- Log Aliran VPC Amazon
- Log akses Elastic Load Balancing
- CloudFront Log Amazon
- CloudWatch Log Amazon
- Pencatatan Layanan Basis Data Relasional Amazon
- Log indeks lambat OpenSearch Layanan Amazon
- Penelusuran X-Ray
- AWS Directory Service log
- AWS Config barang
- Snapshot

Lindungi

Mengembangkan dan menerapkan perlindungan yang tepat untuk memastikan penyampaian layanan infrastruktur penting dan praktik pengkodean yang aman.

Manajemen akses yang aman

Apakah layanan menggunakan praktik hak istimewa paling sedikit dalam IAM atau kebijakan sumber dayanya?

Apakah kata sandi dan rahasia cukup kompleks? Apakah mereka diputar dengan tepat?

Apakah layanan menggunakan otentikasi multi-faktor (MFA)?

Apakah layanan menghindari pengguna root?

Apakah kebijakan berbasis sumber daya memungkinkan akses publik?

Konfigurasi jaringan aman

Apakah layanan menghindari akses jaringan jarak jauh publik dan tidak aman?

Apakah layanan ini digunakan VPCs dengan benar? Misalnya, apakah pekerjaan diperlukan untuk dijalankan VPCs?

Apakah layanan mengelompokkan dan mengisolasi sumber daya sensitif dengan benar?

Perlindungan data

Enkripsi data saat istirahat — Apakah layanan mengenkripsi data saat istirahat?

Enkripsi data dalam perjalanan — Apakah layanan mengenkripsi data dalam perjalanan?

Integritas data — Apakah layanan memvalidasi data untuk integritas?

Perlindungan penghapusan data — Apakah layanan melindungi data dari penghapusan yang tidak disengaja?

Pengelolaan/penggunaan data — Apakah Anda menggunakan layanan seperti Amazon Macie untuk melacak lokasi data sensitif Anda?

Perlindungan API

Apakah layanan digunakan AWS PrivateLink untuk melindungi operasi API layanan?

Layanan pelindung

Apakah layanan perlindungan yang benar ada? Apakah mereka memberikan jumlah pertanggungjawaban yang benar?

Layanan pelindung membantu Anda menangkis serangan dan kompromi yang diarahkan pada layanan. Contoh layanan perlindungan AWS termasuk AWS Control Tower,,, Vanta AWS WAF AWS Shield Advanced, Secrets Manager, IAM Access Analyzer, dan. AWS Resource Access Manager

Pengembangan yang aman

Apakah Anda menggunakan praktik pengkodean yang aman?

Apakah Anda menghindari kerentanan seperti Open Web Application Security Project (OWASP) Top Ten?

Mendeteksi

Mengembangkan dan menerapkan kegiatan yang sesuai untuk mengidentifikasi terjadinya peristiwa keamanan siber.

Layanan deteksi

Apakah layanan deteksi yang benar ada?

Apakah mereka memberikan jumlah pertanggungungan yang benar?

Contoh layanan AWS deteksi termasuk Amazon GuardDuty, AWS Security Hub Cloud Security Posture Management (CSPM), Amazon Inspector, Amazon Detective CloudWatch , Amazon AWS IoT Device Defender Alarm, dan. AWS Trusted Advisor

Menanggapi

Mengembangkan dan menerapkan kegiatan yang sesuai untuk mengambil tindakan terkait peristiwa keamanan siber yang terdeteksi.

Tindakan respons

Apakah Anda menanggapi peristiwa keamanan dengan cepat?

Apakah Anda memiliki temuan kritis atau tingkat keparahan tinggi yang aktif?

Forensik

Bisakah Anda memperoleh data forensik dengan aman untuk layanan ini? Misalnya, apakah Anda memperoleh snapshot Amazon EBS yang terkait dengan temuan positif sejati?

Sudahkah Anda membuat akun forensik?

Memulihkan

Mengembangkan dan mengimplementasikan kegiatan yang sesuai untuk mempertahankan rencana ketahanan dan memulihkan kemampuan atau layanan apa pun yang terganggu karena peristiwa keamanan siber.

Ketahanan

Apakah konfigurasi layanan mendukung kegagalan yang anggun, penskalaan elastis, dan ketersediaan tinggi?

Sudahkah Anda membuat cadangan?

Meninjau rincian kontrol di Security Hub CSPM

Memilih kontrol pada halaman Kontrol atau halaman detail standar konsol CSPM Security Hub akan membawa Anda ke halaman detail kontrol.

Bagian atas halaman detail kontrol menunjukkan status kontrol. Status kontrol merangkum kinerja kontrol berdasarkan status kepatuhan temuan kontrol. Security Hub CSPM biasanya menghasilkan status kontrol awal dalam waktu 30 menit setelah kunjungan pertama Anda ke halaman Ringkasan atau halaman standar Keamanan di konsol CSPM Security Hub. Status hanya tersedia untuk kontrol yang diaktifkan saat Anda mengunjungi halaman tersebut.

Halaman detail kontrol juga memberikan rincian status kepatuhan temuan kontrol dalam 24 jam terakhir. Untuk informasi selengkapnya tentang status kontrol dan status kepatuhan, lihat [Mengevaluasi status kepatuhan dan status kontrol](#).

AWS Config perekaman sumber daya harus dikonfigurasi agar status kontrol muncul. Setelah status kontrol dibuat untuk pertama kalinya, Security Hub CSPM memperbarui status kontrol setiap 24 jam berdasarkan temuan dari 24 jam sebelumnya.

Akun administrator melihat status kontrol gabungan di seluruh akun administrator dan akun anggota. Jika Anda telah menetapkan Wilayah agregasi, status kontrol mencakup temuan di semua Wilayah tertaut. Untuk informasi selengkapnya tentang status kontrol, lihat [the section called “Status kepatuhan dan status kontrol”](#).

Anda juga dapat mengaktifkan atau menonaktifkan kontrol dari halaman detail kontrol.

Note

Ini dapat memakan waktu hingga 24 jam setelah memungkinkan kontrol untuk status kontrol pertama kali yang akan dihasilkan di Wilayah Tiongkok dan. AWS GovCloud (US) Regions

Tab Standar dan Persyaratan mencantumkan standar yang dapat diaktifkan oleh kontrol dan persyaratan yang terkait dengan kontrol dari kerangka kerja kepatuhan yang berbeda.

Tab Cek mencantumkan temuan aktif untuk kontrol selama 24 jam terakhir. Temuan kontrol dihasilkan ketika Security Hub CSPM menjalankan pemeriksaan keamanan untuk kontrol. Daftar di tab ini tidak menyertakan temuan yang diarsipkan.

Untuk setiap temuan, daftar menyediakan akses untuk menemukan detail seperti status kepatuhan dan sumber daya terkait. Anda juga dapat mengatur status alur kerja setiap temuan dan mengirim temuan ke tindakan kustom. Untuk informasi selengkapnya, lihat [the section called “Meninjau dan mengelola temuan kontrol”](#).

Melihat detail untuk kontrol

Pilih metode akses pilihan Anda, dan ikuti langkah-langkah ini untuk meninjau detail untuk kontrol. Detail berlaku untuk akun saat ini dan Wilayah dan termasuk yang berikut:

- Judul dan deskripsi kontrol.
- Tautan ke panduan remediasi untuk temuan kontrol yang gagal.
- Tingkat keparahan kontrol.
- Status kontrol.

Di konsol, Anda juga dapat meninjau daftar temuan terbaru untuk kontrol. Untuk melakukan ini secara terprogram, Anda dapat menggunakan [GetFindings](#) pengoperasian Security Hub CSPM API.

Security Hub CSPM console

1. Buka konsol AWS Security Hub Cloud Security Posture Management (CSPM) di <https://console.aws.amazon.com/securityhub/>
2. Pilih Kontrol di panel navigasi.
3. Pilih kontrol.

Security Hub CSPM API

1. Jalankan [ListSecurityControlDefinitions](#), dan berikan satu atau lebih standar ARNs untuk mendapatkan daftar kontrol IDs untuk standar itu. Untuk mendapatkan standar ARNs, jalankan [DescribeStandards](#). Jika Anda tidak menyediakan ARN standar, API ini mengembalikan semua kontrol CSPM Security Hub. IDs API ini mengembalikan kontrol keamanan agnostik standar IDs, bukan kontrol IDs berbasis standar yang ada sebelum rilis fitur ini.

Contoh permintaan:

```
{
```

```
"StandardsArn": "arn:aws:securityhub:::standards/aws-foundational-security-best-practices/v/1.0.0"
}
```

2. Jalankan [BatchGetSecurityControls](#) untuk mendapatkan detail tentang satu atau lebih kontrol saat ini Akun AWS dan Wilayah AWS.

Contoh permintaan:

```
{
  "SecurityControlIds": ["Config.1", "IAM.1"]
}
```

AWS CLI

1. Jalankan [list-security-control-definitions](#) perintah, dan berikan satu atau lebih standar ARNs untuk mendapatkan daftar kontrol IDs. Untuk mendapatkan standar ARNs, jalankan `describe-standards` perintah. Jika Anda tidak menyediakan ARN standar, perintah ini mengembalikan semua kontrol CSPM Security Hub. IDs Perintah ini mengembalikan kontrol keamanan agnostik standar IDs, bukan kontrol IDs berbasis standar yang ada sebelum rilis fitur ini.

```
aws securityhub --region us-east-1 list-security-control-definitions --
standards-arn "arn:aws:securityhub:us-east-1::standards/aws-foundational-
security-best-practices/v/1.0.0"
```

2. Jalankan [batch-get-security-controls](#) perintah untuk mendapatkan detail tentang satu atau lebih kontrol saat ini Akun AWS dan Wilayah AWS.

```
aws securityhub --region us-east-1 batch-get-security-controls --security-
control-ids '["Config.1", "IAM.1"]'
```

Memfilter dan menyortir kontrol di Security Hub CSPM

Pada konsol AWS Security Hub Cloud Security Posture Management (CSPM), Anda dapat menggunakan halaman Kontrol untuk meninjau tabel kontrol yang tersedia saat ini. Wilayah AWS Pengecualian adalah Wilayah agregasi. Jika Anda [mengonfigurasi Wilayah agregasi](#) dan masuk ke

Wilayah tersebut, konsol akan menampilkan kontrol yang tersedia di Wilayah agregasi atau satu atau beberapa Wilayah tertaut.

Untuk fokus pada subset kontrol tertentu, Anda dapat mengurutkan dan memfilter tabel kontrol. Filter menurut opsi di sebelah tabel dapat membantu Anda dengan cepat fokus pada himpunan bagian tertentu ini:

- Semua kontrol yang diaktifkan, yang merupakan kontrol yang diaktifkan dalam setidaknya satu standar yang diaktifkan.
- Semua kontrol yang dinonaktifkan, yang merupakan kontrol yang dinonaktifkan di semua standar.
- Semua kontrol yang diaktifkan yang memiliki status kontrol tertentu, seperti Gagal. Opsi Tidak ada data hanya menampilkan kontrol yang saat ini tidak memiliki temuan. Untuk informasi tentang status kontrol, lihat [Mengevaluasi status kepatuhan dan status kontrol](#).

Selain Filter menurut opsi, Anda dapat memfilter tabel dengan memasukkan kriteria filter di kotak Kontrol filter di atas tabel. Misalnya, Anda dapat memfilter berdasarkan ID kontrol atau tingkat keparahan.

Secara default, kontrol dengan status Gagal dicantumkan terlebih dahulu, dalam urutan menurun berdasarkan tingkat keparahan. Anda dapat mengubah urutan pengurutan dengan memilih judul kolom yang berbeda.

 Tip

Jika Anda memiliki alur kerja otomatis berdasarkan temuan kontrol, sebaiknya gunakan [bidang SecurityControlId atau SecurityControlArn ASFF](#) sebagai filter, bukan bidang Title atau Description. Bidang yang terakhir dapat berubah sesekali, sedangkan ID kontrol dan ARN adalah pengidentifikasi statis.

Jika Anda masuk ke akun administrator CSPM Security Hub, Kontrol yang diaktifkan menyertakan kontrol yang diaktifkan di setidaknya satu akun anggota. Jika Anda mengonfigurasi Wilayah agregasi, Kontrol yang diaktifkan menyertakan kontrol yang diaktifkan di setidaknya satu Wilayah tertaut.

Jika Anda memilih opsi di sebelah kontrol yang diaktifkan, panel akan muncul dan menampilkan standar di mana kontrol saat ini diaktifkan. Anda juga dapat melihat standar di mana kontrol saat ini dinonaktifkan. Dari panel ini, Anda dapat menonaktifkan kontrol di semua standar. Untuk informasi

selengkapnya, lihat [Menonaktifkan kontrol di Security Hub CSPM](#). Untuk akun administrator, informasi di panel mencerminkan pengaturan untuk semua akun anggota Anda.

Untuk mengambil daftar kontrol secara terprogram, Anda dapat menggunakan [ListSecurityControlDefinitions](#) pengoperasian Security Hub CSPM API. Untuk mengambil rincian kontrol individu, gunakan [BatchGetSecurityControls](#) operasi.

Memahami parameter kontrol di Security Hub CSPM

Beberapa kontrol di AWS Security Hub Cloud Security Posture Management (CSPM) menggunakan parameter yang memengaruhi cara kontrol dievaluasi. Biasanya, kontrol tersebut dievaluasi terhadap nilai parameter default yang didefinisikan oleh Security Hub CSPM. Namun, untuk subset dari kontrol ini, Anda dapat memodifikasi nilai parameter. Saat Anda mengubah nilai parameter kontrol, Security Hub CSPM mulai mengevaluasi kontrol terhadap nilai yang Anda tentukan. Jika sumber daya yang mendasari kontrol memenuhi nilai kustom, Security Hub CSPM menghasilkan temuan. PASSED Jika sumber daya tidak memenuhi nilai kustom, Security Hub CSPM akan menghasilkan temuan. FAILED

Dengan menyesuaikan parameter kontrol, Anda dapat menyempurnakan praktik terbaik keamanan yang direkomendasikan dan dipantau oleh Security Hub CSPM agar sesuai dengan persyaratan bisnis dan harapan keamanan Anda. Alih-alih menekan temuan untuk kontrol, Anda dapat menyesuaikan satu atau lebih parameternya untuk mendapatkan temuan yang sesuai dengan kebutuhan keamanan Anda.

Berikut adalah beberapa contoh kasus penggunaan untuk memodifikasi parameter kontrol dan menyetel nilai kustom:

- [CloudWatch.16] — grup CloudWatch log harus dipertahankan untuk jangka waktu tertentu

Anda dapat menentukan periode waktu retensi.

- [IAM.7] — Kebijakan kata sandi untuk pengguna IAM harus memiliki konfigurasi yang kuat

Anda dapat menentukan parameter yang terkait dengan kekuatan kata sandi.

- [EC2.18] - Grup keamanan seharusnya hanya mengizinkan lalu lintas masuk yang tidak terbatas untuk port resmi

Anda dapat menentukan port mana yang diizinkan untuk mengizinkan lalu lintas masuk yang tidak dibatasi.

- [Lambda.5] - Fungsi VPC Lambda harus beroperasi di beberapa Availability Zone

Anda dapat menentukan jumlah minimum Availability Zones yang menghasilkan temuan yang diteruskan.

Bagian ini mencakup hal-hal yang perlu dipertimbangkan ketika Anda memodifikasi parameter kontrol.

Pengaruh memodifikasi nilai parameter kontrol

Saat Anda mengubah nilai parameter, Anda juga memicu pemeriksaan keamanan baru yang mengevaluasi kontrol berdasarkan nilai baru. Security Hub CSPM kemudian menghasilkan temuan kontrol baru berdasarkan nilai baru. Selama pembaruan berkala untuk mengontrol temuan, Security Hub CSPM juga menggunakan nilai parameter baru. Jika Anda mengubah nilai parameter untuk kontrol, tetapi belum mengaktifkan standar apa pun yang menyertakan kontrol, Security Hub CSPM tidak melakukan pemeriksaan keamanan apa pun menggunakan nilai baru. Anda harus mengaktifkan setidaknya satu standar yang relevan untuk Security Hub CSPM untuk mengevaluasi kontrol berdasarkan nilai parameter baru.

Kontrol dapat memiliki satu atau lebih parameter yang dapat disesuaikan. Jenis data yang mungkin untuk setiap parameter kontrol meliputi yang berikut:

- Boolean
- Ganda
- Enum
- EnumList
- Bilangan Bulat
- IntegerList
- String
- StringList

Nilai parameter kustom berlaku di seluruh standar yang diaktifkan. Anda tidak dapat menyesuaikan parameter untuk kontrol yang tidak didukung di Wilayah Anda saat ini. Untuk daftar batas Regional untuk kontrol individu, lihat [Batas regional pada kontrol CSPM Security Hub](#).

Untuk beberapa kontrol, nilai parameter yang dapat diterima harus jatuh ke dalam rentang tertentu agar valid. Dalam kasus ini, Security Hub CSPM menyediakan rentang yang dapat diterima.

Security Hub CSPM memilih nilai parameter default dan terkadang memperbaruinya. Setelah Anda menyesuaikan parameter kontrol, nilainya terus menjadi nilai yang Anda tentukan untuk parameter kecuali Anda mengubahnya. Artinya, parameter berhenti melacak pembaruan ke nilai CSPM Security Hub default, bahkan jika nilai kustom parameter cocok dengan nilai default saat ini yang ditentukan oleh Security Hub CSPM. Berikut adalah contoh untuk kontrol [ACM.1] - Sertifikat yang diimpor dan diterbitkan ACM harus diperbarui setelah jangka waktu tertentu:

```
{
  "SecurityControlId": "ACM.1",
  "Parameters": {
    "daysToExpiration": {
      "ValueType": "CUSTOM",
      "Value": {
        "Integer": 30
      }
    }
  }
}
```

Dalam contoh sebelumnya, `daysToExpiration` parameter memiliki nilai kustom. 30 Nilai default saat ini untuk parameter ini juga 30. Jika Security Hub CSPM mengubah nilai default menjadi 14, parameter dalam contoh ini tidak akan melacak perubahan tersebut. Ini akan mempertahankan nilai 30.

Jika Anda ingin melacak pemutakhiran ke nilai CSPM Security Hub default untuk parameter, setel `ValueType` bidang ke `DEFAULT` bukan. `CUSTOM` Untuk informasi selengkapnya, lihat [Mengembalikan ke parameter kontrol default dalam satu akun dan Wilayah](#).

Kontrol yang mendukung parameter kustom

Untuk daftar kontrol keamanan yang mendukung parameter kustom, lihat halaman Kontrol konsol CSPM Security Hub atau. [Referensi kontrol untuk Security Hub CSPM](#) Untuk mengambil daftar ini secara terprogram, Anda dapat menggunakan operasi. [ListSecurityControlDefinitions](#) Dalam respons, `CustomizableProperties` objek menunjukkan kontrol mana yang mendukung parameter yang dapat disesuaikan.

Meninjau nilai parameter kontrol saat ini

Akan sangat membantu untuk mengetahui nilai parameter kontrol saat ini sebelum Anda memodifikasinya.

Anda dapat meninjau nilai saat ini untuk parameter kontrol individual di akun Anda. Jika Anda menggunakan konfigurasi pusat, administrator AWS Security Hub Cloud Security Posture Management (CSPM) yang didelegasikan juga dapat meninjau nilai parameter yang ditentukan dalam kebijakan konfigurasi.

Pilih metode pilihan Anda, dan ikuti langkah-langkah untuk meninjau nilai parameter kontrol saat ini.

Security Hub CSPM console

Untuk meninjau nilai parameter kontrol saat ini (konsol)

1. Buka konsol AWS Security Hub Cloud Security Posture Management (CSPM) di <https://console.aws.amazon.com/securityhub/>
2. Di panel navigasi, pilih Kontrol. Pilih kontrol.
3. Pilih tab Parameter. Tab ini menunjukkan nilai parameter saat ini untuk kontrol.

Security Hub CSPM API

Untuk meninjau nilai parameter kontrol saat ini (API)

Panggil [BatchGetSecurityControls](#) API, dan berikan satu atau lebih kontrol keamanan IDs atau ARNs. `Parameters` objek dalam respons menunjukkan nilai parameter saat ini untuk kontrol yang ditentukan.

Misalnya, AWS CLI perintah berikut menunjukkan nilai parameter saat ini untuk `APIGateway.1`, `CloudWatch.15`, dan `IAM.7`. Contoh ini diformat untuk Linux, macOS, atau Unix, dan menggunakan karakter garis miring terbalik (`\`) untuk meningkatkan keterbacaan.

```
$ aws securityhub batch-get-security-controls \
--region us-east-1 \
--security-control-ids '["APIGateway.1", "CloudWatch.15", "IAM.7"]'
```

Pilih metode pilihan Anda untuk melihat nilai parameter saat ini dalam kebijakan konfigurasi pusat.

Security Hub CSPM console

Untuk meninjau nilai parameter kontrol saat ini dalam kebijakan konfigurasi (konsol)

1. Buka konsol AWS Security Hub Cloud Security Posture Management (CSPM) di <https://console.aws.amazon.com/securityhub/>

Masuk menggunakan kredensial akun administrator CSPM Security Hub yang didelegasikan di Wilayah asal.

2. Di panel navigasi, pilih Pengaturan dan Konfigurasi.
3. Pada tab Kebijakan, pilih kebijakan konfigurasi, lalu pilih Lihat detail. Detail kebijakan kemudian muncul, termasuk nilai parameter saat ini.

Security Hub CSPM API

Untuk meninjau nilai parameter kontrol saat ini dalam kebijakan konfigurasi (API)

1. Memanggil [GetConfigurationPolicy](#) API dari akun administrator yang didelegasikan di Wilayah beranda.
2. Berikan ARN atau ID kebijakan konfigurasi yang detailnya ingin Anda lihat. Respons mencakup nilai parameter saat ini.

Misalnya, AWS CLI perintah berikut mengambil nilai parameter kontrol saat ini dalam kebijakan konfigurasi yang ditentukan. Contoh ini diformat untuk Linux, macOS, atau Unix, dan menggunakan karakter garis miring terbalik (\) untuk meningkatkan keterbacaan.

```
$ aws securityhub get-configuration-policy \
--region us-east-1 \
--identifier "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

Temuan kontrol juga mencakup nilai parameter kontrol saat ini. Dalam [AWS Format Pencarian Keamanan \(ASFF\)](#), nilai-nilai ini muncul di Parameters bidang Compliance objek. Untuk meninjau temuan di konsol CSPM Security Hub, pilih Temuan di panel navigasi. Untuk meninjau temuan secara terprogram, gunakan [GetFindings](#) pengoperasian Security Hub CSPM API.

Menyesuaikan nilai parameter kontrol

Petunjuk untuk menyesuaikan parameter kontrol bervariasi berdasarkan apakah Anda menggunakan [konfigurasi pusat](#) di AWS Security Hub Cloud Security Posture Management (CSPM). Konfigurasi pusat adalah fitur yang dapat digunakan oleh administrator CSPM Security Hub yang didelegasikan untuk mengonfigurasi kapabilitas CSPM Security Hub di seluruh Wilayah AWS, akun, dan unit organisasi (). OUs

Jika organisasi Anda menggunakan konfigurasi pusat, administrator yang didelegasikan dapat membuat kebijakan konfigurasi yang menyertakan parameter kontrol kustom. Kebijakan ini dapat dikaitkan dengan akun anggota yang dikelola secara terpusat dan OUs, dan berlaku di Wilayah asal Anda dan semua Wilayah yang ditautkan. Administrator yang didelegasikan juga dapat menetapkan satu atau lebih akun sebagai dikelola sendiri, yang memungkinkan pemilik akun untuk mengonfigurasi parameternya sendiri secara terpisah di setiap Wilayah. Jika organisasi Anda tidak menggunakan konfigurasi pusat, Anda harus menyesuaikan parameter kontrol secara terpisah di setiap akun dan Wilayah.

Sebaiknya gunakan konfigurasi pusat karena memungkinkan Anda menyelaraskan nilai parameter kontrol di berbagai bagian organisasi Anda. Misalnya, semua akun pengujian Anda mungkin menggunakan nilai parameter tertentu, dan semua akun produksi mungkin menggunakan nilai yang berbeda.

Menyesuaikan parameter kontrol di beberapa akun dan Wilayah

Jika Anda adalah administrator CSPM Security Hub yang didelegasikan untuk organisasi yang menggunakan konfigurasi pusat, pilih metode pilihan Anda, dan ikuti langkah-langkah untuk menyesuaikan parameter kontrol di beberapa akun dan Wilayah.

Security Hub CSPM console

Untuk menyesuaikan nilai parameter kontrol di beberapa akun dan Wilayah (konsol)

1. Buka konsol AWS Security Hub Cloud Security Posture Management (CSPM) di. <https://console.aws.amazon.com/securityhub/>

Pastikan Anda masuk ke Wilayah asal.

2. Di panel navigasi, pilih Pengaturan dan Konfigurasi.
3. Pilih tab Kebijakan.

4. Untuk membuat kebijakan konfigurasi baru yang menyertakan parameter kustom, pilih Buat kebijakan. Untuk menentukan parameter kustom dalam kebijakan konfigurasi yang ada, pilih kebijakan, lalu pilih Edit.

Untuk membuat kebijakan konfigurasi baru dengan nilai parameter kontrol kustom

1. Di bagian Kebijakan kustom, pilih standar keamanan dan kontrol yang ingin Anda aktifkan.
2. Pilih Sesuaikan parameter kontrol.
3. Pilih kontrol, lalu tentukan nilai kustom untuk satu atau beberapa parameter.
4. Untuk menyesuaikan parameter untuk kontrol lainnya, pilih Sesuaikan kontrol tambahan.
5. Di bagian Akun, pilih akun atau OUs yang ingin Anda terapkan kebijakan.
6. Pilih Berikutnya.
7. Pilih Buat kebijakan dan terapkan. Di Wilayah beranda dan semua Wilayah yang ditautkan, tindakan ini mengesampingkan pengaturan konfigurasi akun yang ada dan OUs yang terkait dengan kebijakan konfigurasi ini. Akun dan OUs dapat dikaitkan dengan kebijakan konfigurasi melalui aplikasi langsung atau warisan dari orang tua.

Untuk menyesuaikan nilai parameter kontrol dalam kebijakan konfigurasi yang ada

1. Di bagian Kontrol, di bawah Kebijakan khusus, tentukan nilai parameter kustom baru yang Anda inginkan.
2. Jika ini adalah pertama kalinya Anda menyesuaikan parameter kontrol dalam kebijakan ini, pilih Sesuaikan parameter kontrol, lalu pilih kontrol untuk disesuaikan. Untuk menyesuaikan parameter untuk kontrol lainnya, pilih Sesuaikan kontrol tambahan.
3. Di bagian Akun, verifikasi akun atau kebijakan OUs yang ingin Anda terapkan.
4. Pilih Berikutnya.
5. Tinjau perubahan Anda, dan verifikasi bahwa perubahan tersebut benar. Setelah selesai, pilih Simpan kebijakan dan terapkan. Di Wilayah beranda dan semua Wilayah yang ditautkan, tindakan ini mengesampingkan pengaturan konfigurasi akun yang ada dan OUs yang terkait dengan kebijakan konfigurasi ini. Akun dan OUs dapat dikaitkan dengan kebijakan konfigurasi melalui aplikasi langsung atau warisan dari orang tua.

Security Hub CSPM API

Untuk menyesuaikan nilai parameter kontrol di beberapa akun dan Wilayah (API)

Untuk membuat kebijakan konfigurasi baru dengan nilai parameter kontrol kustom

1. Memanggil [CreateConfigurationPolicy](#) API dari akun administrator yang didelegasikan di Wilayah beranda.
2. Untuk `SecurityControlCustomParameters` objek, berikan pengenalan setiap kontrol yang ingin Anda sesuaikan.
3. Untuk `Parameters` objek, berikan nama setiap parameter yang ingin Anda sesuaikan. Untuk setiap parameter yang Anda sesuaikan, `CUSTOM` sediakan `ValueType`. Untuk `Value`, berikan tipe data parameter dan nilai kustom. `Value` bidang tidak bisa kosong kapan `ValueType` ada `CUSTOM`. Jika permintaan Anda menghilangkan parameter yang didukung kontrol, parameter tersebut mempertahankan nilainya saat ini. Anda dapat menemukan parameter yang didukung, tipe data, dan nilai yang valid untuk kontrol dengan menjalankan [GetSecurityControlDefinition](#) API.

Untuk menyesuaikan nilai parameter kontrol dalam kebijakan konfigurasi yang ada

1. Memanggil [UpdateConfigurationPolicy](#) API dari akun administrator yang didelegasikan di Wilayah beranda.
2. Untuk `Identifier` bidang, berikan Nama Sumber Daya Amazon (ARN) atau ID kebijakan konfigurasi yang ingin Anda perbarui.
3. Untuk `SecurityControlCustomParameters` objek, berikan pengenalan setiap kontrol yang ingin Anda sesuaikan.
4. Untuk `Parameters` objek, berikan nama setiap parameter yang ingin Anda sesuaikan. Untuk setiap parameter yang Anda sesuaikan, `CUSTOM` sediakan `ValueType`. Untuk `Value`, berikan tipe data parameter dan nilai kustom. Jika permintaan Anda menghilangkan parameter yang didukung kontrol, parameter tersebut mempertahankan nilainya saat ini. Anda dapat menemukan parameter yang didukung, tipe data, dan nilai yang valid untuk kontrol dengan menjalankan [GetSecurityControlDefinition](#) API.

Misalnya, AWS CLI perintah berikut membuat kebijakan konfigurasi baru dengan nilai kustom untuk `daysToExpiration` parameter `ACM.1`. Contoh ini diformat untuk Linux, macOS, atau Unix, dan menggunakan karakter garis miring terbalik (`\`) untuk meningkatkan keterbacaan.

```
$ aws securityhub create-configuration-policy \
--region us-east-1 \
--name "SampleConfigurationPolicy" \
```

```
--description "Configuration policy for production accounts" \  
--configuration-policy '{"SecurityHub": {"ServiceEnabled": true,  
  "EnabledStandardIdentifiers": ["arn:aws:securityhub:us-east-1::standards/aws-  
foundational-security-best-practices/v/1.0.0", "arn:aws:securityhub:::ruleset/  
cis-aws-foundations-benchmark/v/1.2.0"], "SecurityControlsConfiguration":  
{"DisabledSecurityControlIdentifiers": ["CloudTrail.2"],  
  "SecurityControlCustomParameters": [{"SecurityControlId": "ACM.1", "Parameters":  
{"daysToExpiration": {"ValueType": "CUSTOM", "Value": "Integer": 15}}}]}}}'
```

Menyesuaikan parameter kontrol dalam satu akun dan Wilayah

Jika Anda tidak menggunakan konfigurasi pusat atau memiliki akun yang dikelola sendiri, Anda dapat menyesuaikan parameter kontrol untuk akun Anda di satu Wilayah pada satu waktu saja.

Pilih metode pilihan Anda, dan ikuti langkah-langkah untuk menyesuaikan parameter kontrol. Perubahan Anda hanya berlaku untuk akun Anda di Wilayah saat ini. Untuk menyesuaikan parameter kontrol di Wilayah tambahan, ulangi langkah-langkah berikut di setiap akun tambahan dan Wilayah tempat Anda ingin menyesuaikan parameter. Kontrol yang sama dapat menggunakan nilai parameter yang berbeda di Wilayah yang berbeda.

Security Hub CSPM console

Untuk menyesuaikan nilai parameter kontrol dalam satu akun dan Wilayah (konsol)

1. Buka konsol AWS Security Hub Cloud Security Posture Management (CSPM) di <https://console.aws.amazon.com/securityhub/>
2. Di panel navigasi, pilih Kontrol. Dalam tabel, pilih kontrol yang mendukung parameter khusus dan Anda ingin mengubah parameternya. Kolom parameter Kustom menunjukkan kontrol mana yang mendukung parameter kustom.
3. Pada halaman detail untuk kontrol, pilih tab Parameter, lalu pilih Edit.
4. Tentukan nilai parameter yang Anda inginkan.
5. Secara opsional, di bagian Alasan perubahan, pilih alasan untuk menyesuaikan parameter.
6. Pilih Simpan.

Security Hub CSPM API

Untuk menyesuaikan nilai parameter kontrol dalam satu akun dan Wilayah (API)

1. Memanggil [UpdateSecurityControlAPI](#).
2. Untuk `SecurityControlId`, berikan ID kontrol yang ingin Anda sesuaikan.
3. Untuk `Parameters` objek, berikan nama setiap parameter yang ingin Anda sesuaikan. Untuk setiap parameter yang Anda sesuaikan, `CUSTOM` sediakan `ValueType`. Untuk `Value`, berikan tipe data parameter dan nilai kustom. Jika permintaan Anda menghilangkan parameter yang didukung kontrol, parameter tersebut mempertahankan nilainya saat ini. Anda dapat menemukan parameter yang didukung, tipe data, dan nilai yang valid untuk kontrol dengan menjalankan [GetSecurityControlDefinitionAPI](#).
4. Secara opsional `LastUpdateReason`, untuk, berikan alasan untuk menyesuaikan parameter kontrol.

Misalnya, AWS CLI perintah berikut mendefinisikan nilai kustom untuk `daysToExpiration` parameter. ACM.1 Contoh ini diformat untuk Linux, macOS, atau Unix, dan menggunakan karakter garis miring terbalik (\) untuk meningkatkan keterbacaan.

```
$ aws securityhub update-security-control \  
--region us-east-1 \  
--security-control-id ACM.1 \  
--parameters '{"daysToExpiration": {"ValueType": "CUSTOM", "Value": {"Integer":  
15}}}' \  
--last-update-reason "Internal compliance requirement"
```

Mengembalikan ke nilai parameter kontrol default

Parameter kontrol dapat memiliki nilai default yang didefinisikan oleh AWS Security Hub Cloud Security Posture Management (CSPM). Terkadang, Security Hub CSPM memperbarui nilai default untuk parameter untuk mencerminkan praktik terbaik keamanan yang berkembang. Jika Anda belum menentukan nilai kustom untuk parameter kontrol, kontrol secara otomatis melacak pembaruan tersebut dan menggunakan nilai default yang baru.

Anda dapat kembali menggunakan nilai parameter default untuk kontrol. Petunjuk untuk pengembalian bergantung pada apakah Anda menggunakan [konfigurasi pusat](#) di Security Hub

CSPM. Konfigurasi pusat adalah fitur yang dapat digunakan oleh administrator CSPM Security Hub yang didelegasikan untuk mengonfigurasi kapabilitas CSPM Security Hub di seluruh akun Wilayah AWS, dan unit organisasi (). OUs

 Note

Tidak semua parameter kontrol memiliki nilai CSPM Security Hub default. Dalam kasus seperti itu, ketika `ValueType` disetel ke `DEFAULT`, tidak ada nilai default tertentu yang digunakan CSPM Security Hub. Sebaliknya, Security Hub CSPM mengabaikan parameter tanpa adanya nilai khusus.

Mengembalikan ke parameter kontrol default di beberapa akun dan Wilayah

Jika Anda menggunakan konfigurasi pusat, Anda dapat mengembalikan parameter kontrol untuk beberapa akun yang dikelola secara terpusat dan OUs di Wilayah beranda dan Wilayah yang ditautkan.

Pilih metode pilihan Anda, dan ikuti langkah-langkah untuk kembali ke nilai parameter default di beberapa akun dan Wilayah menggunakan konfigurasi pusat.

Security Hub CSPM console

Untuk kembali ke nilai parameter kontrol default di beberapa akun dan Wilayah (konsol)

1. Buka konsol AWS Security Hub Cloud Security Posture Management (CSPM) di <https://console.aws.amazon.com/securityhub/>

Masuk menggunakan kredensial akun administrator CSPM Security Hub yang didelegasikan di Wilayah asal.

2. Di panel navigasi, pilih Pengaturan dan Konfigurasi.
3. Pilih tab Kebijakan.
4. Pilih kebijakan, lalu pilih Edit.
5. Di bawah Kebijakan khusus, bagian Kontrol menampilkan daftar kontrol yang Anda tetapkan untuk parameter kustom.
6. Temukan kontrol yang memiliki satu atau lebih nilai parameter untuk dikembalikan. Kemudian, pilih Hapus untuk kembali ke nilai default.
7. Di bagian Akun, verifikasi akun atau kebijakan OUs yang ingin Anda terapkan.

8. Pilih Berikutnya.
9. Tinjau perubahan Anda, dan verifikasi bahwa perubahan tersebut benar. Setelah selesai, pilih Simpan kebijakan dan terapkan. Di Wilayah beranda dan semua Wilayah yang ditautkan, tindakan ini mengesampingkan pengaturan konfigurasi akun yang ada dan OUs yang terkait dengan kebijakan konfigurasi ini. Akun dan OUs dapat dikaitkan dengan kebijakan konfigurasi melalui aplikasi langsung atau warisan dari orang tua.

Security Hub CSPM API

Untuk kembali ke nilai parameter kontrol default di beberapa akun dan Wilayah (API)

1. Memanggil [UpdateConfigurationPolicy](#) API dari akun administrator yang didelegasikan di Wilayah beranda.
2. Untuk Identifier bidang, berikan Nama Sumber Daya Amazon (ARN) atau ID kebijakan yang ingin Anda perbarui.
3. Untuk `SecurityControlCustomParameters` objek, berikan pengenalan setiap kontrol yang ingin Anda kembalikan satu atau beberapa parameter.
4. Di `Parameters` objek, untuk setiap parameter yang ingin Anda kembalikan, `DEFAULT` sediakan `ValueType` bidang. Ketika `ValueType` diatur ke `DEFAULT`, Anda tidak perlu memberikan nilai untuk `Value` bidang tersebut. Jika nilai disertakan dalam permintaan Anda, Security Hub CSPM mengabaikannya. Jika permintaan Anda menghilangkan parameter yang didukung kontrol, parameter tersebut mempertahankan nilainya saat ini.

Warning

Jika Anda menghilangkan objek kontrol dari `SecurityControlCustomParameters` bidang, Security Hub CSPM mengembalikan semua parameter kustom untuk kontrol ke nilai defaultnya. Daftar yang benar-benar kosong untuk `SecurityControlCustomParameters` mengembalikan parameter kustom untuk semua kontrol ke nilai defaultnya.

Misalnya, AWS CLI perintah berikut mengembalikan parameter `daysToExpiration` kontrol ACM. 1 ke nilai defaultnya dalam kebijakan konfigurasi yang ditentukan. Contoh ini diformat untuk Linux, macOS, atau Unix, dan menggunakan karakter garis miring terbalik (`\`) untuk meningkatkan keterbacaan.

```
$ aws securityhub create-configuration-policy \
--region us-east-1 \
--identifier "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111" \
--name "TestConfigurationPolicy" \
--description "Updated configuration policy" \
--updated-reason "Revert ACM.1 parameter to default value"
--configuration-policy '{"SecurityHub": {"ServiceEnabled": true,
"EnabledStandardIdentifiers": ["arn:aws:securityhub:us-east-1::standards/aws-foundational-security-best-practices/v/1.0.0","arn:aws:securityhub::ruleset/cis-aws-foundations-benchmark/v/1.2.0"],"SecurityControlsConfiguration":
{"DisabledSecurityControlIdentifiers": ["CloudTrail.2"],
"SecurityControlCustomParameters": [{"SecurityControlId": "ACM.1", "Parameters":
{"daysToExpiration": {"ValueType": "DEFAULT"}}}]}}}'
```

Mengembalikan ke parameter kontrol default dalam satu akun dan Wilayah

Jika Anda tidak menggunakan konfigurasi pusat atau memiliki akun yang dikelola sendiri, Anda dapat kembali menggunakan nilai parameter default untuk akun Anda di satu Wilayah pada satu waktu.

Pilih metode pilihan Anda, dan ikuti langkah-langkah untuk kembali ke nilai parameter default untuk akun Anda di satu Wilayah. Untuk kembali ke nilai parameter default di Wilayah tambahan, ulangi langkah-langkah ini di setiap Wilayah tambahan.

Note

Jika Anda menonaktifkan Security Hub CSPM, parameter kontrol kustom Anda akan diatur ulang. Jika Anda mengaktifkan Security Hub CSPM lagi di masa mendatang, semua kontrol akan menggunakan nilai parameter default untuk memulai.

Security Hub CSPM console

Untuk kembali ke nilai parameter kontrol default dalam satu akun dan Wilayah (konsol)

1. Buka konsol AWS Security Hub Cloud Security Posture Management (CSPM) di <https://console.aws.amazon.com/securityhub/>
2. Di panel navigasi, pilih Kontrol. Pilih kontrol yang ingin Anda kembalikan ke nilai parameter default.

3. Pada **Parameters** tab, pilih **Disesuaikan** di sebelah parameter kontrol. Kemudian, pilih **Hapus kustomisasi**. Parameter ini sekarang menggunakan nilai **CSPM Security Hub default** dan melacak pembaruan masa depan ke nilai default.
4. Ulangi langkah sebelumnya untuk setiap nilai parameter yang ingin Anda kembalikan.

Security Hub CSPM API

Untuk kembali ke nilai parameter kontrol default dalam satu akun dan Wilayah (API)

1. Memanggil [UpdateSecurityControl](#) API.
2. Untuk `SecurityControlId`, berikan ARN atau ID kontrol yang parameternya ingin Anda kembalikan.
3. Di **Parameters** objek, untuk setiap parameter yang ingin Anda kembalikan, **DEFAULT** sediakan `ValueType` bidang. Ketika `ValueType` diatur ke **DEFAULT**, Anda tidak perlu memberikan nilai untuk `Value` bidang tersebut. Jika nilai disertakan dalam permintaan Anda, Security Hub CSPM mengabaikannya.
4. Secara opsional, untuk `LastUpdateReason`, berikan alasan untuk kembali ke nilai parameter default.

Misalnya, AWS CLI perintah berikut mengembalikan parameter `daysToExpiration` kontrol `ACM.1` ke nilai defaultnya. Contoh ini diformat untuk Linux, macOS, atau Unix, dan menggunakan karakter garis miring terbalik (`\`) untuk meningkatkan keterbacaan.

```
$ aws securityhub update-security-control \
--region us-east-1 \
--security-control-id ACM.1 \
--parameters '{"daysToExpiration": {"ValueType": "DEFAULT"}}' \
--last-update-reason "New internal requirement"
```

Memeriksa status perubahan parameter kontrol

Ketika Anda mencoba untuk menyesuaikan parameter kontrol atau kembali ke nilai default, Anda dapat memvalidasi apakah perubahan yang diinginkan efektif. Ini membantu memastikan bahwa kontrol berfungsi seperti yang Anda harapkan dan memberikan nilai keamanan yang diinginkan. Jika

pemutakhiran parameter tidak berhasil, Security Hub CSPM mempertahankan nilai saat ini untuk parameter tersebut.

Untuk memverifikasi bahwa pembaruan parameter berhasil, Anda dapat meninjau detail kontrol pada konsol CSPM Security Hub. Di konsol, pilih Kontrol pada panel navigasi. Kemudian, pilih kontrol untuk menampilkan detailnya. Tab Parameter menunjukkan status perubahan parameter.

Secara terprogram, jika permintaan Anda untuk memperbarui parameter valid, nilai `UpdateStatus` `UPDATING` bidang adalah respons terhadap operasi. [BatchGetSecurityControls](#) Ini berarti bahwa pembaruan itu valid, tetapi semua temuan mungkin belum menyertakan nilai parameter yang diperbarui. Ketika nilai `UpdateState` berubah `READY`, Security Hub CSPM menggunakan nilai parameter kontrol yang diperbarui saat menjalankan pemeriksaan keamanan kontrol. Temuan termasuk nilai parameter yang diperbarui.

`UpdateSecurityControlOperasi` mengembalikan `InvalidInputException` respons untuk nilai parameter yang tidak valid. Tanggapan tersebut memberikan rincian tambahan tentang alasan kegagalan. Misalnya, Anda mungkin telah menetapkan nilai yang berada di luar rentang yang valid untuk parameter. Atau, Anda mungkin telah menentukan nilai yang tidak menggunakan tipe data yang benar. Kirim permintaan Anda lagi dengan masukan yang valid.

Jika terjadi kegagalan internal saat Anda mencoba memperbarui nilai parameter, Security Hub CSPM akan mencoba ulang secara otomatis jika Anda telah mengaktifkannya. AWS Config Lihat informasi yang lebih lengkap di [Pertimbangan sebelum mengaktifkan dan mengonfigurasi AWS Config](#).

Meninjau dan mengelola temuan kontrol di Security Hub CSPM

Halaman detail kontrol menampilkan daftar temuan aktif untuk kontrol. Daftar ini tidak termasuk temuan yang diarsipkan.

Halaman detail kontrol mendukung agregasi lintas wilayah. Jika Anda telah menetapkan Wilayah agregasi, status kontrol dan daftar pemeriksaan keamanan pada halaman detail kontrol mencakup pemeriksaan dari semua yang ditautkan Wilayah AWS.

Daftar ini menyediakan alat untuk memfilter dan mengurutkan temuan, sehingga Anda dapat fokus pada temuan yang lebih mendesak terlebih dahulu. Temuan dapat mencakup tautan ke detail sumber daya di konsol layanan terkait. Untuk kontrol yang didasarkan pada AWS Config aturan, Anda dapat melihat detail tentang aturan.

Anda juga dapat menggunakan AWS Security Hub Cloud Security Posture Management (CSPM) API untuk mengambil daftar temuan dan menemukan detail.

Untuk informasi selengkapnya, lihat [Meninjau detail dan riwayat penemuan](#).

Untuk mencerminkan status investigasi Anda saat ini atas temuan kontrol, Anda menetapkan status alur kerja. Untuk informasi selengkapnya, lihat [the section called “Mengatur status alur kerja temuan”](#).

Anda juga dapat mengirim temuan CSPM Security Hub yang dipilih ke tindakan kustom di Amazon EventBridge. Untuk informasi selengkapnya, lihat [the section called “Mengirim temuan ke tindakan khusus”](#).

Topik

- [Memfilter dan menyortir temuan kontrol](#)
- [Sampel temuan kontrol](#)

Memfilter dan menyortir temuan kontrol

Memilih kontrol dari halaman Kontrol konsol AWS Security Hub Cloud Security Posture Management (CSPM) Security Hub atau dari halaman detail standar akan membawa Anda ke halaman detail kontrol.

Halaman detail kontrol menunjukkan judul dan deskripsi kontrol, status kontrol keseluruhan, dan rincian pemeriksaan keamanan untuk kontrol dalam 24 jam terakhir.

Gunakan opsi Filter menurut di samping daftar pemeriksaan kontrol untuk dengan cepat fokus pada temuan dengan [status alur kerja atau status kepatuhan](#) tertentu.

Selain opsi Filter menurut, Anda dapat menggunakan kotak Tambahkan filter untuk memfilter daftar centang menurut bidang lain, seperti Akun AWS ID atau ID sumber daya.

Secara default, temuan dengan status kepatuhan LULUS dicantumkan terlebih dahulu. Anda dapat mengubah penyortiran default dengan memilih opsi yang berbeda di header kolom.

Dari halaman detail kontrol, Anda dapat memilih Unduh untuk mengunduh halaman temuan kontrol saat ini ke file.csv.

Jika Anda memfilter daftar temuan, maka unduhan hanya menyertakan kontrol yang cocok dengan filter. Jika Anda memilih temuan spesifik dari daftar, maka unduhan hanya menyertakan temuan yang dipilih.

Untuk informasi lebih lanjut tentang temuan penyaringan, lihat [Penyaringan temuan di Security Hub CSPM](#).

Sampel temuan kontrol

Sampel berikut memberikan contoh temuan kontrol AWS Security Hub Cloud Security Posture Management (CSPM) dalam AWS Security Finding Format (ASFF). Isi temuan kontrol bervariasi tergantung pada apakah Anda mengaktifkan temuan kontrol konsolidasi.

Jika Anda mengaktifkan temuan kontrol terkonsolidasi, Security Hub CSPM menghasilkan satu temuan untuk kontrol, bahkan jika kontrol tersebut berlaku untuk beberapa standar yang diaktifkan. Jika Anda tidak mengaktifkan fitur ini, Security Hub CSPM akan menghasilkan temuan kontrol terpisah untuk setiap standar yang diaktifkan yang diterapkan kontrol. Misalnya, jika Anda mengaktifkan dua standar dan kontrol berlaku untuk keduanya, Anda menerima dua temuan terpisah untuk kontrol, satu untuk setiap standar. Jika Anda mengaktifkan temuan kontrol terkonsolidasi, Anda hanya menerima satu temuan untuk kontrol. Untuk informasi selengkapnya, lihat [Temuan kontrol terkonsolidasi](#).

Sampel di halaman ini memberikan contoh untuk kedua skenario. Sampel meliputi: temuan kontrol untuk standar CSPM Security Hub individu ketika temuan kontrol konsolidasi dinonaktifkan, dan temuan kontrol untuk beberapa standar CSPM Security Hub ketika temuan kontrol konsolidasi diaktifkan.

Sampel temuan kontrol

- [Temuan sampel untuk standar Praktik Terbaik Keamanan AWS Dasar](#)
- [Temuan sampel untuk CIS AWS Foundations Benchmark v3.0.0](#)
- [Temuan sampel untuk CIS AWS Foundations Benchmark v1.4.0](#)
- [Temuan sampel untuk CIS AWS Foundations Benchmark v1.2.0](#)
- [Temuan sampel untuk standar NIST SP 800-53 Revisi 5](#)
- [Temuan sampel untuk standar NIST SP 800-171 Revisi 2](#)
- [Temuan sampel untuk Standar Keamanan Data Industri Kartu Pembayaran v3.2.1](#)
- [Temuan sampel untuk standar Penandaan AWS Sumber Daya](#)
- [Temuan sampel untuk standar yang AWS Control Tower dikelola layanan](#)
- [Sampel temuan konsolidasi untuk beberapa standar](#)

Note

Temuan kontrol mengacu pada berbagai bidang dan nilai di Wilayah dan AWS GovCloud (US) Wilayah Tiongkok. Untuk informasi selengkapnya, lihat [Dampak konsolidasi pada bidang dan nilai ASFF](#).

Temuan sampel untuk standar Praktik Terbaik Keamanan AWS Dasar

Contoh berikut memberikan contoh temuan untuk kontrol yang berlaku untuk standar Praktik Terbaik Keamanan AWS Dasar (FSBP). Dalam sampel ini, temuan kontrol konsolidasi dinonaktifkan.

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-2:123456789012:subscription/aws-foundational-security-best-practices/v/1.0.0/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-2::product/aws/securityhub",
  "ProductName": "Security Hub CSPM",
  "CompanyName": "AWS",
  "Region": "us-east-2",
  "GeneratorId": "aws-foundational-security-best-practices/v/1.0.0/CloudTrail.2",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards/AWS-Foundational-Security-Best-Practices"
  ],
  "FirstObservedAt": "2020-08-06T02:18:23.076Z",
  "LastObservedAt": "2021-09-28T16:10:06.956Z",
  "CreatedAt": "2020-08-06T02:18:23.076Z",
  "UpdatedAt": "2021-09-28T16:10:00.093Z",
  "Severity": {
    "Product": 40,
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
  },
  "Title": "CloudTrail.2 CloudTrail should have encryption at-rest enabled",
  "Description": "This AWS control checks whether AWS CloudTrail is configured to use the server side encryption (SSE) AWS Key Management Service (AWS KMS) customer master key (CMK) encryption. The check will pass if the KmsKeyId is defined.",
  "Remediation": {
```

```

    "Recommendation": {
      "Text": "For directions on how to correct this issue, consult the AWS Security
Hub Cloud Security Posture Management (CSPM) controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
    }
  },
  "ProductFields": {
    "StandardsArn": "arn:aws:securityhub::standards/aws-foundational-security-best-
practices/v/1.0.0",
    "StandardsSubscriptionArn": "arn:aws:securityhub:us-
east-2:123456789012:subscription/aws-foundational-security-best-practices/v/1.0.0",
    "ControlId": "CloudTrail.2",
    "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/
remediation",
    "Related AWS Resources:0/name": "securityhub-cloud-trail-encryption-enabled-
fe95bf3f",
    "Related AWS Resources:0/type": "AWS::Config::ConfigRule",
    "StandardsControlArn": "arn:aws:securityhub:us-east-2:123456789012:control/aws-
foundational-security-best-practices/v/1.0.0/CloudTrail.2",
    "aws/securityhub/ProductName": "Security Hub CSPM",
    "aws/securityhub/CompanyName": "AWS",
    "Resources:0/Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWS MacieTrail-
D0-NOT-EDIT",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-2::product/aws/
securityhub/arn:aws:securityhub:us-east-2:123456789012:subscription/aws-foundational-
security-best-practices/v/1.0.0/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111"
  },
  "Resources": [
    {
      "Type": "AwsCloudTrailTrail",
      "Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWS MacieTrail-D0-NOT-
EDIT",
      "Partition": "aws",
      "Region": "us-east-2"
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "SecurityControlId": "CloudTrail.2",
    "AssociatedStandards": [{
      "StandardsId": "standards/aws-foundation-best-practices/v/1.0.0"
    }]
  }
},

```

```

"WorkflowState": "NEW",
"Workflow": {
  "Status": "NEW"
},
"RecordState": "ACTIVE",
"FindingProviderFields": {
  "Severity": {
    "Label": "MEDIUM",
    "Original": "MEDIUM"
  },
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards/AWS-
Foundational-Security-Best-Practices"
  ]
}
}

```

Temuan sampel untuk CIS AWS Foundations Benchmark v3.0.0

Contoh berikut memberikan contoh temuan untuk kontrol yang berlaku untuk CIS AWS Foundations Benchmark v3.0.0. Dalam sampel ini, temuan kontrol konsolidasi dinonaktifkan.

```

{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-1:123456789012:subscription/cis-aws-foundations-
benchmark/v/3.0.0/2.2.1/finding/38a89798-6819-4fae-861f-9cca8034602c",
  "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/securityhub",
  "ProductName": "Security Hub CSPM",
  "CompanyName": "AWS",
  "Region": "us-east-1",
  "GeneratorId": "cis-aws-foundations-benchmark/v/3.0.0/2.2.1",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards/CIS AWS
Foundations Benchmark"
  ],
  "FirstObservedAt": "2024-04-18T07:46:18.193Z",
  "LastObservedAt": "2024-04-23T07:47:01.137Z",
  "CreatedAt": "2024-04-18T07:46:18.193Z",
  "UpdatedAt": "2024-04-23T07:46:46.165Z",
  "Severity": {
    "Product": 40,
    "Label": "MEDIUM",

```

```

    "Normalized": 40,
    "Original": "MEDIUM"
  },
  "Title": "2.2.1 EBS default encryption should be enabled",
  "Description": "Elastic Compute Cloud (EC2) supports encryption at rest when using the Elastic Block Store (EBS) service. While disabled by default, forcing encryption at EBS volume creation is supported.",
  "Remediation": {
    "Recommendation": {
      "Text": "For information on how to correct this issue, consult the AWS Security Hub Cloud Security Posture Management (CSPM) controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/EC2.7/remediation"
    }
  },
  "ProductFields": {
    "StandardsArn": "arn:aws:securityhub::standards/cis-aws-foundations-benchmark/v/3.0.0",
    "StandardsSubscriptionArn": "arn:aws:securityhub:us-east-1:123456789012:subscription/cis-aws-foundations-benchmark/v/3.0.0",
    "ControlId": "2.2.1",
    "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/EC2.7/remediation",
    "RelatedAWSResources:0/name": "securityhub-ec2-ebs-encryption-by-default-2843ed9e",
    "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
    "StandardsControlArn": "arn:aws:securityhub:us-east-1:123456789012:control/cis-aws-foundations-benchmark/v/3.0.0/2.2.1",
    "aws/securityhub/ProductName": "Security Hub CSPM",
    "aws/securityhub/CompanyName": "AWS",
    "aws/securityhub/annotation": "EBS Encryption by default is not enabled.",
    "Resources:0/Id": "arn:aws:iam::123456789012:root",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/securityhub/arn:aws:securityhub:us-east-1:123456789012:subscription/cis-aws-foundations-benchmark/v/3.0.0/2.2.1/finding/38a89798-6819-4fae-861f-9cca8034602c"
  },
  "Resources": [
    {
      "Type": "AwsAccount",
      "Id": "AWS:::Account:123456789012",
      "Partition": "aws",
      "Region": "us-east-1"
    }
  ],
  "Compliance": {
    "Status": "FAILED",

```

```

    "RelatedRequirements": [
      "CIS AWS Foundations Benchmark v3.0.0/2.2.1"
    ],
    "SecurityControlId": "EC2.7",
    "AssociatedStandards": [
      {
        "StandardsId": "standards/cis-aws-foundations-benchmark/v/3.0.0"
      }
    ],
    "WorkflowState": "NEW",
    "Workflow": {
      "Status": "NEW"
    },
    "RecordState": "ACTIVE",
    "FindingProviderFields": {
      "Severity": {
        "Label": "MEDIUM",
        "Original": "MEDIUM"
      },
      "Types": [
        "Software and Configuration Checks/Industry and Regulatory Standards/CIS AWS Foundations Benchmark"
      ]
    },
    "ProcessedAt": "2024-04-23T07:47:07.088Z"
  }

```

Temuan sampel untuk CIS AWS Foundations Benchmark v1.4.0

Contoh berikut memberikan contoh temuan untuk kontrol yang berlaku untuk CIS AWS Foundations Benchmark v1.4.0. Dalam sampel ini, temuan kontrol konsolidasi dinonaktifkan.

```

{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-1:123456789012:subscription/cis-aws-foundations-benchmark/v/1.4.0/3.7/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/securityhub",
  "ProductName": "Security Hub CSPM",
  "CompanyName": "AWS",
  "Region": "us-east-1",
  "GeneratorId": "cis-aws-foundations-benchmark/v/1.4.0/3.7",
  "AwsAccountId": "123456789012",

```

```

"Types": [
  "Software and Configuration Checks/Industry and Regulatory Standards/CIS AWS
Foundations Benchmark"
],
"FirstObservedAt": "2022-10-21T22:14:48.913Z",
"LastObservedAt": "2022-12-22T22:24:56.980Z",
"CreatedAt": "2022-10-21T22:14:48.913Z",
"UpdatedAt": "2022-12-22T22:24:52.409Z",
"Severity": {
  "Product": 40,
  "Label": "MEDIUM",
  "Normalized": 40,
  "Original": "MEDIUM"
},
"Title": "3.7 Ensure CloudTrail logs are encrypted at rest using KMS CMKs",
"Description": "AWS CloudTrail is a web service that records AWS API calls for an
account and makes those logs available to users and resources in accordance with IAM
policies. AWS Key Management Service (KMS) is a managed service that helps create
and control the encryption keys used to encrypt account data, and uses Hardware
Security Modules (HSMs) to protect the security of encryption keys. CloudTrail logs
can be configured to leverage server side encryption (SSE) and AWS KMS customer
created master keys (CMK) to further protect CloudTrail logs. It is recommended that
CloudTrail be configured to use SSE-KMS.",
"Remediation": {
  "Recommendation": {
    "Text": "For directions on how to correct this issue, consult the AWS Security
Hub Cloud Security Posture Management (CSPM) controls documentation.",
    "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
  }
},
"ProductFields": {
  "StandardsArn": "arn:aws:securityhub::standards/cis-aws-foundations-benchmark/
v/1.4.0",
  "StandardsSubscriptionArn": "arn:aws:securityhub:us-
east-1:123456789012:subscription/cis-aws-foundations-benchmark/v/1.4.0",
  "ControlId": "3.7",
  "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/
remediation",
  "RelatedAWSResources:0/name": "securityhub-cloud-trail-encryption-
enabled-855f82d1",
  "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
  "StandardsControlArn": "arn:aws:securityhub:us-east-1:123456789012:control/cis-aws-
foundations-benchmark/v/1.4.0/3.7",
  "aws/securityhub/ProductName": "Security Hub CSPM",

```

```

    "aws/securityhub/CompanyName": "AWS",
    "Resources:0/Id": "arn:aws:cloudtrail:us-west-2:123456789012:trail/AWS MacieTrail-
DO-NOT-EDIT",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/
securityhub/arn:aws:securityhub:us-east-1:123456789012:subscription/cis-aws-
foundations-benchmark/v/1.4.0/3.7/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  },
  "Resources": [
    {
      "Type": "AwsCloudTrailTrail",
      "Id": "arn:aws:cloudtrail:us-west-2:123456789012:trail/AWS MacieTrail-DO-NOT-
EDIT",
      "Partition": "aws",
      "Region": "us-east-1"
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "RelatedRequirements": [
      "CIS AWS Foundations Benchmark v1.4.0/3.7"
    ],
    "SecurityControlId": "CloudTrail.2",
    "AssociatedStandards": [{
      "StandardsId": "standards/cis-aws-foundations-benchmark/v/1.4.0"
    }]
  },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    }
  },
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards/CIS AWS
Foundations Benchmark"
  ]
}

```

Temuan sampel untuk CIS AWS Foundations Benchmark v1.2.0

Contoh berikut memberikan contoh temuan untuk kontrol yang berlaku untuk CIS AWS Foundations Benchmark v1.2.0. Dalam sampel ini, temuan kontrol konsolidasi dinonaktifkan.

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-2:123456789012:subscription/cis-aws-foundations-benchmark/v/1.2.0/2.7/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-2::product/aws/securityhub",
  "ProductName": "Security Hub CSPM",
  "CompanyName": "AWS",
  "Region": "us-east-2",
  "GeneratorId": "arn:aws:securityhub::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/2.7",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards/CIS AWS Foundations Benchmark"
  ],
  "FirstObservedAt": "2020-08-29T04:10:06.337Z",
  "LastObservedAt": "2021-09-28T16:10:05.350Z",
  "CreatedAt": "2020-08-29T04:10:06.337Z",
  "UpdatedAt": "2021-09-28T16:10:00.087Z",
  "Severity": {
    "Product": 40,
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
  },
  "Title": "2.7 Ensure CloudTrail logs are encrypted at rest using KMS CMKs",
  "Description": "AWS Key Management Service (KMS) is a managed service that helps create and control the encryption keys used to encrypt account data, and uses Hardware Security Modules (HSMs) to protect the security of encryption keys. CloudTrail logs can be configured to leverage server side encryption (SSE) and KMS customer created master keys (CMK) to further protect CloudTrail logs. It is recommended that CloudTrail be configured to use SSE-KMS.",
  "Remediation": {
    "Recommendation": {
      "Text": "For directions on how to correct this issue, consult the AWS Security Hub Cloud Security Posture Management (CSPM) controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
    }
  }
}
```



```

    },
    "ProductFields": {
      "StandardsGuideArn": "arn:aws:securityhub::ruleset/cis-aws-foundations-benchmark/
v/1.2.0",
      "StandardsGuideSubscriptionArn": "arn:aws:securityhub:us-
east-2:123456789012:subscription/cis-aws-foundations-benchmark/v/1.2.0",
      "RuleId": "2.7",
      "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/
remediation",
      "Related AWS Resources:0/name": "securityhub-cloud-trail-encryption-enabled-
fe95bf3f",
      "Related AWS Resources:0/type": "AWS::Config::ConfigRule",
      "StandardsControlArn": "arn:aws:securityhub:us-east-2:123456789012:control/cis-aws-
foundations-benchmark/v/1.2.0/2.7",
      "aws/securityhub/ProductName": "Security Hub CSPM",
      "aws/securityhub/CompanyName": "AWS",
      "Resources:0/Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWS MacieTrail-
DO-NOT-EDIT",
      "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-2::product/aws/
securityhub/arn:aws:securityhub:us-east-2:123456789012:subscription/cis-aws-
foundations-benchmark/v/1.2.0/2.7/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
    },
    "Resources": [
      {
        "Type": "AwsCloudTrailTrail",
        "Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWS MacieTrail-DO-NOT-
EDIT",
        "Partition": "aws",
        "Region": "us-east-2"
      }
    ],
    "Compliance": {
      "Status": "FAILED",
      "SecurityControlId": "CloudTrail.2",
      "AssociatedStandards": [{
        "StandardsId": "ruleset/cis-aws-foundations-benchmark/v/1.2.0"
      }]
    },
    "WorkflowState": "NEW",
    "Workflow": {
      "Status": "NEW"
    },
    "RecordState": "ACTIVE",
    "FindingProviderFields": {

```

```

    "Severity": {
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    },
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards/CIS AWS Foundations Benchmark"
    ]
  }
}

```

Temuan sampel untuk standar NIST SP 800-53 Revisi 5

Sampel berikut memberikan contoh temuan untuk kontrol yang berlaku untuk standar NIST SP 800-53 Revisi 5. Dalam sampel ini, temuan kontrol konsolidasi dinonaktifkan.

```

{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-1:123456789012:subscription/nist-800-53/v/5.0.0/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/securityhub",
  "ProductName": "Security Hub CSPM",
  "CompanyName": "AWS",
  "Region": "us-east-1",
  "GeneratorId": "nist-800-53/v/5.0.0/CloudTrail.2",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards"
  ],
  "FirstObservedAt": "2023-02-17T14:22:46.726Z",
  "LastObservedAt": "2023-02-17T14:22:50.846Z",
  "CreatedAt": "2023-02-17T14:22:46.726Z",
  "UpdatedAt": "2023-02-17T14:22:46.726Z",
  "Severity": {
    "Product": 40,
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
  },
  "Title": "CloudTrail.2 CloudTrail should have encryption at-rest enabled",
  "Description": "This AWS control checks whether AWS CloudTrail is configured to use the server side encryption (SSE) AWS Key Management Service (AWS KMS) customer master key (CMK) encryption. The check will pass if the KmsKeyId is defined.",
}

```

```

"Remediation": {
  "Recommendation": {
    "Text": "For directions on how to fix this issue, consult the AWS Security Hub
Cloud Security Posture Management (CSPM) NIST 800-53 R5 documentation.",
    "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
  }
},
"ProductFields": {
  "StandardsArn": "arn:aws:securityhub::standards/nist-800-53/v/5.0.0",
  "StandardsSubscriptionArn": "arn:aws:securityhub:us-
east-1:123456789012:subscription/nist-800-53/v/5.0.0",
  "ControlId": "CloudTrail.2",
  "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.9/
remediation",
  "RelatedAWSResources:0/name": "securityhub-cloud-trail-encryption-enabled-
fe95bf3f",
  "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
  "StandardsControlArn": "arn:aws:securityhub:us-east-2:123456789012:control/aws-
foundational-security-best-practices/v/1.0.0/CloudTrail.2",
  "aws/securityhub/ProductName": "Security Hub CSPM",
  "aws/securityhub/CompanyName": "AWS",
  "Resources:0/Id": "arn:aws:cloudtrail:us-west-2:123456789012:trail/AWS MacieTrail-
D0-NOT-EDIT",
  "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/
securityhub/arn:aws:securityhub:us-east-1:123456789012:subscription/nist-800-53/
v/5.0.0/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
},
"Resources": [
  {
    "Type": "AwsCloudTrailTrail",

    "Id": "arn:aws:cloudtrail:us-east-1:123456789012:trail/AWS MacieTrail-D0-NOT-
EDIT",

    "Partition": "aws",

    "Region": "us-east-1"
  }
],
"Compliance": {
  "Status": "FAILED",
  "RelatedRequirements": [
    "NIST.800-53.r5 AU-9",
    "NIST.800-53.r5 CA-9(1)",

```

```

        "NIST.800-53.r5 CM-3(6)",
        "NIST.800-53.r5 SC-13",
        "NIST.800-53.r5 SC-28",
        "NIST.800-53.r5 SC-28(1)",
        "NIST.800-53.r5 SC-7(10)",
        "NIST.800-53.r5 SI-7(6)"
    ],
    "SecurityControlId": "CloudTrail.2",
    "AssociatedStandards": [
        {
            "StandardsId": "standards/nist-800-53/v/5.0.0"
        }
    ]
},
"WorkflowState": "NEW",
"Workflow": {
    "Status": "NEW"
},
"RecordState": "ACTIVE",
"FindingProviderFields": {
    "Severity": {
        "Label": "MEDIUM",
        "Original": "MEDIUM"
    },
    "Types": [
        "Software and Configuration Checks/Industry and Regulatory Standards"
    ]
},
"ProcessedAt": "2023-02-17T14:22:53.572Z"
}

```

Temuan sampel untuk standar NIST SP 800-171 Revisi 2

Sampel berikut memberikan contoh temuan untuk kontrol yang berlaku untuk standar NIST SP 800-171 Revisi 2. Dalam sampel ini, temuan kontrol konsolidasi dinonaktifkan.

```

{
    "SchemaVersion": "2018-10-08",
    "Id": "arn:aws:securityhub:us-east-1:123456789012:subscription/nist-800-171/v/2.0.0/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/securityhub",
    "ProductName": "Security Hub",
    "CompanyName": "AWS",

```

```

"Region": "us-east-1",
"GeneratorId": "nist-800-171/v/2.0.0/CloudTrail.2",
"AwsAccountId": "123456789012",
"AwsAccountName": "TestAcct",
"Types": [
  "Software and Configuration Checks/Industry and Regulatory Standards"
],
"FirstObservedAt": "2025-05-29T05:23:58.690Z",
"LastObservedAt": "2025-05-30T05:50:11.898Z",
"CreatedAt": "2025-05-29T05:24:24.772Z",
"UpdatedAt": "2025-05-30T05:50:34.292Z",
"Severity": {
  "Product": 40,
  "Label": "MEDIUM",
  "Normalized": 40,
  "Original": "MEDIUM"
},
"Title": "CloudTrail.2 CloudTrail should have encryption at-rest enabled",
>Description": "This AWS control checks whether AWS CloudTrail is configured to use the server side encryption (SSE) AWS Key Management Service (AWS KMS) customer master key (CMK) encryption. The check will pass if the KmsKeyId is defined.",
"Remediation": {
  "Recommendation": {
    "Text": "For information on how to correct this issue, consult the AWS Security Hub Cloud Security Posture Management (CSPM) controls documentation.",
    "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
  }
},
"ProductFields": {
  "StandardsArn": "arn:aws:securityhub::standards/nist-800-171/v/2.0.0",
  "StandardsSubscriptionArn": "arn:aws:securityhub:us-east-1:123456789012:subscription/nist-800-171/v/2.0.0",
  "ControlId": "CloudTrail.2",
  "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation",
  "RelatedAWSResources:0/name": "securityhub-cloud-trail-encryption-enabled-0ab1c2d4",
  "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
  "StandardsControlArn": "arn:aws:securityhub:us-east-1:123456789012:control/nist-800-171/v/2.0.0/CloudTrail.2",
  "aws/securityhub/ProductName": "Security Hub",
  "aws/securityhub/CompanyName": "AWS",
  "Resources:0/Id": "arn:aws:cloudtrail:ca-central-1:123456789012:trail/aws-BaselineCloudTrail",

```

```

    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/
securityhub/arn:aws:securityhub:us-east-1:123456789012:subscription/nist-800-171/
v/2.0.0/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  },
  "Resources": [
    {
      "Id": "arn:aws:cloudtrail:ca-central-1:123456789012:trail/aws-
BaselineCloudTrail",
      "Partition": "aws",
      "Region": "us-east-1",
      "Type": "AwsCloudTrailTrail"
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "SecurityControlId": "CloudTrail.2",
    "RelatedRequirements": [
      "NIST.800-171.r2/3.3.8"
    ],
    "AssociatedStandards": [
      {
        "StandardsId": "standards/nist-800-171/v/2.0.0"
      }
    ]
  },
  "Workflow": {
    "Status": "NEW"
  },
  "WorkflowState": "NEW",
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards"
    ],
    "Severity": {
      "Product": 40,
      "Label": "MEDIUM",
      "Normalized": 40,
      "Original": "MEDIUM"
    }
  },
  "ProcessedAt": "2025-05-30T05:50:40.297Z"
}

```

Temuan sampel untuk Standar Keamanan Data Industri Kartu Pembayaran v3.2.1

Contoh berikut memberikan contoh temuan untuk kontrol yang berlaku untuk Payment Card Industry Data Security Standard (PCI DSS) v3.2.1. Dalam sampel ini, temuan kontrol konsolidasi dinonaktifkan.

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-2:123456789012:subscription/pci-dss/v/3.2.1/PCI.CloudTrail.1/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-2::product/aws/securityhub",
  "ProductName": "Security Hub CSPM",
  "CompanyName": "AWS",
  "Region": "us-east-2",
  "GeneratorId": "pci-dss/v/3.2.1/PCI.CloudTrail.1",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards/PCI-DSS"
  ],
  "FirstObservedAt": "2020-08-06T02:18:23.089Z",
  "LastObservedAt": "2021-09-28T16:10:06.942Z",
  "CreatedAt": "2020-08-06T02:18:23.089Z",
  "UpdatedAt": "2021-09-28T16:10:00.090Z",
  "Severity": {
    "Product": 40,
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
  },
  "Title": "PCI.CloudTrail.1 CloudTrail logs should be encrypted at rest using AWS KMS CMKs",
  "Description": "This AWS control checks whether AWS CloudTrail is configured to use the server side encryption (SSE) AWS Key Management Service (AWS KMS) customer master key (CMK) encryption by checking if the KmsKeyId is defined.",
  "Remediation": {
    "Recommendation": {
      "Text": "For directions on how to correct this issue, consult the AWS Security Hub Cloud Security Posture Management (CSPM) controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
    }
  },
  "ProductFields": {
    "StandardsArn": "arn:aws:securityhub:::standards/pci-dss/v/3.2.1",

```

```

    "StandardsSubscriptionArn": "arn:aws:securityhub:us-
east-2:123456789012:subscription/pci-dss/v/3.2.1",
    "ControlId": "PCI.CloudTrail.1",
    "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/
remediation",
    "Related AWS Resources:0/name": "securityhub-cloud-trail-encryption-enabled-
fe95bf3f",
    "Related AWS Resources:0/type": "AWS::Config::ConfigRule",
    "StandardsControlArn": "arn:aws:securityhub:us-east-2:123456789012:control/pci-dss/
v/3.2.1/PCI.CloudTrail.1",
    "aws/securityhub/Product Name": "Security Hub CSPM",
    "aws/securityhub/Company Name": "AWS",
    "Resources:0/Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWS MacieTrail-
DO-NOT-EDIT",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-2::product/aws/
securityhub/arn:aws:securityhub:us-east-2:123456789012:subscription/pci-dss/v/3.2.1/
PCI.CloudTrail.1/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  },
  "Resources": [
    {
      "Type": "AwsCloudTrailTrail",
      "Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWS MacieTrail-DO-NOT-
EDIT",
      "Partition": "aws",
      "Region": "us-east-2"
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "RelatedRequirements": [
      "PCI DSS 3.4"
    ],
    "SecurityControlId": "CloudTrail.2",
    "AssociatedStandards": [{
      "StandardsId": "standards/pci-dss/v/3.2.1"
    }]
  },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {

```



```

    "Label": "MEDIUM",
    "Original": "MEDIUM"
  },
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards/PCI-DSS"
  ]
}
}

```

Temuan sampel untuk standar Penandaan AWS Sumber Daya

Contoh berikut memberikan contoh temuan untuk kontrol yang berlaku untuk standar AWS Resource Tagging. Dalam sampel ini, temuan kontrol konsolidasi dinonaktifkan.

```

{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:eu-central-1:123456789012:security-control/EC2.44/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:eu-central-1::product/aws/securityhub",
  "ProductName": "Security Hub CSPM",
  "CompanyName": "AWS",
  "Region": "eu-central-1",
  "GeneratorId": "security-control/EC2.44",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards"
  ],
  "FirstObservedAt": "2024-02-19T21:00:32.206Z",
  "LastObservedAt": "2024-04-29T13:01:57.861Z",
  "CreatedAt": "2024-02-19T21:00:32.206Z",
  "UpdatedAt": "2024-04-29T13:01:41.242Z",
  "Severity": {
    "Label": "LOW",
    "Normalized": 1,
    "Original": "LOW"
  },
  "Title": "EC2 subnets should be tagged",
  "Description": "This control checks whether an Amazon EC2 subnet has tags with the specific keys defined in the parameter requiredTagKeys. The control fails if the subnet doesn't have any tag keys or if it doesn't have all the keys specified in the parameter requiredTagKeys. If the parameter requiredTagKeys isn't provided, the control only checks for the existence of a tag key and fails if the subnet isn't

```

```

tagged with any key. System tags, which are automatically applied and begin with aws:,
are ignored.",
  "Remediation": {
    "Recommendation": {
      "Text": "For information on how to correct this issue, consult the AWS Security
Hub Cloud Security Posture Management (CSPM) controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/EC2.44/remediation"
    }
  },
  "ProductFields": {
    "RelatedAWSResources:0/name": "securityhub-tagged-ec2-subnet-6ceafede",
    "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
    "aws/securityhub/ProductName": "Security Hub CSPM",
    "aws/securityhub/CompanyName": "AWS",
    "aws/securityhub/annotation": "No tags are present.",
    "Resources:0/Id": "arn:aws:ec2:eu-central-1:123456789012:subnet/
subnet-1234567890abcdef0",
    "aws/securityhub/FindingId": "arn:aws:securityhub:eu-central-1::product/aws/
securityhub/arn:aws:securityhub:eu-central-1:123456789012:security-control/EC2.44/
finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  },
  "Resources": [
    {
      "Type": "AwsEc2Subnet",
      "Id": "arn:aws:ec2:eu-central-1:123456789012:subnet/subnet-1234567890abcdef0",
      "Partition": "aws",
      "Region": "eu-central-1",
      "Details": {
        "AwsEc2Subnet": {
          "AssignIpv6AddressOnCreation": false,
          "AvailabilityZone": "eu-central-1b",
          "AvailabilityZoneId": "euc1-az3",
          "AvailableIpAddressCount": 4091,
          "CidrBlock": "10.24.34.0/23",
          "DefaultForAz": true,
          "MapPublicIpOnLaunch": true,
          "OwnerId": "123456789012",
          "State": "available",
          "SubnetArn": "arn:aws:ec2:eu-central-1:123456789012:subnet/
subnet-1234567890abcdef0",
          "SubnetId": "subnet-1234567890abcdef0",
          "VpcId": "vpc-021345abcdef6789"
        }
      }
    }
  ]
}

```

```

    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "SecurityControlId": "EC2.44",
    "AssociatedStandards": [
      {
        "StandardsId": "standards/aws-resource-tagging-standard/v/1.0.0"
      }
    ],
    "SecurityControlParameters": [
      {
        "Name": "requiredTagKeys",
        "Value": [
          "peepoo"
        ]
      }
    ]
  },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "LOW",
      "Original": "LOW"
    },
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards"
    ]
  },
  "ProcessedAt": "2024-04-29T13:02:03.259Z"
}

```

Temuan sampel untuk standar yang AWS Control Tower dikelola layanan

Contoh berikut memberikan contoh temuan untuk kontrol yang berlaku untuk standar yang AWS Control Tower dikelola layanan. Dalam sampel ini, temuan kontrol konsolidasi dinonaktifkan.

```

{
  "SchemaVersion": "2018-10-08",

```

```

    "Id": "arn:aws:securityhub:us-east-1:123456789012:subscription/service-managed-aws-control-tower/v/1.0.0/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/securityhub",
    "ProductName": "Security Hub CSPM",
    "CompanyName": "AWS",
    "Region": "us-east-1",
    "GeneratorId": "service-managed-aws-control-tower/v/1.0.0/CloudTrail.2",
    "AwsAccountId": "123456789012",
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards"
    ],
    "FirstObservedAt": "2022-11-17T01:25:30.296Z",
    "LastObservedAt": "2022-11-17T01:25:45.805Z",
    "CreatedAt": "2022-11-17T01:25:30.296Z",
    "UpdatedAt": "2022-11-17T01:25:30.296Z",
    "Severity": {
      "Product": 40,
      "Label": "MEDIUM",
      "Normalized": 40,
      "Original": "MEDIUM"
    },
    "Title": "CT.CloudTrail.2 CloudTrail should have encryption at-rest enabled",
    "Description": "This AWS control checks whether AWS CloudTrail is configured to use the server side encryption (SSE) AWS Key Management Service (AWS KMS) customer master key (CMK) encryption. The check will pass if the KmsKeyId is defined.",
    "Remediation": {
      "Recommendation": {
        "Text": "For information on how to correct this issue, consult the AWS Security Hub Cloud Security Posture Management (CSPM) controls documentation.",
        "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
      }
    },
    "ProductFields": {
      "StandardsArn": "arn:aws:securityhub:::standards/service-managed-aws-control-tower/v/1.0.0",
      "StandardsSubscriptionArn": "arn:aws:securityhub:us-east-1:123456789012:subscription/service-managed-aws-control-tower/v/1.0.0",
      "ControlId": "CT.CloudTrail.2",
      "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation",
      "RelatedAWSResources:0/name": "securityhub-cloud-trail-encryption-enabled-fe95bf3f",
      "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",

```

```

    "StandardsControlArn": "arn:aws:securityhub:us-east-1:123456789012:control/service-
managed-aws-control-tower/v/1.0.0/CloudTrail.2",
    "aws/securityhub/ProductName": "Security Hub CSPM",
    "aws/securityhub/CompanyName": "AWS",
    "Resources/Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWSMacieTrail-
DO-NOT-EDIT",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/
securityhub/arn:aws:securityhub:us-east-1:123456789012:subscription/service-managed-
aws-control-tower/v/1.0.0/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  },
  "Resources": [
    {
      "Type": "AwsAccount",
      "Id": "AWS:::Account:123456789012",
      "Partition": "aws",
      "Region": "us-east-1"
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "SecurityControlId": "CloudTrail.2",
    "AssociatedStandards": [{
      "StandardsId": "standards/service-managed-aws-control-tower/v/1.0.0"
    }]
  },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    },
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards"
    ]
  }
}

```

Sampel temuan konsolidasi untuk beberapa standar

Contoh berikut memberikan contoh temuan untuk kontrol yang berlaku untuk beberapa standar yang diaktifkan. Dalam sampel ini, temuan kontrol konsolidasi diaktifkan.

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-1:123456789012:security-control/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/securityhub",
  "ProductName": "Security Hub",
  "CompanyName": "AWS",
  "Region": "us-east-1",
  "GeneratorId": "security-control/CloudTrail.2",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards"
  ],
  "FirstObservedAt": "2024-08-09T14:57:04.521Z",
  "LastObservedAt": "2025-05-30T03:30:17.407Z",
  "CreatedAt": "2024-08-09T14:57:04.521Z",
  "UpdatedAt": "2025-05-30T03:30:32.781Z",
  "Severity": {
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
  },
  "Title": "CloudTrail should have encryption at-rest enabled",
  "Description": "This AWS control checks whether AWS CloudTrail is configured to use the server side encryption (SSE) AWS Key Management Service (AWS KMS) customer master key (CMK) encryption. The check will pass if the KmsKeyId is defined.",
  "Remediation": {
    "Recommendation": {
      "Text": "For information on how to correct this issue, consult the AWS Security Hub Cloud Security Posture Management (CSPM) controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
    }
  },
  "ProductFields": {
    "RelatedAWSResources:0/name": "securityhub-cloud-trail-encryption-enabled-01a2b345",
    "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
    "aws/securityhub/ProductName": "Security Hub",
  }
}
```

```

    "aws/securityhub/CompanyName": "AWS",
    "Resources/Id": "arn:aws:cloudtrail:us-east-1:123456789012:trail/TestTrail-D0-
NOT-DELETE",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/
securityhub/arn:aws:securityhub:us-east-1:123456789012:security-control/CloudTrail.2/
finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  },
  "Resources": [
    {
      "Type": "AwsCloudTrailTrail",
      "Id": "arn:aws:cloudtrail:us-east-1:123456789012:trail/TestTrail-D0-NOT-DELETE",
      "Partition": "aws",
      "Region": "us-east-1",
      "Details": {
        "AwsCloudTrailTrail": {
          "HasCustomEventSelectors": false,
          "IncludeGlobalServiceEvents": true,
          "LogFileValidationEnabled": true,
          "HomeRegion": "us-east-1",
          "IsMultiRegionTrail": true,
          "S3BucketName": "cloudtrail-awslogs-do-not-delete",
          "IsOrganizationTrail": false,
          "Name": "TestTrail-D0-NOT-DELETE"
        }
      }
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "SecurityControlId": "CloudTrail.2",
    "RelatedRequirements": [
      "CIS AWS Foundations Benchmark v1.2.0/2.7",
      "CIS AWS Foundations Benchmark v1.4.0/3.7",
      "CIS AWS Foundations Benchmark v3.0.0/3.5",
      "NIST.800-171.r2/3.3.8",
      "PCI DSS v3.2.1/3.4",
      "PCI DSS v4.0.1/10.3.2"
    ],
    "AssociatedStandards": [
      { "StandardsId": "ruleset/cis-aws-foundations-benchmark/v/1.2.0"},
      { "StandardsId": "standards/aws-foundational-security-best-practices/v/1.0.0"},
      { "StandardsId": "standards/cis-aws-foundations-benchmark/v/1.4.0"},
      { "StandardsId": "standards/cis-aws-foundations-benchmark/v/3.0.0"},
      { "StandardsId": "standards/nist-800-171/v/2.0.0"},

```

```
{ "StandardsId": "standards/pci-dss/v/3.2.1"},
  { "StandardsId": "standards/pci-dss/v/4.0.1"}
],
},
"Workflow": {
  "Status": "NEW"
},
"WorkflowState": "NEW",
"RecordState": "ACTIVE",
"FindingProviderFields": {
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards"
  ],
  "Severity": {
    "Normalized": 40,
    "Label": "MEDIUM",
    "Original": "MEDIUM"
  }
},
"ProcessedAt": "2025-05-30T03:31:00.831Z"
}
```


Memahami integrasi dalam Security Hub CSPM

AWS Security Hub Cloud Security Posture Management (CSPM) dapat menyerap temuan keamanan dari beberapa Layanan AWS solusi keamanan pihak ketiga AWS Partner Network yang didukung. Integrasi ini dapat membantu Anda mendapatkan pandangan komprehensif tentang keamanan dan kepatuhan di seluruh AWS lingkungan Anda. Security Hub CSPM menyerap temuan dari solusi terintegrasi dan mengubahnya menjadi AWS Security Finding Format (ASFF).

Important

Untuk integrasi produk yang didukung AWS dan pihak ketiga, Security Hub CSPM menerima dan mengkonsolidasikan temuan yang dihasilkan hanya setelah Anda mengaktifkan CSPM Security Hub untuk Anda. Akun AWS Layanan tidak secara surut menerima dan mengkonsolidasikan temuan keamanan yang dihasilkan sebelum Anda mengaktifkan CSPM Security Hub.

Halaman Integrasi konsol CSPM Security Hub menyediakan akses ke integrasi produk yang tersedia AWS dan pihak ketiga. Security Hub CSPM API juga memiliki operasi untuk mengelola integrasi.

Integrasi mungkin tidak tersedia di semua Wilayah AWS. Jika integrasi tidak didukung di Wilayah tempat Anda masuk saat ini di konsol CSPM Security Hub, integrasi tersebut tidak akan muncul di halaman Integrasi konsol. Untuk daftar integrasi yang tersedia di Wilayah Tiongkok dan AWS GovCloud (US) Regions, lihat [Ketersediaan integrasi menurut Wilayah](#)

Selain integrasi pihak ketiga bawaan, Anda dapat mengintegrasikan produk keamanan khusus dengan Security Hub CSPM. Layanan AWS Untuk informasi selengkapnya, lihat [Mengintegrasikan Security Hub CSPM dengan produk khusus](#).

Meninjau daftar integrasi CSPM Security Hub

Pilih metode pilihan Anda, dan ikuti langkah-langkah untuk meninjau daftar integrasi di AWS Security Hub Cloud Security Posture Management (CSPM) atau detail tentang integrasi tertentu.

Security Hub CSPM console

Untuk meninjau opsi dan detail integrasi (konsol)

1. Buka konsol AWS Security Hub Cloud Security Posture Management (CSPM) di. <https://console.aws.amazon.com/securityhub/>
2. Di panel navigasi CSPM Security Hub, pilih Integrasi.

Pada halaman Integrasi, integrasi dengan yang lain Layanan AWS tercantum terlebih dahulu, diikuti oleh integrasi dengan produk pihak ketiga.

Untuk setiap integrasi, halaman Integrasi memberikan informasi berikut:

- Nama perusahaan
- Nama produk
- Deskripsi integrasi
- Kategori yang diterapkan integrasi
- Cara mengaktifkan integrasi
- Status integrasi saat ini

Anda dapat memfilter daftar dengan memasukkan teks dari bidang berikut:

- Nama perusahaan
- Nama produk
- Deskripsi integrasi
- Kategori

Security Hub CSPM API

Untuk meninjau opsi dan detail integrasi (API)

Untuk mendapatkan daftar integrasi, gunakan [DescribeProducts](#) operasi. Jika Anda menggunakan AWS CLI, jalankan [describe-products](#) perintah.

Untuk mengambil detail untuk integrasi produk tertentu, gunakan `ProductArn` parameter untuk menentukan Nama Sumber Daya Amazon (ARN) integrasi.

Misalnya, AWS CLI perintah berikut mengambil rincian tentang integrasi CSPM Security Hub dengan 3. CORESec

```
$ aws securityhub describe-products --product-arn "arn:aws:securityhub:us-east-1::product/3coresec/3coresec"
```

Mengaktifkan alur temuan dari integrasi CSPM Security Hub

Pada halaman Integrasi konsol AWS Security Hub Cloud Security Posture Management (CSPM) Security Hub, Anda dapat melihat langkah-langkah yang diperlukan untuk mengaktifkan setiap integrasi.

Untuk sebagian besar integrasi dengan yang lain Layanan AWS, satu-satunya langkah yang diperlukan untuk mengaktifkan integrasi adalah mengaktifkan layanan lainnya. Informasi integrasi mencakup tautan ke halaman beranda layanan lain. Saat Anda mengaktifkan layanan lain, izin tingkat sumber daya yang memungkinkan CSPM Security Hub menerima temuan dari layanan kemudian dibuat dan diterapkan secara otomatis.

Untuk integrasi produk pihak ketiga, Anda mungkin perlu membeli integrasi dari AWS Marketplace, dan kemudian mengkonfigurasi integrasi. Informasi integrasi menyediakan tautan untuk menyelesaikan tugas-tugas ini.

Jika lebih dari satu versi produk tersedia AWS Marketplace, pilih versi yang ingin Anda berlangganan, lalu pilih Lanjutkan Berlangganan. Misalnya, beberapa produk menawarkan versi standar dan AWS GovCloud (US) versi.

Saat Anda mengaktifkan integrasi produk, kebijakan sumber daya secara otomatis dilampirkan ke langganan produk tersebut. Kebijakan sumber daya ini menentukan izin yang dibutuhkan CSPM Security Hub untuk menerima temuan dari produk tersebut.

Setelah Anda menyelesaikan langkah-langkah awal untuk mengaktifkan integrasi, Anda kemudian dapat menonaktifkan dan mengaktifkan kembali aliran temuan dari integrasi itu. Pada halaman Integrasi, untuk integrasi yang mengirimkan temuan, informasi Status menunjukkan apakah Anda saat ini menerima temuan.

Security Hub CSPM console

Untuk mengaktifkan aliran temuan dari integrasi (konsol)

1. Buka konsol AWS Security Hub Cloud Security Posture Management (CSPM) di <https://console.aws.amazon.com/securityhub/>
2. Di panel navigasi CSPM Security Hub, pilih Integrasi.
3. Untuk integrasi yang mengirimkan temuan, informasi Status menunjukkan apakah Security Hub CSPM saat ini menerima temuan dari integrasi tersebut.
4. Pilih Terima temuan.

Security Hub CSPM API

Gunakan [EnableImportFindingsForProduct](#) operasi. Jika Anda menggunakan AWS CLI, jalankan [enable-import-findings-for-product](#) perintah. Untuk mengaktifkan Security Hub menerima temuan dari integrasi, Anda memerlukan ARN produk. Untuk mendapatkan integrasi yang tersedia, gunakan [DescribeProducts](#) operasi. ARNs Jika Anda menggunakan AWS CLI, jalankan [describe-products](#).

Misalnya, AWS CLI perintah berikut memungkinkan Security Hub CSPM untuk menerima temuan dari integrasi CrowdStrike Falcon. Contoh ini diformat untuk Linux, macOS, atau Unix, dan menggunakan karakter garis miring terbalik (\) untuk meningkatkan keterbacaan.

```
$ aws securityhub enable-import-findings-for product --product-arn  
"arn:aws:securityhub:us-east-1:123456789333:product/crowdstrike/crowdstrike-falcon"
```

Menonaktifkan alur temuan dari integrasi CSPM Security Hub

Pilih metode pilihan Anda, dan ikuti langkah-langkah untuk menonaktifkan alur temuan dari integrasi AWS Security Hub Cloud Security Posture Management (CSPM) Security Hub.

Security Hub CSPM console

Untuk menonaktifkan aliran temuan dari integrasi (konsol)

1. Buka konsol AWS Security Hub Cloud Security Posture Management (CSPM) di <https://console.aws.amazon.com/securityhub/>
2. Di panel navigasi CSPM Security Hub, pilih Integrasi.

3. Untuk integrasi yang mengirimkan temuan, informasi Status menunjukkan apakah Security Hub CSPM saat ini menerima temuan dari integrasi tersebut.
4. Pilih Berhenti menerima temuan.

Security Hub CSPM API

Gunakan [DisableImportFindingsForProduct](#) operasi. Jika Anda menggunakan AWS CLI, jalankan [disable-import-findings-for-product](#) perintah. Untuk menonaktifkan aliran temuan dari integrasi, Anda memerlukan ARN berlangganan untuk integrasi yang diaktifkan. Untuk mendapatkan ARN berlangganan, gunakan operasi. [ListEnabledProductsForImport](#) Jika Anda menggunakan AWS CLI, jalankan [list-enabled-products-for-import](#).

Misalnya, AWS CLI perintah berikut menonaktifkan aliran temuan ke Security Hub CSPM dari integrasi Falcon. CrowdStrike Contoh ini diformat untuk Linux, macOS, atau Unix, dan menggunakan karakter garis miring terbalik (\) untuk meningkatkan keterbacaan.

```
$ aws securityhub disable-import-findings-for-product --product-subscription-arn  
"arn:aws:securityhub:us-west-1:123456789012:product-subscription/crowdstrike/  
crowdstrike-falcon"
```

Melihat temuan dari integrasi CSPM Security Hub

Saat Anda mulai menerima temuan dari integrasi AWS Security Hub Cloud Security Posture Management (CSPM) Security Hub, halaman Integrasi konsol CSPM Security Hub menampilkan Status integrasi sebagai Menerima temuan. Untuk meninjau daftar temuan dari integrasi, pilih Lihat temuan.

Daftar temuan menunjukkan temuan aktif untuk integrasi yang dipilih yang memiliki status alur kerja NEW atau NOTIFIED.

Jika Anda mengaktifkan agregasi lintas wilayah, maka di Wilayah agregasi, daftar tersebut mencakup temuan dari Wilayah agregasi dan dari Wilayah tertaut tempat integrasi diaktifkan. Security Hub tidak secara otomatis mengaktifkan integrasi berdasarkan konfigurasi agregasi lintas wilayah.

Di Wilayah lain, daftar temuan untuk integrasi hanya berisi temuan dari Wilayah saat ini.

Untuk informasi tentang cara mengonfigurasi agregasi lintas wilayah, lihat. [Menggabungkan data CSPM di seluruh Wilayah](#)

Dari daftar temuan, Anda dapat melakukan tindakan berikut.

- [Ubah filter dan pengelompokan untuk daftar](#)
- [Lihat detail untuk temuan individu](#)
- [Perbarui status alur kerja temuan](#)
- [Kirim temuan ke tindakan khusus](#)

Layanan AWS integrasi dengan Security Hub CSPM

AWS Security Hub Cloud Security Posture Management (CSPM) mendukung integrasi dengan beberapa lainnya. Layanan AWS

Note

Integrasi mungkin tidak tersedia di semua Wilayah AWS. Jika integrasi tidak didukung di Wilayah saat ini, integrasi tidak akan muncul di halaman Integrasi.

Untuk daftar integrasi yang tersedia di Wilayah Tiongkok dan AWS GovCloud (US), lihat [the section called “Integrasi yang didukung di Wilayah Tiongkok \(Beijing\) dan Tiongkok \(Ningxia\)”](#) dan [the section called “Integrasi yang didukung di Wilayah AWS GovCloud \(AS-Timur\) dan AWS GovCloud \(AS-Barat\)”](#)

Kecuali ditunjukkan di bawah ini, Layanan AWS integrasi yang mengirimkan temuan ke Security Hub CSPM diaktifkan secara otomatis setelah Anda mengaktifkan Security Hub CSPM dan layanan lainnya. Integrasi yang menerima temuan CSPM Security Hub mungkin memerlukan langkah-langkah tambahan untuk aktivasi. Tinjau informasi tentang setiap integrasi untuk mempelajari lebih lanjut.

Ikhtisar integrasi AWS layanan dengan Security Hub CSPM

Berikut adalah ikhtisar AWS layanan yang mengirimkan temuan ke Security Hub CSPM atau menerima temuan dari Security Hub CSPM.

AWS Layanan terintegrasi	Arahan	
AWS Config	Mengirim temuan	
AWS Firewall Manager	Mengirim temuan	

AWS Layanan terintegrasi	Arahan	
Amazon GuardDuty	Mengirim temuan	
AWS Health	Mengirim temuan	
AWS Identity and Access Management Access Analyzer	Mengirim temuan	
Amazon Inspector	Mengirim temuan	
AWS IoT Device Defender	Mengirim temuan	
Amazon Macie	Mengirim temuan	
AWS Systems Manager Manajer Patch	Mengirim temuan	
AWS Audit Manager	Menerima temuan	
Amazon Q Developer dalam aplikasi obrolan	Menerima temuan	
Amazon Detective	Menerima temuan	
Amazon Security Lake	Menerima temuan	
AWS Systems Manager Explorer dan OpsCenter	Menerima dan memperbarui temuan	
AWS Trusted Advisor	Menerima temuan	

AWS layanan yang mengirimkan temuan ke Security Hub CSPM

AWS Layanan berikut terintegrasi dengan Security Hub CSPM dengan mengirimkan temuan ke Security Hub CSPM. Security Hub CSPM mengubah temuan menjadi [AWS Security](#) Finding Format.

AWS Config (Mengirim temuan)

AWS Config adalah layanan yang memungkinkan Anda menilai, mengaudit, dan mengevaluasi konfigurasi AWS sumber daya Anda. AWS Config terus memantau dan merekam konfigurasi AWS sumber daya Anda dan memungkinkan Anda untuk mengotomatiskan evaluasi konfigurasi yang direkam terhadap konfigurasi yang diinginkan.

Dengan menggunakan integrasi dengan AWS Config, Anda dapat melihat hasil evaluasi aturan AWS Config terkelola dan kustom sebagai temuan di Security Hub CSPM. Temuan ini dapat dilihat bersama temuan CSPM Security Hub lainnya, memberikan gambaran menyeluruh tentang postur keamanan Anda.

AWS Config menggunakan Amazon EventBridge untuk mengirim evaluasi AWS Config aturan ke Security Hub CSPM. [Security Hub CSPM mengubah evaluasi aturan menjadi temuan yang mengikuti Format Pencarian Keamanan.AWS](#) Security Hub CSPM kemudian memperkaya temuan berdasarkan upaya terbaik dengan mendapatkan informasi lebih lanjut tentang sumber daya yang terkena dampak, seperti Nama Sumber Daya Amazon (ARN), tag sumber daya, dan tanggal pembuatan.

Untuk informasi selengkapnya tentang integrasi ini, lihat bagian berikut.

Cara AWS Config mengirimkan temuan ke Security Hub CSPM

Semua temuan di Security Hub CSPM menggunakan format JSON standar ASFF. ASFF mencakup rincian tentang asal temuan, sumber daya yang terpengaruh, dan status temuan saat ini. AWS Config mengirimkan evaluasi aturan terkelola dan kustom ke Security Hub CSPM melalui EventBridge. Security Hub CSPM mengubah evaluasi aturan menjadi temuan yang mengikuti ASFF dan memperkaya temuan berdasarkan upaya terbaik.

Jenis temuan yang AWS Config dikirim ke Security Hub CSPM

Setelah integrasi diaktifkan, AWS Config mengirimkan evaluasi semua aturan AWS Config terkelola dan aturan kustom ke Security Hub CSPM. Hanya evaluasi yang dilakukan setelah Security Hub CSPM diaktifkan yang dikirim. Misalnya, evaluasi AWS Config aturan mengungkapkan lima sumber daya yang gagal. Jika saya mengaktifkan Security Hub CSPM setelah itu, dan aturan kemudian mengungkapkan sumber daya keenam yang gagal, hanya AWS Config mengirimkan evaluasi sumber daya keenam ke Security Hub CSPM.

Evaluasi dari [AWS Config aturan terkait layanan](#), seperti yang digunakan untuk menjalankan pemeriksaan pada kontrol CSPM Security Hub, dikecualikan.

Mengirim AWS Config temuan ke Security Hub CSPM

Ketika integrasi diaktifkan, Security Hub CSPM akan secara otomatis menetapkan izin yang diperlukan untuk menerima temuan dari AWS Config Security Hub CSPM menggunakan izin service-to-service tingkat yang memberi Anda cara aman untuk mengaktifkan integrasi ini dan mengimpor temuan dari melalui AWS Config Amazon. EventBridge

Latensi untuk mengirim temuan

Saat AWS Config membuat temuan baru, Anda biasanya dapat melihat temuan di Security Hub CSPM dalam waktu lima menit.

Mencoba lagi saat Security Hub CSPM tidak tersedia

AWS Config mengirimkan temuan ke Security Hub CSPM dengan upaya terbaik melalui EventBridge. Jika acara tidak berhasil dikirim ke Security Hub CSPM, EventBridge coba ulang pengiriman hingga 24 jam atau 185 kali, mana yang lebih dulu.

Memperbarui AWS Config temuan yang ada di Security Hub CSPM

Setelah AWS Config mengirim temuan ke Security Hub CSPM, itu dapat mengirim pembaruan ke temuan yang sama ke Security Hub CSPM untuk mencerminkan pengamatan tambahan dari aktivitas temuan. Pembaruan hanya dikirim untuk ComplianceChangeNotification acara. Jika tidak terjadi perubahan kepatuhan, pembaruan tidak akan dikirim ke Security Hub CSPM. Security Hub CSPM menghapus temuan 90 hari setelah pembaruan terbaru atau 90 hari setelah pembuatan jika tidak ada pembaruan yang terjadi.

Security Hub CSPM tidak mengarsipkan temuan yang dikirim dari AWS Config meskipun Anda menghapus sumber daya terkait.

Daerah di mana AWS Config temuan ada

AWS Config Temuan ini terjadi secara regional. AWS Config mengirimkan temuan ke Security Hub CSPM di Wilayah atau Wilayah yang sama di mana temuan terjadi.

Melihat AWS Config temuan di Security Hub CSPM

Untuk melihat AWS Config temuan Anda, pilih Temuan dari panel navigasi CSPM Security Hub. Untuk memfilter temuan agar hanya menampilkan AWS Config temuan, pilih Nama produk di drop-down bilah pencarian. Masukkan Config, dan pilih Apply.

Menafsirkan AWS Config pencarian nama di Security Hub CSPM

Security Hub CSPM mengubah evaluasi AWS Config aturan menjadi temuan yang mengikuti [AWS Format Pencarian Keamanan \(ASFF\)](#). AWS Config evaluasi aturan menggunakan pola peristiwa yang berbeda dibandingkan dengan ASFF. Tabel berikut memetakan bidang evaluasi AWS Config aturan dengan rekan ASFF mereka seperti yang muncul di Security Hub CSPM.

Jenis temuan evaluasi aturan Config	Tipe temuan ASFF	Nilai hardcode
detail. awsAccountId	AwsAccountId	
detail. newEvaluationResult. resultRecordedTime	CreatedAt	
detail. newEvaluationResult. resultRecordedTime	UpdatedAt	
	ProductArn	<partition><region> >"arn ::securityhub:::" product/ aws/config
	ProductName	"Config"
	CompanyName	"AWS"
	Wilayah	"eu-sentral-1"
configRuleArn	GeneratorId, ProductFields	
detail. ConfigRuleARN/finding/ hash	Id	
detail. configRuleName	Judul, ProductFields	
detail. configRuleName	Deskripsi	"Temuan ini dibuat untuk perubahan kepatuhan sumber daya untuk aturan konfigura si:\${detail.ConfigRuleName} eName} "

Jenis temuan evaluasi aturan Config	Tipe temuan ASFF	Nilai hardcode
Item Konfigurasi “ARN” atau Security Hub CSPM menghitung ARN	Sumber [i] .id	
detail.ResourceType	Sumber Daya [i] .Type	"AwsS3Bucket"
	Sumber Daya [i] .Partisi	"aws"
	Sumber Daya [i] .Region	"eu-sentral-1"
Item Konfigurasi “konfigurasi”	Sumber Daya [i] .Detail	
	SchemaVersion	"2018-10-08"
	Keparahan. Label	Lihat “Menafsirkan Label Keparahan” di bawah ini
	Tipe	["Pemeriksaan Perangkat Lunak dan Konfigurasi"]
detail. newEvaluationResult.ComplianceType	Kepatuhan.Status	“GAGAL”, “NOT_AVAILABLE”, “LULUS”, atau “PERINGATAN”
	Alur kerja.Status	“DISELESAIKAN” jika AWS Config temuan dihasilkan dengan Compliance.Status dari “LULUS,” atau jika Compliance.Status berubah dari “GAGAL” menjadi “LULUS.” Jika tidak, Workflow.Status akan menjadi “BARU.” Anda dapat mengubah nilai ini dengan operasi BatchUpdateFindingsAPI .

Menafsirkan label keparahan

Semua temuan dari evaluasi AWS Config aturan memiliki label keparahan default MEDIUM di ASFF. Anda dapat memperbarui label keparahan temuan dengan operasi [BatchUpdateFindingsAPI](#).

Temuan khas dari AWS Config

Security Hub CSPM mengubah evaluasi AWS Config aturan menjadi temuan yang mengikuti ASFF. Berikut ini adalah contoh temuan khas dari AWS Config dalam ASFF.

Note

Jika deskripsi lebih dari 1024 karakter, itu akan dipotong menjadi 1024 karakter dan akan mengatakan "(terpotong)" di akhir.

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:config:eu-central-1:123456789012:config-rule/config-rule-mburzq/finding/45g070df80cb50b68fa6a43594kc6fda1e517932",
  "ProductArn": "arn:aws:securityhub:eu-central-1::product/aws/config",
  "ProductName": "Config",
  "CompanyName": "AWS",
  "Region": "eu-central-1",
  "GeneratorId": "arn:aws:config:eu-central-1:123456789012:config-rule/config-rule-mburzq",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks"
  ],
  "CreatedAt": "2022-04-15T05:00:37.181Z",
  "UpdatedAt": "2022-04-19T21:20:15.056Z",
  "Severity": {
    "Label": "MEDIUM",
    "Normalized": 40
  },
  "Title": "s3-bucket-level-public-access-prohibited-config-integration-demo",
  "Description": "This finding is created for a resource compliance change for config rule: s3-bucket-level-public-access-prohibited-config-integration-demo",
  "ProductFields": {
    "aws/securityhub/ProductName": "Config",
    "aws/securityhub/CompanyName": "AWS",
```

```

    "aws/securityhub/FindingId": "arn:aws:securityhub:eu-central-1::product/aws/
    config/arn:aws:config:eu-central-1:123456789012:config-rule/config-rule-mburzq/
    finding/46f070df80cd50b68fa6a43594dc5fda1e517902",
    "aws/config/ConfigRuleArn": "arn:aws:config:eu-central-1:123456789012:config-rule/
    config-rule-mburzq",
    "aws/config/ConfigRuleName": "s3-bucket-level-public-access-prohibited-config-
    integration-demo",
    "aws/config/ConfigComplianceType": "NON_COMPLIANT"
  },
  "Resources": [{
    "Type": "AwsS3Bucket",
    "Id": "arn:aws:s3:::amzn-s3-demo-bucket",
    "Partition": "aws",
    "Region": "eu-central-1",
    "Details": {
      "AwsS3Bucket": {
        "OwnerId": "4edbbba300f1caa608fba2aad2c8fcfe30c32ca32777f64451eec4fb2a0f10d8c",
        "CreatedAt": "2022-04-15T04:32:53.000Z"
      }
    }
  ]},
  "Compliance": {
    "Status": "FAILED"
  },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "MEDIUM"
    },
    "Types": [
      "Software and Configuration Checks"
    ]
  }
}

```

Mengaktifkan dan mengonfigurasi integrasi

Setelah Anda mengaktifkan Security Hub CSPM, integrasi ini diaktifkan secara otomatis. AWS Config segera mulai mengirim temuan ke Security Hub CSPM.

Menghentikan publikasi temuan ke Security Hub CSPM

Untuk menghentikan pengiriman temuan ke Security Hub CSPM, Anda dapat menggunakan konsol CSPM Security Hub atau Security Hub CSPM API.

Untuk petunjuk tentang menghentikan aliran temuan, lihat [Mengaktifkan alur temuan dari integrasi CSPM Security Hub](#).

AWS Firewall Manager (Mengirim temuan)

Firewall Manager mengirimkan temuan ke Security Hub CSPM ketika kebijakan firewall aplikasi web (WAF) untuk sumber daya atau aturan daftar kontrol akses web (web ACL) tidak sesuai. Firewall Manager juga mengirimkan temuan ketika AWS Shield Advanced tidak melindungi sumber daya, atau ketika serangan diidentifikasi.

Setelah Anda mengaktifkan Security Hub CSPM, integrasi ini diaktifkan secara otomatis. Firewall Manager segera mulai mengirimkan temuan ke Security Hub CSPM.

Untuk mempelajari lebih lanjut tentang integrasi, lihat halaman Integrasi di konsol CSPM Security Hub.

Untuk mempelajari lebih lanjut tentang Firewall Manager, lihat [Panduan AWS WAF Pengembang](#).

Amazon GuardDuty (Mengirim temuan)

GuardDuty mengirimkan semua jenis temuan yang dihasilkannya ke Security Hub CSPM. Beberapa jenis temuan memiliki prasyarat, persyaratan pemberdayaan, atau batasan Regional. Untuk informasi selengkapnya, lihat [GuardDuty menemukan jenis](#) di Panduan GuardDuty Pengguna Amazon.

Temuan baru GuardDuty dikirim ke Security Hub CSPM dalam waktu lima menit. Pembaruan temuan dikirim berdasarkan pengaturan temuan yang diperbarui untuk Amazon EventBridge dalam GuardDuty pengaturan.

Saat Anda menghasilkan temuan GuardDuty sampel menggunakan halaman GuardDuty Pengaturan, Security Hub CSPM menerima temuan sampel dan menghilangkan awalan [Sample] dalam jenis temuan. Misalnya, tipe pencarian sampel ditampilkan seperti Recon:IAMUser/ResourcePermissions pada GuardDuty [SAMPLE] Recon:IAMUser/ResourcePermissions Security Hub CSPM.

Setelah Anda mengaktifkan Security Hub CSPM, integrasi ini diaktifkan secara otomatis. GuardDuty segera mulai mengirim temuan ke Security Hub CSPM.

Untuk informasi selengkapnya tentang GuardDuty integrasi, lihat [Mengintegrasikan dengan AWS Security Hub Cloud Security Posture Management \(CSPM\)](#) di Panduan Pengguna Amazon GuardDuty .

AWS Health (Mengirim temuan)

AWS Health memberikan visibilitas berkelanjutan ke kinerja sumber daya Anda dan ketersediaan Anda Layanan AWS dan Akun AWS. Anda dapat menggunakan AWS Health peristiwa untuk mempelajari bagaimana perubahan layanan dan sumber daya dapat memengaruhi aplikasi yang berjalan AWS.

Integrasi dengan AWS Health tidak menggunakan `BatchImportFindings`. Sebagai gantinya, AWS Health gunakan pesan service-to-service acara untuk mengirim temuan ke Security Hub CSPM.

Untuk informasi selengkapnya tentang integrasi, lihat bagian berikut.

Cara AWS Health mengirimkan temuan ke Security Hub CSPM

Di Security Hub CSPM, masalah keamanan dilacak sebagai temuan. Beberapa temuan berasal dari masalah yang terdeteksi oleh AWS layanan lain atau oleh mitra pihak ketiga. Security Hub CSPM juga memiliki seperangkat aturan yang digunakan untuk mendeteksi masalah keamanan dan menghasilkan temuan.

Security Hub CSPM menyediakan alat untuk mengelola temuan dari seluruh sumber ini. Anda dapat melihat dan memfilter daftar temuan dan melihat detail untuk temuan. Lihat [Meninjau detail dan riwayat penemuan di Security Hub CSPM](#). Anda juga dapat melacak status penyelidikan ke temuan. Lihat [Menetapkan status alur kerja temuan di Security Hub CSPM](#).

Semua temuan di Security Hub CSPM menggunakan format JSON standar yang disebut [AWS Format Pencarian Keamanan \(ASFF\)](#). ASFF mencakup rincian tentang sumber masalah, sumber daya yang terpengaruh, dan status temuan saat ini.

AWS Health adalah salah satu AWS layanan yang mengirimkan temuan ke Security Hub CSPM.

Jenis temuan yang AWS Health dikirim ke Security Hub CSPM

Setelah integrasi diaktifkan, AWS Health kirimkan temuan yang memenuhi satu atau lebih spesifikasi yang tercantum ke Security Hub CSPM. Security Hub CSPM mencerna temuan di [AWS Format Pencarian Keamanan \(ASFF\)](#)

- Temuan yang mengandung salah satu nilai berikut untuk Layanan AWS:
 - RISK

- ABUSE
- ACM
- CLOUDHSM
- CLOUDTRAIL
- CONFIG
- CONTROLTOWER
- DETECTIVE
- EVENTS
- GUARDDUTY
- IAM
- INSPECTOR
- KMS
- MACIE
- SES
- SECURITYHUB
- SHIELD
- SSO
- COGNITO
- IOTDEVICEDEFENDER
- NETWORKFIREWALL
- ROUTE53
- WAF
- FIREWALLMANAGER
- SECRETSMANAGER
- BACKUP
- AUDITMANAGER
- ARTIFACT
- CLOUDENDURE
- CODEGURU
- ORGANIZATIONS

- DIRECTORYSERVICE
- RESOURCEMANAGER
- CLOUDWATCH
- DRS
- INSPECTOR2
- RESILIENCEHUB
- Temuan dengan kata-kata securityabuse,, atau certificate di AWS Health typeCode lapangan
- Temuan di mana AWS Health layanan tersebut risk atau abuse

Mengirim AWS Health temuan ke Security Hub CSPM

Ketika Anda memilih untuk menerima temuan dari AWS Health, Security Hub CSPM akan secara otomatis menetapkan izin yang diperlukan untuk menerima temuan dari. AWS Health Security Hub CSPM menggunakan izin service-to-service tingkat yang memberi Anda cara yang aman dan mudah untuk mengaktifkan integrasi ini dan mengimpor temuan dari melalui AWS Health Amazon EventBridge atas nama Anda. Memilih Terima Temuan memberikan izin CSPM Security Hub untuk mengkonsumsi temuan dari. AWS Health

Latensi untuk mengirim temuan

Ketika AWS Health membuat temuan baru, biasanya dikirim ke Security Hub CSPM dalam waktu lima menit.

Mencoba lagi saat Security Hub CSPM tidak tersedia

AWS Health mengirimkan temuan ke Security Hub CSPM dengan upaya terbaik melalui. EventBridge Jika acara tidak berhasil dikirim ke Security Hub CSPM, EventBridge coba lagi mengirimkan acara selama 24 jam.

Memperbarui temuan yang ada di Security Hub CSPM

Setelah AWS Health mengirim temuan ke Security Hub CSPM, itu dapat mengirim pembaruan ke temuan yang sama untuk mencerminkan pengamatan tambahan dari aktivitas temuan ke Security Hub CSPM.

Daerah di mana temuan ada

Untuk acara global, AWS Health kirimkan temuan ke Security Hub CSPM di us-east-1 (partisi AWS), cn-northwest-1 (partisi Tiongkok), dan -1 (partisi). gov-us-west GovCloud AWS Health mengirimkan peristiwa khusus Wilayah ke CSPM Security Hub di Wilayah atau Wilayah yang sama tempat kejadian terjadi.

Melihat AWS Health temuan di Security Hub CSPM

Untuk melihat AWS Health temuan Anda di Security Hub CSPM, pilih Temuan dari panel navigasi. Untuk memfilter temuan agar hanya menampilkan AWS Health temuan, pilih Kesehatan dari bidang Nama produk.

Menafsirkan AWS Health pencarian nama di Security Hub CSPM

AWS Health mengirimkan temuan ke Security Hub CSPM menggunakan [AWS Format Pencarian Keamanan \(ASFF\)](#). AWS Health temuan menggunakan pola peristiwa yang berbeda dibandingkan dengan Security Hub CSPM format ASFF. Tabel di bawah ini merinci semua bidang AWS Health temuan dengan rekan ASFF mereka seperti yang muncul di Security Hub CSPM.

Jenis temuan Kesehatan	Tipe temuan ASFF	Nilai hardcode
akun	AwsAccountId	
detail.starttime	CreatedAt	
Detail.eventDescription.LatestDescription	Deskripsi	
detail.eventTypeCode	GeneratorId	
detail.eventARN (termasuk akun) + hash dari detail.startTime	Id	
<region>"arn:aws:securityhub::" product/aws/health	ProductArn	
akun atau resourceID	Sumber [i] .id	
	Sumber Daya [i] .Type	"Lainnya"

Jenis temuan Kesehatan	Tipe temuan ASFF	Nilai hardcode
	SchemaVersion	"2018-10-08"
	Keparahan. Label	Lihat "Menafsirkan Label Keparahan" di bawah ini
"AWS Health -" detail. eventTypeCode	Judul	
-	Tipe	["Pemeriksaan Perangkat Lunak dan Konfigurasi"]
event.time	UpdatedAt	
URL acara di konsol Health	SourceUrl	

Menafsirkan label keparahan

Label keparahan dalam temuan ASFF ditentukan menggunakan logika berikut:

- **Keparahan KRITIS** jika:
 - serviceBidang dalam AWS Health temuan memiliki nilai Risk
 - typeCodeBidang dalam AWS Health temuan memiliki nilai AWS_S3_OPEN_ACCESS_BUCKET_NOTIFICATION
 - typeCodeBidang dalam AWS Health temuan memiliki nilai AWS_SHIELD_INTERNET_TRAFFIC_LIMITATIONS_PLACED_IN_RESPONSE_TO_DDOS_ATTACK
 - typeCodeBidang dalam AWS Health temuan memiliki nilai AWS_SHIELD_IS_RESPONDING_TO_A_DDOS_ATTACK_AGAINST_YOUR_AWS_RESOURCES

Tingkat keparahan **TINGGI** jika:

- serviceBidang dalam AWS Health temuan memiliki nilai Abuse
- typeCodeBidang dalam AWS Health temuan berisi nilai SECURITY_NOTIFICATION
- typeCodeBidang dalam AWS Health temuan berisi nilai ABUSE_DETECTION

Keparahan **MEDIUM** jika:

- serviceBidang dalam temuan ini adalah salah satu dari yang berikut:ACM,ARTIFACT,AUDITMANAGER,BACKUP,CLOUDENDURE,CLOUDHSM,CLOUDTRAIL,CLOUDWATCH,WAF
- Bidang TypeCode dalam AWS Health temuan berisi nilai CERTIFICATE
- Bidang TypeCode dalam AWS Health temuan berisi nilai END_OF_SUPPORT

Temuan khas dari AWS Health

AWS Health mengirimkan temuan ke Security Hub CSPM menggunakan [AWS Format Pencarian Keamanan \(ASFF\)](#). Berikut ini adalah contoh temuan khas dari AWS Health.

Note

Jika deskripsi lebih dari 1024 karakter, itu akan dipotong menjadi 1024 karakter dan akan mengatakan (terpotong) di akhir.

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:health:us-east-1:123456789012:event/SES/
AWS_SES_CMF_PENDING_TO_SUCCESS/
AWS_SES_CMF_PENDING_TO_SUCCESS_303388638044_33fe2115-8dad-40ce-
b533-78e29f49de96/101F7FBAEFC663977DA09CFF56A29236602834D2D361E6A8CA5140BFB3A69B30",
  "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/health",
  "GeneratorId": "AWS_SES_CMF_PENDING_TO_SUCCESS",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks"
  ],
  "CreatedAt": "2022-01-07T16:34:04.000Z",
  "UpdatedAt": "2022-01-07T19:17:43.000Z",
  "Severity": {
    "Label": "MEDIUM",
    "Normalized": 40
  },
  "Title": "AWS Health - AWS_SES_CMF_PENDING_TO_SUCCESS",
  "Description": "Congratulations! Amazon SES has successfully detected the
MX record required to use 4557227d-9257-4e49-8d5b-18a99ced4be9.cmf.pinpoint.sysmon-
iad.adzel.com as a custom MAIL FROM domain for verified identity cmf.pinpoint.sysmon-
iad.adzel.com in AWS Region US East (N. Virginia).\n\nYou can now use this MAIL
```

```
FROM domain with cmf.pinpoint.sysmon-iad.adzel.com and any other verified identity
that is configured to use it. For information about how to configure a verified
identity to use a custom MAIL FROM domain, see http://docs.aws.amazon.com/ses/latest/DeveloperGuide/mail-from-set.html .\\n\\nPlease note that this email only applies to
AWS Region US East (N. Virginia).",
    "SourceUrl": "https://phd.aws.amazon.com/phd/home#/event-log?
eventID=arn:aws:health:us-east-1::event/SES/AWS_SES_CMF_PENDING_TO_SUCCESS/
AWS_SES_CMF_PENDING_TO_SUCCESS_303388638044_33fe2115-8dad-40ce-b533-78e29f49de96",
    "ProductFields": {
        "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/
aws/health/arn:aws:health:us-east-1::event/SES/AWS_SES_CMF_PENDING_TO_SUCCESS/
AWS_SES_CMF_PENDING_TO_SUCCESS_303388638044_33fe2115-8dad-40ce-b533-78e29f49de96",
        "aws/securityhub/ProductName": "Health",
        "aws/securityhub/CompanyName": "AWS"
    },
    "Resources": [
        {
            "Type": "Other",
            "Id": "4557227d-9257-4e49-8d5b-18a99ced4be9.cmf.pinpoint.sysmon-
iad.adzel.com"
        }
    ],
    "WorkflowState": "NEW",
    "Workflow": {
        "Status": "NEW"
    },
    "RecordState": "ACTIVE",
    "FindingProviderFields": {
        "Severity": {
            "Label": "MEDIUM"
        },
        "Types": [
            "Software and Configuration Checks"
        ]
    }
}
]
```

Mengaktifkan dan mengonfigurasi integrasi

Setelah Anda mengaktifkan Security Hub CSPM, integrasi ini diaktifkan secara otomatis. AWS Health segera mulai mengirim temuan ke Security Hub CSPM.

Menghentikan publikasi temuan ke Security Hub CSPM

Untuk menghentikan pengiriman temuan ke Security Hub CSPM, Anda dapat menggunakan konsol CSPM Security Hub atau Security Hub CSPM API.

Untuk petunjuk tentang menghentikan aliran temuan, lihat [Mengaktifkan alur temuan dari integrasi CSPM Security Hub](#).

AWS Identity and Access Management Access Analyzer (Mengirim temuan)

Dengan IAM Access Analyzer, semua temuan dikirim ke Security Hub CSPM.

IAM Access Analyzer menggunakan penalaran berbasis logika untuk menganalisis kebijakan berbasis sumber daya yang diterapkan pada sumber daya yang didukung di akun Anda. IAM Access Analyzer menghasilkan temuan ketika mendeteksi pernyataan kebijakan yang memungkinkan prinsipal eksternal mengakses sumber daya di akun Anda.

Di IAM Access Analyzer, hanya akun administrator yang dapat melihat temuan untuk penganalisis yang berlaku untuk organisasi. Untuk penganalisis organisasi, bidang `AwsAccountId` ASFF mencerminkan ID akun administrator. Di bawah `ProductFields`, `ResourceOwnerAccount` bidang menunjukkan akun di mana temuan itu ditemukan. Jika Anda mengaktifkan penganalisis satu per satu untuk setiap akun, Security Hub CSPM menghasilkan beberapa temuan, yang mengidentifikasi ID akun administrator dan satu yang mengidentifikasi ID akun sumber daya.

Untuk informasi selengkapnya, lihat [Integrasi dengan AWS Security Hub Cloud Security Posture Management \(CSPM\)](#) di Panduan Pengguna IAM.

Amazon Inspector (Mengirim temuan)

Amazon Inspector adalah layanan manajemen kerentanan yang terus memindai beban kerja Anda AWS untuk mencari kerentanan. Amazon Inspector secara otomatis menemukan dan memindai EC2 instans Amazon dan gambar kontainer yang berada di Amazon Elastic Container Registry. Pemindaian mencari kerentanan perangkat lunak dan eksposur jaringan yang tidak diinginkan.

Setelah Anda mengaktifkan Security Hub CSPM, integrasi ini diaktifkan secara otomatis. Amazon Inspector segera mulai mengirimkan semua temuan yang dihasilkannya ke Security Hub CSPM.

Untuk informasi selengkapnya tentang integrasi, lihat [Integrasi dengan AWS Security Hub Cloud Security Posture Management \(CSPM\)](#) di Panduan Pengguna Amazon Inspector.

Security Hub CSPM juga dapat menerima temuan dari Amazon Inspector Classic. Amazon Inspector Classic mengirimkan temuan ke Security Hub CSPM yang dihasilkan melalui proses penilaian untuk semua paket aturan yang didukung.

Untuk informasi selengkapnya tentang integrasi, lihat [Integrasi dengan AWS Security Hub Cloud Security Posture Management \(CSPM\)](#) di Panduan Pengguna Amazon Inspector Classic.

Temuan untuk Amazon Inspector dan Amazon Inspector Classic menggunakan produk yang sama ARN. Temuan Amazon Inspector memiliki entri berikut di: ProductFields

```
"aws/inspector/ProductVersion": "2",
```

AWS IoT Device Defender (Mengirim temuan)

AWS IoT Device Defender adalah layanan keamanan yang mengaudit konfigurasi perangkat IoT Anda, memantau perangkat yang terhubung untuk mendeteksi perilaku abnormal, dan membantu mengurangi risiko keamanan.

Setelah mengaktifkan keduanya AWS IoT Device Defender dan Security Hub CSPM, kunjungi [halaman Integrasi konsol CSPM Security Hub](#), dan pilih Terima temuan untuk Audit, Deteksi, atau keduanya. AWS IoT Device Defender Audit dan Deteksi mulai mengirimkan semua temuan ke Security Hub CSPM.

AWS IoT Device Defender Audit mengirimkan ringkasan cek ke Security Hub CSPM, yang berisi informasi umum untuk jenis pemeriksaan audit tertentu dan tugas audit. AWS IoT Device Defender Deteksi mengirimkan temuan pelanggaran untuk pembelajaran mesin (ML), statistik, dan perilaku statis ke Security Hub CSPM. Audit juga mengirimkan pembaruan temuan ke Security Hub CSPM.

Untuk informasi selengkapnya tentang integrasi ini, lihat [Integrasi dengan AWS Security Hub Cloud Security Posture Management \(CSPM\)](#) di Panduan AWS IoT Pengembang.

Amazon Macie (Mengirim temuan)

Temuan dari Macie dapat menunjukkan bahwa ada potensi pelanggaran kebijakan atau bahwa data sensitif, seperti informasi identitas pribadi (PII), hadir dalam data yang disimpan organisasi Anda di Amazon S3.

Setelah Anda mengaktifkan Security Hub CSPM, Macie secara otomatis mulai mengirimkan temuan kebijakan ke Security Hub CSPM. Anda dapat mengonfigurasi integrasi untuk juga mengirim temuan data sensitif ke Security Hub CSPM.

Di Security Hub CSPM, jenis temuan untuk kebijakan atau temuan data sensitif diubah menjadi nilai yang kompatibel dengan ASFF. Misalnya, jenis Policy: IAMUser/S3BucketPublic temuan di Macie ditampilkan seperti Effects/Data Exposure/Policy: IAMUser-S3BucketPublic pada Security Hub CSPM.

Macie juga mengirimkan temuan sampel yang dihasilkan ke Security Hub CSPM. Untuk temuan sampel, nama sumber daya yang terpengaruh adalah macie-sample-finding-bucket dan nilai untuk Sample bidang tersebut adalah true.

Untuk informasi selengkapnya, lihat [Integrasi Amazon Macie dengan AWS Security Hub Cloud Security Posture Management \(CSPM\) di Panduan Pengguna](#) Amazon Macie.

AWS Systems Manager Patch Manager (Mengirim temuan)

AWS Systems Manager Patch Manager mengirimkan temuan ke Security Hub CSPM ketika instance dalam armada pelanggan tidak sesuai dengan standar kepatuhan patch mereka.

Patch Manager mengotomatiskan proses patching instans terkelola dengan pembaruan terkait keamanan dan jenis pembaruan lainnya.

Setelah Anda mengaktifkan Security Hub CSPM, integrasi ini diaktifkan secara otomatis. Systems Manager Patch Manager segera mulai mengirimkan temuan ke Security Hub CSPM.

Untuk informasi selengkapnya tentang menggunakan Patch Manager, lihat [AWS Systems Manager Patch Manager](#) di Panduan AWS Systems Manager Pengguna.

AWS layanan yang menerima temuan dari Security Hub CSPM

AWS Layanan berikut terintegrasi dengan Security Hub CSPM dan menerima temuan dari Security Hub CSPM. Jika dicatat, layanan terintegrasi juga dapat memperbarui temuan. Dalam hal ini, menemukan pembaruan yang Anda buat dalam layanan terintegrasi juga akan tercermin dalam Security Hub CSPM.

AWS Audit Manager (Menerima temuan)

AWS Audit Manager menerima temuan dari Security Hub CSPM. Temuan ini membantu pengguna Audit Manager untuk mempersiapkan audit.

Untuk mempelajari Audit Manager selengkapnya, lihat [Panduan Pengguna AWS Audit Manager. AWS Security Hub Cloud Security Posture Management \(CSPM\) memeriksa yang didukung oleh](#)

[AWS Audit Manager](#) daftar kontrol tempat Security Hub CSPM mengirimkan temuannya ke Audit Manager.

Pengembang Amazon Q dalam aplikasi obrolan (Menerima temuan)

Pengembang Amazon Q dalam aplikasi obrolan adalah agen interaktif yang membantu Anda memantau dan berinteraksi dengan AWS sumber daya Anda di saluran Slack dan ruang obrolan Amazon Chime.

Pengembang Amazon Q dalam aplikasi obrolan menerima temuan dari Security Hub CSPM.

Untuk mempelajari lebih lanjut tentang Pengembang Amazon Q dalam integrasi aplikasi obrolan dengan Security Hub CSPM, lihat ikhtisar [integrasi CSPM Security Hub di Panduan Administrator](#) Pengembang Amazon Q dalam aplikasi obrolan.

Detektif Amazon (Menerima temuan)

Detective secara otomatis mengumpulkan data log dari AWS sumber daya Anda dan menggunakan pembelajaran mesin, analisis statistik, dan teori grafik untuk membantu Anda memvisualisasikan dan melakukan penyelidikan keamanan yang lebih cepat dan lebih efisien.

Integrasi CSPM Security Hub dengan Detective memungkinkan Anda untuk beralih dari temuan Amazon di GuardDuty Security Hub CSPM ke Detective. Anda kemudian dapat menggunakan alat Detektif dan visualisasi untuk menyelidikinya. Integrasi tidak memerlukan konfigurasi tambahan di Security Hub CSPM atau Detective.

Untuk temuan yang diterima dari yang lain Layanan AWS, panel rincian temuan di konsol CSPM Security Hub mencakup sub-bagian Investigasi di Detektif. Subbagian itu berisi tautan ke Detektif di mana Anda dapat menyelidiki lebih lanjut masalah keamanan yang ditandai oleh temuan tersebut. Anda juga dapat membuat grafik perilaku di Detective berdasarkan temuan CSPM Security Hub untuk melakukan penyelidikan yang lebih efektif. Untuk informasi selengkapnya, lihat [temuan AWS keamanan](#) di Panduan Administrasi Detektif Amazon.

Jika agregasi lintas wilayah diaktifkan, maka ketika Anda berputar dari Wilayah agregasi, Detektif terbuka di Wilayah tempat temuan itu berasal.

Jika tautan tidak berfungsi, maka untuk saran pemecahan masalah, lihat [Memecahkan masalah pivot](#).

Danau Keamanan Amazon (Menerima temuan)

Security Lake adalah layanan danau data keamanan yang dikelola sepenuhnya. Anda dapat menggunakan Security Lake untuk secara otomatis memusatkan data keamanan dari sumber cloud, lokal, dan kustom ke dalam data lake yang disimpan di akun Anda. Pelanggan dapat menggunakan data dari Security Lake untuk kasus penggunaan investigasi dan analitik.

Untuk mengaktifkan integrasi ini, Anda harus mengaktifkan kedua layanan dan menambahkan Security Hub CSPM sebagai sumber di konsol Security Lake, Security Lake API, atau AWS CLI. Setelah Anda menyelesaikan langkah-langkah ini, Security Hub CSPM mulai mengirimkan semua temuan ke Security Lake.

Security Lake secara otomatis menormalkan temuan CSPM Security Hub dan mengubahnya menjadi skema open-source standar yang disebut Open Cybersecurity Schema Framework (OCSF). Di Security Lake, Anda dapat menambahkan satu atau lebih pelanggan untuk mengkonsumsi temuan CSPM Security Hub.

Untuk informasi selengkapnya tentang integrasi ini, termasuk petunjuk tentang menambahkan CSPM Security Hub sebagai sumber dan membuat pelanggan, lihat [Integrasi dengan AWS Security Hub Cloud Security Posture Management \(CSPM\) di Panduan Pengguna](#) Amazon Security Lake.

AWS Systems Manager Explorer dan OpsCenter (Menerima dan memperbarui temuan)

AWS Systems Manager Jelajahi dan OpsCenter terima temuan dari Security Hub CSPM, dan perbarui temuan tersebut di Security Hub CSPM.

Explorer memberi Anda dasbor yang dapat disesuaikan, memberikan wawasan dan analisis utama tentang kesehatan operasional dan kinerja lingkungan Anda. AWS

OpsCenter memberi Anda lokasi pusat untuk melihat, menyelidiki, dan menyelesaikan item pekerjaan operasional.

Untuk informasi selengkapnya tentang Explorer dan OpsCenter, lihat [Manajemen operasi](#) di Panduan AWS Systems Manager Pengguna.

AWS Trusted Advisor (Menerima temuan)

Trusted Advisor mengacu pada praktik terbaik yang dipelajari dari melayani ratusan ribu AWS pelanggan. Trusted Advisor memeriksa AWS lingkungan Anda, dan kemudian membuat rekomendasi

ketika ada peluang untuk menghemat uang, meningkatkan ketersediaan dan kinerja sistem, atau membantu menutup kesenjangan keamanan.

Ketika Anda mengaktifkan keduanya Trusted Advisor dan Security Hub CSPM, integrasi diperbarui secara otomatis.

Security Hub CSPM mengirimkan hasil pemeriksaan Praktik Terbaik Keamanan AWS Dasar ke Trusted Advisor

Untuk informasi selengkapnya tentang integrasi CSPM Security Hub Trusted Advisor, lihat [Melihat kontrol AWS Security Hub Cloud Security Posture Management \(CSPM\) di Panduan Pengguna AWS Trusted Advisor](#) Support AWS .

Integrasi produk pihak ketiga dengan Security Hub CSPM

AWS Security Hub Cloud Security Posture Management (CSPM) terintegrasi dengan beberapa produk mitra pihak ketiga. Integrasi dapat melakukan satu atau lebih tindakan berikut:

- Kirim temuan yang dihasilkannya ke Security Hub CSPM
- Menerima temuan dari Security Hub CSPM
- Perbarui temuan di Security Hub CSPM

Integrasi yang mengirimkan temuan ke Security Hub CSPM memiliki Amazon Resource Name (ARN).

Integrasi mungkin tidak tersedia di semua Wilayah AWS. Jika integrasi tidak didukung di Wilayah tempat Anda masuk saat ini di konsol CSPM Security Hub, integrasi tersebut tidak akan muncul di halaman Integrasi konsol. Untuk daftar integrasi yang tersedia di Wilayah Tiongkok dan AWS GovCloud (US) Regions, lihat. [Ketersediaan integrasi menurut Wilayah](#)

<Jika Anda memiliki solusi keamanan dan tertarik untuk menjadi mitra CSPM Security Hub. Untuk informasi selengkapnya, lihat Panduan [Integrasi Mitra Manajemen Postur Keamanan Cloud Security Hub \(CSPM\)](#) Security Hub.AWS

Ikhtisar integrasi pihak ketiga dengan Security Hub CSPM

Berikut ikhtisar integrasi pihak ketiga yang mengirimkan temuan ke Security Hub CSPM atau menerima temuan dari Security Hub CSPM:

Integrasi	Arahan	ARN (jika ada)
3CORESec – 3CORESec NTA	Mengirim temuan	arn:aws:securityhub: <REGION> ::product/3coresec/3coresec
Alert Logic – SIEMless Threat Management	Mengirim temuan	arn:aws:securityhub: <REGION> :733251395267:product/alertlogic/althreatmanagement
Aqua Security – Aqua Cloud Native Security Platform	Mengirim temuan	arn:aws:securityhub: <REGION> ::product/aquasecurity/aquasecurity
Aqua Security – Kube-bench	Mengirim temuan	arn:aws:securityhub: <REGION> ::product/aqua-security/kube-bench
Armor – Armor Anywhere	Mengirim temuan	arn:aws:securityhub: <REGION> :679703615338:product/armordefense/armoranywhere
AttackIQ – AttackIQ	Mengirim temuan	arn:aws:securityhub: <REGION> ::product/attackiq/attackiq-platform
Barracuda Networks – Cloud Security Guardian	Mengirim temuan	arn:aws:securityhub: <REGION> :151784055945:product/barracuda

Integrasi	Arahan	ARN (jika ada)
		cuda/cloudsecurityguardian
BigID – BigID Enterprise	Mengirim temuan	arn:aws:securityhub: <REGION>::product/bigid/bigid-enterprise
Blue Hexagon – Blue Hexagon forAWS	Mengirim temuan	arn:aws:securityhub: <REGION>::product/blue-hexagon/blue-hexagon-for-aws
Check Point – CloudGuard IaaS	Mengirim temuan	arn:aws:securityhub: <REGION>:758245563457:product/checkpoint/cloudguard-iaas
Check Point – CloudGuard Posture Management	Mengirim temuan	arn:aws:securityhub: <REGION>:634729597623:product/checkpoint/dome9-arc
Claroty – xDome	Mengirim temuan	arn:aws:securityhub: <REGION>::product/claroty/xdome
Cloud Storage Security—Antivirus for Amazon S3	Mengirim temuan	arn:aws:securityhub: <REGION>::product/cloud-storage-security/antivirus-for-amazon-s3

Integrasi	Arahan	ARN (jika ada)
Contrast Security	Mengirim temuan	arn:aws:securityhub: <REGION>::product/contrast-security/security-assess
CrowdStrike – CrowdStrike Falcon	Mengirim temuan	arn:aws:securityhub: <REGION>:517716713836:product/crowdstrike/crowdstrike-falcon
CyberArk – Privileged Threat Analytics	Mengirim temuan	arn:aws:securityhub: <REGION>:749430749651:product/cyberark/cyberark-pta
Data Theorem – Data Theorem	Mengirim temuan	arn:aws:securityhub: <REGION>::product/data-theorem/api-cloud-web-secure
Drata	Mengirim temuan	arn:aws:securityhub: <REGION>::product/drata/drata-integration
Forcepoint – Forcepoint CASB	Mengirim temuan	arn:aws:securityhub: <REGION>:365761988620:product/forcepoint/forcepoint-casb

Integrasi	Arahan	ARN (jika ada)
Forcepoint – Forcepoint Cloud Security Gateway	Mengirim temuan	arn:aws:securityhub: <REGION>::product/forcepoint/forcepoint-cloud-security-gateway
Forcepoint – Forcepoint DLP	Mengirim temuan	arn:aws:securityhub: <REGION>:365761988620:product/forcepoint/forcepoint-dlp
Forcepoint – Forcepoint NGFW	Mengirim temuan	arn:aws:securityhub: <REGION>:365761988620:product/forcepoint/forcepoint-ngfw
Fugue – Fugue	Mengirim temuan	arn:aws:securityhub: <REGION>::product/fugue/fugue
Guardicore – Centra 4.0	Mengirim temuan	arn:aws:securityhub: <REGION>::product/guardicore/guardicore
HackerOne – Vulnerability Intelligence	Mengirim temuan	arn:aws:securityhub: <REGION>::product/hackerone/vulnerability-intelligence
JFrog – Xray	Mengirim temuan	arn:aws:securityhub: <REGION>::product/jfrog/jfrog-xray

Integrasi	Arahan	ARN (jika ada)
Juniper Networks – vSRX Next Generation Firewall	Mengirim temuan	arn:aws:securityhub: <REGION>::product/juniper-networks/vsrx-next-generation-firewall
k9 Security – Access Analyzer	Mengirim temuan	arn:aws:securityhub: <REGION>::product/k9-security/access-analyzer
Lacework – Lacework	Mengirim temuan	arn:aws:securityhub: <REGION>::product/lacework/lacework
McAfee – MVISION Cloud Native Application Protection Platform (CNAPP)	Mengirim temuan	arn:aws:securityhub: <REGION>::product/mcafee-skyhigh/mcafee-mvision-cloud-aws
NETSCOUT – NETSCOUT Cyber Investigator	Mengirim temuan	arn:aws:securityhub:us-east-1::product/netscout/netscout-cyber-investigator
Palo Alto Networks – Prisma Cloud Compute	Mengirim temuan	arn:aws:securityhub: <REGION>:496947949261:product/twistlock/twistlock-enterprise

Integrasi	Arahan	ARN (jika ada)
Palo Alto Networks – Prisma Cloud Enterprise	Mengirim temuan	arn:aws:securityhub: <REGION>:188619942792:product/paloaltonetworks/redlock
Plerion – Cloud Security Platform	Mengirim temuan	arn:aws:securityhub: <REGION>::product/plerion/cloud-security-platform
Prowler – Prowler	Mengirim temuan	arn:aws:securityhub: <REGION>::product/prowler/prowler
Qualys – Vulnerability Management	Mengirim temuan	arn:aws:securityhub: <REGION>:805950163170:product/qualys/qualys-vm
Rapid7 – InsightVM	Mengirim temuan	arn:aws:securityhub: <REGION>:336818582268:product/rapid7/insightvm
SecureCloudDB – SecureCloudDB	Mengirim temuan	arn:aws:securityhub: <REGION>::product/secureclouddb/secureclouddb
SentinelOne – SentinelOne	Mengirim temuan	arn:aws:securityhub: <REGION>::product/sentinelone/endpoint-protection

Integrasi	Arahan	ARN (jika ada)
Snyk	Mengirim temuan	arn:aws:securityhub: <region>::product/snyk/snyk
Sonrai Security – Sonrai Dig	Mengirim temuan	arn:aws:securityhub: <REGION>::product/sonrai-security/sonrai-dig
Sophos – Server Protection	Mengirim temuan	arn:aws:securityhub: <REGION>:062897671886:product/sophos/sophos-server-protection
StackRox – StackRox Kubernetes Security	Mengirim temuan	arn:aws:securityhub: <REGION>::product/stackrox/kubernetes-security
Sumo Logic – Machine Data Analytics	Mengirim temuan	arn:aws:securityhub: <REGION>:956882708938:product/sumologicinc/sumologic-mda
Symantec – Cloud Workload Protection	Mengirim temuan	arn:aws:securityhub: <REGION>:754237914691:product/symantec-corp/symantec-cwp
Tenable – Tenable.io	Mengirim temuan	arn:aws:securityhub: <REGION>:422820575223:product/tenable/tenable-io

Integrasi	Arahan	ARN (jika ada)
Trend Micro – Cloud One	Mengirim temuan	arn:aws:securityhub:<REGION>::product/trend-micro/cloud-one
Vectra – Cognito Detect	Mengirim temuan	arn:aws:securityhub:<REGION>:978576646331:product/vectra-ai/cognito-detect
Wiz	Mengirim temuan	arn:aws:securityhub:<REGION>::product/wiz-security/wiz-security
Atlassian - Jira Service Management	Menerima dan memperbarui temuan	Tidak berlaku
Atlassian - Jira Service Management Cloud	Menerima dan memperbarui temuan	Tidak berlaku
Atlassian – Opsgenie	Menerima temuan	Tidak berlaku
Fortinet – FortiCNP	Menerima temuan	Tidak berlaku
IBM – QRadar	Menerima temuan	Tidak berlaku
Logz.io Cloud SIEM	Menerima temuan	Tidak berlaku
MetricStream	Menerima temuan	Tidak berlaku
MicroFocus – MicroFocus Arcsight	Menerima temuan	Tidak berlaku
New Relic Vulnerability Management	Menerima temuan	Tidak berlaku
PagerDuty – PagerDuty	Menerima temuan	Tidak berlaku

Integrasi	Arahan	ARN (jika ada)
Palo Alto Networks – Cortex XSOAR	Menerima temuan	Tidak berlaku
Palo Alto Networks – VM-Series	Menerima temuan	Tidak berlaku
Rackspace Technology – Cloud Native Security	Menerima temuan	Tidak berlaku
Rapid7 – InsightConnect	Menerima temuan	Tidak berlaku
RSA – RSA Archer	Menerima temuan	Tidak berlaku
ServiceNow – ITSM	Menerima dan memperbarui temuan	Tidak berlaku
Slack – Slack	Menerima temuan	Tidak berlaku
Splunk – Splunk Enterprise	Menerima temuan	Tidak berlaku
Splunk – Splunk Phantom	Menerima temuan	Tidak berlaku
ThreatModeler	Menerima temuan	Tidak berlaku
Trellix – Trellix Helix	Menerima temuan	Tidak berlaku
Caveonix – Caveonix Cloud	Mengirim dan menerima temuan	arn:aws:securityhub: <REGION>::product/caveonix/caveonix-cloud
Cloud Custodian – Cloud Custodian	Mengirim dan menerima temuan	arn:aws:securityhub: <REGION>::product/cloud-custodian/cloud-custodian

Integrasi	Arahan	ARN (jika ada)
DisruptOps, Inc. – DisruptOPS	Mengirim dan menerima temuan	arn:aws:securityhub:<REGION>::product/disruptops-inc/disruptops
Kion	Mengirim dan menerima temuan	arn:aws:securityhub:<REGION>::product/cloudtamerio/cloudtamerio
Turbot – Turbot	Mengirim dan menerima temuan	arn:aws:securityhub:<REGION>:453761072151:product/turbot/turbot

Integrasi pihak ketiga yang mengirimkan temuan ke Security Hub CSPM

Integrasi produk mitra pihak ketiga berikut mengirimkan temuan ke Security Hub CSPM. Security Hub CSPM mengubah temuan menjadi [AWS Security Finding Format](#).

3CORESec – 3CORESec NTA

Jenis integrasi: Kirim

Produk ARN: arn:aws:securityhub:<REGION>::product/3coresec/3coresec

3CORESec menyediakan layanan deteksi terkelola untuk lokal dan AWS sistem. Integrasi mereka dengan Security Hub CSPM memungkinkan visibilitas ke dalam ancaman seperti malware, eskalasi hak istimewa, pergerakan lateral, dan segmentasi jaringan yang tidak tepat.

[Tautan produk](#)

[Dokumentasi mitra](#)

Alert Logic – SIEMless Threat Management

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>:733251395267:product/alertlogic/albthreatmanagement`

Dapatkan tingkat cakupan yang tepat: kerentanan dan visibilitas aset, deteksi ancaman dan manajemen insiden AWS WAF, dan opsi analisis SOC yang ditetapkan.

[Tautan produk](#)

[Dokumentasi mitra](#)

Aqua Security – Aqua Cloud Native Security Platform

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>::product/aquasecurity/aquasecurity`

Aqua Cloud Native Security Platform (CSP) menyediakan keamanan siklus hidup penuh untuk aplikasi berbasis container dan tanpa server, mulai dari pipeline hingga lingkungan produksi runtime. CI/CD

[Tautan produk](#)

[Dokumentasi mitra](#)

Aqua Security – Kube-bench

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>::product/aqua-security/kube-bench`

Kube-bench adalah alat open-source yang menjalankan Center for Internet Security (CIS) Kubernetes Benchmark terhadap lingkungan Anda.

[Tautan produk](#)

[Dokumentasi mitra](#)

Armor – Armor Anywhere

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>:679703615338:product/armordefense/armoranywhere`

Armor Anywherememberikan keamanan dan kepatuhan terkelola untuk AWS.

[Tautan produk](#)

[Dokumentasi mitra](#)

AttackIQ – AttackIQ

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>::product/attackiq/attackiq-platform`

AttackIQ Platformmengemulasi perilaku permusuhan nyata yang selaras dengan MITRE ATT&CK Framework untuk membantu memvalidasi dan meningkatkan postur keamanan Anda secara keseluruhan.

[Tautan produk](#)

[Dokumentasi mitra](#)

Barracuda Networks – Cloud Security Guardian

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>:151784055945:product/barracuda/cloudsecurityguardian`

Barracuda Cloud Security Sentrymembantu organisasi tetap aman saat membangun aplikasi di, dan memindahkan beban kerja ke, cloud publik.

[AWS Tautan Marketplace](#)

[Tautan produk](#)

BigID – BigID Enterprise

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>::product/bigid/bigid-enterprise`

BigID Enterprise Privacy Management PlatformIni membantu perusahaan mengelola dan melindungi data sensitif (PII) di semua sistem mereka.

[Tautan produk](#)[Dokumentasi mitra](#)

Blue Hexagon— Blue Hexagon untuk AWS

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>::product/blue-hexagon/blue-hexagon-for-aws`

Blue Hexagon adalah platform deteksi ancaman waktu nyata. Ini menggunakan prinsip pembelajaran mendalam untuk mendeteksi ancaman yang diketahui dan tidak diketahui, termasuk malware dan anomali jaringan.

[AWS Tautan Marketplace](#)[Dokumentasi mitra](#)

Check Point – CloudGuard IaaS

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>:758245563457:product/checkpoint/cloudguard-iaas`

Check Point CloudGuard dengan mudah memperluas keamanan pencegahan ancaman yang komprehensif untuk AWS sekaligus melindungi aset di cloud.

[Tautan produk](#)[Dokumentasi mitra](#)

Check Point – CloudGuard Posture Management

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>:634729597623:product/checkpoint/dome9-arc`

Platform SaaS yang memberikan keamanan jaringan cloud yang dapat diverifikasi, perlindungan IAM tingkat lanjut, dan kepatuhan dan tata kelola yang komprehensif.

[Tautan produk](#)[Dokumentasi mitra](#)

Claroty – xDome

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>::product/claroty/xdome`

Claroty xDomemembantu organisasi mengamankan sistem siber-fisik mereka di seluruh Extended Internet of Things (XIoT) dalam lingkungan industri (OT), perawatan kesehatan (IoMT), dan perusahaan (IoT).

[Tautan produk](#)[Dokumentasi mitra](#)

Cloud Storage Security— Antivirus for Amazon S3

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>::product/cloud-storage-security/antivirus-for-amazon-s3`

Cloud Storage Securitymenyediakan pemindaian anti-malware dan antivirus asli cloud untuk objek Amazon S3.

Antivirus for Amazon S3 menawarkan pemindaian objek dan file secara real time dan terjadwal di Amazon S3 untuk malware dan ancaman. Ini memberikan visibilitas dan remediasi untuk masalah dan file yang terinfeksi.

[Tautan produk](#)[Dokumentasi mitra](#)

Contrast Security – Contrast Assess

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>::product/contrast-security/security-assess`

Contrast Security Contrast Assess adalah alat IAST yang menawarkan deteksi kerentanan waktu nyata di aplikasi web, APIs, dan layanan mikro. Contrast Assesster integrasi dengan Security Hub CSPM untuk membantu memberikan visibilitas dan respons terpusat untuk semua beban kerja Anda.

[Tautan produk](#)

[Dokumentasi mitra](#)

CrowdStrike – CrowdStrike Falcon

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>:517716713836:product/crowdstrike/crowdstrike-falcon`

Sensor CrowdStrike Falcon tunggal yang ringan menyatukan antivirus generasi berikutnya, deteksi dan respons titik akhir, dan perburuan terkelola 24/7 melalui cloud.

[AWS Tautan Marketplace](#)

[Dokumentasi mitra](#)

CyberArk – Privileged Threat Analytics

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>:749430749651:product/cyberark/cyberark-pta`

Privileged Threat Analytics mengumpulkan, mendeteksi, memperingatkan, dan menanggapi aktivitas berisiko tinggi dan perilaku akun istimewa untuk menahan serangan yang sedang berlangsung.

[Tautan produk](#)

[Dokumentasi mitra](#)

Data Theorem – Data Theorem

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>::product/data-theorem/api-cloud-web-secure`

Data Theoremterus memindai aplikasi web APIs, dan sumber daya cloud untuk mencari kelemahan keamanan dan kesenjangan privasi data untuk mencegah pelanggaran AppSec data.

[Tautan produk](#)

[Dokumentasi mitra](#)

Drata

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>::product/drata/drata-integration`

Drataadalah platform otomatisasi kepatuhan yang membantu Anda mencapai dan mempertahankan kepatuhan dengan berbagai kerangka kerja, seperti, ISO SOC2, dan GDPR. Integrasi antara Drata dan Security Hub CSPM membantu Anda memusatkan temuan keamanan Anda di satu lokasi.

[AWS Tautan Marketplace](#)

[Dokumentasi mitra](#)

Forcepoint – Forcepoint CASB

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>:365761988620:product/forcepoint/forcepoint-casb`

Forcepoint CASBmemungkinkan Anda menemukan penggunaan aplikasi cloud, menganalisis risiko, dan menerapkan kontrol yang sesuai untuk SaaS dan aplikasi khusus.

[Tautan produk](#)

[Dokumentasi mitra](#)

Forcepoint – Forcepoint Cloud Security Gateway

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>::product/forcepoint/forcepoint-cloud-security-gateway`

Forcepoint Cloud Security Gateway adalah layanan keamanan cloud konvergen yang menyediakan visibilitas, kontrol, dan perlindungan ancaman bagi pengguna dan data, di mana pun mereka berada.

[Tautan produk](#)

[Dokumentasi mitra](#)

Forcepoint – Forcepoint DLP

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>:365761988620:product/forcepoint/forcepoint-dlp`

Forcepoint DLP mengatasi risiko yang berpusat pada manusia dengan visibilitas dan kontrol di mana pun orang-orang Anda bekerja dan di mana pun data Anda berada.

[Tautan produk](#)

[Dokumentasi mitra](#)

Forcepoint – Forcepoint NGFW

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>:365761988620:product/forcepoint/forcepoint-ngfw`

Forcepoint NGFW memungkinkan Anda menghubungkan AWS lingkungan Anda ke jaringan perusahaan Anda dengan skalabilitas, perlindungan, dan wawasan yang diperlukan untuk mengelola jaringan Anda dan menanggapi ancaman.

[Tautan produk](#)

[Dokumentasi mitra](#)

Fugue – Fugue

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>::product/fugue/fugue`

Fugue adalah platform cloud-native tanpa agen dan dapat diskalakan yang mengotomatiskan validasi berkelanjutan infrastructure-as-code dan lingkungan runtime cloud menggunakan kebijakan yang sama.

[Tautan produk](#)

[Dokumentasi mitra](#)

Guardicore – Centra 4.0

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>::product/guardicore/guardicore`

Guardicore Centra menyediakan visualisasi aliran, segmentasi mikro, dan deteksi pelanggaran untuk beban kerja di pusat data dan cloud modern.

[Tautan produk](#)

[Dokumentasi mitra](#)

HackerOne – Vulnerability Intelligence

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>::product/hackerone/vulnerability-intelligence`

HackerOne Platform ini bermitra dengan komunitas peretas global untuk mengungkap masalah keamanan yang paling relevan. Vulnerability Intelligence memungkinkan organisasi Anda melampaui pemindaian otomatis. Ini berbagi kerentanan yang telah divalidasi oleh peretas HackerOne etis dan memberikan langkah-langkah untuk mereproduksi.

[AWS tautan pasar](#)

[Dokumentasi mitra](#)

JFrog – Xray

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>::product/jfrog/jfrog-xray`

JFrog Xray adalah alat Analisis Komposisi Perangkat Lunak keamanan aplikasi universal (SCA) yang terus memindai binari untuk kepatuhan lisensi dan kerentanan keamanan sehingga Anda dapat menjalankan rantai pasokan perangkat lunak yang aman.

[AWS Tautan Marketplace](#)

[Dokumentasi mitra](#)

Juniper Networks – vSRX Next Generation Firewall

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>::product/juniper-networks/vsrx-next-generation-firewall`

Juniper Networks'VsRx Virtual Next Generation Firewall menghadirkan firewall virtual berbasis cloud lengkap dengan keamanan canggih, SD-WAN yang aman, jaringan yang kuat, dan otomatisasi bawaan.

[AWS Tautan Marketplace](#)

[Dokumentasi mitra](#)

[Tautan produk](#)

k9 Security – Access Analyzer

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>::product/k9-security/access-analyzer`

k9 Security memberi tahu Anda ketika perubahan akses penting terjadi di AWS Identity and Access Management akun Anda. Dengan k9 Security, Anda dapat memahami akses yang dimiliki pengguna dan peran IAM terhadap data kritis Layanan AWS dan data Anda.

k9 Security dibangun untuk pengiriman berkelanjutan, memungkinkan Anda untuk mengoperasikan IAM dengan audit akses yang dapat ditindaklanjuti dan otomatisasi kebijakan sederhana untuk dan Terraform. AWS CDK

[Tautan produk](#)

[Dokumentasi mitra](#)

Lacework – Lacework

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>::product/lacework/lacework`

Lacework adalah platform keamanan berbasis data untuk cloud. Platform Keamanan Cloud Lacework mengotomatiskan keamanan cloud dalam skala besar sehingga Anda dapat berinovasi dengan kecepatan dan keamanan.

[Tautan produk](#)[Dokumentasi mitra](#)

McAfee – MVISION Cloud Native Application Protection Platform (CNAPP)

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>::product/mcafee-skyhigh/mcafee-mvision-cloud-aws`

McAfee MVISION Cloud Native Application Protection Platform (CNAPP) menawarkan Cloud Security Posture Management (CSPM) dan Cloud Workload Protection Platform (CWPP) untuk lingkungan Anda. AWS

[Tautan produk](#)[Dokumentasi mitra](#)

NETSCOUT – NETSCOUT Cyber Investigator

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>::product/netscout/netscout-cyber-investigator`

NETSCOUT Cyber Investigator adalah ancaman jaringan di seluruh perusahaan, investigasi risiko, dan platform analisis forensik yang membantu mengurangi dampak ancaman dunia maya pada bisnis.

[Tautan produk](#)

[Dokumentasi mitra](#)

Palo Alto Networks – Prisma Cloud Compute

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>:496947949261:product/twistlock/twistlock-enterprise`

Prisma Cloud Compute adalah platform keamanan siber asli cloud yang melindungi VMs, wadah, dan platform tanpa server.

[Tautan produk](#)[Dokumentasi mitra](#)

Palo Alto Networks – Prisma Cloud Enterprise

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>:188619942792:product/paloaltonetworks/redlock`

Melindungi AWS penyebaran Anda dengan analitik keamanan cloud, deteksi ancaman tingkat lanjut, dan pemantauan kepatuhan.

[Tautan produk](#)[Dokumentasi mitra](#)

Plerion – Cloud Security Platform

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>::product/plerion/cloud-security-platform`

Plerion adalah Platform Keamanan Cloud dengan pendekatan unik yang dipimpin oleh ancaman dan berbasis risiko yang menawarkan tindakan pencegahan, detektif, dan korektif di seluruh beban kerja Anda. Integrasi antara Plerion dan Security Hub CSPM memungkinkan pelanggan untuk memusatkan dan bertindak atas temuan keamanan mereka di satu tempat.

[AWS Tautan Marketplace](#)

[Dokumentasi mitra](#)

Prowler – Prowler

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>::product/prowler/prowler`

Prowler adalah alat keamanan open source untuk melakukan AWS pemeriksaan terkait praktik terbaik keamanan, penguatan, dan pemantauan berkelanjutan.

[Tautan produk](#)

[Dokumentasi mitra](#)

Qualys – Vulnerability Management

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>:805950163170:product/qualys/qualys-vm`

Qualys Vulnerability Management (VM) terus memindai dan mengidentifikasi kerentanan, melindungi aset Anda.

[Tautan produk](#)

[Dokumentasi mitra](#)

Rapid7 – InsightVM

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>:336818582268:product/rapid7/insightvm`

Rapid7 InsightVM menyediakan manajemen kerentanan untuk lingkungan modern, memungkinkan Anda menemukan, memprioritaskan, dan memulihkan kerentanan secara efisien.

[Tautan produk](#)

[Dokumentasi mitra](#)

SecureCloudDB – SecureCloudDB

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>::product/secureclouddb/secureclouddb`

SecureCloudDB adalah alat keamanan database asli cloud yang menyediakan visibilitas komprehensif postur dan aktivitas keamanan internal dan eksternal. Ini menandai pelanggaran keamanan dan memberikan perbaikan pada kerentanan database yang dapat dieksploitasi.

[Tautan produk](#)[Dokumentasi mitra](#)

SentinelOne – SentinelOne

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>::product/sentinelone/endpoint-protection`

SentinelOne adalah platform deteksi dan respons tambahan (XDR) otonom yang mencakup pencegahan, deteksi, respons, dan perburuan bertenaga AI di seluruh titik akhir, wadah, beban kerja cloud, dan perangkat IoT.

[AWS Tautan Marketplace](#)[Tautan produk](#)

Snyk

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>::product/snyk/snyk`

Snyk menyediakan platform keamanan yang memindai komponen aplikasi untuk risiko keamanan dalam beban kerja yang berjalan. AWS Risiko ini dikirim ke Security Hub CSPM sebagai temuan, membantu pengembang dan tim keamanan memvisualisasikan dan memprioritaskannya bersama dengan sisa temuan keamanan mereka. AWS

[AWS Tautan Marketplace](#)[Dokumentasi mitra](#)

Sonrai Security – Sonrai Dig

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>::product/sonrai-security/sonrai-dig`

Sonrai Dig memantau dan memulihkan kesalahan konfigurasi cloud dan pelanggaran kebijakan, sehingga Anda dapat meningkatkan keamanan dan postur kepatuhan Anda.

[Tautan produk](#)[Dokumentasi mitra](#)

Sophos – Server Protection

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>:062897671886:product/sophos/sophos-server-protection`

Sophos Server Protection membela aplikasi dan data penting di inti organisasi Anda, menggunakan defense-in-depth teknik yang komprehensif.

[Tautan produk](#)

StackRox – StackRox Kubernetes Security

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>::product/stackrox/kubernetes-security`

StackRox membantu perusahaan mengamankan container dan penerapan Kubernetes mereka dalam skala besar dengan menegakkan kebijakan kepatuhan dan keamanan mereka di seluruh siklus hidup container — build, deploy, dan run.

[Tautan produk](#)[Dokumentasi mitra](#)

Sumo Logic – Machine Data Analytics

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>:956882708938:product/sumologicinc/sumologic-mda`

Sumo Logic adalah platform analisis data mesin yang aman yang memungkinkan tim operasi pengembangan dan keamanan untuk membangun, menjalankan, dan mengamankan AWS aplikasi mereka.

[Tautan produk](#)

[Dokumentasi mitra](#)

Symantec – Cloud Workload Protection

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>:754237914691:product/symantec-corp/symantec-cwp`

Cloud Workload Protection memberikan perlindungan lengkap untuk EC2 instans Amazon Anda dengan antimalware, pencegahan intrusi, dan pemantauan integritas file.

[Tautan produk](#)

[Dokumentasi mitra](#)

Tenable – Tenable.io

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>:422820575223:product/tenable/tenable-io`

Mengidentifikasi, menyelidiki, dan memprioritaskan kerentanan secara akurat. Dikelola di cloud.

[Tautan produk](#)

[Dokumentasi mitra](#)

Trend Micro – Cloud One

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>::product/trend-micro/cloud-one`

Trend Micro Cloud One memberikan informasi keamanan yang tepat kepada tim pada waktu dan tempat yang tepat. Integrasi ini mengirimkan temuan keamanan ke Security Hub CSPM secara real time, meningkatkan visibilitas ke AWS sumber daya dan detail Trend Micro Cloud One acara Anda di Security Hub CSPM.

[AWS Tautan Marketplace](#)

[Dokumentasi mitra](#)

Vectra – Cognito Detect

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>:978576646331:product/vectra-ai/cognito-detect`

Vectra mengubah keamanan siber dengan menerapkan AI canggih untuk mendeteksi dan merespons penyerang siber tersembunyi sebelum mereka dapat mencuri atau menyebabkan kerusakan.

[AWS Tautan Marketplace](#)

[Dokumentasi mitra](#)

Wiz – Wiz Security

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>::product/wiz-security/wiz-security`

Wiz terus menganalisis konfigurasi, kerentanan, jaringan, pengaturan IAM, rahasia, dan lainnya di seluruh Anda, pengguna Akun AWS, dan beban kerja untuk menemukan masalah penting yang mewakili risiko aktual. Integrasikan Wiz dengan Security Hub CSPM untuk memvisualisasikan dan menanggapi masalah yang dideteksi Wiz dari konsol CSPM Security Hub.

[AWS Tautan Marketplace](#)

[Dokumentasi mitra](#)

Integrasi pihak ketiga yang menerima temuan dari Security Hub CSPM

Integrasi produk mitra pihak ketiga berikut menerima temuan dari Security Hub CSPM. Jika dicatat, produk mungkin juga memperbarui temuan. Dalam hal ini, pembaruan yang Anda buat untuk temuan dalam produk mitra juga tercermin dalam Security Hub CSPM.

Atlassian - Jira Service Management

Jenis integrasi: Terima dan perbarui

The AWS Service Management Connector for Jira mengirimkan temuan dari Security Hub CSPM ke Jira. Jira masalah dibuat berdasarkan temuan. Ketika Jira masalah diperbarui, temuan terkait diperbarui di Security Hub CSPM.

Integrasi hanya mendukung Jira Server dan Jira Data Center.

Untuk gambaran umum tentang integrasi dan cara kerjanya, tonton video [AWS Security Hub Cloud Security Posture Management \(CSPM\) — Integrasi dua arah](#) dengan Atlassian Jira Service Management.

[Tautan produk](#)

[Dokumentasi mitra](#)

Atlassian - Jira Service Management Cloud

Jenis integrasi: Terima dan perbarui

Jira Service Management Cloud adalah komponen cloud dari Jira Service Management.

The AWS Service Management Connector for Jira mengirimkan temuan dari Security Hub CSPM ke Jira. Temuan tersebut memicu terciptanya masalah di Jira Service Management Cloud. Saat Anda memperbarui masalah tersebut di Jira Service Management Cloud, temuan terkait juga diperbarui di Security Hub CSPM.

[Tautan produk](#)

[Dokumentasi mitra](#)

Atlassian – Opsgenie

Jenis integrasi: Terima

Opsgenie adalah solusi manajemen insiden modern untuk mengoperasikan layanan selalu aktif, memberdayakan tim pengembangan dan operasi untuk merencanakan gangguan layanan dan tetap memegang kendali selama insiden.

Mengintegrasikan dengan Security Hub CSPM memastikan bahwa insiden terkait keamanan kritis misi diarahkan ke tim yang sesuai untuk penyelesaian segera.

[Tautan produk](#)

[Dokumentasi mitra](#)

Fortinet – FortiCNP

Jenis integrasi: Terima

FortiCNP adalah produk Cloud Native Protection yang menggabungkan temuan keamanan ke dalam wawasan yang dapat ditindaklanjuti dan memprioritaskan wawasan keamanan berdasarkan skor risiko untuk mengurangi kelelahan waspada dan mempercepat remediasi.

[AWS Tautan Marketplace](#)

[Dokumentasi mitra](#)

IBM – QRadar

Jenis integrasi: Terima

IBM QRadar SIEM memberi tim keamanan kemampuan untuk mendeteksi, memprioritaskan, menyelidiki, dan merespons ancaman dengan cepat dan akurat.

[Tautan produk](#)

[Dokumentasi mitra](#)

Logz.io Cloud SIEM

Jenis integrasi: Terima

Logz.io adalah penyedia Cloud SIEM yang menyediakan korelasi lanjutan data log dan peristiwa untuk membantu tim keamanan mendeteksi, menganalisis, dan menanggapi ancaman keamanan secara real time.

[Tautan produk](#)

[Dokumentasi mitra](#)

MetricStream – CyberGRC

Jenis integrasi: Terima

MetricStream CyberGRC membantu Anda mengelola, mengukur, dan mengurangi risiko keamanan siber. Dengan menerima temuan CSPM Security Hub, CyberGRC memberikan lebih banyak visibilitas terhadap risiko ini, sehingga Anda dapat memprioritaskan investasi keamanan siber dan mematuhi kebijakan TI.

[AWS Tautan Marketplace](#)[Tautan produk](#)

MicroFocus – MicroFocus Arcsight

Jenis integrasi: Terima

ArcSight mempercepat deteksi dan respons ancaman yang efektif secara real time, mengintegrasikan korelasi peristiwa dan analitik yang diawasi dan tanpa pengawasan dengan otomatisasi respons dan orkestrasi.

[Tautan produk](#)[Dokumentasi mitra](#)

New Relic Vulnerability Management

Jenis integrasi: Terima

New Relic Vulnerability Management menerima temuan keamanan dari Security Hub CSPM, sehingga Anda bisa mendapatkan tampilan keamanan terpusat di samping telemetri kinerja dalam konteks di seluruh tumpukan Anda.

[AWS Tautan Marketplace](#)[Dokumentasi mitra](#)

PagerDuty – PagerDuty

Jenis integrasi: Terima

Platform manajemen operasi PagerDuty digital memberdayakan tim untuk secara proaktif mengurangi masalah yang berdampak pelanggan dengan secara otomatis mengubah sinyal apa pun menjadi wawasan dan tindakan yang tepat.

AWS pengguna dapat menggunakan PagerDuty serangkaian AWS integrasi untuk menskalakan lingkungan mereka AWS dan hibrida dengan percaya diri.

Ketika digabungkan dengan peringatan keamanan gabungan dan terorganisir CSPM Security Hub, PagerDuty memungkinkan tim untuk mengotomatiskan proses respons ancaman mereka dan dengan cepat mengatur tindakan khusus untuk mencegah potensi masalah.

PagerDutypengguna yang melakukan proyek migrasi cloud dapat bergerak dengan cepat, sekaligus mengurangi dampak masalah yang terjadi di seluruh siklus hidup migrasi.

[Tautan produk](#)

[Dokumentasi mitra](#)

Palo Alto Networks – Cortex XSOAR

Jenis integrasi: Terima

Cortex XSOAR adalah platform Security Orchestration, Automation, and Response (SOAR) yang terintegrasi dengan seluruh tumpukan produk keamanan Anda untuk mempercepat respons insiden dan operasi keamanan.

[Tautan produk](#)

[Dokumentasi mitra](#)

Palo Alto Networks – VM-Series

Jenis integrasi: Terima

Palo Alto VM-Series Integrasi dengan Security Hub CSPM mengumpulkan intelijen ancaman dan mengirimkannya ke firewall VM-Series generasi berikutnya sebagai pembaruan kebijakan keamanan otomatis yang memblokir aktivitas alamat IP berbahaya.

[Tautan produk](#)

[Dokumentasi mitra](#)

Rackspace Technology – Cloud Native Security

Jenis integrasi: Terima

Rackspace Technology menyediakan layanan keamanan terkelola di atas produk AWS keamanan asli untuk pemantauan 24x7x365 oleh Rackspace SOC, analisis lanjutan, dan remediasi ancaman.

[Tautan produk](#)

Rapid7 – InsightConnect

Jenis integrasi: Terima

Rapid7 InsightConnect adalah solusi orkestrasi dan otomatisasi keamanan yang memungkinkan tim Anda mengoptimalkan operasi SOC dengan sedikit atau tanpa kode.

[Tautan produk](#)

[Dokumentasi mitra](#)

RSA – RSA Archer

Jenis integrasi: Terima

RSA Archer Manajemen Risiko TI dan Keamanan memungkinkan Anda untuk menentukan aset mana yang penting bagi bisnis Anda, menetapkan dan mengkomunikasikan kebijakan dan standar keamanan, mendeteksi dan menanggapi serangan, mengidentifikasi dan memulihkan kekurangan keamanan, dan menetapkan praktik terbaik manajemen risiko TI yang jelas.

[Tautan produk](#)

[Dokumentasi mitra](#)

ServiceNow – ITSM

Jenis integrasi: Terima dan perbarui

ServiceNow Integrasi dengan Security Hub CSPM memungkinkan temuan keamanan dari Security Hub CSPM untuk dilihat di dalamnya. ServiceNow ITSM Anda juga dapat mengonfigurasi ServiceNow untuk secara otomatis membuat insiden atau masalah saat menerima temuan dari Security Hub CSPM.

Setiap pembaruan untuk insiden dan masalah ini menghasilkan pembaruan temuan di Security Hub CSPM.

Untuk ikhtisar integrasi dan cara kerjanya, tonton video [AWS Security Hub Cloud Security Posture Management \(CSPM\) - Integrasi dua arah](#) dengan. ServiceNow ITSM

[Tautan produk](#)

[Dokumentasi mitra](#)

Slack – Slack

Jenis integrasi: Terima

Slack adalah lapisan tumpukan teknologi bisnis yang menyatukan orang, data, dan aplikasi. Ini adalah satu tempat di mana orang dapat bekerja sama secara efektif, menemukan informasi penting, dan mengakses ratusan ribu aplikasi dan layanan penting untuk melakukan pekerjaan terbaik mereka.

[Tautan produk](#)

[Dokumentasi mitra](#)

Splunk – Splunk Enterprise

Jenis integrasi: Terima

Splunk menggunakan Amazon CloudWatch Events sebagai konsumen temuan CSPM Security Hub. Kirim data Anda ke Splunk untuk analitik keamanan tingkat lanjut dan SIEM.

[Tautan produk](#)

[Dokumentasi mitra](#)

Splunk – Splunk Phantom

Jenis integrasi: Terima

Dengan Splunk Phantom aplikasi AWS Security Hub Cloud Security Posture Management (CSPM), temuan dikirim ke Phantom pengayaan konteks otomatis dengan informasi intelijen ancaman tambahan atau untuk melakukan tindakan respons otomatis.

[Tautan produk](#)

[Dokumentasi mitra](#)

ThreatModeler

Jenis integrasi: Terima

ThreatModeler adalah solusi pemodelan ancaman otomatis yang mengamankan dan meningkatkan skala perangkat lunak perusahaan dan siklus hidup pengembangan cloud.

[Tautan produk](#)[Dokumentasi mitra](#)

Trellix – Trellix Helix

Jenis integrasi: Terima

Trellix Helix adalah platform operasi keamanan yang dihosting cloud yang memungkinkan organisasi mengendalikan insiden apa pun dari peringatan untuk diperbaiki.

[Tautan produk](#)[Dokumentasi mitra](#)

Integrasi pihak ketiga yang mengirimkan temuan ke dan menerima temuan dari Security Hub CSPM

Integrasi produk mitra pihak ketiga berikut mengirimkan temuan ke dan menerima temuan dari Security Hub CSPM.

Caveonix – Caveonix Cloud

Jenis integrasi: Kirim dan terima

Produk ARN: `arn:aws:securityhub:<REGION>::product/caveonix/caveonix-cloud`

Platform yang Caveonix didukung AI mengotomatiskan visibilitas, penilaian, dan mitigasi di cloud hybrid, yang mencakup layanan cloud-native, dan container. VMs Terintegrasi dengan AWS Security Hub Cloud Security Posture Management (CSPM), Caveonix menggabungkan AWS data dan analitik lanjutan untuk wawasan tentang peringatan keamanan dan kepatuhan.

[AWS Tautan Marketplace](#)

[Dokumentasi mitra](#)

Cloud Custodian – Cloud Custodian

Jenis integrasi: Kirim dan terima

Produk ARN: `arn:aws:securityhub:<REGION>::product/cloud-custodian/cloud-custodian`

Cloud Custodian memungkinkan pengguna untuk dikelola dengan baik di cloud. YAMM DSL yang sederhana memungkinkan aturan yang mudah didefinisikan untuk memungkinkan infrastruktur cloud yang dikelola dengan baik yang aman dan dioptimalkan biaya.

[Tautan produk](#)[Dokumentasi mitra](#)

DisruptOps, Inc. – DisruptOPS

Jenis integrasi: Kirim dan terima

Produk ARN: `arn:aws:securityhub:<REGION>::product/disruptops-inc/disruptops`

Platform Operasi DisruptOps Keamanan membantu organisasi mempertahankan praktik keamanan terbaik di cloud Anda melalui penggunaan pagar pembatas otomatis.

[Tautan produk](#)[Dokumentasi mitra](#)

Kion

Jenis integrasi: Kirim dan terima

Produk ARN: `arn:aws:securityhub:<REGION>::product/cloudtamerio/cloudtamerio`

Kion(sebelumnya cloudtamer.io) adalah solusi tata kelola cloud lengkap untuk. AWSKionmemberikan visibilitas pemangku kepentingan ke dalam operasi cloud dan membantu pengguna cloud mengelola akun, mengontrol anggaran dan biaya, dan memastikan kepatuhan berkelanjutan.

[Tautan produk](#)[Dokumentasi mitra](#)

Turbot – Turbo

Jenis integrasi: Kirim dan terima

Produk ARN: `arn:aws:securityhub:<REGION>::product/turbot/turbot`

Turbot memastikan bahwa infrastruktur cloud Anda aman, sesuai, dapat diskalakan, dan dioptimalkan biaya.

[Tautan produk](#)

[Dokumentasi mitra](#)

Mengintegrasikan Security Hub CSPM dengan produk khusus

Selain temuan yang dihasilkan oleh AWS layanan terintegrasi dan produk pihak ketiga, AWS Security Hub Cloud Security Posture Management (CSPM) dapat mengkonsumsi temuan yang dihasilkan oleh produk keamanan khusus lainnya.

Anda dapat mengirimkan temuan ini ke Security Hub CSPM dengan menggunakan [BatchImportFindings](#) pengoperasian Security Hub CSPM API. Anda dapat menggunakan operasi yang sama untuk memperbarui temuan dari produk kustom yang telah Anda kirim ke Security Hub CSPM.

Saat menyiapkan integrasi kustom, gunakan [pedoman dan daftar periksa](#) yang disediakan di Panduan Integrasi Mitra CSPM Security Hub.

Persyaratan dan rekomendasi untuk integrasi produk khusus

Sebelum Anda berhasil menjalankan operasi [BatchImportFindings](#) API, Anda harus mengaktifkan Security Hub CSPM.

Anda juga harus memberikan rincian temuan untuk produk kustom menggunakan [the section called “Menemukan format: ASFF”](#). Tinjau persyaratan dan rekomendasi berikut untuk integrasi produk khusus:

Mengatur ARN produk

Saat Anda mengaktifkan Security Hub CSPM, produk default Amazon Resource Name (ARN) untuk Security Hub CSPM akan dibuat di akun Anda saat ini.

Produk ARN ini memiliki format sebagai berikut:

`arn:aws:securityhub:<region>:<account-id>:product/<account-id>/default`

Misalnya, `arn:aws:securityhub:us-west-2:123456789012:product/123456789012/default`.

Gunakan ARN produk ini sebagai nilai untuk [ProductArn](#) atribut saat menjalankan operasi API `BatchImportFindings`.

Menetapkan nama perusahaan dan produk

Anda dapat menggunakan `BatchImportFindings` untuk menetapkan nama perusahaan dan nama produk pilihan untuk integrasi kustom yang mengirimkan temuan ke Security Hub CSPM.

Nama yang Anda tentukan menggantikan nama perusahaan dan nama produk yang telah dikonfigurasi sebelumnya, masing-masing disebut nama pribadi dan nama default, dan muncul di konsol CSPM Security Hub dan JSON dari setiap temuan. Lihat [BatchImportFindings untuk menemukan penyedia](#).

Mengatur temuan IDs

Anda harus menyediakan, mengelola, dan meningkatkan temuan Anda sendiri IDs, menggunakan [Id](#) atribut.

Setiap temuan baru harus memiliki ID temuan unik. Jika produk kustom mengirimkan beberapa temuan dengan ID temuan yang sama, Security Hub CSPM hanya memproses temuan pertama.

Mengatur ID akun

Anda harus menentukan ID akun Anda sendiri, menggunakan [AwsAccountId](#) atribut.

Mengatur yang dibuat pada dan diperbarui pada tanggal

Anda harus menyediakan stempel waktu Anda sendiri untuk atribut [CreatedAt](#) dan [UpdatedAt](#).

Memperbarui temuan dari produk khusus

Selain mengirimkan temuan baru dari produk kustom, Anda juga dapat menggunakan operasi [BatchImportFindings](#) API untuk memperbarui temuan yang ada dari produk kustom.

Untuk memperbarui temuan yang ada, gunakan ID temuan yang ada (melalui [Id](#) atribut). Kirim ulang temuan lengkap dengan informasi yang sesuai yang diperbarui dalam permintaan, termasuk [UpdatedAt](#) stempel waktu yang dimodifikasi.

Contoh integrasi kustom

Anda dapat menggunakan contoh integrasi produk kustom berikut sebagai panduan untuk membuat solusi kustom Anda sendiri:

Mengirim temuan dari Chef InSpec pemindaian ke Security Hub CSPM

Anda dapat membuat AWS CloudFormation template yang menjalankan [Chef InSpec](#) pemindaian kepatuhan dan kemudian mengirimkan temuan ke Security Hub CSPM.

Untuk detail selengkapnya, lihat [Pemantauan kepatuhan berkelanjutan dengan Chef InSpec dan AWS Security Hub Cloud Security Posture Management \(CSPM\)](#).

Mengirim kerentanan kontainer terdeteksi oleh Trivy ke Security Hub CSPM

Anda dapat membuat AWS CloudFormation templat yang digunakan [AquaSecurity Trivy](#) untuk memindai kerentanan kontainer, lalu mengirimkan temuan kerentanan tersebut ke Security Hub CSPM.

Untuk detail selengkapnya, lihat [Cara membuat CI/CD pipeline untuk pemindaian kerentanan kontainer dengan Trivy dan AWS Security Hub Cloud Security Posture Management \(CSPM\)](#).

Membuat dan memperbarui temuan di Security Hub CSPM

Dalam AWS Security Hub Cloud Security Posture Management (CSPM), temuan adalah catatan yang dapat diamati dari pemeriksaan keamanan atau deteksi terkait keamanan. Temuan dapat berasal dari salah satu sumber berikut:

- Pemeriksaan keamanan untuk kontrol di Security Hub CSPM.
- Integrasi dengan yang lain Layanan AWS.
- Integrasi dengan produk pihak ketiga.
- Integrasi kustom.

Security Hub CSPM menormalkan temuan dari semua sumber ke dalam sintaks dan format standar yang disebut AWS Security Finding Format (ASFF). Untuk informasi rinci tentang format ini, termasuk deskripsi bidang ASFF individual, lihat [AWS Format Pencarian Keamanan \(ASFF\)](#). Jika Anda mengaktifkan agregasi Lintas wilayah, Security Hub CSPM juga mengumpulkan temuan baru dan yang diperbarui secara otomatis dari semua Wilayah tertaut ke Wilayah agregasi yang Anda tentukan. Untuk informasi selengkapnya, lihat [Memahami agregasi lintas wilayah di Security Hub CSPM](#).

Setelah temuan dibuat, itu dapat diperbarui sebagai berikut:

- Penyedia temuan dapat menggunakan [BatchImportFindings](#) pengoperasian Security Hub CSPM API untuk memperbarui informasi umum tentang temuan tersebut. Penyedia pencarian hanya dapat memperbarui temuan yang mereka buat.
- Pelanggan dapat menggunakan konsol CSPM Security Hub atau [BatchUpdateFindings](#) pengoperasian Security Hub CSPM API untuk memperbarui status penyelidikan ke dalam temuan. BatchUpdateFindings Operasi ini juga dapat digunakan oleh SIEM, tiket, manajemen insiden, SOAR, atau jenis alat lain atas nama pelanggan.

Untuk mengurangi kebisingan penemuan dan merampingkan pelacakan dan analisis temuan individu, Security Hub CSPM secara otomatis menghapus temuan yang belum diperbarui baru-baru ini. Waktu dimana Security Hub CSPM melakukan hal ini tergantung pada apakah suatu temuan aktif atau diarsipkan:

- Temuan aktif adalah temuan yang status catatannya (RecordState) ACTIVE. Security Hub CSPM menyimpan temuan aktif selama 90 hari. Jika temuan aktif belum diperbarui selama 90 hari, itu kedaluwarsa dan Security Hub CSPM menghapusnya secara permanen.
- Temuan yang diarsipkan adalah temuan yang status catatan (RecordState) adalah ARCHIVED. Security Hub CSPM menyimpan temuan yang diarsipkan selama 30 hari. Jika temuan yang diarsipkan belum diperbarui selama 30 hari, temuan tersebut akan kedaluwarsa dan Security Hub CSPM menghapusnya secara permanen.

Untuk temuan kontrol, yang merupakan temuan yang dihasilkan oleh Security Hub CSPM dari pemeriksaan keamanan untuk kontrol, Security Hub CSPM menentukan apakah temuan telah kedaluwarsa berdasarkan nilai bidang temuan. UpdatedAt Jika nilai ini lebih dari 90 hari yang lalu untuk temuan aktif, Security Hub CSPM secara permanen menghapus temuan tersebut. Jika nilai ini lebih dari 30 hari yang lalu untuk temuan yang diarsipkan, Security Hub CSPM secara permanen menghapus temuan tersebut.

Untuk semua jenis temuan lainnya, Security Hub CSPM menentukan apakah temuan telah kedaluwarsa berdasarkan nilai untuk ProcessedAt dan UpdatedAt bidang temuan. Security Hub CSPM membandingkan nilai untuk bidang ini dan menentukan mana yang lebih baru. Jika nilai yang lebih baru lebih dari 90 hari yang lalu untuk temuan aktif, Security Hub CSPM secara permanen menghapus temuan tersebut. Jika nilai yang lebih baru lebih dari 30 hari yang lalu untuk temuan yang diarsipkan, Security Hub CSPM secara permanen menghapus temuan tersebut. Penyedia pencarian dapat mengubah nilai untuk UpdatedAt bidang satu atau lebih temuan dengan menggunakan [BatchImportFindings](#) pengoperasian Security Hub CSPM API.

Untuk retensi temuan jangka panjang, Anda dapat mengekspor temuan ke ember S3. Anda dapat melakukan ini dengan menggunakan tindakan kustom dengan EventBridge aturan Amazon. Untuk informasi selengkapnya, lihat [Menggunakan EventBridge untuk respon otomatis dan remediasi](#).

Topik

- [BatchImportFindings untuk menemukan penyedia](#)
- [BatchUpdateFindings untuk pelanggan](#)
- [Meninjau detail dan riwayat penemuan di Security Hub CSPM](#)
- [Penyaringan temuan di Security Hub CSPM](#)
- [Mengelompokkan temuan di Security Hub CSPM](#)
- [Menetapkan status alur kerja temuan di Security Hub CSPM](#)
- [Mengirim temuan ke tindakan CSPM Security Hub kustom](#)

- [AWS Format Pencarian Keamanan \(ASFF\)](#)

BatchImportFindings untuk menemukan penyedia

Penyedia pencarian dapat menggunakan [BatchImportFindings](#) operasi untuk membuat temuan baru di AWS Security Hub Cloud Security Posture Management (CSPM). Mereka juga dapat menggunakan operasi ini untuk memperbarui temuan yang mereka buat. Menemukan penyedia tidak dapat memperbarui temuan yang tidak mereka buat.

Pelanggan SIEMs, tiket, SOAR, dan jenis alat lainnya harus menggunakan [BatchUpdateFindings](#) operasi untuk membuat pembaruan terkait dengan penyelidikan mereka terhadap temuan dari penyedia pencarian. Untuk informasi selengkapnya, lihat [the section called “BatchUpdateFindings untuk pelanggan”](#).

Ketika Security Hub CSPM menerima BatchImportFindings permintaan untuk membuat atau memperbarui temuan, itu secara otomatis menghasilkan Security Hub Findings - Imported peristiwa di Amazon. EventBridge Anda dapat mengambil tindakan otomatis pada acara itu. Untuk informasi selengkapnya, lihat [the section called “Respon dan remediasi otomatis”](#).

Prasyarat untuk menggunakan BatchImportFindings

BatchImportFindings harus dipanggil oleh salah satu dari berikut ini:

- Akun yang terkait dengan temuan. Pengidentifikasi akun terkait harus sesuai dengan nilai `AwsAccountId` atribut untuk temuan.
- Akun yang diizinkan terdaftar sebagai integrasi mitra CSPM Security Hub resmi.

Security Hub CSPM hanya dapat menerima pembaruan pencarian untuk akun yang mengaktifkan Security Hub CSPM. Penyedia temuan juga harus diaktifkan. Jika Security Hub CSPM dinonaktifkan, atau integrasi penyedia pencarian tidak diaktifkan, maka temuan akan dikembalikan dalam `FailedFindings` daftar, dengan kesalahan `InvalidAccess`.

Menentukan apakah akan membuat atau memperbarui temuan

Untuk menentukan apakah akan membuat atau memperbarui temuan, Security Hub CSPM memeriksa bidang tersebut. ID Jika nilai ID tidak sesuai dengan temuan yang ada, Security Hub CSPM akan membuat temuan baru.

Jika ID cocok dengan temuan yang ada, Security Hub CSPM memeriksa UpdatedAt bidang untuk pembaruan, dan melanjutkan sebagai berikut:

- Jika UpdatedAt pada pembaruan cocok atau terjadi sebelumnya UpdatedAt pada temuan yang ada, Security Hub CSPM mengabaikan permintaan pembaruan.
- Jika UpdatedAt pada pembaruan terjadi setelah UpdatedAt pada temuan yang ada, Security Hub CSPM memperbarui temuan yang ada.

Pembatasan untuk menemukan pembaruan dengan **BatchImportFindings**

Penyedia pencarian tidak dapat digunakan BatchImportFindings untuk memperbarui atribut berikut dari temuan yang ada:

- Note
- UserDefinedFields
- VerificationState
- Workflow

Security Hub CSPM mengabaikan konten apa pun yang disediakan dalam BatchImportFindings permintaan atribut ini. Pelanggan, atau entitas yang bertindak atas nama mereka (seperti alat tiket), dapat menggunakannya BatchUpdateFindings untuk memperbarui atribut ini.

Memperbarui temuan dengan FindingProviderFields

Penyedia pencarian juga tidak boleh digunakan BatchImportFindings untuk memperbarui atribut tingkat atas berikut di AWS Security Finding Format (ASFF):

- Confidence
- Criticality
- RelatedFindings
- Severity
- Types

Sebaliknya, mencari penyedia harus menggunakan [FindingProviderFields](#) objek untuk memberikan nilai untuk atribut ini.

Contoh

```
"FindingProviderFields": {
  "Confidence": 42,
  "Criticality": 99,
  "RelatedFindings": [
    {
      "ProductArn": "arn:aws:securityhub:us-west-2::product/aws/guardduty",
      "Id": "123e4567-e89b-12d3-a456-426655440000"
    }
  ],
  "Severity": {
    "Label": "MEDIUM",
    "Original": "MEDIUM"
  },
  "Types": [ "Software and Configuration Checks/Vulnerabilities/CVE" ]
}
```

Untuk `BatchImportFindings` permintaan, Security Hub CSPM menangani nilai di atribut tingkat atas dan sebagai berikut. [FindingProviderFields](#)

(Preferred) **BatchImportFindings** memberikan nilai untuk atribut di [FindingProviderFields](#), tetapi tidak memberikan nilai untuk atribut tingkat atas yang sesuai.

Misalnya, `BatchImportFindings` menyediakan `FindingProviderFields.Confidence`, tetapi tidak menyediakan `Confidence`. Ini adalah opsi yang lebih disukai untuk `BatchImportFindings` permintaan.

Security Hub CSPM memperbarui nilai atribut di `FindingProviderFields`

Ini mereplikasi nilai ke atribut tingkat atas hanya jika atribut belum diperbarui oleh `BatchUpdateFindings`

BatchImportFindings memberikan nilai untuk atribut tingkat atas, tetapi tidak memberikan nilai untuk atribut yang sesuai di **FindingProviderFields**.

Misalnya, `BatchImportFindings` menyediakan `Confidence`, tetapi tidak menyediakan `FindingProviderFields.Confidence`.

Security Hub CSPM menggunakan nilai untuk memperbarui atribut di `FindingProviderFields` ini menimpa nilai yang ada.

Security Hub CSPM memperbarui atribut tingkat atas hanya jika atribut belum diperbarui oleh `BatchUpdateFindings`.

BatchImportFindings memberikan nilai untuk atribut tingkat atas dan atribut yang sesuai di **`FindingProviderFields`**.

Misalnya, `BatchImportFindings` menyediakan keduanya `Confidence` dan `FindingProviderFields.Confidence`.

Untuk temuan baru, Security Hub CSPM menggunakan nilai dalam `FindingProviderFields` untuk mengisi atribut tingkat atas dan atribut yang sesuai. `FindingProviderFields` itu tidak menggunakan nilai atribut tingkat atas yang disediakan.

Untuk temuan yang ada, Security Hub CSPM menggunakan kedua nilai. Namun, itu memperbarui nilai atribut tingkat atas hanya jika atribut belum diperbarui oleh `BatchUpdateFindings`.

BatchUpdateFindings untuk pelanggan

AWS Pelanggan Security Hub Cloud Security Posture Management (CSPM), dan entitas yang bertindak atas nama mereka, dapat menggunakan [BatchUpdateFindings](#) operasi ini untuk memperbarui informasi terkait pemrosesan temuan CSPM Security Hub dari penyedia pencarian. Sebagai pelanggan, Anda dapat menggunakan operasi ini secara langsung. SIEM, tiket, manajemen insiden, dan alat SOAR juga dapat menggunakan operasi ini atas nama pelanggan.

Anda tidak dapat menggunakan `BatchUpdateFindings` operasi untuk membuat temuan baru. Namun, Anda dapat menggunakannya untuk memperbarui hingga 100 temuan yang ada sekaligus. Dalam `BatchUpdateFindings` permintaan, Anda menentukan temuan mana yang akan diperbarui, bidang AWS Security Finding Format (ASFF) mana yang akan diperbarui untuk temuan, dan nilai baru untuk bidang tersebut. Security Hub CSPM kemudian memperbarui temuan seperti yang ditentukan dalam permintaan Anda. Proses ini dapat memakan waktu beberapa menit. Jika Anda memperbarui temuan dengan menggunakan `BatchUpdateFindings` operasi, pembaruan Anda tidak memengaruhi nilai yang ada untuk `UpdatedAt` bidang temuan.

Ketika Security Hub CSPM menerima `BatchUpdateFindings` permintaan untuk memperbarui temuan, itu secara otomatis menghasilkan Security Hub Findings – Imported peristiwa di Amazon. EventBridge Anda dapat menggunakan acara ini secara opsional untuk mengambil tindakan otomatis

pada temuan yang ditentukan. Untuk informasi selengkapnya, lihat [the section called “Respon dan remediasi otomatis”](#).

Bidang yang tersedia untuk BatchUpdateFindings

Jika Anda masuk ke akun administrator CSPM Security Hub, Anda dapat menggunakannya BatchUpdateFindings untuk memperbarui temuan yang dihasilkan oleh akun administrator atau akun anggota. Akun anggota dapat digunakan BatchUpdateFindings untuk memperbarui temuan hanya untuk akun mereka.

Pelanggan dapat menggunakan BatchUpdateFindings untuk memperbarui bidang dan objek berikut:

- Confidence
- Criticality
- Note
- RelatedFindings
- Severity
- Types
- UserDefinedFields
- VerificationState
- Workflow

Mengkonfigurasi akses ke BatchUpdateFindings

Anda dapat mengonfigurasi kebijakan AWS Identity and Access Management (IAM) untuk membatasi akses penggunaan BatchUpdateFindings untuk memperbarui bidang pencarian dan nilai bidang.

Dalam pernyataan untuk membatasi akses keBatchUpdateFindings, gunakan nilai-nilai berikut:

- Actionadalah securityhub:BatchUpdateFindings
- Effectadalah Deny
- UntukCondition, Anda dapat menolak BatchUpdateFindings permintaan berdasarkan hal berikut:
 - Temuan ini mencakup bidang tertentu.
 - Temuan ini mencakup nilai bidang tertentu.

Kunci syarat

Ini adalah kunci kondisi untuk membatasi akses ke `BatchUpdateFindings`.

Bidang ASFF

Kunci kondisi untuk bidang ASFF adalah sebagai berikut:

```
securityhub:ASFFSyntaxPath/<fieldName>
```

Ganti `<fieldName>` dengan bidang ASFF. Saat mengonfigurasi akses ke `BatchUpdateFindings`, sertakan satu atau lebih bidang ASFF spesifik dalam kebijakan IAM Anda, bukan bidang tingkat induk. Misalnya, untuk membatasi akses ke `Workflow.Status` bidang, Anda harus menyertakan `securityhub:ASFFSyntaxPath/Workflow.Status` dalam kebijakan, bukan bidang tingkat `Workflow` induk.

Melarangi semua pembaruan ke bidang

Untuk mencegah pengguna melakukan pembaruan apa pun ke bidang tertentu, gunakan kondisi seperti ini:

```
"Condition": {
    "Null": {
        "securityhub:ASFFSyntaxPath/<fieldName>": "false"
    }
}
```

Misalnya, pernyataan berikut menunjukkan bahwa tidak `BatchUpdateFindings` dapat digunakan untuk memperbarui `Workflow.Status` bidang temuan.

```
{
  "Sid": "VisualEditor0",
  "Effect": "Deny",
  "Action": "securityhub:BatchUpdateFindings",
  "Resource": "*",
  "Condition": {
    "Null": {
      "securityhub:ASFFSyntaxPath/Workflow.Status": "false"
    }
  }
}
```



```
}
```

Melarangkan nilai bidang tertentu

Untuk mencegah pengguna menyetel bidang ke nilai tertentu, gunakan kondisi seperti ini:

```
"Condition": {
  "StringEquals": {
    "securityhub:ASFFSyntaxPath/<fieldName>": "<fieldValue>"
  }
}
```

Misalnya, pernyataan berikut menunjukkan bahwa tidak BatchUpdateFindings dapat digunakan untuk mengatur Workflow.Status ke SUPPRESSED.

```
{
  "Sid": "VisualEditor0",
  "Effect": "Deny",
  "Action": "securityhub:BatchUpdateFindings",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "securityhub:ASFFSyntaxPath/Workflow.Status": "SUPPRESSED"
    }
  }
}
```

Anda juga dapat memberikan daftar nilai yang tidak diizinkan.

```
"Condition": {
  "StringEquals": {
    "securityhub:ASFFSyntaxPath/<fieldName>": [ "<fieldValue1>",
    "<fieldValue2>", "<fieldValue3>" ]
  }
}
```

Misalnya, pernyataan berikut menunjukkan bahwa tidak BatchUpdateFindings dapat digunakan untuk mengatur Workflow.Status ke salah satu RESOLVED atau SUPPRESSED.

```
{
  "Sid": "VisualEditor0",
  "Effect": "Deny",
```

```
"Action": "securityhub:BatchUpdateFindings",
"Resource": "*",
"Condition": {
  "StringEquals": {
    "securityhub:ASFFSyntaxPath/Workflow.Status": [
      "RESOLVED",
      "NOTIFIED"
    ]
  }
}
```

Meninjau detail dan riwayat penemuan di Security Hub CSPM

Dalam AWS Security Hub Cloud Security Posture Management (CSPM), temuan adalah catatan yang dapat diamati dari pemeriksaan keamanan atau deteksi terkait keamanan. Security Hub CSPM menghasilkan temuan ketika menyelesaikan pemeriksaan keamanan kontrol dan ketika menelan temuan dari produk terintegrasi Layanan AWS atau pihak ketiga. Setiap temuan mencakup riwayat perubahan dan detail lainnya, seperti peringkat keparahan dan informasi tentang sumber daya yang terpengaruh.

Anda dapat meninjau riwayat dan detail lain dari temuan individual di konsol CSPM Security Hub atau secara terprogram dengan Security Hub CSPM API atau AWS CLI

Untuk membantu Anda merampingkan analisis, konsol CSPM Security Hub menampilkan panel pencarian saat Anda memilih temuan tertentu. Panel mencakup berbagai menu dan tab untuk meninjau detail spesifik dari sebuah temuan.

Menu tindakan

Dari menu ini, Anda dapat meninjau JSON lengkap dari sebuah temuan atau menambahkan catatan. Sebuah temuan hanya dapat memiliki satu catatan yang melekat padanya pada satu waktu. Menu ini juga menyediakan opsi untuk [mengatur status alur kerja temuan](#) atau [mengirim temuan ke tindakan khusus](#) di Amazon EventBridge.

Selidiki menu

Dari menu ini, Anda dapat menyelidiki temuan di Amazon Detective. Detective mengekstrak entitas, seperti alamat IP dan AWS pengguna, dari temuan dan memvisualisasikan aktivitas mereka. Anda dapat menggunakan aktivitas entitas sebagai titik awal untuk menyelidiki penyebab dan dampak temuan.

Tab Ikhtisar

Tab ini memberikan ringkasan temuan. Misalnya, Anda dapat menentukan kapan temuan dibuat dan terakhir diperbarui, di akun mana itu ada, dan sumber temuan. Untuk temuan kontrol, tab ini juga menampilkan nama AWS Config aturan terkait dan tautan ke panduan remediasi dalam dokumentasi CSPM Security Hub.

Dalam snapshot Sumber Daya pada tab Ikhtisar, Anda bisa mendapatkan gambaran singkat tentang sumber daya yang terlibat dalam temuan. Untuk beberapa sumber daya, ini termasuk opsi sumber daya terbuka, yang menautkan langsung ke sumber daya yang terkena dampak pada Layanan AWS konsol yang relevan. Snapshot Sejarah menunjukkan hingga dua perubahan yang dibuat pada temuan pada tanggal terbaru di mana sejarah sedang dilacak. Misalnya, jika Anda membuat satu perubahan kemarin dan satu lagi hari ini, snapshot menunjukkan perubahan hari ini. Untuk meninjau entri sebelumnya, beralih ke tab Riwayat.

Baris Kepatuhan diperluas untuk menampilkan detail selengkapnya. Misalnya, jika kontrol menyertakan parameter, Anda dapat meninjau nilai parameter yang saat ini digunakan Security Hub CSPM saat ini saat melakukan pemeriksaan keamanan untuk kontrol.

Tab sumber daya

Tab ini memberikan rincian tentang sumber daya yang terlibat dalam temuan. Jika Anda masuk ke akun yang memiliki sumber daya, Anda dapat meninjau sumber daya di Layanan AWS konsol yang berlaku. Jika Anda bukan pemilik sumber daya, tab ini menampilkan Akun AWS ID untuk pemiliknya.

Baris Detail menunjukkan detail spesifik sumber daya dalam sebuah temuan. Ini menunjukkan [ResourceDetails](#) bagian temuan dalam format JSON.

Baris Tag menunjukkan kunci tag dan nilai yang ditetapkan ke sumber daya yang terlibat dalam temuan. Sumber daya yang [didukung oleh GetResources pengoperasian](#) API AWS Resource Groups Tagging dapat diberi tag. Security Hub CSPM memanggil operasi ini dengan menggunakan [peran terkait layanan](#) saat memproses temuan baru atau yang diperbarui, dan mengambil tag sumber daya jika bidang AWS Security Finding Format (ASFF) Resource . Id diisi dengan ARN sumber daya. Security Hub CSPM mengabaikan sumber daya yang tidak valid. IDs Untuk informasi lebih lanjut tentang penyertaan tag sumber daya dalam temuan, lihat [Tanda](#).

Tab sejarah

Tab ini melacak riwayat temuan. Menemukan riwayat tersedia untuk temuan aktif dan diarsipkan. Ini memberikan jejak perubahan yang tidak dapat diubah yang dibuat untuk temuan dari waktu

ke waktu, termasuk bidang ASFF apa yang diubah, kapan perubahan terjadi, dan oleh pengguna mana. Setiap halaman pada tab menampilkan hingga 20 perubahan. Perubahan yang lebih baru ditampilkan terlebih dahulu.

Untuk temuan aktif, riwayat penemuan tersedia hingga 90 hari. Untuk temuan yang diarsipkan, riwayat penemuan tersedia hingga 30 hari. Menemukan riwayat mencakup perubahan yang dilakukan secara manual, atau secara otomatis oleh aturan [otomatisasi CSPM Security Hub](#). Itu tidak termasuk perubahan pada bidang stempel waktu tingkat atas, seperti bidang `CreatedAt`. `UpdatedAt`

Jika Anda masuk ke akun administrator CSPM Security Hub, menemukan riwayat adalah untuk akun administrator dan semua akun anggota.

Tab ancaman

Tab ini mencakup data dari [ActionMalware](#), dan [ProcessDetails](#) objek ASFF, termasuk jenis ancaman dan apakah sumber daya adalah target atau aktor. Rincian ini biasanya berlaku untuk temuan yang berasal dari Amazon GuardDuty.

Tab Kerentanan

Tab ini menampilkan data dari [Vulnerability](#) objek ASFF, termasuk apakah ada eksploitasi atau perbaikan yang tersedia terkait dengan temuan. Rincian ini biasanya berlaku untuk temuan yang berasal dari Amazon Inspector.

Baris pada setiap tab menyertakan opsi salin atau filter. Misalnya, jika Anda membuka panel untuk temuan yang memiliki status alur kerja `Notified`, Anda dapat memilih opsi filter di sebelah baris status Alur Kerja. Jika Anda memilih Tampilkan semua temuan dengan nilai ini, CSPM Security Hub memfilter tabel temuan dan hanya menampilkan temuan dengan status alur kerja yang sama.

Meninjau detail dan riwayat penemuan

Pilih metode yang Anda inginkan, dan ikuti langkah-langkah untuk meninjau detail pencarian di Security Hub CSPM.

Jika Anda mengaktifkan agregasi lintas wilayah dan masuk ke Wilayah agregasi, menemukan data mencakup data dari Wilayah agregasi dan Wilayah tertaut. Di Wilayah lain, menemukan data khusus untuk Wilayah itu saja. Untuk informasi selengkapnya tentang agregasi lintas wilayah, lihat [Menggabungkan data CSPM di seluruh Wilayah](#)

Security Hub CSPM console

Meninjau detail dan riwayat penemuan

1. Buka konsol AWS Security Hub Cloud Security Posture Management (CSPM) di <https://console.aws.amazon.com/securityhub/>
2. Untuk menampilkan daftar temuan, lakukan salah satu hal berikut:
 - Di panel navigasi, pilih Temuan. Tambahkan filter pencarian seperlunya untuk mempersempit daftar temuan.
 - Pada panel navigasi, silakan pilih Wawasan. Pilih wawasan. Kemudian, dalam daftar hasil, pilih hasil wawasan.
 - Di panel navigasi, pilih Integrasi. Pilih Lihat temuan untuk integrasi.
 - Di panel navigasi, pilih Kontrol.
3. Pilih temuan. Panel temuan menampilkan detail temuan.
4. Di panel pencarian, lakukan salah satu hal berikut:
 - Untuk meninjau detail spesifik untuk temuan, pilih tab.
 - Untuk mengambil tindakan pada temuan, pilih opsi dari menu Tindakan.
 - Untuk menyelidiki temuan di Detektif Amazon, pilih opsi Selidiki.

Note

Jika Anda berintegrasi dengan AWS Organizations dan Anda masuk ke akun anggota, panel pencarian menyertakan nama akun. Untuk akun anggota yang diundang secara manual, bukan melalui Organizations, panel pencarian hanya menyertakan ID akun.

Security Hub CSPM API

Gunakan [GetFindings](#) pengoperasian Security Hub CSPM API, atau jika Anda menggunakan AWS CLI, jalankan perintah. [get-findings](#) Anda dapat memberikan satu atau lebih nilai untuk `Filters` parameter untuk mempersempit temuan untuk diambil.

Jika volume hasil terlalu besar, Anda dapat menggunakan `MaxResults` parameter untuk membatasi temuan ke angka tertentu dan `NextToken` parameter untuk membuat halaman

temuan. Gunakan `SortCriteria` parameter untuk mengurutkan temuan berdasarkan bidang tertentu.

Misalnya, AWS CLI perintah berikut mengambil temuan yang cocok dengan kriteria filter yang ditentukan, dan mengurutkan hasil dalam urutan menurun menurut bidang. `LastObservedAt` Contoh ini diformat untuk Linux, macOS, atau Unix, dan menggunakan karakter garis miring terbalik (`\`) untuk meningkatkan keterbacaan.

```
$ aws securityhub get-findings \
--filters '{"GeneratorId":[{"Value": "aws-
foundational","Comparison":"PREFIX"}],"WorkflowStatus": [{"Value":
"NEW","Comparison":"EQUALS"}],"Confidence": [{"Gte": 85}]}' --sort-criteria
'{"Field": "LastObservedAt","SortOrder": "desc"}' --page-size 5 --max-items 100
```

Untuk meninjau riwayat penemuan, gunakan [GetFindingHistory](#) operasi. Jika Anda menggunakan AWS CLI, jalankan `get-finding-history` perintah. Identifikasi temuan yang ingin Anda dapatkan riwayat dengan Id bidang `ProductArn` dan. Untuk informasi tentang bidang ini, lihat [AwsSecurityFindingIdentifier](#). Setiap permintaan dapat mengambil riwayat hanya untuk satu temuan.

Misalnya, AWS CLI perintah berikut mengambil riwayat untuk temuan yang ditentukan. Contoh ini diformat untuk Linux, macOS, atau Unix, dan menggunakan karakter garis miring terbalik (`\`) untuk meningkatkan keterbacaan.

```
$ aws securityhub get-finding-history \
--region us-west-2 \
--finding-identifier Id="a1b2c3d4-5678-90ab-cdef-
EXAMPLE1111",ProductArn="arn:aws:securityhub:us-
west-2:123456789012:product/123456789012/default" \
--max-results 2 \
--start-time "2021-09-30T15:53:35.573Z" \
--end-time "2021-09-31T15:53:35.573Z"
```

PowerShell

Gunakan `Get-SHUBFinding` cmdlet. Secara opsional mengisi `Filter` parameter untuk mempersempit temuan untuk diambil.

Misalnya, cmdlet berikut mengambil temuan yang cocok dengan filter yang ditentukan.

```
Get-SHUBFinding -Filter @{AwsAccountId =  
[Amazon.SecurityHub.Model.StringFilter]@{Comparison = "EQUALS"; Value =  
"XXX"};ComplianceStatus = [Amazon.SecurityHub.Model.StringFilter]@{Comparison =  
"EQUALS"; Value = 'FAILED'}}
```

Note

Jika Anda memfilter temuan oleh `CompanyName` atau `ProductName`, Security Hub CSPM menggunakan nilai yang merupakan bagian dari objek `ProductFields ASFF`. Security Hub CSPM tidak menggunakan top-level `CompanyName` dan field. `ProductName`

Penyaringan temuan di Security Hub CSPM

AWS Security Hub Cloud Security Posture Management (CSPM) menghasilkan temuannya sendiri dari pemeriksaan keamanan dan menerima temuan dari produk terintegrasi. Anda dapat menampilkan daftar temuan di halaman Temuan, Integrasi, dan Wawasan konsol CSPM Security Hub. Anda dapat menambahkan filter untuk mempersempit daftar temuan sehingga daftar tersebut relevan dengan organisasi atau kasus penggunaan Anda.

Untuk informasi tentang memfilter temuan untuk kontrol keamanan tertentu, lihat [the section called “Memfilter dan menyortir temuan kontrol”](#). Informasi di halaman ini berlaku untuk halaman Temuan, Wawasan, dan Integrasi.

Filter default pada daftar pencarian

Secara default, daftar pencarian di konsol CSPM Security Hub difilter berdasarkan `RecordState` dan `Workflow.Status` bidang AWS Security Finding Format (ASFF). Ini adalah tambahan untuk filter untuk wawasan atau integrasi tertentu.

Status rekaman menunjukkan apakah temuan aktif atau diarsipkan. Secara default, daftar temuan hanya menunjukkan temuan aktif. Penyedia pencarian dapat mengarsipkan temuan jika tidak lagi aktif atau penting. Security Hub CSPM juga secara otomatis mengarsipkan temuan kontrol jika sumber daya terkait dihapus.

Status alur kerja menunjukkan status investigasi terhadap suatu temuan. Secara default, daftar temuan hanya menampilkan temuan dengan status alur kerja `NEW` atau `NOTIFIED`. Anda dapat memperbarui status alur kerja temuan.

Petunjuk untuk menambahkan filter

Anda dapat memfilter daftar temuan hingga sepuluh atribut. Untuk setiap atribut, Anda dapat memberikan hingga 20 nilai filter.

Saat memfilter daftar temuan, Security Hub CSPM menerapkan AND logika ke kumpulan filter. Temuan hanya cocok jika cocok dengan semua filter yang disediakan. Misalnya, jika Anda menambahkan GuardDuty sebagai filter untuk nama Produk, dan AwsS3Bucket sebagai filter untuk jenis Sumber Daya, CSPM Security Hub menampilkan temuan yang cocok dengan kedua kriteria ini.

Security Hub CSPM menerapkan OR logika untuk filter yang menggunakan atribut yang sama tetapi nilai yang berbeda. Misalnya, jika Anda menambahkan keduanya GuardDuty dan Amazon Inspector sebagai nilai filter untuk nama Produk, Security Hub CSPM menampilkan temuan yang dihasilkan oleh salah satu atau Amazon GuardDuty Inspector.

Untuk menambahkan filter ke daftar temuan (konsol)

1. Buka konsol AWS Security Hub Cloud Security Posture Management (CSPM) di <https://console.aws.amazon.com/securityhub/>
2. Untuk menampilkan daftar temuan, lakukan salah satu tindakan berikut dari panel navigasi:
 - Pilih Temuan.
 - Pilih Wawasan. Pilih wawasan. Kemudian, pada daftar hasil, pilih hasil wawasan.
 - Pilih Integrasi. Pilih Lihat temuan untuk integrasi.
3. Di kotak Tambahkan filter, pilih satu atau beberapa file untuk difilter.

Saat Anda memfilter berdasarkan nama Perusahaan atau Nama Produk, konsol menggunakan tingkat atas `CompanyName` dan `ProductName` bidang AWS Security Finding Format (ASFF). API menggunakan nilai yang bersarang di `bawahProductFields`.

4. Pilih jenis kecocokan filter.

Untuk filter string, Anda dapat memilih dari opsi berikut:

- `is` — Temukan nilai yang sama persis dengan nilai filter.
- `dimulai dengan` - Temukan nilai yang dimulai dengan nilai filter.
- `is not` — Temukan nilai yang tidak cocok dengan nilai filter.
- `tidak dimulai dengan` — Temukan nilai yang tidak dimulai dengan nilai filter.

Untuk bidang Tag sumber daya, Anda dapat memfilter berdasarkan kunci atau nilai tertentu.

Untuk filter numerik, Anda dapat memilih apakah akan memberikan nomor tunggal (Sederhana) atau rentang angka (Rentang).

Untuk filter tanggal atau waktu, Anda dapat memilih apakah akan memberikan jangka waktu dari tanggal dan waktu saat ini (Jendela bergulir) atau rentang tanggal tertentu (Rentang tetap).

Menambahkan beberapa filter memiliki interaksi berikut:

- adalah dan dimulai dengan filter bergabung dengan OR. Nilai cocok jika berisi salah satu nilai filter. Misalnya, jika Anda menentukan label Keparahan adalah KRITIS dan label Keparahan TINGGI, hasilnya mencakup temuan tingkat keparahan kritis dan tinggi.
- tidak dan tidak dimulai dengan filter bergabung dengan AND. Nilai hanya cocok jika tidak mengandung nilai filter tersebut. Misalnya, jika Anda menentukan label Keparahan tidak RENDAH dan label Keparahan tidak SEDANG, hasilnya tidak termasuk temuan tingkat keparahan rendah atau sedang.

Jika Anda memiliki filter is di bidang, Anda tidak dapat memiliki is not atau tidak dimulai dengan filter pada bidang yang sama.

5. Tentukan nilai filter. Untuk filter string, nilai filter peka huruf besar/kecil.
6. Pilih Terapkan.

Untuk filter yang ada, Anda dapat mengubah jenis atau nilai kecocokan filter. Pada daftar temuan yang difilter, pilih filter. Di kotak Edit filter, pilih jenis atau nilai kecocokan baru, lalu pilih Terapkan.

Untuk menghapus filter, pilih ikon x. Daftar diperbarui secara otomatis untuk mencerminkan perubahan.

Mengelompokkan temuan di Security Hub CSPM

Anda dapat mengelompokkan temuan di AWS Security Hub Cloud Security Posture Management (CSPM) berdasarkan nilai atribut yang dipilih.

Saat Anda mengelompokkan temuan, daftar temuan diganti dengan daftar nilai untuk atribut yang dipilih dalam temuan yang cocok. Untuk setiap nilai, daftar menampilkan jumlah temuan yang cocok.

Misalnya, jika Anda mengelompokkan temuan berdasarkan Akun AWS ID, Anda akan melihat daftar pengidentifikasi akun, dengan jumlah temuan yang cocok untuk setiap akun.

Security Hub CSPM dapat menampilkan hingga 100 nilai untuk atribut yang dipilih. Jika ada lebih dari 100 nilai, Anda hanya melihat 100 yang pertama.

Bila Anda memilih nilai atribut, Security Hub CSPM menampilkan daftar temuan yang cocok untuk nilai tersebut.

Untuk mengelompokkan temuan dalam daftar temuan (konsol)

1. Buka konsol AWS Security Hub Cloud Security Posture Management (CSPM) di <https://console.aws.amazon.com/securityhub/>
2. Untuk menampilkan daftar temuan, lakukan salah satu tindakan berikut dari panel navigasi:
 - Pilih Temuan.
 - Pilih Wawasan. Pilih wawasan. Kemudian, pada daftar hasil, pilih hasil wawasan.
 - Pilih Integrasi. Pilih Lihat temuan untuk integrasi.
3. Di Drop-down Group by, pilih atribut yang akan digunakan untuk pengelompokan.

Untuk menghapus atribut pengelompokan, pilih ikon x. Saat Anda menghapus atribut pengelompokan, daftar berubah dari daftar nilai atribut ke daftar temuan.

Menetapkan status alur kerja temuan di Security Hub CSPM

Status alur kerja melacak kemajuan penyelidikan Anda ke dalam sebuah temuan. Status alur kerja spesifik untuk temuan individu dan tidak mempengaruhi generasi temuan baru. Misalnya, jika Anda mengubah status alur kerja temuan ke SUPPRESSED atau RESOLVED, perubahan Anda tidak mencegah CSPM Security Hub menghasilkan temuan baru untuk masalah yang sama.

Status alur kerja temuan dapat menjadi salah satu nilai berikut.

BARU

Keadaan awal temuan sebelum Anda memeriksanya.

Temuan yang dicerna dari terintegrasi Layanan AWS, seperti AWS Config, memiliki NEW status awal mereka.

Security Hub CSPM juga mengatur ulang status alur kerja dari salah satu NOTIFIED atau RESOLVED ke NEW dalam kasus berikut:

- RecordStateperubahan dari ARCHIVED keACTIVE.
- Compliance.Statusperubahan dari PASSED keFAILED,WARNING, atauNOT_AVAILABLE.

Perubahan ini menyiratkan bahwa penyelidikan tambahan diperlukan.

DIBERITAHU

Menunjukkan bahwa Anda memberi tahu pemilik sumber daya tentang masalah keamanan. Anda dapat menggunakan status ini ketika Anda bukan pemilik sumber daya, dan Anda memerlukan intervensi dari pemilik sumber daya untuk menyelesaikan masalah keamanan.

Jika salah satu hal berikut terjadi, status alur kerja diubah secara otomatis dari NOTIFIED menjadiNEW:

- RecordStateperubahan dari ARCHIVED keACTIVE.
- Compliance.Statusperubahan dari PASSED keFAILED,WARNING, atauNOT_AVAILABLE.

DITEKAN

Menunjukkan bahwa Anda meninjau temuan dan tidak percaya bahwa tindakan apa pun diperlukan.

Status alur kerja SUPPRESSED temuan tidak berubah jika RecordState berubah dari ARCHIVED keACTIVE.

DISELESAIKAN

Temuan ini ditinjau dan diperbaiki dan sekarang dianggap telah diselesaikan.

Temuan tetap ada RESOLVED kecuali salah satu dari berikut ini terjadi:

- RecordStateperubahan dari ARCHIVED keACTIVE.
- Compliance.Statusperubahan dari PASSED keFAILED,WARNING, atauNOT_AVAILABLE.

Dalam kasus tersebut, status alur kerja diatur ulang secara otomatis. NEW

Untuk temuan dari kontrol, jika Compliance.Status adaPASSED, Security Hub CSPM secara otomatis menyetel status alur kerja ke. RESOLVED

Mengatur status alur kerja temuan

Untuk mengubah status alur kerja dari satu atau beberapa temuan, Anda dapat menggunakan konsol CSPM Security Hub atau Security Hub CSPM API. Jika Anda mengubah status alur kerja temuan, perhatikan bahwa CSPM Security Hub dapat memakan waktu beberapa menit untuk memproses permintaan Anda dan memperbarui temuannya.

Tip

Anda juga dapat mengubah status alur kerja temuan secara otomatis dengan menggunakan aturan otomatisasi. Dengan aturan otomatisasi, Anda mengonfigurasi CSPM Security Hub untuk memperbarui status alur kerja temuan secara otomatis berdasarkan kriteria yang Anda tentukan. Untuk informasi selengkapnya, lihat [Memahami aturan otomatisasi di Security Hub CSPM](#).

Untuk mengubah status alur kerja dari satu atau beberapa temuan, pilih metode pilihan Anda dan ikuti langkah-langkahnya.

Security Hub CSPM console

Untuk mengubah status alur kerja temuan

1. Buka konsol AWS Security Hub Cloud Security Posture Management (CSPM) di <https://console.aws.amazon.com/securityhub/>
2. Di panel navigasi, lakukan salah satu hal berikut untuk menampilkan tabel temuan:
 - Pilih Temuan.
 - Pilih Wawasan. Kemudian pilih wawasan. Dalam hasil wawasan, pilih hasilnya.
 - Pilih Integrasi. Kemudian, di bagian untuk integrasi, pilih Lihat temuan.
 - Pilih standar keamanan. Kemudian, di bagian untuk standar, pilih Lihat hasil. Dalam tabel kontrol, pilih kontrol untuk menampilkan temuan untuk kontrol.
3. Dalam tabel temuan, pilih kotak centang untuk setiap temuan yang status alur kerjanya ingin Anda ubah.
4. Di bagian atas halaman, pilih Status alur kerja, lalu pilih status alur kerja baru untuk temuan yang dipilih.

5. Dalam kotak dialog Setel status alur kerja, secara opsional masukkan catatan yang merinci alasan untuk mengubah status alur kerja. Kemudian pilih Tetapkan status.

Security Hub CSPM API

Gunakan [BatchUpdateFindings](#) operasi. Berikan ID temuan dan ARN dari produk yang menghasilkan temuan. Anda bisa mendapatkan detail ini dengan menggunakan [GetFindings](#) operasi.

AWS CLI

Jalankan perintah [batch-update-findings](#). Berikan ID temuan dan ARN dari produk yang menghasilkan temuan. Anda bisa mendapatkan detail ini dengan menjalankan perintah [get-findings](#).

```
batch-update-findings --finding-identifiers
  Id="<findingID>",ProductArn="<productARN>" --workflow Status="<workflowStatus>"
```

Contoh

```
aws securityhub batch-update-findings --finding-identifiers
  Id="arn:aws:securityhub:us-west-1:123456789012:subscription/
pci-dss/v/3.2.1/PCI.Lambda.2/finding/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111",ProductArn="arn:aws:securityhub:us-west-1::product/aws/securityhub" --
workflow Status="RESOLVED"
```

Mengirim temuan ke tindakan CSPM Security Hub kustom

Anda dapat membuat tindakan kustom AWS Security Hub Cloud Security Posture Management (CSPM) untuk mengotomatiskan Security Hub CSPM dengan Amazon. EventBridge Untuk tindakan kustom, jenis acara adalah Security Hub Findings - Custom Action. Setelah menyiapkan tindakan kustom, Anda dapat mengirim temuan ke sana. Untuk informasi selengkapnya dan langkah-langkah mendetail dalam membuat tindakan kustom, lihat [the section called “Respon dan remediasi otomatis”](#).

Untuk mengirim temuan ke tindakan kustom (konsol)

1. Buka konsol AWS Security Hub Cloud Security Posture Management (CSPM) di <https://console.aws.amazon.com/securityhub/>
2. Untuk menampilkan daftar temuan, lakukan salah satu hal berikut:

- Di panel navigasi CSPM Security Hub, pilih Temuan.
 - Di panel navigasi CSPM Security Hub, pilih Wawasan. Pilih wawasan. Kemudian pada daftar hasil, pilih hasil wawasan.
 - Di panel navigasi CSPM Security Hub, pilih Integrasi. Pilih Lihat temuan untuk integrasi.
 - Di panel navigasi CSPM Security Hub, pilih Standar keamanan. Pilih Lihat hasil untuk menampilkan daftar kontrol. Kemudian pilih nama kontrol.
3. Dalam daftar temuan, pilih kotak centang untuk setiap temuan untuk dikirim ke tindakan kustom.
- Anda dapat mengirim hingga 20 temuan sekaligus.
4. Untuk Tindakan, pilih tindakan kustom.

AWS Format Pencarian Keamanan (ASFF)

AWS Security Hub Cloud Security Posture Management (CSPM) mengkonsumsi dan mengumpulkan temuan dari produk terintegrasi Layanan AWS dan pihak ketiga. Security Hub CSPM memproses temuan ini menggunakan format temuan standar yang disebut AWS Security Finding Format (ASFF), yang menghilangkan kebutuhan akan upaya konversi data yang memakan waktu.

Halaman ini memberikan garis besar lengkap JSON untuk temuan di AWS Security Finding Format (ASFF). Formatnya berasal dari Skema [JSON](#). Pilih nama objek tertaut untuk meninjau contoh temuan untuk objek itu. Membandingkan temuan CSPM Security Hub Anda dengan sumber daya dan contoh yang ditampilkan di sini dapat membantu Anda menafsirkan temuan Anda.

Untuk deskripsi atribut ASFF individu, lihat [the section called “Atribut ASFF tingkat atas yang diperlukan”](#) dan [the section called “Atribut ASFF tingkat atas opsional”](#)

```
"Findings": [  
  {  
    "Action": {  
      "ActionType": "string",  
      "AwsApiCallAction": {  
        "AffectedResources": {  
          "string": "string"  
        },  
        "Api": "string",  
        "CallerType": "string",  
        "DomainDetails": {  
          "Domain": "string"  
        }  
      }  
    }  
  }  
]
```

```
},
"FirstSeen": "string",
"LastSeen": "string",
"RemoteIpDetails": {
  "City": {
    "CityName": "string"
  },
  "Country": {
    "CountryCode": "string",
    "CountryName": "string"
  },
  "IpAddressV4": "string",
  "Geolocation": {
    "Lat": number,
    "Lon": number
  },
  "Organization": {
    "Asn": number,
    "AsnOrg": "string",
    "Isp": "string",
    "Org": "string"
  }
},
"ServiceName": "string"
},
"DnsRequestAction": {
  "Blocked": boolean,
  "Domain": "string",
  "Protocol": "string"
},
"NetworkConnectionAction": {
  "Blocked": boolean,
  "ConnectionDirection": "string",
  "LocalPortDetails": {
    "Port": number,
    "PortName": "string"
  },
  "Protocol": "string",
  "RemoteIpDetails": {
    "City": {
      "CityName": "string"
    },
    "Country": {
      "CountryCode": "string",
```

```
    "CountryName": "string"
  },
  "IpAddressV4": "string",
  "Geolocation": {
    "Lat": number,
    "Lon": number
  },
  "Organization": {
    "Asn": number,
    "AsnOrg": "string",
    "Isp": "string",
    "Org": "string"
  }
},
"RemotePortDetails": {
  "Port": number,
  "PortName": "string"
}
},
"PortProbeAction": {
  "Blocked": boolean,
  "PortProbeDetails": [{
    "LocalIpDetails": {
      "IpAddressV4": "string"
    },
    "LocalPortDetails": {
      "Port": number,
      "PortName": "string"
    },
    "RemoteIpDetails": {
      "City": {
        "CityName": "string"
      },
      "Country": {
        "CountryCode": "string",
        "CountryName": "string"
      },
      "GeoLocation": {
        "Lat": number,
        "Lon": number
      },
      "IpAddressV4": "string",
      "Organization": {
        "Asn": number,
```



```

        "AsnOrg": "string",
        "Isp": "string",
        "Org": "string"
    }
}
]]
}
},
"AwsAccountId": "string",
"AwsAccountName": "string",
"CompanyName": "string",
"Compliance": {
    "AssociatedStandards": [{
        "StandardsId": "string"
    }],
    "RelatedRequirements": ["string"],
    "SecurityControlId": "string",
    "SecurityControlParameters": [
        {
            "Name": "string",
            "Value": ["string"]
        }
    ],
    "Status": "string",
    "StatusReasons": [
        {
            "Description": "string",
            "ReasonCode": "string"
        }
    ]
},
"Confidence": number,
"CreatedAt": "string",
"Criticality": number,
"Description": "string",
"Detection": {
    "Sequence": {
        "Uid": "string",
        "Actors": [{
            "Id": "string",
            "Session": {
                "Uid": "string",
                "MfaStatus": "string",
                "CreatedTime": "string",

```

```
    "Issuer": "string"
  },
  "User": {
    "CredentialUid": "string",
    "Name": "string",
    "Type": "string",
    "Uid": "string",
    "Account": {
      "Uid": "string",
      "Name": "string"
    }
  }
}],
"Endpoints": [{
  "Id": "string",
  "Ip": "string",
  "Domain": "string",
  "Port": number,
  "Location": {
    "City": "string",
    "Country": "string",
    "Lat": number,
    "Lon": number
  },
  "AutonomousSystem": {
    "Name": "string",
    "Number": number
  },
  "Connection": {
    "Direction": "string"
  }
}],
"Signals": [{
  "Id": "string",
  "Title": "string",
  "ActorIds": ["string"],
  "Count": number,
  "FirstSeenAt": number,
  "SignalIndicators": [
    {
      "Key": "string",
      "Title": "string",
      "Values": ["string"]
    }
  ],
  "Values": ["string"]
}],
}
```

```

    {
      "Key": "string",
      "Title": "string",
      "Values": ["string"]
    }
  ],
  "LastSeenAt": number,
  "Name": "string",
  "ResourceIds": ["string"],
  "Type": "string"
}],
"SequenceIndicators": [
  {
    "Key": "string",
    "Title": "string",
    "Values": ["string"]
  },
  {
    "Key": "string",
    "Title": "string",
    "Values": ["string"]
  }
]
},
"FindingProviderFields": {
  "Confidence": number,
  "Criticality": number,
  "RelatedFindings": [{
    "ProductArn": "string",
    "Id": "string"
  }],
  "Severity": {
    "Label": "string",
    "Normalized": number,
    "Original": "string"
  },
  "Types": ["string"]
},
"FirstObservedAt": "string",
"GeneratorId": "string",
"Id": "string",
"LastObservedAt": "string",
"Malware": [{

```

```
"Name": "string",
"Path": "string",
"State": "string",
"Type": "string"
}],
"Network": {
  "DestinationDomain": "string",
  "DestinationIPv4": "string",
  "DestinationIPv6": "string",
  "DestinationPort": number,
  "Direction": "string",
  "OpenPortRange": {
    "Begin": integer,
    "End": integer
  },
  "Protocol": "string",
  "SourceDomain": "string",
  "SourceIPv4": "string",
  "SourceIPv6": "string",
  "SourceMac": "string",
  "SourcePort": number
},
"NetworkPath": [{
  "ComponentId": "string",
  "ComponentType": "string",
  "Egress": {
    "Destination": {
      "Address": ["string"],
      "PortRanges": [{
        "Begin": integer,
        "End": integer
      }]
    },
    "Protocol": "string",
    "Source": {
      "Address": ["string"],
      "PortRanges": [{
        "Begin": integer,
        "End": integer
      }]
    }
  },
  "Ingress": {
    "Destination": {
```

```

    "Address": ["string"],
    "PortRanges": [{
      "Begin": integer,
      "End": integer
    }]
  },
  "Protocol": "string",
  "Source": {
    "Address": ["string"],
    "PortRanges": [{
      "Begin": integer,
      "End": integer
    }]
  }
}],
"Note": {
  "Text": "string",
  "UpdatedAt": "string",
  "UpdatedBy": "string"
},
"PatchSummary": {
  "FailedCount": number,
  "Id": "string",
  "InstalledCount": number,
  "InstalledOtherCount": number,
  "InstalledPendingReboot": number,
  "InstalledRejectedCount": number,
  "MissingCount": number,
  "Operation": "string",
  "OperationEndTime": "string",
  "OperationStartTime": "string",
  "RebootOption": "string"
},
"Process": {
  "LaunchedAt": "string",
  "Name": "string",
  "ParentPid": number,
  "Path": "string",
  "Pid": number,
  "TerminatedAt": "string"
},
"ProductArn": "string",
"ProductFields": {

```

```
    "string": "string"
  },
  "ProductName": "string",
  "RecordState": "string",
  "Region": "string",
  "RelatedFindings": [{
    "Id": "string",
    "ProductArn": "string"
  }],
  "Remediation": {
    "Recommendation": {
      "Text": "string",
      "Url": "string"
    }
  },
  "Resources": [{
    "ApplicationArn": "string",
    "ApplicationName": "string",
    "DataClassification": {
      "DetailedResultsLocation": "string",
      "Result": {
        "AdditionalOccurrences": boolean,
        "CustomDataIdentifiers": {
          "Detections": [{
            "Arn": "string",
            "Count": integer,
            "Name": "string",
            "Occurrences": {
              "Cells": [{
                "CellReference": "string",
                "Column": integer,
                "ColumnName": "string",
                "Row": integer
              }],
              "LineRanges": [{
                "End": integer,
                "Start": integer,
                "StartColumn": integer
              }],
              "OffsetRanges": [{
                "End": integer,
                "Start": integer,
                "StartColumn": integer
              }],
            }
          }
        }
      }
    }
  }],
```

```
"Pages": [{
  "LineRange": {
    "End": integer,
    "Start": integer,
    "StartColumn": integer
  },
  "OffsetRange": {
    "End": integer,
    "Start": integer,
    "StartColumn": integer
  },
  "PageNumber": integer
}],
"Records": [{
  "JsonPath": "string",
  "RecordIndex": integer
}]
}
}],
"TotalCount": integer
},
"MimeType": "string",
"SensitiveData": [{
  "Category": "string",
  "Detections": [{
    "Count": integer,
    "Occurrences": {
      "Cells": [{
        "CellReference": "string",
        "Column": integer,
        "ColumnName": "string",
        "Row": integer
      }],
      "LineRanges": [{
        "End": integer,
        "Start": integer,
        "StartColumn": integer
      }],
      "OffsetRanges": [{
        "End": integer,
        "Start": integer,
        "StartColumn": integer
      }],
      "Pages": [{
```

```

    "LineRange": {
      "End": integer,
      "Start": integer,
      "StartColumn": integer
    },
    "OffsetRange": {
      "End": integer,
      "Start": integer,
      "StartColumn": integer
    },
    "PageNumber": integer
  ]],
  "Records": [{
    "JsonPath": "string",
    "RecordIndex": integer
  }]
},
"Type": "string"
]],
"TotalCount": integer
]],
"SizeClassified": integer,
"Status": {
  "Code": "string",
  "Reason": "string"
}
},
"Details": {
  "AwsAmazonMQBroker": {
    "AutoMinorVersionUpgrade": boolean,
    "BrokerArn": "string",
    "BrokerId": "string",
    "BrokerName": "string",
    "Configuration": {
      "Id": "string",
      "Revision": integer
    },
    "DeploymentMode": "string",
    "EncryptionOptions": {
      "UseAwsOwnedKey": boolean
    },
    "EngineType": "string",
    "EngineVersion": "string",

```



```

    "HostInstanceType": "string",
    "Logs": {
      "Audit": boolean,
      "AuditLogGroup": "string",
      "General": boolean,
      "GeneralLogGroup": "string"
    },
    "MaintenanceWindowStartTime": {
      "DayOfWeek": "string",
      "TimeOfDay": "string",
      "TimeZone": "string"
    },
    "PubliclyAccessible": boolean,
    "SecurityGroups": [
      "string"
    ],
    "StorageType": "string",
    "SubnetIds": [
      "string",
      "string"
    ],
    "Users": [{
      "Username": "string"
    }]
  },
  "AwsApiGatewayRestApi": {
    "ApiKeySource": "string",
    "BinaryMediaTypes": ["string"],
    "CreateDate": "string",
    "Description": "string",
    "EndpointConfiguration": {
      "Types": ["string"]
    },
    "Id": "string",
    "MinimumCompressionSize": number,
    "Name": "string",
    "Version": "string"
  },
  "AwsApiGatewayStage": {
    "AccessLogSettings": {
      "DestinationArn": "string",
      "Format": "string"
    },
    "CacheClusterEnabled": boolean,

```

```

    "CacheClusterSize": "string",
    "CacheClusterStatus": "string",
    "CanarySettings": {
      "DeploymentId": "string",
      "PercentTraffic": number,
      "StageVariableOverrides": [{
        "string": "string"
      }],
      "UseStageCache": boolean
    },
    "ClientCertificateId": "string",
    "CreatedDate": "string",
    "DeploymentId": "string",
    "Description": "string",
    "DocumentationVersion": "string",
    "LastUpdatedDate": "string",
    "MethodSettings": [{
      "CacheDataEncrypted": boolean,
      "CachingEnabled": boolean,
      "CacheTtlInSeconds": number,
      "DataTraceEnabled": boolean,
      "HttpMethod": "string",
      "LoggingLevel": "string",
      "MetricsEnabled": boolean,
      "RequireAuthorizationForCacheControl": boolean,
      "ResourcePath": "string",
      "ThrottlingBurstLimit": number,
      "ThrottlingRateLimit": number,
      "UnauthorizedCacheControlHeaderStrategy": "string"
    }],
    "StageName": "string",
    "TracingEnabled": boolean,
    "Variables": {
      "string": "string"
    },
    "WebAclArn": "string"
  },
  "AwsApiGatewayV2Api": {
    "ApiEndpoint": "string",
    "ApiId": "string",
    "ApiKeySelectionExpression": "string",
    "CorsConfiguration": {
      "AllowCredentials": boolean,
      "AllowHeaders": ["string"],

```

```

    "AllowMethods": ["string"],
    "AllowOrigins": ["string"],
    "ExposeHeaders": ["string"],
    "MaxAge": number
  },
  "CreateDate": "string",
  "Description": "string",
  "Name": "string",
  "ProtocolType": "string",
  "RouteSelectionExpression": "string",
  "Version": "string"
},
"AwsApiGatewayV2Stage": {
  "AccessLogSettings": {
    "DestinationArn": "string",
    "Format": "string"
  },
  "ApiGatewayManaged": boolean,
  "AutoDeploy": boolean,
  "ClientCertificateId": "string",
  "CreateDate": "string",
  "DefaultRouteSettings": {
    "DataTraceEnabled": boolean,
    "DetailedMetricsEnabled": boolean,
    "LoggingLevel": "string",
    "ThrottlingBurstLimit": number,
    "ThrottlingRateLimit": number
  },
  "DeploymentId": "string",
  "Description": "string",
  "LastDeploymentStatusMessage": "string",
  "LastUpdatedDate": "string",
  "RouteSettings": {
    "DetailedMetricsEnabled": boolean,
    "LoggingLevel": "string",
    "DataTraceEnabled": boolean,
    "ThrottlingBurstLimit": number,
    "ThrottlingRateLimit": number
  },
  "StageName": "string",
  "StageVariables": [{
    "string": "string"
  }]
},

```

```

"AwsAppSyncGraphQLApi": {
  "AwsAppSyncGraphQLApi": {
    "AdditionalAuthenticationProviders": [
      {
        "AuthenticationType": "string",
        "LambdaAuthorizerConfig": {
          "AuthorizerResultTtlInSeconds": integer,
          "AuthorizerUri": "string"
        }
      },
      {
        "AuthenticationType": "string"
      }
    ],
    "ApiId": "string",
    "Arn": "string",
    "AuthenticationType": "string",
    "Id": "string",
    "LogConfig": {
      "CloudWatchLogsRoleArn": "string",
      "ExcludeVerboseContent": boolean,
      "FieldLogLevel": "string"
    },
    "Name": "string",
    "XrayEnabled": boolean
  }
},
"AwsAthenaWorkGroup": {
  "Description": "string",
  "Name": "string",
  "WorkgroupConfiguration": {
    "ResultConfiguration": {
      "EncryptionConfiguration": {
        "EncryptionOption": "string",
        "KmsKey": "string"
      }
    }
  },
  "State": "string"
},
"AwsAutoScalingAutoScalingGroup": {
  "AvailabilityZones": [{
    "Value": "string"
  }],

```

```

    "CreatedTime": "string",
    "HealthCheckGracePeriod": integer,
    "HealthCheckType": "string",
    "LaunchConfigurationName": "string",
    "LoadBalancerNames": ["string"],
    "LaunchTemplate": {
        "LaunchTemplateId": "string",
        "LaunchTemplateName": "string",
        "Version": "string"
    },
    "MixedInstancesPolicy": {
        "InstancesDistribution": {
            "OnDemandAllocationStrategy": "string",
            "OnDemandBaseCapacity": number,
            "OnDemandPercentageAboveBaseCapacity": number,
            "SpotAllocationStrategy": "string",
            "SpotInstancePools": number,
            "SpotMaxPrice": "string"
        },
        "LaunchTemplate": {
            "LaunchTemplateSpecification": {
                "LaunchTemplateId": "string",
                "LaunchTemplateName": "string",
                "Version": "string"
            },
            "CapacityRebalance": boolean,
            "Overrides": [{
                "InstanceType": "string",
                "WeightedCapacity": "string"
            }]
        }
    },
    "AwsAutoScalingLaunchConfiguration": {
        "AssociatePublicIpAddress": boolean,
        "BlockDeviceMappings": [{
            "DeviceName": "string",
            "Ebs": {
                "DeleteOnTermination": boolean,
                "Encrypted": boolean,
                "Iops": number,
                "SnapshotId": "string",
                "VolumeSize": number,
                "VolumeType": "string"
            }
        }]
    }
}

```

```

    },
    "NoDevice": boolean,
    "VirtualName": "string"
  ]],
  "ClassicLinkVpcId": "string",
  "ClassicLinkVpcSecurityGroups": ["string"],
  "CreatedTime": "string",
  "EbsOptimized": boolean,
  "IamInstanceProfile": "string"
},
"ImageId": "string",
"InstanceMonitoring": {
  "Enabled": boolean
},
"InstanceType": "string",
"KernelId": "string",
"KeyName": "string",
"LaunchConfigurationName": "string",
"MetadataOptions": {
  "HttpEndPoint": "string",
  "HttpPutReponseHopLimit": number,
  "HttpTokens": "string"
},
"PlacementTenancy": "string",
"RamdiskId": "string",
"SecurityGroups": ["string"],
"SpotPrice": "string",
"UserData": "string"
},
"AwsBackupBackupPlan": {
  "BackupPlan": {
    "AdvancedBackupSettings": [{
      "BackupOptions": {
        "WindowsVSS": "string"
      },
      "ResourceType": "string"
    }],
    "BackupPlanName": "string",
    "BackupPlanRule": [{
      "CompletionWindowMinutes": integer,
      "CopyActions": [{
        "DestinationBackupVaultArn": "string",
        "Lifecycle": {
          "DeleteAfterDays": integer,

```

```

        "MoveToColdStorageAfterDays": integer
    }
  ]],
  "Lifecycle": {
    "DeleteAfterDays": integer
  },
  "RuleName": "string",
  "ScheduleExpression": "string",
  "StartWindowMinutes": integer,
  "TargetBackupVault": "string"
  ]]
},
"BackupPlanArn": "string",
"BackupPlanId": "string",
"VersionId": "string"
},
"AwsBackupBackupVault": {
  "AccessPolicy": {
    "Statement": [{
      "Action": ["string"],
      "Effect": "string",
      "Principal": {
        "AWS": "string"
      },
      "Resource": "string"
    }],
    "Version": "string"
  },
  "BackupVaultArn": "string",
  "BackupVaultName": "string",
  "EncryptionKeyArn": "string",
  "Notifications": {
    "BackupVaultEvents": ["string"],
    "SNSTopicArn": "string"
  }
},
"AwsBackupRecoveryPoint": {
  "BackupSizeInBytes": integer,
  "BackupVaultName": "string",
  "BackupVaultArn": "string",
  "CalculatedLifecycle": {
    "DeleteAt": "string",
    "MoveToColdStorageAt": "string"
  }
},

```

```

"CompletionDate": "string",
"CreatedBy": {
  "BackupPlanArn": "string",
  "BackupPlanId": "string",
  "BackupPlanVersion": "string",
  "BackupRuleId": "string"
},
"CreationDate": "string",
"EncryptionKeyArn": "string",
"IamRoleArn": "string",
"IsEncrypted": boolean,
"LastRestoreTime": "string",
"Lifecycle": {
  "DeleteAfterDays": integer,
  "MoveToColdStorageAfterDays": integer
},
"RecoveryPointArn": "string",
"ResourceArn": "string",
"ResourceType": "string",
"SourceBackupVaultArn": "string",
"Status": "string",
"StatusMessage": "string",
"StorageClass": "string"
},
"AwsCertificateManagerCertificate": {
  "CertificateAuthorityArn": "string",
  "CreatedAt": "string",
  "DomainName": "string",
  "DomainValidationOptions": [{
    "DomainName": "string",
    "ResourceRecord": {
      "Name": "string",
      "Type": "string",
      "Value": "string"
    },
    "ValidationDomain": "string",
    "ValidationEmails": ["string"],
    "ValidationMethod": "string",
    "ValidationStatus": "string"
  }],
  "ExtendedKeyUsages": [{
    "Name": "string",
    "Oid": "string"
  }],

```



```

"FailureReason": "string",
"ImportedAt": "string",
"InUseBy": ["string"],
"IssuedAt": "string",
"Issuer": "string",
"KeyAlgorithm": "string",
"KeyUsages": [{
  "Name": "string"
}],
"NotAfter": "string",
"NotBefore": "string",
"Options": {
  "CertificateTransparencyLoggingPreference": "string"
},
"RenewalEligibility": "string",
"RenewalSummary": {
  "DomainValidationOptions": [{
    "DomainName": "string",
    "ResourceRecord": {
      "Name": "string",
      "Type": "string",
      "Value": "string"
    },
    "ValidationDomain": "string",
    "ValidationEmails": ["string"],
    "ValidationMethod": "string",
    "ValidationStatus": "string"
  }],
  "RenewalStatus": "string",
  "RenewalStatusReason": "string",
  "UpdatedAt": "string"
},
"Serial": "string",
"SignatureAlgorithm": "string",
"Status": "string",
"Subject": "string",
"SubjectAlternativeNames": ["string"],
"Type": "string"
},
"awsCloudFormationStack": {
  "Capabilities": ["string"],
  "CreationTime": "string",
  "Description": "string",
  "DisableRollback": boolean,

```

```

    "DriftInformation": {
      "StackDriftStatus": "string"
    },
    "EnableTerminationProtection": boolean,
    "LastUpdatedTime": "string",
    "NotificationArns": ["string"],
    "Outputs": [{
      "Description": "string",
      "OutputKey": "string",
      "OutputValue": "string"
    }],
    "RoleArn": "string",
    "StackId": "string",
    "StackName": "string",
    "StackStatus": "string",
    "StackStatusReason": "string",
    "TimeoutInMinutes": number
  },
  "AwsCloudFrontDistribution": {
    "CacheBehaviors": {
      "Items": [{
        "ViewerProtocolPolicy": "string"
      }]
    },
    "DefaultCacheBehavior": {
      "ViewerProtocolPolicy": "string"
    },
    "DefaultRootObject": "string",
    "DomainName": "string",
    "Etag": "string",
    "LastModifiedTime": "string",
    "Logging": {
      "Bucket": "string",
      "Enabled": boolean,
      "IncludeCookies": boolean,
      "Prefix": "string"
    },
    "OriginGroups": {
      "Items": [{
        "FailoverCriteria": {
          "StatusCodes": {
            "Items": [number],
            "Quantity": number
          }
        }
      }]
    }
  }
}

```

```

    }
  ]]
},
"Origins": {
  "Items": [{
    "CustomOriginConfig": {
      "HttpPort": number,
      "HttpsPort": number,
      "OriginKeepaliveTimeout": number,
      "OriginProtocolPolicy": "string",
      "OriginReadTimeout": number,
      "OriginSslProtocols": {
        "Items": ["string"],
        "Quantity": number
      }
    },
    "DomainName": "string",
    "Id": "string",
    "OriginPath": "string",
    "S3OriginConfig": {
      "OriginAccessIdentity": "string"
    }
  }]
},
"Status": "string",
"ViewerCertificate": {
  "AcmCertificateArn": "string",
  "Certificate": "string",
  "CertificateSource": "string",
  "CloudFrontDefaultCertificate": boolean,
  "IamCertificateId": "string",
  "MinimumProtocolVersion": "string",
  "SslSupportMethod": "string"
},
"WebAclId": "string"
},
"AwsCloudTrailTrail": {
  "CloudWatchLogsLogGroupArn": "string",
  "CloudWatchLogsRoleArn": "string",
  "HasCustomEventSelectors": boolean,
  "HomeRegion": "string",
  "IncludeGlobalServiceEvents": boolean,
  "IsMultiRegionTrail": boolean,
  "IsOrganizationTrail": boolean,

```

```

    "KmsKeyId": "string",
    "LogFileValidationEnabled": boolean,
    "Name": "string",
    "S3BucketName": "string",
    "S3KeyPrefix": "string",
    "SnsTopicArn": "string",
    "SnsTopicName": "string",
    "TrailArn": "string"
  },
  "AwsCloudWatchAlarm": {
    "ActionsEnabled": boolean,
    "AlarmActions": ["string"],
    "AlarmArn": "string",
    "AlarmConfigurationUpdatedTimestamp": "string",
    "AlarmDescription": "string",
    "AlarmName": "string",
    "ComparisonOperator": "string",
    "DatapointsToAlarm": number,
    "Dimensions": [{
      "Name": "string",
      "Value": "string"
    }],
    "EvaluateLowSampleCountPercentile": "string",
    "EvaluationPeriods": number,
    "ExtendedStatistic": "string",
    "InsufficientDataActions": ["string"],
    "MetricName": "string",
    "Namespace": "string",
    "OkActions": ["string"],
    "Period": number,
    "Statistic": "string",
    "Threshold": number,
    "ThresholdMetricId": "string",
    "TreatMissingData": "string",
    "Unit": "string"
  },
  "AwsCodeBuildProject": {
    "Artifacts": [{
      "ArtifactIdentifier": "string",
      "EncryptionDisabled": boolean,
      "Location": "string",
      "Name": "string",
      "NamespaceType": "string",
      "OverrideArtifactName": boolean,

```

```

    "Packaging": "string",
    "Path": "string",
    "Type": "string"
  }],
  "SecondaryArtifacts": [{
    "ArtifactIdentifier": "string",
    "Type": "string",
    "Location": "string",
    "Name": "string",
    "NamespaceType": "string",
    "Packaging": "string",
    "Path": "string",
    "EncryptionDisabled": boolean,
    "OverrideArtifactName": boolean
  }],
  "EncryptionKey": "string",
  "Certificate": "string",
  "Environment": {
    "Certificate": "string",
    "EnvironmentVariables": [{
      "Name": "string",
      "Type": "string",
      "Value": "string"
    }],
    "ImagePullCredentialsType": "string",
    "PrivilegedMode": boolean,
    "RegistryCredential": {
      "Credential": "string",
      "CredentialProvider": "string"
    },
    "Type": "string"
  },
  "LogsConfig": {
    "CloudWatchLogs": {
      "GroupName": "string",
      "Status": "string",
      "StreamName": "string"
    },
    "S3Logs": {
      "EncryptionDisabled": boolean,
      "Location": "string",
      "Status": "string"
    }
  }
},

```

```
"Name": "string",
"ServiceRole": "string",
"Source": {
  "Type": "string",
  "Location": "string",
  "GitCloneDepth": integer
},
"VpcConfig": {
  "VpcId": "string",
  "Subnets": ["string"],
  "SecurityGroupIds": ["string"]
},
"AwsDmsEndpoint": {
  "CertificateArn": "string",
  "DatabaseName": "string",
  "EndpointArn": "string",
  "EndpointIdentifier": "string",
  "EndpointType": "string",
  "EngineName": "string",
  "KmsKeyId": "string",
  "Port": integer,
  "ServerName": "string",
  "SslMode": "string",
  "Username": "string"
},
"AwsDmsReplicationInstance": {
  "AllocatedStorage": integer,
  "AutoMinorVersionUpgrade": boolean,
  "AvailabilityZone": "string",
  "EngineVersion": "string",
  "KmsKeyId": "string",
  "MultiAZ": boolean,
  "PreferredMaintenanceWindow": "string",
  "PubliclyAccessible": boolean,
  "ReplicationInstanceClass": "string",
  "ReplicationInstanceIdentifier": "string",
  "ReplicationSubnetGroup": {
    "ReplicationSubnetGroupIdentifier": "string"
  },
  "VpcSecurityGroups": [
    {
      "VpcSecurityGroupId": "string"
    }
  ]
}
```

```

    ]
  },
  "AwsDmsReplicationTask": {
    "CdcStartPosition": "string",
    "Id": "string",
    "MigrationType": "string",
    "ReplicationInstanceArn": "string",
    "ReplicationTaskIdentifier": "string",
    "ReplicationTaskSettings": {
      "string": "string"
    },
    "SourceEndpointArn": "string",
    "TableMappings": {
      "string": "string"
    },
    "TargetEndpointArn": "string"
  },
  "AwsDynamoDbTable": {
    "AttributeDefinitions": [{
      "AttributeName": "string",
      "AttributeType": "string"
    }],
    "BillingModeSummary": {
      "BillingMode": "string",
      "LastUpdateToPayPerRequestDateTime": "string"
    },
    "CreationDateTime": "string",
    "DeletionProtectionEnabled": boolean,
    "GlobalSecondaryIndexes": [{
      "Backfilling": boolean,
      "IndexArn": "string",
      "IndexName": "string",
      "IndexSizeBytes": number,
      "IndexStatus": "string",
      "ItemCount": number,
      "KeySchema": [{
        "AttributeName": "string",
        "KeyType": "string"
      }],
      "Projection": {
        "NonKeyAttributes": ["string"],
        "ProjectionType": "string"
      },
      "ProvisionedThroughput": {

```

```

        "LastDecreaseDateTime": "string",
        "LastIncreaseDateTime": "string",
        "NumberOfDecreasesToday": number,
        "ReadCapacityUnits": number,
        "WriteCapacityUnits": number
    }
}],
"GlobalTableVersion": "string",
"ItemCount": number,
"KeySchema": [{
    "AttributeName": "string",
    "KeyType": "string"
}],
"LatestStreamArn": "string",
"LatestStreamLabel": "string",
"LocalSecondaryIndexes": [{
    "IndexArn": "string",
    "IndexName": "string",
    "KeySchema": [{
        "AttributeName": "string",
        "KeyType": "string"
    }],
    "Projection": {
        "NonKeyAttributes": ["string"],
        "ProjectionType": "string"
    }
}],
"ProvisionedThroughput": {
    "LastDecreaseDateTime": "string",
    "LastIncreaseDateTime": "string",
    "NumberOfDecreasesToday": number,
    "ReadCapacityUnits": number,
    "WriteCapacityUnits": number
},
"Replicas": [{
    "GlobalSecondaryIndexes": [{
        "IndexName": "string",
        "ProvisionedThroughputOverride": {
            "ReadCapacityUnits": number
        }
    }],
    "KmsMasterKeyId": "string",
    "ProvisionedThroughputOverride": {
        "ReadCapacityUnits": number
    }
}

```



```

    },
    "RegionName": "string",
    "ReplicaStatus": "string",
    "ReplicaStatusDescription": "string"
  ]],
  "RestoreSummary": {
    "RestoreDateTime": "string",
    "RestoreInProgress": boolean,
    "SourceBackupArn": "string",
    "SourceTableArn": "string"
  },
  "SseDescription": {
    "InaccessibleEncryptionDateTime": "string",
    "KmsMasterKeyArn": "string",
    "SseType": "string",
    "Status": "string"
  },
  "StreamSpecification": {
    "StreamEnabled": boolean,
    "StreamViewType": "string"
  },
  "TableId": "string",
  "TableName": "string",
  "TableSizeBytes": number,
  "TableStatus": "string"
},
"AwsEc2ClientVpnEndpoint": {
  "AuthenticationOptions": [
    {
      "MutualAuthentication": {
        "ClientRootCertificateChainArn": "string"
      },
      "Type": "string"
    }
  ],
  "ClientCidrBlock": "string",
  "ClientConnectOptions": {
    "Enabled": boolean
  },
  "ClientLoginBannerOptions": {
    "Enabled": boolean
  },
  "ClientVpnEndpointId": "string",
  "ConnectionLogOptions": {

```

```
    "Enabled": boolean
  },
  "Description": "string",
  "DnsServer": ["string"],
  "ServerCertificateArn": "string",
  "SecurityGroupIdSet": [
    "string"
  ],
  "SelfServicePortalUrl": "string",
  "SessionTimeoutHours": "integer",
  "SplitTunnel": boolean,
  "TransportProtocol": "string",
  "VpcId": "string",
  "VpnPort": integer
},
"AwsEc2Eip": {
  "AllocationId": "string",
  "AssociationId": "string",
  "Domain": "string",
  "InstanceId": "string",
  "NetworkBorderGroup": "string",
  "NetworkInterfaceId": "string",
  "NetworkInterfaceOwnerId": "string",
  "PrivateIpAddress": "string",
  "PublicIp": "string",
  "PublicIpv4Pool": "string"
},
"AwsEc2Instance": {
  "IamInstanceProfileArn": "string",
  "ImageId": "string",
  "IPv4Addresses": ["string"],
  "IPv6Addresses": ["string"],
  "KeyName": "string",
  "LaunchedAt": "string",
  "MetadataOptions": {
    "HttpEndpoint": "string",
    "HttpProtocolIpv6": "string",
    "HttpPutResponseHopLimit": number,
    "HttpTokens": "string",
    "InstanceMetadataTags": "string"
  },
  "Monitoring": {
    "State": "string"
  }
},
```

```

    "NetworkInterfaces": [{
      "NetworkInterfaceId": "string"
    }],
    "SubnetId": "string",
    "Type": "string",
    "VirtualizationType": "string",
    "VpcId": "string"
  },
  "AwsEc2LaunchTemplate": {
    "DefaultVersionNumber": "string",
    "ElasticGpuSpecifications": ["string"],
    "ElasticInferenceAccelerators": ["string"],
    "Id": "string",
    "ImageId": "string",
    "LatestVersionNumber": "string",
    "LaunchTemplateData": {
      "BlockDeviceMappings": [{
        "DeviceName": "string",
        "Ebs": {
          "DeleteonTermination": boolean,
          "Encrypted": boolean,
          "SnapshotId": "string",
          "VolumeSize": number,
          "VolumeType": "string"
        }
      }],
      "MetadataOptions": {
        "HttpTokens": "string",
        "HttpPutResponseHopLimit" : number
      },
      "Monitoring": {
        "Enabled": boolean
      },
      "NetworkInterfaces": [{
        "AssociatePublicIpAddress" : boolean
      }]
    },
    "LaunchTemplateName": "string",
    "LicenseSpecifications": ["string"],
    "SecurityGroupIds": ["string"],
    "SecurityGroups": ["string"],
    "TagSpecifications": ["string"]
  },
  "AwsEc2NetworkAcl": {

```

```

"Associations": [{
  "NetworkAclAssociationId": "string",
  "NetworkAclId": "string",
  "SubnetId": "string"
}],
"Entries": [{
  "CidrBlock": "string",
  "Egress": boolean,
  "IcmpTypeCode": {
    "Code": number,
    "Type": number
  },
  "Ipv6CidrBlock": "string",
  "PortRange": {
    "From": number,
    "To": number
  },
  "Protocol": "string",
  "RuleAction": "string",
  "RuleNumber": number
}],
"IsDefault": boolean,
"NetworkAclId": "string",
"OwnerId": "string",
"VpcId": "string"
},
"AwsEc2NetworkInterface": {
  "Attachment": {
    "AttachmentId": "string",
    "AttachTime": "string",
    "DeleteOnTermination": boolean,
    "DeviceIndex": number,
    "InstanceId": "string",
    "InstanceOwnerId": "string",
    "Status": "string"
  },
  "Ipv6Addresses": [{
    "Ipv6Address": "string"
  }],
  "NetworkInterfaceId": "string",
  "PrivateIpAddresses": [{
    "PrivateDnsName": "string",
    "PrivateIpAddress": "string"
  }],

```

```

    "PublicDnsName": "string",
    "PublicIp": "string",
    "SecurityGroups": [{
      "GroupId": "string",
      "GroupName": "string"
    }],
    "SourceDestCheck": boolean
  },
  "AwsEc2RouteTable": {
    "AssociationSet": [{
      "AssociationState": {
        "State": "string"
      },
      "Main": boolean,
      "RouteTableAssociationId": "string",
      "RouteTableId": "string"
    }],
    "PropogatingVgwSet": [],
    "RouteTableId": "string",
    "RouteSet": [
      {
        "DestinationCidrBlock": "string",
        "GatewayId": "string",
        "Origin": "string",
        "State": "string"
      },
      {
        "DestinationCidrBlock": "string",
        "GatewayId": "string",
        "Origin": "string",
        "State": "string"
      }
    ],
    "VpcId": "string"
  },
  "AwsEc2SecurityGroup": {
    "GroupId": "string",
    "GroupName": "string",
    "IpPermissions": [{
      "FromPort": number,
      "IpProtocol": "string",
      "IpRanges": [{
        "CidrIp": "string"
      }],

```

```

    "Ipv6Ranges": [{
      "CidrIpv6": "string"
    }],
    "PrefixListIds": [{
      "PrefixListId": "string"
    }],
    "ToPort": number,
    "UserIdGroupPairs": [{
      "GroupId": "string",
      "GroupName": "string",
      "PeeringStatus": "string",
      "UserId": "string",
      "VpcId": "string",
      "VpcPeeringConnectionId": "string"
    }]
  }],
  "IpPermissionsEgress": [{
    "FromPort": number,
    "IpProtocol": "string",
    "IpRanges": [{
      "CidrIp": "string"
    }],
    "Ipv6Ranges": [{
      "CidrIpv6": "string"
    }],
    "PrefixListIds": [{
      "PrefixListId": "string"
    }],
    "ToPort": number,
    "UserIdGroupPairs": [{
      "GroupId": "string",
      "GroupName": "string",
      "PeeringStatus": "string",
      "UserId": "string",
      "VpcId": "string",
      "VpcPeeringConnectionId": "string"
    }]
  }],
  "OwnerId": "string",
  "VpcId": "string"
},
"AwsEc2Subnet": {
  "AssignIpv6AddressOnCreation": boolean,
  "AvailabilityZone": "string",

```

```

    "AvailabilityZoneId": "string",
    "AvailableIpAddressCount": number,
    "CidrBlock": "string",
    "DefaultForAz": boolean,
    "Ipv6CidrBlockAssociationSet": [{
      "AssociationId": "string",
      "Ipv6CidrBlock": "string",
      "CidrBlockState": "string"
    }],
    "MapPublicIpOnLaunch": boolean,
    "OwnerId": "string",
    "State": "string",
    "SubnetArn": "string",
    "SubnetId": "string",
    "VpcId": "string"
  },
  "AwsEc2TransitGateway": {
    "AmazonSideAsn": number,
    "AssociationDefaultRouteTableId": "string",
    "AutoAcceptSharedAttachments": "string",
    "DefaultRouteTableAssociation": "string",
    "DefaultRouteTablePropagation": "string",
    "Description": "string",
    "DnsSupport": "string",
    "Id": "string",
    "MulticastSupport": "string",
    "PropagationDefaultRouteTableId": "string",
    "TransitGatewayCidrBlocks": ["string"],
    "VpnEcmpSupport": "string"
  },
  "AwsEc2Volume": {
    "Attachments": [{
      "AttachTime": "string",
      "DeleteOnTermination": boolean,
      "InstanceId": "string",
      "Status": "string"
    }],
    "CreateTime": "string",
    "DeviceName": "string",
    "Encrypted": boolean,
    "KmsKeyId": "string",
    "Size": number,
    "SnapshotId": "string",
    "Status": "string",

```

```

    "VolumeId": "string",
    "VolumeScanStatus": "string",
    "VolumeType": "string"
  },
  "AwsEc2Vpc": {
    "CidrBlockAssociationSet": [{
      "AssociationId": "string",
      "CidrBlock": "string",
      "CidrBlockState": "string"
    }],
    "DhcpOptionsId": "string",
    "Ipv6CidrBlockAssociationSet": [{
      "AssociationId": "string",
      "CidrBlockState": "string",
      "Ipv6CidrBlock": "string"
    }],
    "State": "string"
  },
  "AwsEc2VpcEndpointService": {
    "AcceptanceRequired": boolean,
    "AvailabilityZones": ["string"],
    "BaseEndpointDnsNames": ["string"],
    "ManagesVpcEndpoints": boolean,
    "GatewayLoadBalancerArns": ["string"],
    "NetworkLoadBalancerArns": ["string"],
    "PrivateDnsName": "string",
    "ServiceId": "string",
    "ServiceName": "string",
    "ServiceState": "string",
    "ServiceType": [{
      "ServiceType": "string"
    }]
  },
  "AwsEc2VpcPeeringConnection": {
    "AcceptorVpcInfo": {
      "CidrBlock": "string",
      "CidrBlockSet": [{
        "CidrBlock": "string"
      }],
      "Ipv6CidrBlockSet": [{
        "Ipv6CidrBlock": "string"
      }],
      "OwnerId": "string",
      "PeeringOptions": {

```



```

    "AllowDnsResolutionFromRemoteVpc": boolean,
    "AllowEgressFromLocalClassicLinkToRemoteVpc": boolean,
    "AllowEgressFromLocalVpcToRemoteClassicLink": boolean
  },
  "Region": "string",
  "VpcId": "string"
},
"ExpirationTime": "string",
"RequesterVpcInfo": {
  "CidrBlock": "string",
  "CidrBlockSet": [{
    "CidrBlock": "string"
  }],
  "Ipv6CidrBlockSet": [{
    "Ipv6CidrBlock": "string"
  }],
  "OwnerId": "string",
  "PeeringOptions": {
    "AllowDnsResolutionFromRemoteVpc": boolean,
    "AllowEgressFromLocalClassicLinkToRemoteVpc": boolean,
    "AllowEgressFromLocalVpcToRemoteClassicLink": boolean
  },
  "Region": "string",
  "VpcId": "string"
},
"Status": {
  "Code": "string",
  "Message": "string"
},
"VpcPeeringConnectionId": "string"
},
"AwsEcrContainerImage": {
  "Architecture": "string",
  "ImageDigest": "string",
  "ImagePublishedAt": "string",
  "ImageTags": ["string"],
  "RegistryId": "string",
  "RepositoryName": "string"
},
"AwsEcrRepository": {
  "Arn": "string",
  "ImageScanningConfiguration": {
    "ScanOnPush": boolean
  },

```

```

    "ImageTagMutability": "string",
    "LifecyclePolicy": {
      "LifecyclePolicyText": "string",
      "RegistryId": "string"
    },
    "RepositoryName": "string",
    "RepositoryPolicyText": "string"
  },
  "AwsEcsCluster": {
    "ActiveServicesCount": number,
    "CapacityProviders": ["string"],
    "ClusterArn": "string",
    "ClusterName": "string",
    "ClusterSettings": [{
      "Name": "string",
      "Value": "string"
    }],
    "Configuration": {
      "ExecuteCommandConfiguration": {
        "KmsKeyId": "string",
        "LogConfiguration": {
          "CloudWatchEncryptionEnabled": boolean,
          "CloudWatchLogGroupName": "string",
          "S3BucketName": "string",
          "S3EncryptionEnabled": boolean,
          "S3KeyPrefix": "string"
        },
        "Logging": "string"
      }
    },
    "DefaultCapacityProviderStrategy": [{
      "Base": number,
      "CapacityProvider": "string",
      "Weight": number
    }],
    "RegisteredContainerInstancesCount": number,
    "RunningTasksCount": number,
    "Status": "string"
  },
  "AwsEcsContainer": {
    "Image": "string",
    "MountPoints": [{
      "ContainerPath": "string",
      "SourceVolume": "string"
    }],

```

```

    }],
    "Name": "string",
    "Privileged": boolean
  },
  "AwsEcsService": {
    "CapacityProviderStrategy": [{
      "Base": number,
      "CapacityProvider": "string",
      "Weight": number
    }],
    "Cluster": "string",
    "DeploymentConfiguration": {
      "DeploymentCircuitBreaker": {
        "Enable": boolean,
        "Rollback": boolean
      },
      "MaximumPercent": number,
      "MinimumHealthyPercent": number
    },
    "DeploymentController": {
      "Type": "string"
    },
    "DesiredCount": number,
    "EnableEcsManagedTags": boolean,
    "EnableExecuteCommand": boolean,
    "HealthCheckGracePeriodSeconds": number,
    "LaunchType": "string",
    "LoadBalancers": [{
      "ContainerName": "string",
      "ContainerPort": number,
      "LoadBalancerName": "string",
      "TargetGroupArn": "string"
    }],
    "Name": "string",
    "NetworkConfiguration": {
      "AwsVpcConfiguration": {
        "AssignPublicIp": "string",
        "SecurityGroups": ["string"],
        "Subnets": ["string"]
      }
    },
    "PlacementConstraints": [{
      "Expression": "string",
      "Type": "string"
    }],

```

```

    ]],
    "PlacementStrategies": [{
      "Field": "string",
      "Type": "string"
    }],
    "PlatformVersion": "string",
    "PropagateTags": "string",
    "Role": "string",
    "SchedulingStrategy": "string",
    "ServiceArn": "string",
    "ServiceName": "string",
    "ServiceRegistries": [{
      "ContainerName": "string",
      "ContainerPort": number,
      "Port": number,
      "RegistryArn": "string"
    }],
    "TaskDefinition": "string"
  },
  "AwsEcsTask": {
    "CreatedAt": "string",
    "ClusterArn": "string",
    "Group": "string",
    "StartedAt": "string",
    "StartedBy": "string",
    "TaskDefinitionArn": "string",
    "Version": number,
    "Volumes": [{
      "Name": "string",
      "Host": {
        "SourcePath": "string"
      }
    }],
    "Containers": [{
      "Image": "string",
      "MountPoints": [{
        "ContainerPath": "string",
        "SourceVolume": "string"
      }],
      "Name": "string",
      "Privileged": boolean
    }]
  },
  "AwsEcsTaskDefinition": {

```

```
"ContainerDefinitions": [{
  "Command": ["string"],
  "Cpu": number,
  "DependsOn": [{
    "Condition": "string",
    "ContainerName": "string"
  }],
  "DisableNetworking": boolean,
  "DnsSearchDomains": ["string"],
  "DnsServers": ["string"],
  "DockerLabels": {
    "string": "string"
  },
  "DockerSecurityOptions": ["string"],
  "EntryPoint": ["string"],
  "Environment": [{
    "Name": "string",
    "Value": "string"
  }],
  "EnvironmentFiles": [{
    "Type": "string",
    "Value": "string"
  }],
  "Essential": boolean,
  "ExtraHosts": [{
    "Hostname": "string",
    "IpAddress": "string"
  }],
  "FirelensConfiguration": {
    "Options": {
      "string": "string"
    },
    "Type": "string"
  },
  "HealthCheck": {
    "Command": ["string"],
    "Interval": number,
    "Retries": number,
    "StartPeriod": number,
    "Timeout": number
  },
  "Hostname": "string",
  "Image": "string",
  "Interactive": boolean,
```

```
"Links": ["string"],
"LinuxParameters": {
  "Capabilities": {
    "Add": ["string"],
    "Drop": ["string"]
  },
  "Devices": [{
    "ContainerPath": "string",
    "HostPath": "string",
    "Permissions": ["string"]
  }],
  "InitProcessEnabled": boolean,
  "MaxSwap": number,
  "SharedMemorySize": number,
  "Swappiness": number,
  "Tmpfs": [{
    "ContainerPath": "string",
    "MountOptions": ["string"],
    "Size": number
  }]
},
"LogConfiguration": {
  "LogDriver": "string",
  "Options": {
    "string": "string"
  },
  "SecretOptions": [{
    "Name": "string",
    "ValueFrom": "string"
  }]
},
"Memory": number,
"MemoryReservation": number,
"MountPoints": [{
  "ContainerPath": "string",
  "ReadOnly": boolean,
  "SourceVolume": "string"
}],
"Name": "string",
"PortMappings": [{
  "ContainerPort": number,
  "HostPort": number,
  "Protocol": "string"
}],
```

```
"Privileged": boolean,
"PseudoTerminal": boolean,
"ReadOnlyRootFilesystem": boolean,
"RepositoryCredentials": {
  "CredentialsParameter": "string"
},
"ResourceRequirements": [{
  "Type": "string",
  "Value": "string"
}],
"Secrets": [{
  "Name": "string",
  "ValueFrom": "string"
}],
"StartTimeout": number,
"StopTimeout": number,
"SystemControls": [{
  "Namespace": "string",
  "Value": "string"
}],
"Ulimits": [{
  "HardLimit": number,
  "Name": "string",
  "SoftLimit": number
}],
"User": "string",
"VolumesFrom": [{
  "ReadOnly": boolean,
  "SourceContainer": "string"
}],
"WorkingDirectory": "string"
}],
"Cpu": "string",
"ExecutionRoleArn": "string",
"Family": "string",
"InferenceAccelerators": [{
  "DeviceName": "string",
  "DeviceType": "string"
}],
"IpcMode": "string",
"Memory": "string",
"NetworkMode": "string",
"PidMode": "string",
"PlacementConstraints": [{
```

```

    "Expression": "string",
    "Type": "string"
  ]],
  "ProxyConfiguration": {
    "ContainerName": "string",
    "ProxyConfigurationProperties": [{
      "Name": "string",
      "Value": "string"
    }],
    "Type": "string"
  },
  "RequiresCompatibilities": ["string"],
  "Status": "string",
  "TaskRoleArn": "string",
  "Volumes": [{
    "DockerVolumeConfiguration": {
      "Autoprovision": boolean,
      "Driver": "string",
      "DriverOpts": {
        "string": "string"
      },
      "Labels": {
        "string": "string"
      },
      "Scope": "string"
    },
    "EfsVolumeConfiguration": {
      "AuthorizationConfig": {
        "AccessPointId": "string",
        "Iam": "string"
      },
      "FilesystemId": "string",
      "RootDirectory": "string",
      "TransitEncryption": "string",
      "TransitEncryptionPort": number
    },
    "Host": {
      "SourcePath": "string"
    },
    "Name": "string"
  }],
  "AwsEfsAccessPoint": {
    "AccessPointId": "string",

```



```
"Arn": "string",
"ClientToken": "string",
"FileSystemId": "string",
"PosixUser": {
  "Gid": "string",
  "SecondaryGids": ["string"],
  "Uid": "string"
},
"RootDirectory": {
  "CreationInfo": {
    "OwnerGid": "string",
    "OwnerUid": "string",
    "Permissions": "string"
  },
  "Path": "string"
},
},
"AwsEksCluster": {
  "Arn": "string",
  "CertificateAuthorityData": "string",
  "ClusterStatus": "string",
  "Endpoint": "string",
  "Logging": {
    "ClusterLogging": [{
      "Enabled": boolean,
      "Types": ["string"]
    }]
  },
  "Name": "string",
  "ResourcesVpcConfig": {
    "EndpointPublicAccess": boolean,
    "SecurityGroupIds": ["string"],
    "SubnetIds": ["string"]
  },
  "RoleArn": "string",
  "Version": "string"
},
"AwsElasticBeanstalkEnvironment": {
  "ApplicationName": "string",
  "Cname": "string",
  "DateCreated": "string",
  "DateUpdated": "string",
  "Description": "string",
  "EndpointUrl": "string",
```

```

"EnvironmentArn": "string",
"EnvironmentId": "string",
"EnvironmentLinks": [{
  "EnvironmentName": "string",
  "LinkName": "string"
}],
"EnvironmentName": "string",
"OptionSettings": [{
  "Namespace": "string",
  "OptionName": "string",
  "ResourceName": "string",
  "Value": "string"
}],
"PlatformArn": "string",
"SolutionStackName": "string",
"Status": "string",
"Tier": {
  "Name": "string",
  "Type": "string",
  "Version": "string"
},
"VersionLabel": "string"
},
"AwsElasticSearchDomain": {
  "AccessPolicies": "string",
  "DomainStatus": {
    "DomainId": "string",
    "DomainName": "string",
    "Endpoint": "string",
    "Endpoints": {
      "string": "string"
    }
  },
  "DomainEndpointOptions": {
    "EnforceHTTPS": boolean,
    "TLSSecurityPolicy": "string"
  },
  "ElasticsearchClusterConfig": {
    "DedicatedMasterCount": number,
    "DedicatedMasterEnabled": boolean,
    "DedicatedMasterType": "string",
    "InstanceCount": number,
    "InstanceType": "string",
    "ZoneAwarenessConfig": {

```

```
    "AvailabilityZoneCount": number
  },
  "ZoneAwarenessEnabled": boolean
},
"ElasticsearchVersion": "string",
"EncryptionAtRestOptions": {
  "Enabled": boolean,
  "KmsKeyId": "string"
},
"LogPublishingOptions": {
  "AuditLogs": {
    "CloudWatchLogsLogGroupArn": "string",
    "Enabled": boolean
  },
  "IndexSlowLogs": {
    "CloudWatchLogsLogGroupArn": "string",
    "Enabled": boolean
  },
  "SearchSlowLogs": {
    "CloudWatchLogsLogGroupArn": "string",
    "Enabled": boolean
  }
},
"NodeToNodeEncryptionOptions": {
  "Enabled": boolean
},
"ServiceSoftwareOptions": {
  "AutomatedUpdateDate": "string",
  "Cancellable": boolean,
  "CurrentVersion": "string",
  "Description": "string",
  "NewVersion": "string",
  "UpdateAvailable": boolean,
  "UpdateStatus": "string"
},
"VPCOptions": {
  "AvailabilityZones": [
    "string"
  ],
  "SecurityGroupIds": [
    "string"
  ],
  "SubnetIds": [
    "string"
  ]
}
```

```

    ],
    "VPCId": "string"
  }
},
"AwsElbLoadBalancer": {
  "AvailabilityZones": ["string"],
  "BackendServerDescriptions": [{
    "InstancePort": number,
    "PolicyNames": ["string"]
  }],
  "CanonicalHostedZoneName": "string",
  "CanonicalHostedZoneNameID": "string",
  "CreateTime": "string",
  "DnsName": "string",
  "HealthCheck": {
    "HealthyThreshold": number,
    "Interval": number,
    "Target": "string",
    "Timeout": number,
    "UnhealthyThreshold": number
  },
  "Instances": [{
    "InstanceId": "string"
  }],
  "ListenerDescriptions": [{
    "Listener": {
      "InstancePort": number,
      "InstanceProtocol": "string",
      "LoadBalancerPort": number,
      "Protocol": "string",
      "SslCertificateId": "string"
    },
    "PolicyNames": ["string"]
  }],
  "LoadBalancerAttributes": {
    "AccessLog": {
      "EmitInterval": number,
      "Enabled": boolean,
      "S3BucketName": "string",
      "S3BucketPrefix": "string"
    },
    "ConnectionDraining": {
      "Enabled": boolean,
      "Timeout": number
    }
  }
}

```

```

    },
    "ConnectionSettings": {
      "IdleTimeout": number
    },
    "CrossZoneLoadBalancing": {
      "Enabled": boolean
    },
    "AdditionalAttributes": [{
      "Key": "string",
      "Value": "string"
    }
  ],
  "LoadBalancerName": "string",
  "Policies": {
    "AppCookieStickinessPolicies": [{
      "CookieName": "string",
      "PolicyName": "string"
    }],
    "LbCookieStickinessPolicies": [{
      "CookieExpirationPeriod": number,
      "PolicyName": "string"
    }],
    "OtherPolicies": ["string"]
  },
  "Scheme": "string",
  "SecurityGroups": ["string"],
  "SourceSecurityGroup": {
    "GroupName": "string",
    "OwnerAlias": "string"
  },
  "Subnets": ["string"],
  "VpcId": "string"
},
"aws:elbv2:LoadBalancer": {
  "AvailabilityZones": {
    "SubnetId": "string",
    "ZoneName": "string"
  },
  "CanonicalHostedZoneId": "string",
  "CreatedTime": "string",
  "DNSName": "string",
  "IpAddressType": "string",
  "LoadBalancerAttributes": [{
    "Key": "string",

```

```

    "Value": "string"
  }],
  "Scheme": "string",
  "SecurityGroups": ["string"],
  "State": {
    "Code": "string",
    "Reason": "string"
  },
  "Type": "string",
  "VpcId": "string"
},
"AwsEventSchemasRegistry": {
  "Description": "string",
  "RegistryArn": "string",
  "RegistryName": "string"
},
"AwsEventsEndpoint": {
  "Arn": "string",
  "Description": "string",
  "EndpointId": "string",
  "EndpointUrl": "string",
  "EventBuses": [
    {
      "EventBusArn": "string"
    },
    {
      "EventBusArn": "string"
    }
  ],
  "Name": "string",
  "ReplicationConfig": {
    "State": "string"
  },
  "RoleArn": "string",
  "RoutingConfig": {
    "FailoverConfig": {
      "Primary": {
        "HealthCheck": "string"
      },
      "Secondary": {
        "Route": "string"
      }
    }
  }
},

```

```
"State": "string",
},
"AwsEventsEventBus": {
  "Arn": "string",
  "Name": "string",
  "Policy": "string"
},
"AwsGuardDutyDetector": {
  "FindingPublishingFrequency": "string",
  "ServiceRole": "string",
  "Status": "string",
  "DataSources": {
    "CloudTrail": {
      "Status": "string"
    },
    "DnsLogs": {
      "Status": "string"
    },
    "FlowLogs": {
      "Status": "string"
    },
    "S3Logs": {
      "Status": "string"
    },
    "Kubernetes": {
      "AuditLogs": {
        "Status": "string"
      }
    }
  },
  "MalwareProtection": {
    "ScanEc2InstanceWithFindings": {
      "EbsVolumes": {
        "Status": "string"
      }
    },
    "ServiceRole": "string"
  }
},
"AwsIamAccessKey": {
  "AccessKeyId": "string",
  "AccountId": "string",
  "CreatedAt": "string",
  "PrincipalId": "string",
```

```
"PrincipalName": "string",
"PrincipalType": "string",
"SessionContext": {
  "Attributes": {
    "CreationDate": "string",
    "MfaAuthenticated": boolean
  },
  "SessionIssuer": {
    "AccountId": "string",
    "Arn": "string",
    "PrincipalId": "string",
    "Type": "string",
    "UserName": "string"
  }
},
"Status": "string"
},
"AwsIamGroup": {
  "AttachedManagedPolicies": [{
    "PolicyArn": "string",
    "PolicyName": "string"
  }],
  "CreateDate": "string",
  "GroupId": "string",
  "GroupName": "string",
  "GroupPolicyList": [{
    "PolicyName": "string"
  }],
  "Path": "string"
},
"AwsIamPolicy": {
  "AttachmentCount": number,
  "CreateDate": "string",
  "DefaultVersionId": "string",
  "Description": "string",
  "IsAttachable": boolean,
  "Path": "string",
  "PermissionsBoundaryUsageCount": number,
  "PolicyId": "string",
  "PolicyName": "string",
  "PolicyVersionList": [{
    "CreateDate": "string",
    "IsDefaultVersion": boolean,
    "VersionId": "string"
  }]
```



```

    }],
    "UpdateDate": "string"
  },
  "AwsIamRole": {
    "AssumeRolePolicyDocument": "string",
    "AttachedManagedPolicies": [{
      "PolicyArn": "string",
      "PolicyName": "string"
    }],
    "CreateDate": "string",
    "InstanceProfileList": [{
      "Arn": "string",
      "CreateDate": "string",
      "InstanceProfileId": "string",
      "InstanceProfileName": "string",
      "Path": "string",
      "Roles": [{
        "Arn": "string",
        "AssumeRolePolicyDocument": "string",
        "CreateDate": "string",
        "Path": "string",
        "RoleId": "string",
        "RoleName": "string"
      }]
    }],
    "MaxSessionDuration": number,
    "Path": "string",
    "PermissionsBoundary": {
      "PermissionsBoundaryArn": "string",
      "PermissionsBoundaryType": "string"
    },
    "RoleId": "string",
    "RoleName": "string",
    "RolePolicyList": [{
      "PolicyName": "string"
    }]
  },
  "AwsIamUser": {
    "AttachedManagedPolicies": [{
      "PolicyArn": "string",
      "PolicyName": "string"
    }],
    "CreateDate": "string",
    "GroupList": ["string"],

```

```
"Path": "string",
"PermissionsBoundary": {
  "PermissionsBoundaryArn": "string",
  "PermissionsBoundaryType": "string"
},
"UserId": "string",
"UserName": "string",
"UserPolicyList": [{
  "PolicyName": "string"
}]
},
"AwsKinesisStream": {
  "Arn": "string",
  "Name": "string",
  "RetentionPeriodHours": number,
  "ShardCount": number,
  "StreamEncryption": {
    "EncryptionType": "string",
    "KeyId": "string"
  }
},
"AwsKmsKey": {
  "AWSAccountId": "string",
  "CreationDate": "string",
  "Description": "string",
  "KeyId": "string",
  "KeyManager": "string",
  "KeyRotationStatus": boolean,
  "KeyState": "string",
  "Origin": "string"
},
"AwsLambdaFunction": {
  "Architectures": [
    "string"
  ],
  "Code": {
    "S3Bucket": "string",
    "S3Key": "string",
    "S3ObjectVersion": "string",
    "ZipFile": "string"
  },
  "CodeSha256": "string",
  "DeadLetterConfig": {
    "TargetArn": "string"
```

```

    },
    "Environment": {
      "Variables": {
        "Stage": "string"
      },
    },
    "Error": {
      "ErrorCode": "string",
      "Message": "string"
    }
  },
  "FunctionName": "string",
  "Handler": "string",
  "KmsKeyArn": "string",
  "LastModified": "string",
  "Layers": {
    "Arn": "string",
    "CodeSize": number
  },
  "PackageType": "string",
  "RevisionId": "string",
  "Role": "string",
  "Runtime": "string",
  "Timeout": integer,
  "TracingConfig": {
    "Mode": "string"
  },
  "Version": "string",
  "VpcConfig": {
    "SecurityGroupIds": ["string"],
    "SubnetIds": ["string"]
  },
  "MasterArn": "string",
  "MemorySize": number
},
"AwsLambdaLayerVersion": {
  "CompatibleRuntimes": [
    "string"
  ],
  "CreateDate": "string",
  "Version": number
},
"AwsMskCluster": {
  "ClusterInfo": {
    "ClientAuthentication": {

```

```

    "Sasl": {
      "Scram": {
        "Enabled": boolean
      },
      "Iam": {
        "Enabled": boolean
      }
    },
    "Tls": {
      "CertificateAuthorityArnList": [],
      "Enabled": boolean
    },
    "Unauthenticated": {
      "Enabled": boolean
    }
  },
  "ClusterName": "string",
  "CurrentVersion": "string",
  "EncryptionInfo": {
    "EncryptionAtRest": {
      "DataVolumeKMSKeyId": "string"
    },
    "EncryptionInTransit": {
      "ClientBroker": "string",
      "InCluster": boolean
    }
  },
  "EnhancedMonitoring": "string",
  "NumberOfBrokerNodes": integer
}
},
"AwsNetworkFirewallFirewall": {
  "DeleteProtection": boolean,
  "Description": "string",
  "FirewallArn": "string",
  "FirewallId": "string",
  "FirewallName": "string",
  "FirewallPolicyArn": "string",
  "FirewallPolicyChangeProtection": boolean,
  "SubnetChangeProtection": boolean,
  "SubnetMappings": [{
    "SubnetId": "string"
  }],
  "VpcId": "string"
}

```

```

},
"AwsNetworkFirewallFirewallPolicy": {
  "Description": "string",
  "FirewallPolicy": {
    "StatefulRuleGroupReferences": [{
      "ResourceArn": "string"
    }],
    "StatelessCustomActions": [{
      "ActionDefinition": {
        "PublishMetricAction": {
          "Dimensions": [{
            "Value": "string"
          }]
        }
      }
    ],
    "ActionName": "string"
  },
  "StatelessDefaultActions": ["string"],
  "StatelessFragmentDefaultActions": ["string"],
  "StatelessRuleGroupReferences": [{
    "Priority": number,
    "ResourceArn": "string"
  }]
},
"FirewallPolicyArn": "string",
"FirewallPolicyId": "string",
"FirewallPolicyName": "string"
},
"AwsNetworkFirewallRuleGroup": {
  "Capacity": number,
  "Description": "string",
  "RuleGroup": {
    "RulesSource": {
      "RulesSourceList": {
        "GeneratedRulesType": "string",
        "Targets": ["string"],
        "TargetTypes": ["string"]
      }
    },
    "RulesString": "string",
    "StatefulRules": [{
      "Action": "string",
      "Header": {
        "Destination": "string",
        "DestinationPort": "string",

```

```
    "Direction": "string",
    "Protocol": "string",
    "Source": "string",
    "SourcePort": "string"
  },
  "RuleOptions": [{
    "Keyword": "string",
    "Settings": ["string"]
  }]
}],
"StatelessRulesAndCustomActions": {
  "CustomActions": [{
    "ActionDefinition": {
      "PublishMetricAction": {
        "Dimensions": [{
          "Value": "string"
        }]
      }
    },
    "ActionName": "string"
  }],
  "StatelessRules": [{
    "Priority": number,
    "RuleDefinition": {
      "Actions": ["string"],
      "MatchAttributes": {
        "DestinationPorts": [{
          "FromPort": number,
          "ToPort": number
        }],
        "Destinations": [{
          "AddressDefinition": "string"
        }],
        "Protocols": [number],
        "SourcePorts": [{
          "FromPort": number,
          "ToPort": number
        }],
        "Sources": [{
          "AddressDefinition": "string"
        }],
        "TcpFlags": [{
          "Flags": ["string"],
          "Masks": ["string"]
        }],

```

```

        ]]
    }
}
]]
}
},
"RuleVariables": {
    "IpSets": {
        "Definition": ["string"]
    },
    "PortSets": {
        "Definition": ["string"]
    }
}
},
"RuleGroupArn": "string",
"RuleGroupId": "string",
"RuleGroupName": "string",
"Type": "string"
},
"AwsOpenSearchServiceDomain": {
    "AccessPolicies": "string",
    "AdvancedSecurityOptions": {
        "Enabled": boolean,
        "InternalUserDatabaseEnabled": boolean,
        "MasterUserOptions": {
            "MasterUserArn": "string",
            "MasterUserName": "string",
            "MasterUserPassword": "string"
        }
    },
    "Arn": "string",
    "ClusterConfig": {
        "DedicatedMasterCount": number,
        "DedicatedMasterEnabled": boolean,
        "DedicatedMasterType": "string",
        "InstanceCount": number,
        "InstanceType": "string",
        "WarmCount": number,
        "WarmEnabled": boolean,
        "WarmType": "string",
        "ZoneAwarenessConfig": {
            "AvailabilityZoneCount": number
        }
    },

```

```
    "ZoneAwarenessEnabled": boolean
  },
  "DomainEndpoint": "string",
  "DomainEndpointOptions": {
    "CustomEndpoint": "string",
    "CustomEndpointCertificateArn": "string",
    "CustomEndpointEnabled": boolean,
    "EnforceHTTPS": boolean,
    "TLSSecurityPolicy": "string"
  },
  "DomainEndpoints": {
    "string": "string"
  },
  "DomainName": "string",
  "EncryptionAtRestOptions": {
    "Enabled": boolean,
    "KmsKeyId": "string"
  },
  "EngineVersion": "string",
  "Id": "string",
  "LogPublishingOptions": {
    "AuditLogs": {
      "CloudWatchLogsLogGroupArn": "string",
      "Enabled": boolean
    },
    "IndexSlowLogs": {
      "CloudWatchLogsLogGroupArn": "string",
      "Enabled": boolean
    },
    "SearchSlowLogs": {
      "CloudWatchLogsLogGroupArn": "string",
      "Enabled": boolean
    }
  },
  "NodeToNodeEncryptionOptions": {
    "Enabled": boolean
  },
  "ServiceSoftwareOptions": {
    "AutomatedUpdateDate": "string",
    "Cancellable": boolean,
    "CurrentVersion": "string",
    "Description": "string",
    "NewVersion": "string",
    "OptionalDeployment": boolean,
```



```

    "UpdateAvailable": boolean,
    "UpdateStatus": "string"
  },
  "VpcOptions": {
    "SecurityGroupIds": ["string"],
    "SubnetIds": ["string"]
  }
},
"AwsRdsDbCluster": {
  "ActivityStreamStatus": "string",
  "AllocatedStorage": number,
  "AssociatedRoles": [{
    "RoleArn": "string",
    "Status": "string"
  }],
  "AutoMinorVersionUpgrade": boolean,
  "AvailabilityZones": ["string"],
  "BackupRetentionPeriod": integer,
  "ClusterCreateTime": "string",
  "CopyTagsToSnapshot": boolean,
  "CrossAccountClone": boolean,
  "CustomEndpoints": ["string"],
  "DatabaseName": "string",
  "DbClusterIdentifier": "string",
  "DbClusterMembers": [{
    "DbClusterParameterGroupStatus": "string",
    "DbInstanceIdentifier": "string",
    "IsClusterWriter": boolean,
    "PromotionTier": integer
  }],
  "DbClusterOptionGroupMemberships": [{
    "DbClusterOptionGroupName": "string",
    "Status": "string"
  }],
  "DbClusterParameterGroup": "string",
  "DbClusterResourceId": "string",
  "DbSubnetGroup": "string",
  "DeletionProtection": boolean,
  "DomainMemberships": [{
    "Domain": "string",
    "Fqdn": "string",
    "IamRoleName": "string",
    "Status": "string"
  }],

```

```

    "EnabledCloudwatchLogsExports": ["string"],
    "Endpoint": "string",
    "Engine": "string",
    "EngineMode": "string",
    "EngineVersion": "string",
    "HostedZoneId": "string",
    "HttpEndpointEnabled": boolean,
    "IamDatabaseAuthenticationEnabled": boolean,
    "KmsKeyId": "string",
    "MasterUsername": "string",
    "MultiAz": boolean,
    "Port": integer,
    "PreferredBackupWindow": "string",
    "PreferredMaintenanceWindow": "string",
    "ReaderEndpoint": "string",
    "ReadReplicaIdentifiers": ["string"],
    "Status": "string",
    "StorageEncrypted": boolean,
    "VpcSecurityGroups": [{
      "Status": "string",
      "VpcSecurityGroupId": "string"
    }]
  },
  "AwsRdsDbClusterSnapshot": {
    "AllocatedStorage": integer,
    "AvailabilityZones": ["string"],
    "ClusterCreateTime": "string",
    "DbClusterIdentifier": "string",
    "DbClusterSnapshotAttributes": [{
      "AttributeName": "string",
      "AttributeValues": ["string"]
    }],
    "DbClusterSnapshotIdentifier": "string",
    "Engine": "string",
    "EngineVersion": "string",
    "IamDatabaseAuthenticationEnabled": boolean,
    "KmsKeyId": "string",
    "LicenseModel": "string",
    "MasterUsername": "string",
    "PercentProgress": integer,
    "Port": integer,
    "SnapshotCreateTime": "string",
    "SnapshotType": "string",
    "Status": "string",

```

```

    "StorageEncrypted": boolean,
    "VpcId": "string"
  },
  "AwsRdsDbInstance": {
    "AllocatedStorage": number,
    "AssociatedRoles": [{
      "RoleArn": "string",
      "FeatureName": "string",
      "Status": "string"
    }],
    "AutoMinorVersionUpgrade": boolean,
    "AvailabilityZone": "string",
    "BackupRetentionPeriod": number,
    "CACertificateIdentifier": "string",
    "CharacterSetName": "string",
    "CopyTagsToSnapshot": boolean,
    "DBClusterIdentifier": "string",
    "DBInstanceClass": "string",
    "DBInstanceIdentifier": "string",
    "DbInstancePort": number,
    "DbInstanceStatus": "string",
    "DbiResourceId": "string",
    "DBName": "string",
    "DbParameterGroups": [{
      "DbParameterGroupName": "string",
      "ParameterApplyStatus": "string"
    }],
    "DbSecurityGroups": ["string"],
    "DbSubnetGroup": {
      "DbSubnetGroupArn": "string",
      "DbSubnetGroupDescription": "string",
      "DbSubnetGroupName": "string",
      "SubnetGroupStatus": "string",
      "Subnets": [{
        "SubnetAvailabilityZone": {
          "Name": "string"
        },
        "SubnetIdentifier": "string",
        "SubnetStatus": "string"
      }],
      "VpcId": "string"
    },
    "DeletionProtection": boolean,
    "Endpoint": {

```

```
"Address": "string",
"Port": number,
"HostedZoneId": "string"
},
"DomainMemberships": [{
  "Domain": "string",
  "Fqdn": "string",
  "IamRoleName": "string",
  "Status": "string"
}],
"EnabledCloudwatchLogsExports": ["string"],
"Engine": "string",
"EngineVersion": "string",
"EnhancedMonitoringResourceArn": "string",
"IAMDatabaseAuthenticationEnabled": boolean,
"InstanceCreateTime": "string",
"Iops": number,
"KmsKeyId": "string",
"LatestRestorableTime": "string",
"LicenseModel": "string",
"ListenerEndpoint": {
  "Address": "string",
  "HostedZoneId": "string",
  "Port": number
},
"MasterUsername": "admin",
"MaxAllocatedStorage": number,
"MonitoringInterval": number,
"MonitoringRoleArn": "string",
"MultiAz": boolean,
"OptionGroupMemberships": [{
  "OptionGroupName": "string",
  "Status": "string"
}],
"PendingModifiedValues": {
  "AllocatedStorage": number,
  "BackupRetentionPeriod": number,
  "CaCertificateIdentifier": "string",
  "DbInstanceClass": "string",
  "DbInstanceIdentifier": "string",
  "DbSubnetGroupName": "string",
  "EngineVersion": "string",
  "Iops": number,
  "LicenseModel": "string",
```

```

    "MasterUserPassword": "string",
    "MultiAZ": boolean,
    "PendingCloudWatchLogsExports": {
      "LogTypesToDisable": ["string"],
      "LogTypesToEnable": ["string"]
    },
    "Port": number,
    "ProcessorFeatures": [{
      "Name": "string",
      "Value": "string"
    }],
    "StorageType": "string"
  },
  "PerformanceInsightsEnabled": boolean,
  "PerformanceInsightsKmsKeyId": "string",
  "PerformanceInsightsRetentionPeriod": number,
  "PreferredBackupWindow": "string",
  "PreferredMaintenanceWindow": "string",
  "ProcessorFeatures": [{
    "Name": "string",
    "Value": "string"
  }],
  "PromotionTier": number,
  "PubliclyAccessible": boolean,
  "ReadReplicaDBClusterIdentifiers": ["string"],
  "ReadReplicaDBInstanceIdentifiers": ["string"],
  "ReadReplicaSourceDBInstanceIdentifier": "string",
  "SecondaryAvailabilityZone": "string",
  "StatusInfos": [{
    "Message": "string",
    "Normal": boolean,
    "Status": "string",
    "StatusType": "string"
  }],
  "StorageEncrypted": boolean,
  "TdeCredentialArn": "string",
  "Timezone": "string",
  "VpcSecurityGroups": [{
    "VpcSecurityGroupId": "string",
    "Status": "string"
  }]
},
"AwsRdsDbSecurityGroup": {
  "DbSecurityGroupArn": "string",

```

```

    "DbSecurityGroupDescription": "string",
    "DbSecurityGroupName": "string",
    "Ec2SecurityGroups": [{
        "Ec2SecurityGroupuId": "string",
        "Ec2SecurityGroupName": "string",
        "Ec2SecurityGroupOwnerId": "string",
        "Status": "string"
    }],
    "IpRanges": [{
        "CidrIp": "string",
        "Status": "string"
    }],
    "OwnerId": "string",
    "VpcId": "string"
},
"AwsRdsDbSnapshot": {
    "AllocatedStorage": integer,
    "AvailabilityZone": "string",
    "DbInstanceIdentifier": "string",
    "DbiResourceId": "string",
    "DbSnapshotIdentifier": "string",
    "Encrypted": boolean,
    "Engine": "string",
    "EngineVersion": "string",
    "IamDatabaseAuthenticationEnabled": boolean,
    "InstanceCreateTime": "string",
    "Iops": number,
    "KmsKeyId": "string",
    "LicenseModel": "string",
    "MasterUsername": "string",
    "OptionGroupName": "string",
    "PercentProgress": integer,
    "Port": integer,
    "ProcessorFeatures": [],
    "SnapshotCreateTime": "string",
    "SnapshotType": "string",
    "SourceDbSnapshotIdentifier": "string",
    "SourceRegion": "string",
    "Status": "string",
    "StorageType": "string",
    "TdeCredentialArn": "string",
    "Timezone": "string",
    "VpcId": "string"
},

```

```
"AwsRdsEventSubscription": {
  "CustomerAwsId": "string",
  "CustSubscriptionId": "string",
  "Enabled": boolean,
  "EventCategoriesList": ["string"],
  "EventSubscriptionArn": "string",
  "SnsTopicArn": "string",
  "SourceIdsList": ["string"],
  "SourceType": "string",
  "Status": "string",
  "SubscriptionCreationTime": "string"
},
"AwsRedshiftCluster": {
  "AllowVersionUpgrade": boolean,
  "AutomatedSnapshotRetentionPeriod": number,
  "AvailabilityZone": "string",
  "ClusterAvailabilityStatus": "string",
  "ClusterCreateTime": "string",
  "ClusterIdentifier": "string",
  "ClusterNodes": [{
    "NodeRole": "string",
    "PrivateIpAddress": "string",
    "PublicIpAddress": "string"
  }],
  "ClusterParameterGroups": [{
    "ClusterParameterStatusList": [{
      "ParameterApplyErrorDescription": "string",
      "ParameterApplyStatus": "string",
      "ParameterName": "string"
    }],
    "ParameterApplyStatus": "string",
    "ParameterGroupName": "string"
  }],
  "ClusterPublicKey": "string",
  "ClusterRevisionNumber": "string",
  "ClusterSecurityGroups": [{
    "ClusterSecurityGroupName": "string",
    "Status": "string"
  }],
  "ClusterSnapshotCopyStatus": {
    "DestinationRegion": "string",
    "ManualSnapshotRetentionPeriod": number,
    "RetentionPeriod": number,
    "SnapshotCopyGrantName": "string"
  }
}
```

```

},
"ClusterStatus": "string",
"ClusterSubnetGroupName": "string",
"ClusterVersion": "string",
"DBName": "string",
"DeferredMaintenanceWindows": [{
  "DeferMaintenanceEndTime": "string",
  "DeferMaintenanceIdentifier": "string",
  "DeferMaintenanceStartTime": "string"
}],
"ElasticIpStatus": {
  "ElasticIp": "string",
  "Status": "string"
},
"ElasticResizeNumberOfNodeOptions": "string",
"Encrypted": boolean,
"Endpoint": {
  "Address": "string",
  "Port": number
},
"EnhancedVpcRouting": boolean,
"ExpectedNextSnapshotScheduleTime": "string",
"ExpectedNextSnapshotScheduleTimeStatus": "string",
"HsmStatus": {
  "HsmClientCertificateIdentifier": "string",
  "HsmConfigurationIdentifier": "string",
  "Status": "string"
},
"IamRoles": [{
  "ApplyStatus": "string",
  "IamRoleArn": "string"
}],
"KmsKeyId": "string",
"LoggingStatus":{
  "BucketName": "string",
  "LastFailureMessage": "string",
  "LastFailureTime": "string",
  "LastSuccessfulDeliveryTime": "string",
  "LoggingEnabled": boolean,
  "S3KeyPrefix": "string"
},
"MaintenanceTrackName": "string",
"ManualSnapshotRetentionPeriod": number,
"MasterUsername": "string",

```



```

    "NextMaintenanceWindowStartTime": "string",
    "NodeType": "string",
    "NumberOfNodes": number,
    "PendingActions": ["string"],
    "PendingModifiedValues": {
      "AutomatedSnapshotRetentionPeriod": number,
      "ClusterIdentifier": "string",
      "ClusterType": "string",
      "ClusterVersion": "string",
      "EncryptionType": "string",
      "EnhancedVpcRouting": boolean,
      "MaintenanceTrackName": "string",
      "MasterUserPassword": "string",
      "NodeType": "string",
      "NumberOfNodes": number,
      "PubliclyAccessible": "string"
    },
    "PreferredMaintenanceWindow": "string",
    "PubliclyAccessible": boolean,
    "ResizeInfo": {
      "AllowCancelResize": boolean,
      "ResizeType": "string"
    },
    "RestoreStatus": {
      "CurrentRestoreRateInMegaBytesPerSecond": number,
      "ElapsedTimeInSeconds": number,
      "EstimatedTimeToCompletionInSeconds": number,
      "ProgressInMegaBytes": number,
      "SnapshotSizeInMegaBytes": number,
      "Status": "string"
    },
    "SnapshotScheduleIdentifier": "string",
    "SnapshotScheduleState": "string",
    "VpcId": "string",
    "VpcSecurityGroups": [{
      "Status": "string",
      "VpcSecurityGroupId": "string"
    }]
  },
  "AwsRoute53HostedZone": {
    "HostedZone": {
      "Id": "string",
      "Name": "string",
      "Config": {

```

```

    "Comment": "string"
  },
  "NameServers": ["string"],
  "QueryLoggingConfig": {
    "CloudWatchLogsLogGroupArn": {
      "CloudWatchLogsLogGroupArn": "string",
      "Id": "string",
      "HostedZoneId": "string"
    }
  },
  "Vpcs": [
    {
      "Id": "string",
      "Region": "string"
    }
  ],
  "AwsS3AccessPoint": {
    "AccessPointArn": "string",
    "Alias": "string",
    "Bucket": "string",
    "BucketAccountId": "string",
    "Name": "string",
    "NetworkOrigin": "string",
    "PublicAccessBlockConfiguration": {
      "BlockPublicAcls": boolean,
      "BlockPublicPolicy": boolean,
      "IgnorePublicAcls": boolean,
      "RestrictPublicBuckets": boolean
    },
    "VpcConfiguration": {
      "VpcId": "string"
    }
  },
  "AwsS3AccountPublicAccessBlock": {
    "BlockPublicAcls": boolean,
    "BlockPublicPolicy": boolean,
    "IgnorePublicAcls": boolean,
    "RestrictPublicBuckets": boolean
  },
  "AwsS3Bucket": {
    "AccessControlList": "string",
    "BucketLifecycleConfiguration": {

```

```

"Rules": [{
  "AbortIncompleteMultipartUpload": {
    "DaysAfterInitiation": number
  },
  "ExpirationDate": "string",
  "ExpirationInDays": number,
  "ExpiredObjectDeleteMarker": boolean,
  "Filter": {
    "Predicate": {
      "Operands": [{
        "Prefix": "string",
        "Type": "string"
      },
      {
        "Tag": {
          "Key": "string",
          "Value": "string"
        },
        "Type": "string"
      }
    ],
    "Type": "string"
  },
  "Id": "string",
  "NoncurrentVersionExpirationInDays": number,
  "NoncurrentVersionTransitions": [{
    "Days": number,
    "StorageClass": "string"
  }],
  "Prefix": "string",
  "Status": "string",
  "Transitions": [{
    "Date": "string",
    "Days": number,
    "StorageClass": "string"
  }]
}],
"BucketLoggingConfiguration": {
  "DestinationBucketName": "string",
  "LogFilePrefix": "string"
},
"BucketName": "string",

```

```

"BucketNotificationConfiguration": {
  "Configurations": [{
    "Destination": "string",
    "Events": ["string"],
    "Filter": {
      "S3KeyFilter": {
        "FilterRules": [{
          "Name": "string",
          "Value": "string"
        }]
      }
    },
    "Type": "string"
  ]
},
"BucketVersioningConfiguration": {
  "IsMfaDeleteEnabled": boolean,
  "Status": "string"
},
"BucketWebsiteConfiguration": {
  "ErrorDocument": "string",
  "IndexDocumentSuffix": "string",
  "RedirectAllRequestsTo": {
    "HostName": "string",
    "Protocol": "string"
  },
  "RoutingRules": [{
    "Condition": {
      "HttpErrorCodeReturnedEquals": "string",
      "KeyPrefixEquals": "string"
    },
    "Redirect": {
      "HostName": "string",
      "HttpRedirectCode": "string",
      "Protocol": "string",
      "ReplaceKeyPrefixWith": "string",
      "ReplaceKeyWith": "string"
    }
  ]
},
"CreatedAt": "string",
"ObjectLockConfiguration": {
  "ObjectLockEnabled": "string",
  "Rule": {

```

```

    "DefaultRetention": {
      "Days": integer,
      "Mode": "string",
      "Years": integer
    }
  },
  "OwnerAccountId": "string",
  "OwnerId": "string",
  "OwnerName": "string",
  "PublicAccessBlockConfiguration": {
    "BlockPublicAcls": boolean,
    "BlockPublicPolicy": boolean,
    "IgnorePublicAcls": boolean,
    "RestrictPublicBuckets": boolean
  },
  "ServerSideEncryptionConfiguration": {
    "Rules": [{
      "ApplyServerSideEncryptionByDefault": {
        "KMSEMasterKeyID": "string",
        "SSEAlgorithm": "string"
      }
    }]
  },
  "AwsS3Object": {
    "ContentType": "string",
    "ETag": "string",
    "LastModified": "string",
    "ServerSideEncryption": "string",
    "SSEKMSKeyId": "string",
    "VersionId": "string"
  },
  "AwsSagemakerNotebookInstance": {
    "DirectInternetAccess": "string",
    "InstanceMetadataServiceConfiguration": {
      "MinimumInstanceMetadataServiceVersion": "string"
    },
    "InstanceType": "string",
    "LastModifiedTime": "string",
    "NetworkInterfaceId": "string",
    "NotebookInstanceArn": "string",
    "NotebookInstanceName": "string",
    "NotebookInstanceStatus": "string",

```

```

    "PlatformIdentifier": "string",
    "RoleArn": "string",
    "RootAccess": "string",
    "SecurityGroups": ["string"],
    "SubnetId": "string",
    "Url": "string",
    "VolumeSizeInGB": number
  },
  "AwsSecretsManagerSecret": {
    "Deleted": boolean,
    "Description": "string",
    "KmsKeyId": "string",
    "Name": "string",
    "RotationEnabled": boolean,
    "RotationLambdaArn": "string",
    "RotationOccurredWithinFrequency": boolean,
    "RotationRules": {
      "AutomaticallyAfterDays": integer
    }
  },
  "AwsSnsTopic": {
    "ApplicationSuccessFeedbackRoleArn": "string",
    "FirehoseFailureFeedbackRoleArn": "string",
    "FirehoseSuccessFeedbackRoleArn": "string",
    "HttpFailureFeedbackRoleArn": "string",
    "HttpSuccessFeedbackRoleArn": "string",
    "KmsMasterKeyId": "string",
    "Owner": "string",
    "SqsFailureFeedbackRoleArn": "string",
    "SqsSuccessFeedbackRoleArn": "string",
    "Subscription": {
      "Endpoint": "string",
      "Protocol": "string"
    },
    "TopicName": "string"
  },
  "AwsSqsQueue": {
    "DeadLetterTargetArn": "string",
    "KmsDataKeyReusePeriodSeconds": number,
    "KmsMasterKeyId": "string",
    "QueueName": "string"
  },
  "AwsSsmPatchCompliance": {
    "Patch": {

```

```

    "ComplianceSummary": {
      "ComplianceType": "string",
      "CompliantCriticalCount": integer,
      "CompliantHighCount": integer,
      "CompliantInformationalCount": integer,
      "CompliantLowCount": integer,
      "CompliantMediumCount": integer,
      "CompliantUnspecifiedCount": integer,
      "ExecutionType": "string",
      "NonCompliantCriticalCount": integer,
      "NonCompliantHighCount": integer,
      "NonCompliantInformationalCount": integer,
      "NonCompliantLowCount": integer,
      "NonCompliantMediumCount": integer,
      "NonCompliantUnspecifiedCount": integer,
      "OverallSeverity": "string",
      "PatchBaselineId": "string",
      "PatchGroup": "string",
      "Status": "string"
    }
  },
  "AwsStepFunctionStateMachine": {
    "StateMachineArn": "string",
    "Name": "string",
    "Status": "string",
    "RoleArn": "string",
    "Type": "string",
    "LoggingConfiguration": {
      "Level": "string",
      "IncludeExecutionData": boolean
    },
    "TracingConfiguration": {
      "Enabled": boolean
    }
  },
  "AwsWafRateBasedRule": {
    "MatchPredicates": [{
      "DataId": "string",
      "Negated": boolean,
      "Type": "string"
    }],
    "MetricName": "string",
    "Name": "string",

```

```

    "RateKey": "string",
    "RateLimit": number,
    "RuleId": "string"
  },
  "AwsWafRegionalRateBasedRule": {
    "MatchPredicates": [{
      "DataId": "string",
      "Negated": boolean,
      "Type": "string"
    }],
    "MetricName": "string",
    "Name": "string",
    "RateKey": "string",
    "RateLimit": number,
    "RuleId": "string"
  },
  "AwsWafRegionalRule": {
    "MetricName": "string",
    "Name": "string",
    "RuleId": "string",
    "PredicateList": [{
      "DataId": "string",
      "Negated": boolean,
      "Type": "string"
    }]
  },
  "AwsWafRegionalRuleGroup": {
    "MetricName": "string",
    "Name": "string",
    "RuleGroupId": "string",
    "Rules": [{
      "Action": {
        "Type": "string"
      },
      "Priority": number,
      "RuleId": "string",
      "Type": "string"
    }]
  },
  "AwsWafRegionalWebAcl": {
    "DefaultAction": "string",
    "MetricName": "string",
    "Name": "string",
    "RulesList": [{

```



```

    "Action": {
      "Type": "string"
    },
    "Priority": number,
    "RuleId": "string",
    "Type": "string",
    "ExcludedRules": [{
      "ExclusionType": "string",
      "RuleId": "string"
    }],
    "OverrideAction": {
      "Type": "string"
    }
  }],
  "WebAclId": "string"
},
"AwsWafRule": {
  "MetricName": "string",
  "Name": "string",
  "PredicateList": [{
    "DataId": "string",
    "Negated": boolean,
    "Type": "string"
  }],
  "RuleId": "string"
},
"AwsWafRuleGroup": {
  "MetricName": "string",
  "Name": "string",
  "RuleGroupId": "string",
  "Rules": [{
    "Action": {
      "Type": "string"
    },
    "Priority": number,
    "RuleId": "string",
    "Type": "string"
  }]
},
"AwsWafv2RuleGroup": {
  "Arn": "string",
  "Capacity": number,
  "Description": "string",
  "Id": "string",

```

```

    "Name": "string",
    "Rules": [{
      "Action": {
        "Allow": {
          "CustomRequestHandling": {
            "InsertHeaders": [
              {
                "Name": "string",
                "Value": "string"
              },
              {
                "Name": "string",
                "Value": "string"
              }
            ]
          }
        }
      },
      "Name": "string",
      "Priority": number,
      "VisibilityConfig": {
        "CloudWatchMetricsEnabled": boolean,
        "MetricName": "string",
        "SampledRequestsEnabled": boolean
      }
    }],
    "VisibilityConfig": {
      "CloudWatchMetricsEnabled": boolean,
      "MetricName": "string",
      "SampledRequestsEnabled": boolean
    }
  },
  "AwsWafWebAcl": {
    "DefaultAction": "string",
    "Name": "string",
    "Rules": [{
      "Action": {
        "Type": "string"
      },
      "ExcludedRules": [{
        "RuleId": "string"
      }],
      "OverrideAction": {
        "Type": "string"
      }
    }
  }
}

```

```

    },
    "Priority": number,
    "RuleId": "string",
    "Type": "string"
  }],
  "WebAclId": "string"
},
"AwsWafv2WebAcl": {
  "Arn": "string",
  "Capacity": number,
  "CaptchaConfig": {
    "ImmunityTimeProperty": {
      "ImmunityTime": number
    }
  },
  "DefaultAction": {
    "Block": {}
  },
  "Description": "string",
  "ManagedbyFirewallManager": boolean,
  "Name": "string",
  "Rules": [{
    "Action": {
      "RuleAction": {
        "Block": {}
      }
    },
    "Name": "string",
    "Priority": number,
    "VisibilityConfig": {
      "SampledRequestsEnabled": boolean,
      "CloudWatchMetricsEnabled": boolean,
      "MetricName": "string"
    }
  }],
  "VisibilityConfig": {
    "SampledRequestsEnabled": boolean,
    "CloudWatchMetricsEnabled": boolean,
    "MetricName": "string"
  }
},
"AwsXrayEncryptionConfig": {
  "KeyId": "string",
  "Status": "string",

```

```
    "Type": "string"
  },
  "Container": {
    "ContainerRuntime": "string",
    "ImageId": "string",
    "ImageName": "string",
    "LaunchedAt": "string",
    "Name": "string",
    "Privileged": boolean,
    "VolumeMounts": [{
      "Name": "string",
      "MountPath": "string"
    }]
  },
  "Other": {
    "string": "string"
  },
  "Id": "string",
  "Partition": "string",
  "Region": "string",
  "ResourceRole": "string",
  "Tags": {
    "string": "string"
  },
  "Type": "string"
}],
"SchemaVersion": "string",
"Severity": {
  "Label": "string",
  "Normalized": number,
  "Original": "string"
},
"Sample": boolean,
"SourceUrl": "string",
"Threats": [{
  "FilePaths": [{
    "FileName": "string",
    "FilePath": "string",
    "Hash": "string",
    "ResourceId": "string"
  }],
  "ItemCount": number,
  "Name": "string",
  "Severity": "string"
```

```

  ]],
  "ThreatIntelIndicators": [{
    "Category": "string",
    "LastObservedAt": "string",
    "Source": "string",
    "SourceUrl": "string",
    "Type": "string",
    "Value": "string"
  }],
  "Title": "string",
  "Types": ["string"],
  "UpdatedAt": "string",
  "UserDefinedFields": {
    "string": "string"
  },
  "VerificationState": "string",
  "Vulnerabilities": [{
    "CodeVulnerabilities": [{
      "Cwes": [
        "string",
        "string"
      ],
      "FilePath": {
        "EndLine": integer,
        "FileName": "string",
        "FilePath": "string",
        "StartLine": integer
      },
      "SourceArn": "string"
    }],
    "Cvss": [{
      "Adjustments": [{
        "Metric": "string",
        "Reason": "string"
      }],
      "BaseScore": number,
      "BaseVector": "string",
      "Source": "string",
      "Version": "string"
    }],
    "EpssScore": number,
    "ExploitAvailable": "string",
    "FixAvailable": "string",
    "Id": "string",

```

```

    "LastKnownExploitAt": "string",
    "ReferenceUrls": ["string"],
    "RelatedVulnerabilities": ["string"],
    "Vendor": {
      "Name": "string",
      "Url": "string",
      "VendorCreatedAt": "string",
      "VendorSeverity": "string",
      "VendorUpdatedAt": "string"
    },
    "VulnerablePackages": [{
      "Architecture": "string",
      "Epoch": "string",
      "FilePath": "string",
      "FixedInVersion": "string",
      "Name": "string",
      "PackageManager": "string",
      "Release": "string",
      "Remediation": "string",
      "SourceLayerArn": "string",
      "SourceLayerHash": "string",
      "Version": "string"
    }]
  },
  "Workflow": {
    "Status": "string"
  },
  "WorkflowState": "string"
}
]

```

Dampak konsolidasi pada bidang dan nilai ASFF

AWS Security Hub Cloud Security Posture Management (CSPM) menawarkan dua jenis konsolidasi untuk kontrol:

- **Tampilan kontrol konsolidasi** — Dengan jenis konsolidasi ini, setiap kontrol memiliki pengidentifikasi tunggal di semua standar. Selain itu, pada konsol CSPM Security Hub, halaman Kontrol menampilkan semua kontrol di semua standar.
- **Temuan kontrol konsolidasi** — Dengan jenis konsolidasi ini, Security Hub CSPM menghasilkan satu temuan untuk kontrol, bahkan jika kontrol berlaku untuk beberapa standar yang diaktifkan. Hal ini dapat mengurangi kebisingan.

Anda tidak dapat mengaktifkan atau menonaktifkan tampilan kontrol konsolidasi. Temuan kontrol konsolidasi diaktifkan secara default jika Anda mengaktifkan CSPM Security Hub pada atau setelah 23 Februari 2023. Jika tidak, itu dinonaktifkan secara default. Namun, untuk organisasi, temuan kontrol konsolidasi diaktifkan untuk akun anggota CSPM Security Hub hanya jika diaktifkan untuk akun administrator. Untuk mempelajari lebih lanjut tentang temuan kontrol terkonsolidasi, lihat [Menghasilkan dan memperbarui temuan kontrol](#).

Kedua jenis konsolidasi mempengaruhi bidang dan nilai untuk temuan kontrol di. [AWS Format Pencarian Keamanan \(ASFF\)](#)

Topik

- [Tampilan kontrol konsolidasi - perubahan ASFF](#)
- [Temuan kontrol konsolidasi - perubahan ASFF](#)
- [Generator IDs sebelum dan sesudah memungkinkan temuan kontrol terkonsolidasi](#)
- [Bagaimana konsolidasi memengaruhi kontrol IDs dan judul](#)
- [Memperbarui alur kerja untuk konsolidasi](#)

Tampilan kontrol konsolidasi - perubahan ASFF

Fitur tampilan kontrol terkonsolidasi memperkenalkan perubahan berikut pada bidang dan nilai untuk temuan kontrol di ASFF. Jika alur kerja Anda tidak bergantung pada nilai untuk bidang ASFF ini, tidak diperlukan tindakan. Jika Anda memiliki alur kerja yang bergantung pada nilai tertentu untuk bidang ini, perbarui alur kerja Anda untuk menggunakan nilai saat ini.

Bidang ASFF	Nilai sampel sebelum tampilan kontrol konsolidasi	Nilai sampel setelah tampilan kontrol terkonsolidasi, dan deskripsi perubahan
Kepatuhan. SecurityControlId	Tidak berlaku (bidang baru)	EC2.2 Memperkenalkan ID kontrol tunggal di seluruh standar. ProductFields.RuleId masih menyediakan ID kontrol berbasis standar untuk kontrol CIS v1.2.0. ProductFields.Cont

Bidang ASFF	Nilai sampel sebelum tampilan kontrol konsolidasi	Nilai sampel setelah tampilan kontrol terkonsolidasi, dan deskripsi perubahan
		rolId masih menyediakan ID kontrol berbasis standar untuk kontrol dalam standar lain.
Kepatuhan. Associate dStandards	Tidak berlaku (bidang baru)	[{" StandardsId ":" standards /aws-foundational-security-best-practices/v /1.0.0 "}] Menunjukkan standar mana kontrol diaktifkan.
ProductFields. ArchivalReasons:0/Deskripsi	Tidak berlaku (bidang baru)	"Temuan ini dalam keadaan ARCHIVED karena temuan kontrol terkonsolidasi telah diaktifkan atau dimatikan. Hal ini menyebabkan temuan di negara bagian sebelumnya diarsipkan ketika temuan baru sedang dihasilkan." Menjelaskan mengapa Security Hub CSPM telah mengarsipkan temuan yang ada.
ProductFields. ArchivalReasons:0/ ReasonCode	Tidak berlaku (bidang baru)	"CONSOLIDATED_CONTROL_FINDINGS_UPDATE" Memberikan alasan mengapa Security Hub CSPM telah mengarsipkan temuan yang ada.

Bidang ASFF	Nilai sampel sebelum tampilan kontrol konsolidasi	Nilai sampel setelah tampilan kontrol terkonsolidasi, dan deskripsi perubahan
ProductFields.RecommendationUrl	https://docs.aws.amazon.com/console/securityhub/PCI.EC2.2/remediation	https://docs.aws.amazon.com/console/securityhub/EC2.2/remediation Bidang ini tidak lagi mereferensikan standar.
Remediation.Recommendation.Text	“Untuk petunjuk tentang cara memperbaiki masalah ini, lihat dokumentasi PCI DSS AWS Security Hub Cloud Security Posture Management (CSPM) Security Hub.”	“Untuk petunjuk tentang cara memperbaiki masalah ini, lihat dokumentasi kontrol AWS Security Hub Cloud Security Posture Management (CSPM) Security Hub.” Bidang ini tidak lagi mereferensikan standar.
Remediasi.Rekomendasi.Url	https://docs.aws.amazon.com/console/securityhub/PCI.EC2.2/remediation	https://docs.aws.amazon.com/console/securityhub/EC2.2/remediation Bidang ini tidak lagi mereferensikan standar.

Temuan kontrol konsolidasi - perubahan ASFF

Jika Anda mengaktifkan temuan kontrol terkonsolidasi, Anda mungkin terpengaruh oleh perubahan bidang dan nilai berikut untuk temuan kontrol di ASFF. Perubahan ini merupakan tambahan dari perubahan yang diperkenalkan oleh fitur tampilan kontrol terkonsolidasi. Jika alur kerja Anda tidak bergantung pada nilai untuk bidang ASFF ini, tidak diperlukan tindakan. Jika Anda memiliki alur kerja yang bergantung pada nilai tertentu untuk bidang ini, perbarui alur kerja Anda untuk menggunakan nilai saat ini.

Tip

Jika Anda menggunakan [Respons Keamanan Otomatis pada solusi AWS v2.0.0](#), perhatikan bahwa solusi ini mendukung temuan kontrol terkonsolidasi. Ini berarti Anda dapat mempertahankan alur kerja saat ini jika Anda mengaktifkan temuan kontrol terkonsolidasi.

Bidang ASFF	Nilai contoh sebelum mengaktifkan temuan kontrol konsolidasi	Nilai contoh setelah mengaktifkan temuan kontrol konsolidasi, dan deskripsi perubahan
GeneratorId	aws-foundational-security-best-practices/v/1.0.0/Config .1	Kontrol keamanan/config.1 Bidang ini tidak lagi mereferensikan standar.
Judul	PCI.config.1 harus diaktifkan AWS Config	AWS Config harus diaktifkan Bidang ini tidak lagi mereferensikan informasi khusus standar.
Id	arn:aws:securityhub: eu-central-1:123456789012:6d6a26-a156-48f0-9403-115983e5a956 subscription/pci-dss/v/3.2.1/PCI.IAM.5/finding/ab	arn:aws:securityhub: eu-central-1:123456789012: keamanan-6d6a26-a156-48f0-9403-115983e5a956 control/iam.9/finding/ab Bidang ini tidak lagi mereferensikan standar.
ProductFields.ControlId	PCI. EC2.2	Dihapus. Lihat Compliance.SecurityControlId sebagai gantinya. Bidang ini dihapus demi ID kontrol agnostik standar tunggal.
ProductFields.RuleId	1.3	Dihapus. Lihat Compliance.SecurityControlId sebagai gantinya.

Bidang ASFF	Nilai contoh sebelum mengaktifkan temuan kontrol konsolidasi	Nilai contoh setelah mengaktifkan temuan kontrol konsolidasi, dan deskripsi perubahan Bidang ini dihapus demi ID kontrol agnostik standar tunggal.
Deskripsi	Kontrol PCI DSS ini memeriksa apakah AWS Config diaktifkan di akun dan wilayah saat ini.	AWS Kontrol ini memeriksa apakah AWS Config diaktifkan di akun dan wilayah saat ini. Bidang ini tidak lagi mereferensikan standar.
Kepelikan	<pre> "Keparahan": { "Produk": 90, "Label": "KRITIS", "Dinormalisasi": 90, "Asli": "KRITIS" } </pre>	<pre> "Keparahan": { "Label": "KRITIS", "Dinormalisasi": 90, "Asli": "KRITIS" } </pre> Security Hub CSPM tidak lagi menggunakan bidang Produk untuk menggambarkan tingkat keparahan temuan.
Tipe	["Perangkat Lunak dan Konfigurasi Checks/Industry dan Standar Regulasi/PCI-DSS"]	["Perangkat Lunak dan Konfigurasi Checks/Industry dan Standar Peraturan"] Bidang ini tidak lagi mereferensikan standar.

Bidang ASFF	Nilai contoh sebelum mengaktifkan temuan kontrol konsolidasi	Nilai contoh setelah mengaktifkan temuan kontrol konsolidasi, dan deskripsi perubahan
Kepatuhan. RelatedRequirements	["PCI DSS 10.5.2", "PCI DSS 11.5", "AWS Yayasan CIS 2.5"]	["PCI DSS v3.2.1/10.5.2", "PCI DSS v3.2.1/11.5", "Tolok Ukur AWS Yayasan CIS v1.2.0/2.5"] Bidang ini menunjukkan persyaratan terkait di semua standar yang diaktifkan.
CreatedAt	2022-05-05T 08:18:13.138 Z	2022-09-25T 08:18:13.138 Z Format tetap sama, tetapi nilai diatur ulang saat Anda mengaktifkan temuan kontrol terkonsolidasi.
FirstObservedAt	2022-05-07T 08:18:13.138 Z	2022-09-28T 08:18:13.138 Z Format tetap sama, tetapi nilai diatur ulang saat Anda mengaktifkan temuan kontrol terkonsolidasi.
ProductFields.RecommendationUrl	https://docs.aws.amazon.com/console/securityhub/EC2.2/remediation	Dihapus. Lihat Remediation.Recommendation.Url sebagai gantinya.
ProductFields.StandardsArn	arn:aws:securityhub:::/1.0.0/standards/aws-foundational-security-best-practices/v	Dihapus. Lihat Compliance.AssociatedStandards sebagai gantinya.

Bidang ASFF	Nilai contoh sebelum mengaktifkan temuan kontrol konsolidasi	Nilai contoh setelah mengaktifkan temuan kontrol konsolidasi, dan deskripsi perubahan
ProductFields.StandardsControlArn	arn:aws:securityhub: us-timur-1:123456789012: .1 control/aws-foundational-security-best-practices/v/1.0.0/Config	Dihapus. Security Hub CSPM menghasilkan satu temuan untuk pemeriksaan keamanan di seluruh standar.
ProductFields.StandardsGuideArn	arn:aws:securityhub::: /1.2.0 ruleset/cis-aws-foundations-benchmark/v	Dihapus. Lihat Compliance.AssociatedStandards sebagai gantinya.
ProductFields.StandardsGuideSubscriptionArn	arn:aws:securityhub: us-timur-2:123456789012: /1.2.0 subscription/cis-aws-foundations-benchmark/v	Dihapus. Security Hub CSPM menghasilkan satu temuan untuk pemeriksaan keamanan di seluruh standar.
ProductFields.StandardsSubscriptionArn	arn:aws:securityhub: us-timur-1:123456789012: /1.0.0 subscription/aws-foundational-security-best-practices/v	Dihapus. Security Hub CSPM menghasilkan satu temuan untuk pemeriksaan keamanan di seluruh standar.
ProductFields.aws/securityhub/FindingId	arn:aws:securityhub: us-east-1:: /751c2173-7372-4e12-8656-a5210dfb1d67 product/aws/securityhub/arn:aws:securityhub:us-east-1:123456789012:subscription/aws-foundational-security-best-practices/v/1.0.0/Config.1/finding	arn:aws:securityhub: us-east-1:: /751c2173-7372-4e12-8656-a5210dfb1d67 product/aws/securityhub/arn:aws:securityhub:us-east-1:123456789012:security-control/Config.1/finding Bidang ini tidak lagi mereferensikan standar.

Nilai untuk bidang ASFF yang disediakan pelanggan setelah mengaktifkan temuan kontrol terkonsolidasi

Jika Anda mengaktifkan temuan kontrol terkonsolidasi, Security Hub CSPM menghasilkan satu temuan di seluruh standar dan mengarsipkan temuan asli (temuan terpisah untuk setiap standar).

Pembaruan yang Anda buat untuk temuan asli dengan menggunakan konsol CSPM Security Hub atau [BatchUpdateFindings](#) operasi tidak akan disimpan dalam temuan baru. Jika perlu, Anda dapat memulihkan data ini dengan merujuk pada temuan yang diarsipkan. Untuk meninjau temuan yang diarsipkan, Anda dapat menggunakan halaman Temuan di konsol CSPM Security Hub dan menyetel filter status Record ke ARCHIVED. Atau, Anda dapat menggunakan [GetFindings](#) pengoperasian Security Hub CSPM API.

Bidang ASFF yang disediakan pelanggan	Deskripsi perubahan setelah memungkinkan temuan kontrol konsolidasi
Kepercayaan	Reset ke status kosong.
Kekritisan	Reset ke status kosong.
Catatan	Reset ke status kosong.
RelatedFindings	Reset ke status kosong.
Kepelikan	Tingkat keparahan default temuan (cocok dengan tingkat keparahan kontrol).
Tipe	Reset ke nilai agnostik standar.
UserDefinedFields	Reset ke status kosong.
VerificationState	Reset ke status kosong.
Alur kerja	Temuan baru yang gagal memiliki nilai defaultNEW. Temuan baru yang lulus memiliki nilai defaultRESOLVED.

Generator IDs sebelum dan sesudah memungkinkan temuan kontrol terkonsolidasi

Tabel berikut mencantumkan perubahan nilai ID generator untuk kontrol saat Anda mengaktifkan temuan kontrol terkonsolidasi. Perubahan ini berlaku untuk kontrol yang didukung CSPM Security Hub per 15 Februari 2023.

generatorId sebelum mengaktifkan temuan kontrol terkonsolidasi	generatorId setelah mengaktifkan temuan kontrol terkonsolidasi
arn:aws:securityhub::: /1.1 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	kontrol keamanan/ .1 CloudWatch
arn:aws:securityhub::: /1.10 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	Kontrol keamanan/IAM.16
arn:aws:securityhub::: /1.11 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	Kontrol keamanan/IAM.17
arn:aws:securityhub::: /1.12 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	Kontrol keamanan/IAM.4
arn:aws:securityhub::: /1.13 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	Kontrol keamanan/IAM.9
arn:aws:securityhub::: /1.14 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	Kontrol keamanan/IAM.6
arn:aws:securityhub::: /1.16 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	Kontrol keamanan/IAM.2
arn:aws:securityhub::: /1.2 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	Kontrol keamanan/IAM.5
arn:aws:securityhub::: /1.20 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	Kontrol keamanan/IAM.18
arn:aws:securityhub::: /1.22 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	Kontrol keamanan/IAM.1
arn:aws:securityhub::: /1.3 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	Kontrol keamanan/IAM.8
arn:aws:securityhub::: /1.4 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	Kontrol keamanan/IAM.3

generatorId sebelum mengaktifkan temuan kontrol terkonsolidasi	generatorId setelah mengaktifkan temuan kontrol terkonsolidasi
arn:aws:securityhub::: /1.5 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	Kontrol keamanan/IAM.11
arn:aws:securityhub::: /1.6 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	Kontrol keamanan/IAM.12
arn:aws:securityhub::: /1.7 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	Kontrol keamanan/IAM.13
arn:aws:securityhub::: /1.8 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	Kontrol keamanan/IAM.14
arn:aws:securityhub::: /1.9 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	Kontrol keamanan/IAM.15
arn:aws:securityhub::: /2.1 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	kontrol keamanan/ .1 CloudTrail
arn:aws:securityhub::: /2.2 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	kontrol keamanan/ .4 CloudTrail
arn:aws:securityhub::: /2.3 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	kontrol keamanan/ .6 CloudTrail
arn:aws:securityhub::: /2.4 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	kontrol keamanan/ .5 CloudTrail
arn:aws:securityhub::: /2.5 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	Kontrol keamanan/config.1
arn:aws:securityhub::: /2.6 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	kontrol keamanan/ .7 CloudTrail
arn:aws:securityhub::: /2.7 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	kontrol keamanan/ .2 CloudTrail

generatorId sebelum mengaktifkan temuan kontrol terkonsolidasi	generatorId setelah mengaktifkan temuan kontrol terkonsolidasi
arn:aws:securityhub::: /2.8 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	Kontrol keamanan/KMS.4
arn:aws:securityhub::: /2.9 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	kontrol keamanan/ .6 EC2
arn:aws:securityhub::: /3.1 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	kontrol keamanan/ .2 CloudWatch
arn:aws:securityhub::: /3.2 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	kontrol keamanan/ .3 CloudWatch
arn:aws:securityhub::: /3.3 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	kontrol keamanan/ .1 CloudWatch
arn:aws:securityhub::: /3.4 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	kontrol keamanan/ .4 CloudWatch
arn:aws:securityhub::: /3.5 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	kontrol keamanan/ .5 CloudWatch
arn:aws:securityhub::: /3.6 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	kontrol keamanan/ .6 CloudWatch
arn:aws:securityhub::: /3.7 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	kontrol keamanan/ .7 CloudWatch
arn:aws:securityhub::: /3.8 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	kontrol keamanan/ .8 CloudWatch
arn:aws:securityhub::: /3.9 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	kontrol keamanan/ .9 CloudWatch
arn:aws:securityhub::: /3.10 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	kontrol keamanan/ .10 CloudWatch

generatorId sebelum mengaktifkan temuan kontrol terkonsolidasi	generatorId setelah mengaktifkan temuan kontrol terkonsolidasi
arn:aws:securityhub:::/3.11 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	kontrol keamanan/ .11 CloudWatch
arn:aws:securityhub:::/3.12 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	kontrol keamanan/ .12 CloudWatch
arn:aws:securityhub:::/3.13 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	kontrol keamanan/ .13 CloudWatch
arn:aws:securityhub:::/3.14 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	kontrol keamanan/ .14 CloudWatch
arn:aws:securityhub:::/4.1 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	kontrol keamanan/ .13 EC2
arn:aws:securityhub:::/4.2 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	kontrol keamanan/ .14 EC2
arn:aws:securityhub:::/4.3 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	kontrol keamanan/ .2 EC2
cis-aws-foundations-benchmark/v/1.4.0/1.10	Kontrol keamanan/IAM.5
cis-aws-foundations-benchmark/v/1.4.0/1.14	Kontrol keamanan/IAM.3
cis-aws-foundations-benchmark/v/1.4.0/1.16	Kontrol keamanan/IAM.1
cis-aws-foundations-benchmark/v/1.4.0/1.17	Kontrol keamanan/IAM.18
cis-aws-foundations-benchmark/v/1.4.0/1.4	Kontrol keamanan/IAM.4
cis-aws-foundations-benchmark/v/1.4.0/1.5	Kontrol keamanan/IAM.9
cis-aws-foundations-benchmark/v/1.4.0/1.6	Kontrol keamanan/IAM.6
cis-aws-foundations-benchmark/v/1.4.0/1.7	kontrol keamanan/ .1 CloudWatch
cis-aws-foundations-benchmark/v/1.4.0/1.8	Kontrol keamanan/IAM.15

generatorId sebelum mengaktifkan temuan kontrol terkonsolidasi	generatorId setelah mengaktifkan temuan kontrol terkonsolidasi
cis-aws-foundations-benchmark/v/1.4.0/1.9	Kontrol keamanan/IAM.16
cis-aws-foundations-benchmark/v/1.4.0/2.1.2	Kontrol keamanan/S3.5
cis-aws-foundations-benchmark/v/1.4.0/2.1.5.1	Kontrol keamanan/S3.1
cis-aws-foundations-benchmark/v/1.4.0/2.1.5.2	Kontrol keamanan/S3.8
cis-aws-foundations-benchmark/v/1.4.0/2.2.1	kontrol keamanan/ .7 EC2
cis-aws-foundations-benchmark/v/1.4.0/2.3.1	Kontrol keamanan/RDS.3
cis-aws-foundations-benchmark/v/1.4.0/3.1	kontrol keamanan/ .1 CloudTrail
cis-aws-foundations-benchmark/v/1.4.0/3.2	kontrol keamanan/ .4 CloudTrail
cis-aws-foundations-benchmark/v/1.4.0/3.4	kontrol keamanan/ .5 CloudTrail
cis-aws-foundations-benchmark/v/1.4.0/3.5	Kontrol keamanan/config.1
cis-aws-foundations-benchmark/v/1.4.0/3.6	Kontrol keamanan/S3.9
cis-aws-foundations-benchmark/v/1.4.0/3.7	kontrol keamanan/ .2 CloudTrail
cis-aws-foundations-benchmark/v/1.4.0/3.8	Kontrol keamanan/KMS.4
cis-aws-foundations-benchmark/v/1.4.0/3.9	kontrol keamanan/ .6 EC2
cis-aws-foundations-benchmark/v/1.4.0/4.3	kontrol keamanan/ .1 CloudWatch
cis-aws-foundations-benchmark/v/1.4.0/4.4	kontrol keamanan/ .4 CloudWatch
cis-aws-foundations-benchmark/v/1.4.0/4.5	kontrol keamanan/ .5 CloudWatch
cis-aws-foundations-benchmark/v/1.4.0/4.6	kontrol keamanan/ .6 CloudWatch
cis-aws-foundations-benchmark/v/1.4.0/4.7	kontrol keamanan/ .7 CloudWatch
cis-aws-foundations-benchmark/v/1.4.0/4.8	kontrol keamanan/ .8 CloudWatch

generatorId sebelum mengaktifkan temuan kontrol terkonsolidasi	generatorId setelah mengaktifkan temuan kontrol terkonsolidasi
cis-aws-foundations-benchmark/v/1.4.0/4.9	kontrol keamanan/ .9 CloudWatch
cis-aws-foundations-benchmark/v/1.4.0/4.10	kontrol keamanan/ .10 CloudWatch
cis-aws-foundations-benchmark/v/1.4.0/4.11	kontrol keamanan/ .11 CloudWatch
cis-aws-foundations-benchmark/v/1.4.0/4.12	kontrol keamanan/ .12 CloudWatch
cis-aws-foundations-benchmark/v/1.4.0/4.13	kontrol keamanan/ .13 CloudWatch
cis-aws-foundations-benchmark/v/1.4.0/4.14	kontrol keamanan/ .14 CloudWatch
cis-aws-foundations-benchmark/v/1.4.0/5.1	kontrol keamanan/ .21 EC2
cis-aws-foundations-benchmark/v/1.4.0/5.3	kontrol keamanan/ .2 EC2
aws-foundational-security-best-practices/ v/1.0.0/Account .1	Kontrol keamanan/akun.1
aws-foundational-security-best-practices/ v/1.0.0/ACM .1	Kontrol keamanan/ACM.1
aws-foundational-security-best-practices/ v/1.0.0/APIGateway .1	kontrol keamanan/ .1 APIGateway
aws-foundational-security-best-practices/ v/1.0.0/APIGateway .2	kontrol keamanan/ .2 APIGateway
aws-foundational-security-best-practices/ v/1.0.0/APIGateway .3	kontrol keamanan/ .3 APIGateway
aws-foundational-security-best-practices/ v/1.0.0/APIGateway .4	kontrol keamanan/ .4 APIGateway
aws-foundational-security-best-practices/ v/1.0.0/APIGateway .5	kontrol keamanan/ .5 APIGateway

generatorId sebelum mengaktifkan temuan kontrol terkonsolidasi	generatorId setelah mengaktifkan temuan kontrol terkonsolidasi
aws-foundational-security-best-practices/v/1.0.0/APIGateway .8	kontrol keamanan/ .8 APIGateway
aws-foundational-security-best-practices/v/1.0.0/APIGateway .9	kontrol keamanan/ .9 APIGateway
aws-foundational-security-best-practices/v/1.0.0/AutoScaling .1	kontrol keamanan/ .1 AutoScaling
aws-foundational-security-best-practices/v/1.0.0/AutoScaling .2	kontrol keamanan/ .2 AutoScaling
aws-foundational-security-best-practices/v/1.0.0/AutoScaling .3	kontrol keamanan/ .3 AutoScaling
aws-foundational-security-best-practices/v/1.0.0/AutoScaling .5	Kontrol keamanan/Autoscaling.5
aws-foundational-security-best-practices/v/1.0.0/AutoScaling .6	kontrol keamanan/ .6 AutoScaling
aws-foundational-security-best-practices/v/1.0.0/AutoScaling .9	kontrol keamanan/ .9 AutoScaling
aws-foundational-security-best-practices/v/1.0.0/CloudFront .1	kontrol keamanan/ .1 CloudFront
aws-foundational-security-best-practices/v/1.0.0/CloudFront .3	kontrol keamanan/ .3 CloudFront
aws-foundational-security-best-practices/v/1.0.0/CloudFront .4	kontrol keamanan/ .4 CloudFront
aws-foundational-security-best-practices/v/1.0.0/CloudFront .5	kontrol keamanan/ .5 CloudFront

generatorId sebelum mengaktifkan temuan kontrol terkonsolidasi	generatorId setelah mengaktifkan temuan kontrol terkonsolidasi
aws-foundational-security-best-practices/v/1.0.0/CloudFront .6	kontrol keamanan/ .6 CloudFront
aws-foundational-security-best-practices/v/1.0.0/CloudFront .7	kontrol keamanan/ .7 CloudFront
aws-foundational-security-best-practices/v/1.0.0/CloudFront .8	kontrol keamanan/ .8 CloudFront
aws-foundational-security-best-practices/v/1.0.0/CloudFront .9	kontrol keamanan/ .9 CloudFront
aws-foundational-security-best-practices/v/1.0.0/CloudFront .10	kontrol keamanan/ .10 CloudFront
aws-foundational-security-best-practices/v/1.0.0/CloudFront .12	kontrol keamanan/ .12 CloudFront
aws-foundational-security-best-practices/v/1.0.0/CloudTrail .1	kontrol keamanan/ .1 CloudTrail
aws-foundational-security-best-practices/v/1.0.0/CloudTrail .2	kontrol keamanan/ .2 CloudTrail
aws-foundational-security-best-practices/v/1.0.0/CloudTrail .4	kontrol keamanan/ .4 CloudTrail
aws-foundational-security-best-practices/v/1.0.0/CloudTrail .5	kontrol keamanan/ .5 CloudTrail
aws-foundational-security-best-practices/v/1.0.0/CodeBuild .1	kontrol keamanan/ .1 CodeBuild
aws-foundational-security-best-practices/v/1.0.0/CodeBuild .2	kontrol keamanan/ .2 CodeBuild

generatorId sebelum mengaktifkan temuan kontrol terkonsolidasi	generatorId setelah mengaktifkan temuan kontrol terkonsolidasi
aws-foundational-security-best-practices/v/1.0.0/CodeBuild .3	kontrol keamanan/ .3 CodeBuild
aws-foundational-security-best-practices/v/1.0.0/CodeBuild .4	kontrol keamanan/ .4 CodeBuild
aws-foundational-security-best-practices/v/1.0.0/Config .1	Kontrol keamanan/config.1
aws-foundational-security-best-practices/v/1.0.0/DMS .1	Kontrol keamanan/DMS.1
aws-foundational-security-best-practices/v/1.0.0/DynamoDB .1	Kontrol keamanan/DynamoDB.1
aws-foundational-security-best-practices/v/1.0.0/DynamoDB .2	Kontrol keamanan/Dynamodb.2
aws-foundational-security-best-practices/v/1.0.0/DynamoDB .3	Kontrol keamanan/Dynamodb.3
aws-foundational-security-best-practices/v/1.0.0/EC 2.1	kontrol keamanan/ .1 EC2
aws-foundational-security-best-practices/v/1.0.0/EC 2.3	kontrol keamanan/ .3 EC2
aws-foundational-security-best-practices/v/1.0.0/EC 2,4	kontrol keamanan/ .4 EC2
aws-foundational-security-best-practices/v/1.0.0/EC 2.6	kontrol keamanan/ .6 EC2
aws-foundational-security-best-practices/v/1.0.0/EC 2,7	kontrol keamanan/ .7 EC2

generatorId sebelum mengaktifkan temuan kontrol terkonsolidasi	generatorId setelah mengaktifkan temuan kontrol terkonsolidasi
aws-foundational-security-best-practices/v/1.0.0/EC 2,8	kontrol keamanan/ .8 EC2
aws-foundational-security-best-practices/v/1.0.0/EC 2,9	kontrol keamanan/ .9 EC2
aws-foundational-security-best-practices/v/1.0.0/EC 2.10	kontrol keamanan/ .10 EC2
aws-foundational-security-best-practices/v/1.0.0/EC 2.15	kontrol keamanan/ .15 EC2
aws-foundational-security-best-practices/v/1.0.0/EC 2.16	kontrol keamanan/ .16 EC2
aws-foundational-security-best-practices/v/1.0.0/EC 2.17	kontrol keamanan/ .17 EC2
aws-foundational-security-best-practices/v/1.0.0/EC 2.18	kontrol keamanan/ .18 EC2
aws-foundational-security-best-practices/v/1.0.0/EC 2.19	kontrol keamanan/ .19 EC2
aws-foundational-security-best-practices/v/1.0.0/EC 2.2	kontrol keamanan/ .2 EC2
aws-foundational-security-best-practices/v/1.0.0/EC 2.20	kontrol keamanan/ .20 EC2
aws-foundational-security-best-practices/v/1.0.0/EC 2,21	kontrol keamanan/ .21 EC2
aws-foundational-security-best-practices/v/1.0.0/EC 2,23	kontrol keamanan/ .23 EC2

generatorId sebelum mengaktifkan temuan kontrol terkonsolidasi	generatorId setelah mengaktifkan temuan kontrol terkonsolidasi
aws-foundational-security-best-practices/v/1.0.0/EC 2,24	kontrol keamanan/ .24 EC2
aws-foundational-security-best-practices/v/1.0.0/EC 2,25	kontrol keamanan/ .25 EC2
aws-foundational-security-best-practices/v/1.0.0/ECR .1	Kontrol keamanan/ECR.1
aws-foundational-security-best-practices/v/1.0.0/ECR .2	Kontrol keamanan/ECR.2
aws-foundational-security-best-practices/v/1.0.0/ECR .3	Kontrol keamanan/ECR.3
aws-foundational-security-best-practices/v/1.0.0/ECS .1	Kontrol keamanan/ECS.1
aws-foundational-security-best-practices/v/1.0.0/ECS .10	Kontrol keamanan/ECS.10
aws-foundational-security-best-practices/v/1.0.0/ECS .12	Kontrol keamanan/ECS.12
aws-foundational-security-best-practices/v/1.0.0/ECS .2	Kontrol keamanan/ECS.2
aws-foundational-security-best-practices/v/1.0.0/ECS .3	Kontrol keamanan/ECS.3
aws-foundational-security-best-practices/v/1.0.0/ECS .4	Kontrol keamanan/ECS.4
aws-foundational-security-best-practices/v/1.0.0/ECS .5	Kontrol keamanan/ECS.5

generatorId sebelum mengaktifkan temuan kontrol terkonsolidasi	generatorId setelah mengaktifkan temuan kontrol terkonsolidasi
aws-foundational-security-best-practices/v/1.0.0/ECS .8	Kontrol keamanan/ECS.8
aws-foundational-security-best-practices/v/1.0.0/EFS .1	Kontrol keamanan/EFS.1
aws-foundational-security-best-practices/v/1.0.0/EFS .2	Kontrol keamanan/EFS.2
aws-foundational-security-best-practices/v/1.0.0/EFS .3	Kontrol keamanan/EFS.3
aws-foundational-security-best-practices/v/1.0.0/EFS .4	Kontrol keamanan/EFS.4
aws-foundational-security-best-practices/v/1.0.0/EKS .2	Kontrol keamanan/EKS.2
aws-foundational-security-best-practices/v/1.0.0/ElasticBeanstalk .1	kontrol keamanan/ .1 ElasticBeanstalk
aws-foundational-security-best-practices/v/1.0.0/ElasticBeanstalk .2	kontrol keamanan/ .2 ElasticBeanstalk
aws-foundational-security-best-practices/v/1.0.0/ELBv 2.1	Kontrol keamanan/ELB.1
aws-foundational-security-best-practices/v/1.0.0/ELB .2	Kontrol keamanan/ELB.2
aws-foundational-security-best-practices/v/1.0.0/ELB .3	Kontrol keamanan/ELB.3
aws-foundational-security-best-practices/v/1.0.0/ELB .4	Kontrol keamanan/ELB.4

generatorId sebelum mengaktifkan temuan kontrol terkonsolidasi	generatorId setelah mengaktifkan temuan kontrol terkonsolidasi
aws-foundational-security-best-practices/v/1.0.0/ELB .5	Kontrol keamanan/ELB.5
aws-foundational-security-best-practices/v/1.0.0/ELB .6	Kontrol keamanan/ELB.6
aws-foundational-security-best-practices/v/1.0.0/ELB .7	Kontrol keamanan/ELB.7
aws-foundational-security-best-practices/v/1.0.0/ELB .8	Kontrol keamanan/ELB.8
aws-foundational-security-best-practices/v/1.0.0/ELB .9	Kontrol keamanan/ELB.9
aws-foundational-security-best-practices/v/1.0.0/ELB .10	Kontrol keamanan/ELB.10
aws-foundational-security-best-practices/v/1.0.0/ELB .11	Kontrol keamanan/ELB.11
aws-foundational-security-best-practices/v/1.0.0/ELB .12	Kontrol keamanan/ELB.12
aws-foundational-security-best-practices/v/1.0.0/ELB .13	Kontrol keamanan/ELB.13
aws-foundational-security-best-practices/v/1.0.0/ELB .14	Kontrol keamanan/ELB.14
aws-foundational-security-best-practices/v/1.0.0/EMR .1	Kontrol keamanan/EMR.1
aws-foundational-security-best-practices/v/1.0.0/ES .1	Kontrol keamanan/ES.1

generatorId sebelum mengaktifkan temuan kontrol terkonsolidasi	generatorId setelah mengaktifkan temuan kontrol terkonsolidasi
aws-foundational-security-best-practices/v/1.0.0/ES .2	Kontrol keamanan/ES.2
aws-foundational-security-best-practices/v/1.0.0/ES .3	Kontrol keamanan/ES.3
aws-foundational-security-best-practices/v/1.0.0/ES .4	Kontrol keamanan/ES.4
aws-foundational-security-best-practices/v/1.0.0/ES .5	Kontrol keamanan/ES.5
aws-foundational-security-best-practices/v/1.0.0/ES .6	Kontrol keamanan/ES.6
aws-foundational-security-best-practices/v/1.0.0/ES .7	Kontrol keamanan/ES.7
aws-foundational-security-best-practices/v/1.0.0/ES .8	Kontrol keamanan/ES.8
aws-foundational-security-best-practices/v/1.0.0/GuardDuty .1	kontrol keamanan/ .1 GuardDuty
aws-foundational-security-best-practices/v/1.0.0/IAM .1	Kontrol keamanan/IAM.1
aws-foundational-security-best-practices/v/1.0.0/IAM .2	Kontrol keamanan/IAM.2
aws-foundational-security-best-practices/v/1.0.0/IAM .21	Kontrol keamanan/IAM.21
aws-foundational-security-best-practices/v/1.0.0/IAM .3	Kontrol keamanan/IAM.3

generatorId sebelum mengaktifkan temuan kontrol terkonsolidasi	generatorId setelah mengaktifkan temuan kontrol terkonsolidasi
aws-foundational-security-best-practices/v/1.0.0/IAM .4	Kontrol keamanan/IAM.4
aws-foundational-security-best-practices/v/1.0.0/IAM .5	Kontrol keamanan/IAM.5
aws-foundational-security-best-practices/v/1.0.0/IAM .6	Kontrol keamanan/IAM.6
aws-foundational-security-best-practices/v/1.0.0/IAM .7	Kontrol keamanan/IAM.7
aws-foundational-security-best-practices/v/1.0.0/IAM .8	Kontrol keamanan/IAM.8
aws-foundational-security-best-practices/v/1.0.0/Kinesis .1	Kontrol keamanan/kinesis.1
aws-foundational-security-best-practices/v/1.0.0/KMS .1	Kontrol keamanan/KMS.1
aws-foundational-security-best-practices/v/1.0.0/KMS .2	Kontrol keamanan/KMS.2
aws-foundational-security-best-practices/v/1.0.0/KMS .3	Kontrol keamanan/KMS.3
aws-foundational-security-best-practices/v/1.0.0/Lambda .1	Kontrol keamanan/Lambda.1
aws-foundational-security-best-practices/v/1.0.0/Lambda .2	Kontrol keamanan/Lambda.2
aws-foundational-security-best-practices/v/1.0.0/Lambda .5	Kontrol keamanan/Lambda.5

generatorId sebelum mengaktifkan temuan kontrol terkonsolidasi	generatorId setelah mengaktifkan temuan kontrol terkonsolidasi
aws-foundational-security-best-practices/v/1.0.0/NetworkFirewall .3	kontrol keamanan/ .3 NetworkFirewall
aws-foundational-security-best-practices/v/1.0.0/NetworkFirewall .4	kontrol keamanan/ .4 NetworkFirewall
aws-foundational-security-best-practices/v/1.0.0/NetworkFirewall .5	kontrol keamanan/ .5 NetworkFirewall
aws-foundational-security-best-practices/v/1.0.0/NetworkFirewall .6	kontrol keamanan/ .6 NetworkFirewall
aws-foundational-security-best-practices/v/1.0.0/Opensearch .1	Kontrol keamanan/OpenSearch.1
aws-foundational-security-best-practices/v/1.0.0/Opensearch .2	Kontrol keamanan/OpenSearch.2
aws-foundational-security-best-practices/v/1.0.0/Opensearch .3	Kontrol keamanan/OpenSearch.3
aws-foundational-security-best-practices/v/1.0.0/Opensearch .4	Kontrol keamanan/OpenSearch.4
aws-foundational-security-best-practices/v/1.0.0/Opensearch .5	Kontrol keamanan/OpenSearch.5
aws-foundational-security-best-practices/v/1.0.0/Opensearch .6	Kontrol keamanan/OpenSearch.6
aws-foundational-security-best-practices/v/1.0.0/Opensearch .7	Kontrol keamanan/OpenSearch.7
aws-foundational-security-best-practices/v/1.0.0/Opensearch .8	Kontrol keamanan/OpenSearch.8

generatorId sebelum mengaktifkan temuan kontrol terkonsolidasi	generatorId setelah mengaktifkan temuan kontrol terkonsolidasi
aws-foundational-security-best-practices/v/1.0.0/RDS .1	Kontrol keamanan/RDS.1
aws-foundational-security-best-practices/v/1.0.0/RDS .10	Kontrol keamanan/RDS.10
aws-foundational-security-best-practices/v/1.0.0/RDS .11	Kontrol keamanan/RDS.11
aws-foundational-security-best-practices/v/1.0.0/RDS .12	Kontrol keamanan/RDS.12
aws-foundational-security-best-practices/v/1.0.0/RDS .13	Kontrol keamanan/RDS.13
aws-foundational-security-best-practices/v/1.0.0/RDS .14	Kontrol keamanan/RDS.14
aws-foundational-security-best-practices/v/1.0.0/RDS .15	Kontrol keamanan/RDS.15
aws-foundational-security-best-practices/v/1.0.0/RDS .16	Kontrol keamanan/RDS.16
aws-foundational-security-best-practices/v/1.0.0/RDS .17	Kontrol keamanan/RDS.17
aws-foundational-security-best-practices/v/1.0.0/RDS .19	Kontrol keamanan/RDS.19
aws-foundational-security-best-practices/v/1.0.0/RDS .2	Kontrol keamanan/RDS.2
aws-foundational-security-best-practices/v/1.0.0/RDS .20	Kontrol keamanan/RDS.20

generatorId sebelum mengaktifkan temuan kontrol terkonsolidasi	generatorId setelah mengaktifkan temuan kontrol terkonsolidasi
aws-foundational-security-best-practices/v/1.0.0/RDS .21	Kontrol keamanan/RDS.21
aws-foundational-security-best-practices/v/1.0.0/RDS .22	Kontrol keamanan/RDS.22
aws-foundational-security-best-practices/v/1.0.0/RDS .23	Kontrol keamanan/RDS.23
aws-foundational-security-best-practices/v/1.0.0/RDS .24	Kontrol keamanan/RDS.24
aws-foundational-security-best-practices/v/1.0.0/RDS .25	Kontrol keamanan/RDS.25
aws-foundational-security-best-practices/v/1.0.0/RDS .3	Kontrol keamanan/RDS.3
aws-foundational-security-best-practices/v/1.0.0/RDS .4	Kontrol keamanan/RDS.4
aws-foundational-security-best-practices/v/1.0.0/RDS .5	Kontrol keamanan/RDS.5
aws-foundational-security-best-practices/v/1.0.0/RDS .6	Kontrol keamanan/RDS.6
aws-foundational-security-best-practices/v/1.0.0/RDS .7	Kontrol keamanan/RDS.7
aws-foundational-security-best-practices/v/1.0.0/RDS .8	Kontrol keamanan/RDS.8
aws-foundational-security-best-practices/v/1.0.0/RDS .9	Kontrol keamanan/RDS.9

generatorId sebelum mengaktifkan temuan kontrol terkonsolidasi	generatorId setelah mengaktifkan temuan kontrol terkonsolidasi
aws-foundational-security-best-practices/v/1.0.0/Redshift .1	Kontrol keamanan/pergeseran merah.1
aws-foundational-security-best-practices/v/1.0.0/Redshift .2	Kontrol keamanan/pergeseran merah.2
aws-foundational-security-best-practices/v/1.0.0/Redshift .3	Kontrol keamanan/pergeseran merah.3
aws-foundational-security-best-practices/v/1.0.0/Redshift .4	Kontrol keamanan/Redshift.4
aws-foundational-security-best-practices/v/1.0.0/Redshift .6	Kontrol keamanan/pergeseran merah.6
aws-foundational-security-best-practices/v/1.0.0/Redshift .7	Kontrol keamanan/pergeseran merah.7
aws-foundational-security-best-practices/v/1.0.0/Redshift .8	Kontrol keamanan/pergeseran merah.8
aws-foundational-security-best-practices/v/1.0.0/Redshift .9	Kontrol keamanan/pergeseran merah.9
aws-foundational-security-best-practices/v/1.0.0/S 3.1	Kontrol keamanan/S3.1
aws-foundational-security-best-practices/v/1.0.0/S 3.12	Kontrol keamanan/S3.12
aws-foundational-security-best-practices/v/1.0.0/S 3.13	Kontrol keamanan/S3.13
aws-foundational-security-best-practices/v/1.0.0/S 3.2	Kontrol keamanan/S3.2

generatorId sebelum mengaktifkan temuan kontrol terkonsolidasi	generatorId setelah mengaktifkan temuan kontrol terkonsolidasi
aws-foundational-security-best-practices/v/1.0.0/S 3.3	Kontrol keamanan/S3.3
aws-foundational-security-best-practices/v/1.0.0/S 3,5	Kontrol keamanan/S3.5
aws-foundational-security-best-practices/v/1.0.0/S 3,6	Kontrol keamanan/S3.6
aws-foundational-security-best-practices/v/1.0.0/S 3,8	Kontrol keamanan/S3.8
aws-foundational-security-best-practices/v/1.0.0/S 3,9	Kontrol keamanan/S3.9
aws-foundational-security-best-practices/v/1.0.0/SageMaker .1	kontrol keamanan/ .1 SageMaker
aws-foundational-security-best-practices/v/1.0.0/SageMaker .2	kontrol keamanan/ .2 SageMaker
aws-foundational-security-best-practices/v/1.0.0/SageMaker .3	kontrol keamanan/ .3 SageMaker
aws-foundational-security-best-practices/v/1.0.0/SecretsManager .1	kontrol keamanan/ .1 SecretsManager
aws-foundational-security-best-practices/v/1.0.0/SecretsManager .2	kontrol keamanan/ .2 SecretsManager
aws-foundational-security-best-practices/v/1.0.0/SecretsManager .3	kontrol keamanan/ .3 SecretsManager
aws-foundational-security-best-practices/v/1.0.0/SecretsManager .4	kontrol keamanan/ .4 SecretsManager

generatorId sebelum mengaktifkan temuan kontrol terkonsolidasi	generatorId setelah mengaktifkan temuan kontrol terkonsolidasi
aws-foundational-security-best-practices/v/1.0.0/SQS .1	Kontrol keamanan/SQS.1
aws-foundational-security-best-practices/v/1.0.0/SSM .1	Kontrol keamanan/SSM.1
aws-foundational-security-best-practices/v/1.0.0/SSM .2	Kontrol keamanan/SSM.2
aws-foundational-security-best-practices/v/1.0.0/SSM .3	Kontrol keamanan/SSM.3
aws-foundational-security-best-practices/v/1.0.0/SSM .4	Kontrol keamanan/SSM.4
aws-foundational-security-best-practices/v/1.0.0/WAF .1	Kontrol keamanan/WAF.1
aws-foundational-security-best-practices/v/1.0.0/WAF .2	Kontrol keamanan/WAF.2
aws-foundational-security-best-practices/v/1.0.0/WAF .3	Kontrol keamanan/WAF.3
aws-foundational-security-best-practices/v/1.0.0/WAF .4	Kontrol keamanan/WAF.4
aws-foundational-security-best-practices/v/1.0.0/WAF .6	Kontrol keamanan/WAF.6
aws-foundational-security-best-practices/v/1.0.0/WAF .7	Kontrol keamanan/WAF.7
aws-foundational-security-best-practices/v/1.0.0/WAF .8	Kontrol keamanan/WAF.8

generatorId sebelum mengaktifkan temuan kontrol terkonsolidasi	generatorId setelah mengaktifkan temuan kontrol terkonsolidasi
aws-foundational-security-best-practices/v/1.0.0/WAF .10	Kontrol keamanan/WAF.10
pci-dss/v/3.2.1/PCI. AutoScaling.1	kontrol keamanan/ .1 AutoScaling
pci-dss/v/3.2.1/PCI. CloudTrail.1	kontrol keamanan/ .2 CloudTrail
pci-dss/v/3.2.1/PCI. CloudTrail.2	kontrol keamanan/ .3 CloudTrail
pci-dss/v/3.2.1/PCI. CloudTrail.3	kontrol keamanan/ .4 CloudTrail
pci-dss/v/3.2.1/PCI. CloudTrail.4	kontrol keamanan/ .5 CloudTrail
pci-dss/v/3.2.1/PCI. CodeBuild.1	kontrol keamanan/ .1 CodeBuild
pci-dss/v/3.2.1/PCI. CodeBuild.2	kontrol keamanan/ .2 CodeBuild
pci- dss/v/3.2.1/PCI .config.1	Kontrol keamanan/config.1
pci- dss/v/3.2.1/PCI .CW.1	kontrol keamanan/ .1 CloudWatch
pci- dss/v/3.2.1/PCI .DMS.1	Kontrol keamanan/DMS.1
pci-dss/v/3.2.1/PCI. EC2.1	kontrol keamanan/ .1 EC2
pci-dss/v/3.2.1/PCI. EC2.2	kontrol keamanan/ .2 EC2
pci-dss/v/3.2.1/PCI. EC2.4	kontrol keamanan/ .12 EC2
pci-dss/v/3.2.1/PCI. EC2.5	kontrol keamanan/ .13 EC2
pci-dss/v/3.2.1/PCI. EC2.6	kontrol keamanan/ .6 EC2
pci-dss/v/3.2.1/PCI. ELBv2.1	Kontrol keamanan/ELB.1
pci- dss/v/3.2.1/PCI .ES1	Kontrol keamanan/ES.2
pci- dss/v/3.2.1/PCI .ES2	Kontrol keamanan/ES.1

generatorId sebelum mengaktifkan temuan kontrol terkonsolidasi	generatorId setelah mengaktifkan temuan kontrol terkonsolidasi
pci-dss/v/3.2.1/PCI.GuardDuty.1	kontrol keamanan/.1 GuardDuty
pci-dss/v/3.2.1/PCI.IAM.1	Kontrol keamanan/IAM.4
pci-dss/v/3.2.1/PCI.IAM.2	Kontrol keamanan/IAM.2
pci-dss/v/3.2.1/PCI.IAM.3	Kontrol keamanan/IAM.1
pci-dss/v/3.2.1/PCI.IAM.4	Kontrol keamanan/IAM.6
pci-dss/v/3.2.1/PCI.IAM.5	Kontrol keamanan/IAM.9
pci-dss/v/3.2.1/PCI.IAM.6	Kontrol keamanan/IAM.19
pci-dss/v/3.2.1/PCI.IAM.7	Kontrol keamanan/IAM.8
pci-dss/v/3.2.1/PCI.IAM.8	Kontrol keamanan/IAM.10
pci-dss/v/3.2.1/PCI.KMS.1	Kontrol keamanan/KMS.4
pci-dss/v/3.2.1/PCI.Lambda.1	Kontrol keamanan/Lambda.1
pci-dss/v/3.2.1/PCI.Lambda.2	Kontrol keamanan/Lambda.3
pci-dss/v/3.2.1/PCI.Opensearch.1	Kontrol keamanan/OpenSearch.2
pci-dss/v/3.2.1/PCI.Opensearch.2	Kontrol keamanan/OpenSearch.1
pci-dss/v/3.2.1/PCI.RDS.1	Kontrol keamanan/RDS.1
pci-dss/v/3.2.1/PCI.RDS.2	Kontrol keamanan/RDS.2
pci-dss/v/3.2.1/PCI.Redshift.1	Kontrol keamanan/pergeseran merah.1
pci-dss/v/3.2.1/PCI.S3.1	Kontrol keamanan/S3.3
pci-dss/v/3.2.1/PCI.S3.2	Kontrol keamanan/S3.2
pci-dss/v/3.2.1/PCI.S3.3	Kontrol keamanan/S3.7

generatorId sebelum mengaktifkan temuan kontrol terkonsolidasi	generatorId setelah mengaktifkan temuan kontrol terkonsolidasi
pci- dss/v/3.2.1/PCI .S3.5	Kontrol keamanan/S3.5
pci- dss/v/3.2.1/PCI .S3.6	Kontrol keamanan/S3.1
pci-dss/v/3.2.1/PCI. SageMaker.1	kontrol keamanan/ .1 SageMaker
pci- dss/v/3.2.1/PCI .SSM.1	Kontrol keamanan/SSM.2
pci- dss/v/3.2.1/PCI .SSM.2	Kontrol keamanan/SSM.3
pci- dss/v/3.2.1/PCI .SSM.3	Kontrol keamanan/SSM.1
service-managed-aws-control- tower/v/1.0.0/ ACM .1	Kontrol keamanan/ACM.1
service-managed-aws-control- tower/v/1.0.0/ APIGateway .1	kontrol keamanan/ .1 APIGateway
service-managed-aws-control- tower/v/1.0.0/ APIGateway .2	kontrol keamanan/ .2 APIGateway
service-managed-aws-control- tower/v/1.0.0/ APIGateway .3	kontrol keamanan/ .3 APIGateway
service-managed-aws-control- tower/v/1.0.0/ APIGateway .4	kontrol keamanan/ .4 APIGateway
service-managed-aws-control- tower/v/1.0.0/ APIGateway .5	kontrol keamanan/ .5 APIGateway
service-managed-aws-control- tower/v/1.0.0/ AutoScaling .1	kontrol keamanan/ .1 AutoScaling
service-managed-aws-control- tower/v/1.0.0/ AutoScaling .2	kontrol keamanan/ .2 AutoScaling

generatorId sebelum mengaktifkan temuan kontrol terkonsolidasi	generatorId setelah mengaktifkan temuan kontrol terkonsolidasi
service-managed-aws-control- tower/v/1.0.0/ AutoScaling .3	kontrol keamanan/ .3 AutoScaling
service-managed-aws-control- tower/v/1.0.0/ AutoScaling .4	kontrol keamanan/ .4 AutoScaling
service-managed-aws-control- tower/v/1.0.0/ Autoscaling .5	Kontrol keamanan/penskalan.5
service-managed-aws-control- tower/v/1.0.0/ AutoScaling .6	kontrol keamanan/ .6 AutoScaling
service-managed-aws-control- tower/v/1.0.0/ AutoScaling .9	kontrol keamanan/ .9 AutoScaling
service-managed-aws-control- tower/v/1.0.0/ CloudTrail .1	kontrol keamanan/ .1 CloudTrail
service-managed-aws-control- tower/v/1.0.0/ CloudTrail .2	kontrol keamanan/ .2 CloudTrail
service-managed-aws-control- tower/v/1.0.0/ CloudTrail .4	kontrol keamanan/ .4 CloudTrail
service-managed-aws-control- tower/v/1.0.0/ CloudTrail .5	kontrol keamanan/ .5 CloudTrail
service-managed-aws-control- tower/v/1.0.0/ CodeBuild .1	kontrol keamanan/ .1 CodeBuild
service-managed-aws-control- tower/v/1.0.0/ CodeBuild .2	kontrol keamanan/ .2 CodeBuild
service-managed-aws-control- tower/v/1.0.0/ CodeBuild .4	kontrol keamanan/ .4 CodeBuild

generatorId sebelum mengaktifkan temuan kontrol terkonsolidasi	generatorId setelah mengaktifkan temuan kontrol terkonsolidasi
service-managed-aws-control- tower/v/1.0.0/ CodeBuild .5	kontrol keamanan/ .5 CodeBuild
service-managed-aws-control- tower/v/1.0.0/ DMS .1	Kontrol keamanan/DMS.1
service-managed-aws-control- tower/v/1.0.0/ DynamoDB .1	Kontrol keamanan/DynamoDB.1
service-managed-aws-control- tower/v/1.0.0/ DynamoDB .2	Kontrol keamanan/Dynamodb.2
service-managed-aws-control- tower/v/1.0.0/EC 2.1	kontrol keamanan/ .1 EC2
service-managed-aws-control- tower/v/1.0.0/EC 2.2	kontrol keamanan/ .2 EC2
service-managed-aws-control- tower/v/1.0.0/EC 2.3	kontrol keamanan/ .3 EC2
service-managed-aws-control- tower/v/1.0.0/EC 2.4	kontrol keamanan/ .4 EC2
service-managed-aws-control- tower/v/1.0.0/EC 2.6	kontrol keamanan/ .6 EC2
service-managed-aws-control- tower/v/1.0.0/EC 2,7	kontrol keamanan/ .7 EC2
service-managed-aws-control- tower/v/1.0.0/EC 2,8	kontrol keamanan/ .8 EC2
service-managed-aws-control- tower/v/1.0.0/EC 2,9	kontrol keamanan/ .9 EC2

generatorId sebelum mengaktifkan temuan kontrol terkonsolidasi	generatorId setelah mengaktifkan temuan kontrol terkonsolidasi
service-managed-aws-control- tower/v/1.0.0/EC 2.10	kontrol keamanan/ .10 EC2
service-managed-aws-control- tower/v/1.0.0/EC 2.15	kontrol keamanan/ .15 EC2
service-managed-aws-control- tower/v/1.0.0/EC 2.16	kontrol keamanan/ .16 EC2
service-managed-aws-control- tower/v/1.0.0/EC 2.17	kontrol keamanan/ .17 EC2
service-managed-aws-control- tower/v/1.0.0/EC 2.18	kontrol keamanan/ .18 EC2
service-managed-aws-control- tower/v/1.0.0/EC 2.19	kontrol keamanan/ .19 EC2
service-managed-aws-control- tower/v/1.0.0/EC 2.20	kontrol keamanan/ .20 EC2
service-managed-aws-control- tower/v/1.0.0/EC 2,21	kontrol keamanan/ .21 EC2
service-managed-aws-control- tower/v/1.0.0/EC 2,22	kontrol keamanan/ .22 EC2
service-managed-aws-control- tower/v/1.0.0/ ECR .1	Kontrol keamanan/ECR.1
service-managed-aws-control- tower/v/1.0.0/ ECR .2	Kontrol keamanan/ECR.2
service-managed-aws-control- tower/v/1.0.0/ ECR .3	Kontrol keamanan/ECR.3

generatorId sebelum mengaktifkan temuan kontrol terkonsolidasi	generatorId setelah mengaktifkan temuan kontrol terkonsolidasi
service-managed-aws-control- tower/v/1.0.0/ ECS .1	Kontrol keamanan/ECS.1
service-managed-aws-control- tower/v/1.0.0/ ECS .2	Kontrol keamanan/ECS.2
service-managed-aws-control- tower/v/1.0.0/ ECS .3	Kontrol keamanan/ECS.3
service-managed-aws-control- tower/v/1.0.0/ ECS .4	Kontrol keamanan/ECS.4
service-managed-aws-control- tower/v/1.0.0/ ECS .5	Kontrol keamanan/ECS.5
service-managed-aws-control- tower/v/1.0.0/ ECS .8	Kontrol keamanan/ECS.8
service-managed-aws-control- tower/v/1.0.0/ ECS .10	Kontrol keamanan/ECS.10
service-managed-aws-control- tower/v/1.0.0/ ECS .12	Kontrol keamanan/ECS.12
service-managed-aws-control- tower/v/1.0.0/ EFS .1	Kontrol keamanan/EFS.1
service-managed-aws-control- tower/v/1.0.0/ EFS .2	Kontrol keamanan/EFS.2
service-managed-aws-control- tower/v/1.0.0/ EFS .3	Kontrol keamanan/EFS.3
service-managed-aws-control- tower/v/1.0.0/ EFS .4	Kontrol keamanan/EFS.4

generatorId sebelum mengaktifkan temuan kontrol terkonsolidasi	generatorId setelah mengaktifkan temuan kontrol terkonsolidasi
service-managed-aws-control- tower/v/1.0.0/ EKS .2	Kontrol keamanan/EKS.2
service-managed-aws-control- tower/v/1.0.0/ ELB .2	Kontrol keamanan/ELB.2
service-managed-aws-control- tower/v/1.0.0/ ELB .3	Kontrol keamanan/ELB.3
service-managed-aws-control- tower/v/1.0.0/ ELB .4	Kontrol keamanan/ELB.4
service-managed-aws-control- tower/v/1.0.0/ ELB .5	Kontrol keamanan/ELB.5
service-managed-aws-control- tower/v/1.0.0/ ELB .6	Kontrol keamanan/ELB.6
service-managed-aws-control- tower/v/1.0.0/ ELB .7	Kontrol keamanan/ELB.7
service-managed-aws-control- tower/v/1.0.0/ ELB .8	Kontrol keamanan/ELB.8
service-managed-aws-control- tower/v/1.0.0/ ELB .9	Kontrol keamanan/ELB.9
service-managed-aws-control- tower/v/1.0.0/ ELB .10	Kontrol keamanan/ELB.10
service-managed-aws-control- tower/v/1.0.0/ ELB .12	Kontrol keamanan/ELB.12
service-managed-aws-control- tower/v/1.0.0/ ELB .13	Kontrol keamanan/ELB.13

generatorId sebelum mengaktifkan temuan kontrol terkonsolidasi	generatorId setelah mengaktifkan temuan kontrol terkonsolidasi
service-managed-aws-control- tower/v/1.0.0/ ELB .14	Kontrol keamanan/ELB.14
service-managed-aws-control- tower/v/1.0.0/ ELBv 2.1	kontrol keamanan/ .1 ELBv2
service-managed-aws-control- tower/v/1.0.0/ EMR .1	Kontrol keamanan/EMR.1
service-managed-aws-control- tower/v/1.0.0/ ES .1	Kontrol keamanan/ES.1
service-managed-aws-control- tower/v/1.0.0/ ES .2	Kontrol keamanan/ES.2
service-managed-aws-control- tower/v/1.0.0/ ES .3	Kontrol keamanan/ES.3
service-managed-aws-control- tower/v/1.0.0/ ES .4	Kontrol keamanan/ES.4
service-managed-aws-control- tower/v/1.0.0/ ES .5	Kontrol keamanan/ES.5
service-managed-aws-control- tower/v/1.0.0/ ES .6	Kontrol keamanan/ES.6
service-managed-aws-control- tower/v/1.0.0/ ES .7	Kontrol keamanan/ES.7
service-managed-aws-control- tower/v/1.0.0/ ES .8	Kontrol keamanan/ES.8
service-managed-aws-control- tower/v/1.0.0/ ElasticBeanstalk .1	kontrol keamanan/ .1 ElasticBeanstalk

generatorId sebelum mengaktifkan temuan kontrol terkonsolidasi	generatorId setelah mengaktifkan temuan kontrol terkonsolidasi
service-managed-aws-control- tower/v/1.0.0/ ElasticBeanstalk .2	kontrol keamanan/ .2 ElasticBeanstalk
service-managed-aws-control- tower/v/1.0.0/ GuardDuty .1	kontrol keamanan/ .1 GuardDuty
service-managed-aws-control- tower/v/1.0.0/ IAM .1	Kontrol keamanan/IAM.1
service-managed-aws-control- tower/v/1.0.0/ IAM .2	Kontrol keamanan/IAM.2
service-managed-aws-control- tower/v/1.0.0/ IAM .3	Kontrol keamanan/IAM.3
service-managed-aws-control- tower/v/1.0.0/ IAM .4	Kontrol keamanan/IAM.4
service-managed-aws-control- tower/v/1.0.0/ IAM .5	Kontrol keamanan/IAM.5
service-managed-aws-control- tower/v/1.0.0/ IAM .6	Kontrol keamanan/IAM.6
service-managed-aws-control- tower/v/1.0.0/ IAM .7	Kontrol keamanan/IAM.7
service-managed-aws-control- tower/v/1.0.0/ IAM .8	Kontrol keamanan/IAM.8
service-managed-aws-control- tower/v/1.0.0/ IAM .21	Kontrol keamanan/IAM.21
service-managed-aws-control- tower/v/1.0.0/ Kinesis .1	Kontrol keamanan/kinesis.1

generatorId sebelum mengaktifkan temuan kontrol terkonsolidasi	generatorId setelah mengaktifkan temuan kontrol terkonsolidasi
service-managed-aws-control- tower/v/1.0.0/ KMS .1	Kontrol keamanan/KMS.1
service-managed-aws-control- tower/v/1.0.0/ KMS .2	Kontrol keamanan/KMS.2
service-managed-aws-control- tower/v/1.0.0/ KMS .3	Kontrol keamanan/KMS.3
service-managed-aws-control- tower/v/1.0.0/ Lambda .1	Kontrol keamanan/Lambda.1
service-managed-aws-control- tower/v/1.0.0/ Lambda .2	Kontrol keamanan/Lambda.2
service-managed-aws-control- tower/v/1.0.0/ Lambda .5	Kontrol keamanan/Lambda.5
service-managed-aws-control- tower/v/1.0.0/ NetworkFirewall .3	kontrol keamanan/ .3 NetworkFirewall
service-managed-aws-control- tower/v/1.0.0/ NetworkFirewall .4	kontrol keamanan/ .4 NetworkFirewall
service-managed-aws-control- tower/v/1.0.0/ NetworkFirewall .5	kontrol keamanan/ .5 NetworkFirewall
service-managed-aws-control- tower/v/1.0.0/ NetworkFirewall .6	kontrol keamanan/ .6 NetworkFirewall
service-managed-aws-control- tower/v/1.0.0/ Opensearch .1	Kontrol keamanan/OpenSearch.1
service-managed-aws-control- tower/v/1.0.0/ Opensearch .2	Kontrol keamanan/OpenSearch.2

generatorId sebelum mengaktifkan temuan kontrol terkonsolidasi	generatorId setelah mengaktifkan temuan kontrol terkonsolidasi
service-managed-aws-control- tower/v/1.0.0/ Opensearch .3	Kontrol keamanan/OpenSearch.3
service-managed-aws-control- tower/v/1.0.0/ Opensearch .4	Kontrol keamanan/OpenSearch.4
service-managed-aws-control- tower/v/1.0.0/ Opensearch .5	Kontrol keamanan/OpenSearch.5
service-managed-aws-control- tower/v/1.0.0/ Opensearch .6	Kontrol keamanan/OpenSearch.6
service-managed-aws-control- tower/v/1.0.0/ Opensearch .7	Kontrol keamanan/OpenSearch.7
service-managed-aws-control- tower/v/1.0.0/ Opensearch .8	Kontrol keamanan/OpenSearch.8
service-managed-aws-control- tower/v/1.0.0/ RDS .1	Kontrol keamanan/RDS.1
service-managed-aws-control- tower/v/1.0.0/ RDS .2	Kontrol keamanan/RDS.2
service-managed-aws-control- tower/v/1.0.0/ RDS .3	Kontrol keamanan/RDS.3
service-managed-aws-control- tower/v/1.0.0/ RDS .4	Kontrol keamanan/RDS.4
service-managed-aws-control- tower/v/1.0.0/ RDS .5	Kontrol keamanan/RDS.5
service-managed-aws-control- tower/v/1.0.0/ RDS .6	Kontrol keamanan/RDS.6

generatorId sebelum mengaktifkan temuan kontrol terkonsolidasi	generatorId setelah mengaktifkan temuan kontrol terkonsolidasi
service-managed-aws-control- tower/v/1.0.0/ RDS .8	Kontrol keamanan/RDS.8
service-managed-aws-control- tower/v/1.0.0/ RDS .9	Kontrol keamanan/RDS.9
service-managed-aws-control- tower/v/1.0.0/ RDS .10	Kontrol keamanan/RDS.10
service-managed-aws-control- tower/v/1.0.0/ RDS .11	Kontrol keamanan/RDS.11
service-managed-aws-control- tower/v/1.0.0/ RDS .13	Kontrol keamanan/RDS.13
service-managed-aws-control- tower/v/1.0.0/ RDS .17	Kontrol keamanan/RDS.17
service-managed-aws-control- tower/v/1.0.0/ RDS .18	Kontrol keamanan/RDS.18
service-managed-aws-control- tower/v/1.0.0/ RDS .19	Kontrol keamanan/RDS.19
service-managed-aws-control- tower/v/1.0.0/ RDS .20	Kontrol keamanan/RDS.20
service-managed-aws-control- tower/v/1.0.0/ RDS .21	Kontrol keamanan/RDS.21
service-managed-aws-control- tower/v/1.0.0/ RDS .22	Kontrol keamanan/RDS.22
service-managed-aws-control- tower/v/1.0.0/ RDS .23	Kontrol keamanan/RDS.23

generatorId sebelum mengaktifkan temuan kontrol terkonsolidasi	generatorId setelah mengaktifkan temuan kontrol terkonsolidasi
service-managed-aws-control- tower/v/1.0.0/RDS .25	Kontrol keamanan/RDS.25
service-managed-aws-control- tower/v/1.0.0/Redshift .1	Kontrol keamanan/pergeseran merah.1
service-managed-aws-control- tower/v/1.0.0/Redshift .2	Kontrol keamanan/pergeseran merah.2
service-managed-aws-control- tower/v/1.0.0/Redshift .4	Kontrol keamanan/Redshift.4
service-managed-aws-control- tower/v/1.0.0/Redshift .6	Kontrol keamanan/pergeseran merah.6
service-managed-aws-control- tower/v/1.0.0/Redshift .7	Kontrol keamanan/pergeseran merah.7
service-managed-aws-control- tower/v/1.0.0/Redshift .8	Kontrol keamanan/pergeseran merah.8
service-managed-aws-control- tower/v/1.0.0/Redshift .9	Kontrol keamanan/pergeseran merah.9
service-managed-aws-control- tower/v/1.0.0/S 3.1	Kontrol keamanan/S3.1
service-managed-aws-control- tower/v/1.0.0/S 3.2	Kontrol keamanan/S3.2
service-managed-aws-control- tower/v/1.0.0/S 3.3	Kontrol keamanan/S3.3
service-managed-aws-control- tower/v/1.0.0/S 3,5	Kontrol keamanan/S3.5

generatorId sebelum mengaktifkan temuan kontrol terkonsolidasi	generatorId setelah mengaktifkan temuan kontrol terkonsolidasi
service-managed-aws-control- tower/v/1.0.0/S 3,6	Kontrol keamanan/S3.6
service-managed-aws-control- tower/v/1.0.0/S 3,8	Kontrol keamanan/S3.8
service-managed-aws-control- tower/v/1.0.0/S 3,9	Kontrol keamanan/S3.9
service-managed-aws-control- tower/v/1.0.0/S 3.12	Kontrol keamanan/S3.12
service-managed-aws-control- tower/v/1.0.0/S 3.13	Kontrol keamanan/S3.13
service-managed-aws-control- tower/v/1.0.0/ SageMaker .1	kontrol keamanan/ .1 SageMaker
service-managed-aws-control- tower/v/1.0.0/ SecretsManager .1	kontrol keamanan/ .1 SecretsManager
service-managed-aws-control- tower/v/1.0.0/ SecretsManager .2	kontrol keamanan/ .2 SecretsManager
service-managed-aws-control- tower/v/1.0.0/ SecretsManager .3	kontrol keamanan/ .3 SecretsManager
service-managed-aws-control- tower/v/1.0.0/ SecretsManager .4	kontrol keamanan/ .4 SecretsManager
service-managed-aws-control- tower/v/1.0.0/ SQS .1	Kontrol keamanan/SQS.1
service-managed-aws-control- tower/v/1.0.0/ SSM .1	Kontrol keamanan/SSM.1

generatorId sebelum mengaktifkan temuan kontrol terkonsolidasi	generatorId setelah mengaktifkan temuan kontrol terkonsolidasi
service-managed-aws-control- tower/v/1.0.0/SSM .2	Kontrol keamanan/SSM.2
service-managed-aws-control- tower/v/1.0.0/SSM .3	Kontrol keamanan/SSM.3
service-managed-aws-control- tower/v/1.0.0/SSM .4	Kontrol keamanan/SSM.4
service-managed-aws-control- tower/v/1.0.0/WAF .2	Kontrol keamanan/WAF.2
service-managed-aws-control- tower/v/1.0.0/WAF .3	Kontrol keamanan/WAF.3
service-managed-aws-control- tower/v/1.0.0/WAF .4	Kontrol keamanan/WAF.4

Bagaimana konsolidasi memengaruhi kontrol IDs dan judul

Tampilan kontrol terkonsolidasi dan temuan kontrol terkonsolidasi menstandarisasi kontrol IDs dan judul di seluruh standar. Istilah ID kontrol keamanan dan judul kontrol keamanan mengacu pada nilai agnostik standar ini.

Konsol CSPM Security Hub menampilkan kontrol keamanan agnostik standar IDs dan judul kontrol keamanan, terlepas dari apakah temuan kontrol konsolidasi diaktifkan atau dinonaktifkan untuk akun Anda. Namun, temuan CSPM Security Hub berisi judul kontrol khusus standar, untuk PCI DSS dan CIS v1.2.0, jika temuan kontrol konsolidasi dinonaktifkan untuk akun Anda. Selain itu, temuan CSPM Security Hub berisi ID kontrol khusus standar dan ID kontrol keamanan. Untuk contoh bagaimana konsolidasi berdampak pada temuan kontrol, lihat [Sampel temuan kontrol](#).

Untuk kontrol yang merupakan bagian dari [standar yang AWS Control Tower dikelola layanan](#), awalan CT . dihapus dari ID kontrol dan judul dalam temuan saat temuan kontrol terkonsolidasi diaktifkan.

Untuk menonaktifkan kontrol keamanan di Security Hub CSPM, Anda harus menonaktifkan semua kontrol standar yang sesuai dengan kontrol keamanan. Tabel berikut menunjukkan pemetaan kontrol keamanan IDs dan judul ke kontrol dan judul khusus standar. IDs IDs dan judul untuk kontrol yang termasuk dalam standar Praktik Terbaik Keamanan AWS Dasar (FSBP) sudah agnostik standar. Untuk pemetaan kontrol ke persyaratan Center for Internet Security (CIS) v3.0.0, lihat. [Pemetaan kontrol ke persyaratan CIS di setiap versi](#) Untuk menjalankan skrip Anda sendiri di tabel ini, Anda dapat [mengunduhnya sebagai file.csv](#).

Standar	ID kontrol standar dan judul	ID dan judul kontrol keamanan
CIS v1.2.0	1.1 Hindari penggunaan pengguna root	[CloudWatch.1] Filter metrik log dan alarm harus ada untuk penggunaan pengguna "root"
CIS v1.2.0	1.10 Pastikan kebijakan kata sandi IAM mencegah penggunaan kembali kata sandi	[IAM.16] Pastikan kebijakan kata sandi IAM mencegah penggunaan kembali kata sandi
CIS v1.2.0	1.11 Pastikan kebijakan kata sandi IAM kedaluwarsa kata sandi dalam waktu 90 hari atau kurang	[IAM.17] Pastikan kebijakan kata sandi IAM kedaluwarsa kata sandi dalam waktu 90 hari atau kurang
CIS v1.2.0	1.12 Pastikan tidak ada kunci akses pengguna root	[IAM.4] Kunci akses pengguna root IAM seharusnya tidak ada
CIS v1.2.0	1.13 Pastikan MFA diaktifkan untuk pengguna root	[IAM.9] MFA harus diaktifkan untuk pengguna root
CIS v1.2.0	1.14 Pastikan MFA perangkat keras diaktifkan untuk pengguna root	[IAM.6] MFA perangkat keras harus diaktifkan untuk pengguna root
CIS v1.2.0	1.16 Pastikan kebijakan IAM hanya dilampirkan pada grup atau peran	[IAM.2] Pengguna IAM seharusnya tidak memiliki kebijakan IAM yang dilampirkan
CIS v1.2.0	1.2 Pastikan otentikasi multi-faktor (MFA) diaktifkan untuk semua	[IAM.5] MFA harus diaktifkan untuk semua pengguna IAM yang memiliki kata sandi konsol

Standar	ID kontrol standar dan judul	ID dan judul kontrol keamanan
	pengguna IAM yang memiliki kata sandi konsol	
CIS v1.2.0	1.20 Memastikan peran dukungan telah dibuat untuk mengelola insiden dengan Dukungan	[IAM.18] Memastikan peran dukungan telah dibuat untuk mengelola insiden dengan AWS Dukungan
CIS v1.2.0	1.22 Pastikan kebijakan IAM yang memungkinkan hak administratif “*: *” penuh tidak dibuat	[IAM.1] Kebijakan IAM seharusnya tidak mengizinkan hak administratif “*: *” penuh
CIS v1.2.0	1.3 Pastikan kredensial yang tidak digunakan selama 90 hari atau lebih dinonaktifkan	[IAM.8] Kredensi pengguna IAM yang tidak digunakan harus dihapus
CIS v1.2.0	1.4 Pastikan kunci akses diputar setiap 90 hari atau kurang	[IAM.3] Kunci akses pengguna IAM harus diputar setiap 90 hari atau kurang
CIS v1.2.0	1.5 Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu huruf besar	[IAM.11] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu huruf besar
CIS v1.2.0	1.6 Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu huruf kecil	[IAM.12] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu huruf kecil
CIS v1.2.0	1.7 Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu simbol	[IAM.13] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu simbol
CIS v1.2.0	1.8 Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu nomor	[IAM.14] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu nomor

Standar	ID kontrol standar dan judul	ID dan judul kontrol keamanan
CIS v1.2.0	1.9 Pastikan kebijakan kata sandi IAM memerlukan panjang kata sandi minimum 14 atau lebih	[IAM.15] Pastikan kebijakan kata sandi IAM membutuhkan panjang kata sandi minimum 14 atau lebih
CIS v1.2.0	2.1 Pastikan CloudTrail diaktifkan di semua wilayah	[CloudTrail.1] CloudTrail harus diaktifkan dan dikonfigurasi dengan setidaknya satu jejak Multi-wilayah yang mencakup acara manajemen baca dan tulis
CIS v1.2.0	2.2 Pastikan validasi file CloudTrail log diaktifkan	[CloudTrail.4] validasi file CloudTrail log harus diaktifkan
CIS v1.2.0	2.3 Pastikan bucket S3 yang digunakan untuk menyimpan CloudTrail log tidak dapat diakses publik	[CloudTrail.6] Pastikan bucket S3 yang digunakan untuk menyimpan CloudTrail log tidak dapat diakses publik
CIS v1.2.0	2.4 Pastikan CloudTrail jalur terintegrasi dengan Log CloudWatch	[CloudTrail.5] CloudTrail jalur harus diintegrasikan dengan Amazon Logs CloudWatch
CIS v1.2.0	2.5 Pastikan AWS Config diaktifkan	[Config.1] AWS Config harus diaktifkan dan menggunakan peran terkait layanan untuk perekaman sumber daya
CIS v1.2.0	2.6 Pastikan pencatatan akses bucket S3 diaktifkan pada bucket CloudTrail S3	[CloudTrail.7] Pastikan pencatatan akses bucket S3 diaktifkan pada bucket CloudTrail S3
CIS v1.2.0	2.7 Pastikan CloudTrail log dienkripsi saat istirahat menggunakan KMS CMKs	[CloudTrail.2] CloudTrail harus mengaktifkan enkripsi saat istirahat
CIS v1.2.0	2.8 Pastikan rotasi untuk pelanggan yang dibuat CMKs diaktifkan	[KMS.4] rotasi AWS KMS tombol harus diaktifkan

Standar	ID kontrol standar dan judul	ID dan judul kontrol keamanan
CIS v1.2.0	2.9 Pastikan pencatatan aliran VPC diaktifkan di semua VPCs	[EC2.6] Pencatatan aliran VPC harus diaktifkan di semua VPCs
CIS v1.2.0	3.1 Pastikan filter metrik log dan alarm ada untuk panggilan API yang tidak sah	[CloudWatch.2] Pastikan filter metrik log dan alarm ada untuk panggilan API yang tidak sah
CIS v1.2.0	3.10 Pastikan filter metrik log dan alarm ada untuk perubahan grup keamanan	[CloudWatch.10] Pastikan filter metrik log dan alarm ada untuk perubahan grup keamanan
CIS v1.2.0	3.11 Pastikan filter metrik log dan alarm ada untuk perubahan pada Daftar Kontrol Akses Jaringan (NACL)	[CloudWatch.11] Pastikan filter metrik log dan alarm ada untuk perubahan pada Daftar Kontrol Akses Jaringan (NACL)
CIS v1.2.0	3.12 Pastikan filter metrik log dan alarm ada untuk perubahan gateway jaringan	[CloudWatch.12] Pastikan filter metrik log dan alarm ada untuk perubahan pada gateway jaringan
CIS v1.2.0	3.13 Pastikan filter metrik log dan alarm ada untuk perubahan tabel rute	[CloudWatch.13] Pastikan filter metrik log dan alarm ada untuk perubahan tabel rute
CIS v1.2.0	3.14 Pastikan filter metrik log dan alarm ada untuk perubahan VPC	[CloudWatch.14] Pastikan filter metrik log dan alarm ada untuk perubahan VPC
CIS v1.2.0	3.2 Pastikan filter metrik log dan alarm ada untuk login Konsol Manajemen tanpa MFA	[CloudWatch.3] Pastikan filter metrik log dan alarm ada untuk login Konsol Manajemen tanpa MFA
CIS v1.2.0	3.3 Pastikan filter metrik log dan alarm ada untuk penggunaan pengguna root	[CloudWatch.1] Filter metrik log dan alarm harus ada untuk penggunaan pengguna "root"

Standar	ID kontrol standar dan judul	ID dan judul kontrol keamanan
CIS v1.2.0	3.4 Pastikan filter metrik log dan alarm ada untuk perubahan kebijakan IAM	[CloudWatch.4] Pastikan filter metrik log dan alarm ada untuk perubahan kebijakan IAM
CIS v1.2.0	3.5 Pastikan filter metrik log dan alarm ada untuk perubahan CloudTrail konfigurasi	[CloudWatch.5] Pastikan filter metrik log dan alarm ada untuk perubahan CloudTrail konfigurasi
CIS v1.2.0	3.6 Pastikan filter metrik log dan alarm ada untuk kegagalan AWS Management Console otentikasi	[CloudWatch.6] Pastikan filter metrik log dan alarm ada untuk kegagalan AWS Management Console otentikasi
CIS v1.2.0	3.7 Pastikan filter metrik log dan alarm ada untuk menonaktifkan atau terjadwal penghapusan pelanggan yang dibuat CMKs	[CloudWatch.7] Pastikan filter metrik log dan alarm ada untuk menonaktifkan atau menjadwalkan penghapusan kunci yang dikelola pelanggan
CIS v1.2.0	3.8 Pastikan filter metrik log dan alarm ada untuk perubahan kebijakan bucket S3	[CloudWatch.8] Pastikan filter metrik log dan alarm ada untuk perubahan kebijakan bucket S3
CIS v1.2.0	3.9 Pastikan filter metrik log dan alarm ada untuk perubahan AWS Config konfigurasi	[CloudWatch.9] Pastikan filter metrik log dan alarm ada untuk perubahan AWS Config konfigurasi
CIS v1.2.0	4.1 Pastikan tidak ada grup keamanan yang mengizinkan masuknya dari 0.0.0.0/0 ke port 22	[EC2.13] Grup keamanan seharusnya tidak mengizinkan masuknya dari 0.0.0.0/0 atau: :/0 ke port 22
CIS v1.2.0	4.2 Pastikan tidak ada grup keamanan yang mengizinkan masuknya dari 0.0.0.0/0 ke port 3389	[EC2.14] Grup keamanan seharusnya tidak mengizinkan masuknya dari 0.0.0.0/0 atau: :/0 ke port 3389
CIS v1.2.0	4.3 Pastikan grup keamanan default dari setiap VPC membatasi semua lalu lintas	[EC2.2] Grup keamanan default VPC tidak boleh mengizinkan lalu lintas masuk atau keluar

Standar	ID kontrol standar dan judul	ID dan judul kontrol keamanan
CIS v1.4.0	1.10 Pastikan otentikasi multi-faktor (MFA) diaktifkan untuk semua pengguna IAM yang memiliki kata sandi konsol	[IAM.5] MFA harus diaktifkan untuk semua pengguna IAM yang memiliki kata sandi konsol
CIS v1.4.0	1.14 Pastikan kunci akses diputar setiap 90 hari atau kurang	[IAM.3] Kunci akses pengguna IAM harus diputar setiap 90 hari atau kurang
CIS v1.4.0	1.16 Pastikan kebijakan IAM yang memungkinkan hak administratif “*: *” penuh tidak dilampirkan	[IAM.1] Kebijakan IAM seharusnya tidak mengizinkan hak administratif “*” penuh
CIS v1.4.0	1.17 Memastikan peran dukungan telah dibuat untuk mengelola insiden dengan Dukungan	[IAM.18] Memastikan peran dukungan telah dibuat untuk mengelola insiden dengan AWS Dukungan
CIS v1.4.0	1.4 Pastikan tidak ada kunci akses akun pengguna root	[IAM.4] Kunci akses pengguna root IAM seharusnya tidak ada
CIS v1.4.0	1.5 Pastikan MFA diaktifkan untuk akun pengguna root	[IAM.9] MFA harus diaktifkan untuk pengguna root
CIS v1.4.0	1.6 Pastikan MFA perangkat keras diaktifkan untuk akun pengguna root	[IAM.6] MFA perangkat keras harus diaktifkan untuk pengguna root
CIS v1.4.0	1.7 Hilangkan penggunaan pengguna root untuk tugas administratif dan harian	[CloudWatch.1] Filter metrik log dan alarm harus ada untuk penggunaan pengguna “root”
CIS v1.4.0	1.8 Pastikan kebijakan kata sandi IAM membutuhkan panjang minimum 14 atau lebih	[IAM.15] Pastikan kebijakan kata sandi IAM membutuhkan panjang kata sandi minimum 14 atau lebih

Standar	ID kontrol standar dan judul	ID dan judul kontrol keamanan
CIS v1.4.0	1.9 Pastikan kebijakan kata sandi IAM mencegah penggunaan kembali kata sandi	[IAM.16] Pastikan kebijakan kata sandi IAM mencegah penggunaan kembali kata sandi
CIS v1.4.0	2.1.2 Pastikan Kebijakan Bucket S3 disetel untuk menolak permintaan HTTP	[S3.5] Bucket tujuan umum S3 harus memerlukan permintaan untuk menggunakan SSL
CIS v1.4.0	2.1.5.1 Pengaturan Akses Publik Blok S3 harus diaktifkan	[S3.1] Bucket tujuan umum S3 harus mengaktifkan pengaturan akses publik blok
CIS v1.4.0	2.1.5.2 Pengaturan Akses Publik Blok S3 harus diaktifkan pada tingkat bucket	[S3.8] Bucket tujuan umum S3 harus memblokir akses publik
CIS v1.4.0	2.2.1 Pastikan enkripsi volume EBS diaktifkan	[EC2.7] Enkripsi default EBS harus diaktifkan
CIS v1.4.0	2.3.1 Pastikan enkripsi diaktifkan untuk Instans RDS	[RDS.3] Instans RDS DB harus mengaktifkan enkripsi saat istirahat
CIS v1.4.0	3.1 Pastikan CloudTrail diaktifkan di semua wilayah	[CloudTrail.1] CloudTrail harus diaktifkan dan dikonfigurasi dengan setidaknya satu jejak Multi-wilayah yang mencakup acara manajemen baca dan tulis
CIS v1.4.0	3.2 Pastikan validasi file CloudTrail log diaktifkan	[CloudTrail.4] validasi file CloudTrail log harus diaktifkan
CIS v1.4.0	3.4 Pastikan CloudTrail jalur terintegrasi dengan Log CloudWatch	[CloudTrail.5] CloudTrail jalur harus diintegrasikan dengan Amazon Logs CloudWatch

Standar	ID kontrol standar dan judul	ID dan judul kontrol keamanan
CIS v1.4.0	3.5 Pastikan AWS Config diaktifkan di semua wilayah	[Config.1] AWS Config harus diaktifkan dan menggunakan peran terkait layanan untuk perekaman sumber daya
CIS v1.4.0	3.6 Pastikan pencatatan akses bucket S3 diaktifkan pada bucket CloudTrail S3	[CloudTrail.7] Pastikan pencatatan akses bucket S3 diaktifkan pada bucket CloudTrail S3
CIS v1.4.0	3.7 Pastikan CloudTrail log dienkripsi saat istirahat menggunakan KMS CMKs	[CloudTrail.2] CloudTrail harus mengaktifkan enkripsi saat istirahat
CIS v1.4.0	3.8 Pastikan rotasi untuk pelanggan yang dibuat CMKs diaktifkan	[KMS.4] rotasi AWS KMS tombol harus diaktifkan
CIS v1.4.0	3.9 Pastikan pencatatan aliran VPC diaktifkan di semua VPCs	[EC2.6] Pencatatan aliran VPC harus diaktifkan di semua VPCs
CIS v1.4.0	4.4 Pastikan filter metrik log dan alarm ada untuk perubahan kebijakan IAM	[CloudWatch.4] Pastikan filter metrik log dan alarm ada untuk perubahan kebijakan IAM
CIS v1.4.0	4.5 Pastikan filter metrik log dan alarm ada untuk perubahan CloudTrail konfigurasi	[CloudWatch.5] Pastikan filter metrik log dan alarm ada untuk perubahan CloudTrail konfigurasi
CIS v1.4.0	4.6 Pastikan filter metrik log dan alarm ada untuk kegagalan AWS Management Console otentikasi	[CloudWatch.6] Pastikan filter metrik log dan alarm ada untuk kegagalan AWS Management Console otentikasi
CIS v1.4.0	4.7 Pastikan filter metrik log dan alarm ada untuk menonaktifkan atau terjadwal penghapusan pelanggan yang dibuat CMKs	[CloudWatch.7] Pastikan filter metrik log dan alarm ada untuk menonaktifkan atau menjadwalkan penghapusan kunci yang dikelola pelanggan

Standar	ID kontrol standar dan judul	ID dan judul kontrol keamanan
CIS v1.4.0	4.8 Pastikan filter metrik log dan alarm ada untuk perubahan kebijakan bucket S3	[CloudWatch.8] Pastikan filter metrik log dan alarm ada untuk perubahan kebijakan bucket S3
CIS v1.4.0	4.9 Pastikan filter metrik log dan alarm ada untuk perubahan AWS Config konfigurasi	[CloudWatch.9] Pastikan filter metrik log dan alarm ada untuk perubahan AWS Config konfigurasi
CIS v1.4.0	4.10 Pastikan filter metrik log dan alarm ada untuk perubahan grup keamanan	[CloudWatch.10] Pastikan filter metrik log dan alarm ada untuk perubahan grup keamanan
CIS v1.4.0	4.11 Pastikan filter metrik log dan alarm ada untuk perubahan pada Daftar Kontrol Akses Jaringan (NACL)	[CloudWatch.11] Pastikan filter metrik log dan alarm ada untuk perubahan pada Daftar Kontrol Akses Jaringan (NACL)
CIS v1.4.0	4.12 Pastikan filter metrik log dan alarm ada untuk perubahan gateway jaringan	[CloudWatch.12] Pastikan filter metrik log dan alarm ada untuk perubahan pada gateway jaringan
CIS v1.4.0	4.13 Pastikan filter metrik log dan alarm ada untuk perubahan tabel rute	[CloudWatch.13] Pastikan filter metrik log dan alarm ada untuk perubahan tabel rute
CIS v1.4.0	4.14 Pastikan filter metrik log dan alarm ada untuk perubahan VPC	[CloudWatch.14] Pastikan filter metrik log dan alarm ada untuk perubahan VPC
CIS v1.4.0	5.1 Pastikan tidak ada Jaringan yang ACLs mengizinkan masuknya dari 0.0.0.0/0 ke port administrasi server jarak jauh	[EC2.21] Jaringan ACLs seharusnya tidak mengizinkan masuknya dari 0.0.0.0/0 ke port 22 atau port 3389.
CIS v1.4.0	5.3 Pastikan grup keamanan default dari setiap VPC membatasi semua lalu lintas	[EC2.2] Grup keamanan default VPC tidak boleh mengizinkan lalu lintas masuk atau keluar

Standar	ID kontrol standar dan judul	ID dan judul kontrol keamanan
PCI DSS v3.2.1	PCI. AutoScaling.1 Grup penskalaan otomatis yang terkait dengan penyeimbang beban harus menggunakan pemeriksaan kesehatan penyeimbang beban	[AutoScaling.1] Grup Auto Scaling yang terkait dengan penyeimbang beban harus menggunakan pemeriksaan kesehatan ELB
PCI DSS v3.2.1	PCI. CloudTrail.1 CloudTrail log harus dienkrpsi saat istirahat menggunakan AWS KMS CMKs	[CloudTrail.2] CloudTrail harus mengaktifkan enkripsi saat istirahat
PCI DSS v3.2.1	PCI. CloudTrail.2 CloudTrail harus diaktifkan	[CloudTrail.3] Setidaknya satu CloudTrail jejak harus diaktifkan
PCI DSS v3.2.1	PCI. CloudTrail.3 validasi file CloudTrail log harus diaktifkan	[CloudTrail.4] validasi file CloudTrail log harus diaktifkan
PCI DSS v3.2.1	PCI. CloudTrail.4 CloudTrail jalur harus diintegrasikan dengan Amazon Logs CloudWatch	[CloudTrail.5] CloudTrail jalur harus diintegrasikan dengan Amazon Logs CloudWatch
PCI DSS v3.2.1	PCI. CodeBuild.1 CodeBuild GitHub atau repositori sumber Bitbucket harus digunakan URLs OAuth	[CodeBuild.1] Repositori sumber CodeBuild Bitbucket tidak URLs boleh berisi kredensial sensitif
PCI DSS v3.2.1	PCI. CodeBuild.2 variabel lingkungan CodeBuild proyek tidak boleh berisi kredensial teks yang jelas	[CodeBuild.2] variabel lingkungan CodeBuild proyek tidak boleh berisi kredensial teks yang jelas
PCI DSS v3.2.1	PCI.config.1 harus diaktifkan AWS Config	[Config.1] AWS Config harus diaktifkan dan menggunakan peran terkait layanan untuk perekaman sumber daya
PCI DSS v3.2.1	PCI.CW.1 Filter metrik log dan alarm harus ada untuk penggunaan pengguna "root"	[CloudWatch.1] Filter metrik log dan alarm harus ada untuk penggunaan pengguna "root"

Standar	ID kontrol standar dan judul	ID dan judul kontrol keamanan
PCI DSS v3.2.1	Instans replikasi Layanan Migrasi Database PCI.DMS.1 tidak boleh bersifat publik	[DMS.1] Instans replikasi Layanan Migrasi Database tidak boleh bersifat publik
PCI DSS v3.2.1	PCI. EC2.1 Snapshot EBS tidak boleh dipulihkan secara publik	[EC2.1] Cuplikan Amazon EBS tidak boleh dipulihkan secara publik
PCI DSS v3.2.1	PCI. EC2.2 Grup keamanan default VPC harus melarang lalu lintas masuk dan keluar	[EC2.2] Grup keamanan default VPC tidak boleh mengizinkan lalu lintas masuk atau keluar
PCI DSS v3.2.1	PCI. EC2.4 Tidak terpakai EC2 EIPs harus dihapus	[EC2.12] Amazon yang tidak terpakai EC2 EIPs harus dihapus
PCI DSS v3.2.1	PCI. EC2.5 Grup keamanan tidak boleh mengizinkan masuknya dari 0.0.0.0/0 ke port 22	[EC2.13] Grup keamanan seharusnya tidak mengizinkan masuknya dari 0.0.0.0/0 atau: :/0 ke port 22
PCI DSS v3.2.1	PCI. EC2.6 Pencatatan aliran VPC harus diaktifkan di semua VPCs	[EC2.6] Pencatatan aliran VPC harus diaktifkan di semua VPCs
PCI DSS v3.2.1	PCI. ELBv2.1 Application Load Balancer harus dikonfigurasi untuk mengalihkan semua permintaan HTTP ke HTTPS	[ELB.1] Application Load Balancer harus dikonfigurasi untuk mengalihkan semua permintaan HTTP ke HTTPS
PCI DSS v3.2.1	Domain PCI.ES.1 Elasticsearch harus dalam VPC	[ES.2] Domain Elasticsearch tidak boleh diakses publik
PCI DSS v3.2.1	Domain PCI.ES.2 Elasticsearch harus mengaktifkan enkripsi saat istirahat	[ES.1] Domain Elasticsearch harus mengaktifkan enkripsi saat istirahat
PCI DSS v3.2.1	PCI. GuardDuty.1 GuardDuty harus diaktifkan	[GuardDuty.1] GuardDuty harus diaktifkan

Standar	ID kontrol standar dan judul	ID dan judul kontrol keamanan
PCI DSS v3.2.1	Kunci akses pengguna root PCI.IAM.1 IAM seharusnya tidak ada	[IAM.4] Kunci akses pengguna root IAM seharusnya tidak ada
PCI DSS v3.2.1	Pengguna IAM PCI.IAM.2 tidak boleh memiliki kebijakan IAM yang dilampirkan	[IAM.2] Pengguna IAM seharusnya tidak memiliki kebijakan IAM yang dilampirkan
PCI DSS v3.2.1	Kebijakan IAM PCI.IAM.3 tidak boleh mengizinkan hak administratif “*” penuh	[IAM.1] Kebijakan IAM seharusnya tidak mengizinkan hak administratif “*” penuh
PCI DSS v3.2.1	MFA Perangkat Keras PCI.IAM.4 harus diaktifkan untuk pengguna root	[IAM.6] MFA perangkat keras harus diaktifkan untuk pengguna root
PCI DSS v3.2.1	PCI.IAM.5 MFA Virtual harus diaktifkan untuk pengguna root	[IAM.9] MFA harus diaktifkan untuk pengguna root
PCI DSS v3.2.1	MFA PCI.IAM.6 harus diaktifkan untuk semua pengguna IAM	[IAM.19] MFA harus diaktifkan untuk semua pengguna IAM
PCI DSS v3.2.1	Kredensi pengguna IAM PCI.IAM.7 harus dinonaktifkan jika tidak digunakan dalam jumlah hari yang ditentukan sebelumnya	[IAM.8] Kredensi pengguna IAM yang tidak digunakan harus dihapus
PCI DSS v3.2.1	Kebijakan kata sandi PCI.IAM.8 untuk pengguna IAM harus memiliki konfigurasi yang kuat	[IAM.10] Kebijakan kata sandi untuk pengguna IAM harus memiliki konfigurasi yang kuat
PCI DSS v3.2.1	PCI.KMS.1 Rotasi kunci master pelanggan (CMK) harus diaktifkan	[KMS.4] rotasi AWS KMS tombol harus diaktifkan
PCI DSS v3.2.1	Fungsi Lambda PCI.lambda.1 harus melarang akses publik	[Lambda.1] Kebijakan fungsi Lambda harus melarang akses publik
PCI DSS v3.2.1	PCI.lambda.2 Fungsi Lambda harus dalam VPC	[Lambda.3] Fungsi Lambda harus dalam VPC

Standar	ID kontrol standar dan judul	ID dan judul kontrol keamanan
PCI DSS v3.2.1	Domain OpenSearch PCI.openSearch.1 harus dalam VPC	[Opensearch.2] OpenSearch domain tidak boleh diakses publik
PCI DSS v3.2.1	Snapshot EBS PCI.openSearch.2 tidak boleh dipulihkan secara publik	[Opensearch.1] OpenSearch domain harus mengaktifkan enkripsi saat istirahat
PCI DSS v3.2.1	Snapshot PCI.RDS.1 RDS harus bersifat pribadi	[RDS.1] Snapshot RDS harus bersifat pribadi
PCI DSS v3.2.1	Instans PCI.RDS.2 RDS DB harus melarang akses publik	[RDS.2] Instans RDS DB harus melarang akses publik, sebagaimana ditentukan oleh konfigurasi PubliclyAccessible
PCI DSS v3.2.1	PCI.redshift.1 Cluster Amazon Redshift harus melarang akses publik	[Redshift.1] Cluster Amazon Redshift harus melarang akses publik
PCI DSS v3.2.1	Bucket PCI.S3.1 S3 harus melarang akses tulis publik	[S3.3] Bucket tujuan umum S3 harus memblokir akses tulis publik
PCI DSS v3.2.1	Bucket PCI.S3.2 S3 harus melarang akses baca publik	[S3.2] Bucket tujuan umum S3 harus memblokir akses baca publik
PCI DSS v3.2.1	Bucket PCI.S3.3 S3 harus mengaktifkan replikasi lintas wilayah	[S3.7] Ember tujuan umum S3 harus menggunakan replikasi lintas wilayah
PCI DSS v3.2.1	Bucket PCI.S3.5 S3 harus memerlukan permintaan untuk menggunakan Secure Socket Layer	[S3.5] Bucket tujuan umum S3 harus memerlukan permintaan untuk menggunakan SSL
PCI DSS v3.2.1	Pengaturan Akses Publik Blok PCI.S3.6 S3 harus diaktifkan	[S3.1] Bucket tujuan umum S3 harus mengaktifkan pengaturan akses publik blok

Standar	ID kontrol standar dan judul	ID dan judul kontrol keamanan
PCI DSS v3.2.1	PCI. SageMaker.1 Instans SageMaker notebook Amazon seharusnya tidak memiliki akses internet langsung	[SageMaker.1] Instans SageMaker notebook Amazon seharusnya tidak memiliki akses internet langsung
PCI DSS v3.2.1	Instans PCI.SSM.1 yang EC2 dikelola oleh Systems Manager harus memiliki status kepatuhan patch COMPLIANT setelah instalasi patch	[SSM.2] EC2 Instans Amazon yang dikelola oleh Systems Manager harus memiliki status kepatuhan patch COMPLIANT setelah instalasi patch
PCI DSS v3.2.1	Instans PCI.SSM.2 yang EC2 dikelola oleh Systems Manager harus memiliki status kepatuhan asosiasi COMPLIANT	[SSM.3] EC2 Instans Amazon yang dikelola oleh Systems Manager harus memiliki status kepatuhan asosiasi COMPLIANT
PCI DSS v3.2.1	Instans EC2 PCI.SSM.3 harus dikelola oleh AWS Systems Manager	[SSM.1] EC2 Instans Amazon harus dikelola oleh AWS Systems Manager

Memperbarui alur kerja untuk konsolidasi

Jika alur kerja Anda tidak bergantung pada format spesifik bidang apa pun dalam temuan kontrol, tidak diperlukan tindakan.

Jika alur kerja Anda bergantung pada format tertentu dari satu atau beberapa bidang dalam temuan kontrol, seperti yang disebutkan dalam tabel sebelumnya, Anda harus memperbarui alur kerja Anda. Misalnya, Jika Anda membuat EventBridge aturan Amazon yang memicu tindakan untuk ID kontrol tertentu, seperti menjalankan AWS Lambda fungsi jika ID kontrol sama dengan CIS 2.7, perbarui aturan untuk menggunakan CloudTrail .2, yang merupakan nilai untuk bidang untuk kontrol tersebut `Compliance.SecurityControlId`.

Jika Anda membuat [wawasan khusus](#) yang menggunakan bidang atau nilai apa pun yang berubah, perbarui wawasan tersebut untuk menggunakan bidang atau nilai baru.

Atribut ASFF tingkat atas yang diperlukan

Atribut tingkat atas berikut dalam AWS Security Finding Format (ASFF) diperlukan untuk semua temuan di Security Hub CSPM. Untuk informasi selengkapnya tentang atribut ini, lihat [AwsSecurityFinding](#) di Referensi API AWS Security Hub.

AwsAccountId

Akun AWS ID yang berlaku untuk temuan tersebut.

Contoh

```
"AwsAccountId": "111111111111"
```

CreatedAt

Menunjukkan kapan potensi masalah keamanan atau peristiwa yang ditangkap oleh temuan dibuat.

Contoh

```
"CreatedAt": "2017-03-22T13:22:13.933Z"
```

Deskripsi

Deskripsi temuan. Bidang ini dapat berupa teks boilerplate nonspesifik atau detail yang spesifik untuk contoh temuan.

Untuk temuan kontrol yang dihasilkan oleh Security Hub CSPM, bidang ini memberikan deskripsi kontrol.

Bidang ini tidak mereferensikan standar jika Anda mengaktifkan [temuan kontrol terkonsolidasi](#).

Contoh

```
"Description": "This AWS control checks whether AWS Config is enabled in the current account and Region."
```

GeneratorId

Pengidentifikasi untuk komponen spesifik solusi (unit logika diskrit) yang menghasilkan temuan.

Untuk temuan kontrol yang dihasilkan CSPM Security Hub, bidang ini tidak mereferensikan standar jika Anda mengaktifkan temuan kontrol [konsolidasi](#).

Contoh

```
"GeneratorId": "security-control/Config.1"
```

Id

Pengidentifikasi khusus produk untuk sebuah temuan. Untuk temuan kontrol yang dihasilkan oleh Security Hub CSPM, bidang ini menyediakan Nama Sumber Daya Amazon (ARN) dari temuan tersebut.

Bidang ini tidak mereferensikan standar jika Anda mengaktifkan [temuan kontrol terkonsolidasi](#).

Contoh

```
"Id": "arn:aws:securityhub:eu-central-1:123456789012:security-control/iam.9/finding/ab6d6a26-a156-48f0-9403-115983e5a956"
```

ProductArn

Nama Sumber Daya Amazon (ARN) yang dihasilkan oleh Security Hub CSPM yang secara unik mengidentifikasi produk temuan pihak ketiga setelah produk terdaftar di Security Hub CSPM.

Format bidang ini adalah `arn:partition:securityhub:region:account-id:product/company-id/product-id`.

- Untuk Layanan AWS itu terintegrasi dengan Security Hub CSPM, `company-id` harus "aws", dan `product-id` harus menjadi nama layanan AWS publik. Karena AWS produk dan layanan tidak terkait dengan akun, `account-id` bagian ARN kosong. Layanan AWS yang belum terintegrasi dengan Security Hub CSPM dianggap sebagai produk pihak ketiga.
- Untuk produk publik, `company-id` dan `product-id` harus berupa nilai ID yang ditentukan pada saat pendaftaran.
- Untuk produk pribadi, `company-id` harus ID akun. `product-id` Harus berupa kata cadangan "default" atau ID yang ditentukan pada saat pendaftaran.

Contoh

```
// Private ARN
  "ProductArn": "arn:aws:securityhub:us-east-1:111111111111:product/111111111111/default"

// Public ARN
  "ProductArn": "arn:aws:securityhub:us-west-2::product/aws/guardduty"
  "ProductArn": "arn:aws:securityhub:us-west-2:222222222222:product/generico/secure-pro"
```

Sumber daya

ResourcesArray objek menyediakan satu set tipe data sumber daya yang menggambarkan AWS sumber daya yang mengacu pada temuan tersebut. Untuk detail tentang bidang yang mungkin berisi Resources objek, termasuk bidang mana yang diperlukan, lihat [Resourcedi Referensi API AWS Security Hub](#). Untuk contoh Resources objek untuk spesifik Layanan AWS, lihat [ResourcesObjek ASFF](#).

Contoh

```
"Resources": [
  {
    "ApplicationArn": "arn:aws:resource-groups:us-west-2:123456789012:group/SampleApp/1234567890abcdef0",
    "ApplicationName": "SampleApp",
    "DataClassification": {
    "DetailedResultsLocation": "Path_to_Folder_Or_File",
    "Result": {
      "MimeType": "text/plain",
      "SizeClassified": 2966026,
      "AdditionalOccurrences": false,
      "Status": {
        "Code": "COMPLETE",
        "Reason": "Unsupportedfield"
      },
      "SensitiveData": [
        {
          "Category": "PERSONAL_INFORMATION",
          "Detections": [
            {
              "Count": 34,
              "Type": "GE_PERSONAL_ID",
              "Occurrences": {
```

```

        "LineRanges": [
            {
                "Start": 1,
                "End": 10,
                "StartColumn": 20
            }
        ],
        "Pages": [],
        "Records": [],
        "Cells": []
    }
},
{
    "Count": 59,
    "Type": "EMAIL_ADDRESS",
    "Occurrences": {
        "Pages": [
            {
                "PageNumber": 1,
                "OffsetRange": {
                    "Start": 1,
                    "End": 100,
                    "StartColumn": 10
                },
                "LineRange": {
                    "Start": 1,
                    "End": 100,
                    "StartColumn": 10
                }
            }
        ]
    }
},
{
    "Count": 2229,
    "Type": "URL",
    "Occurrences": {
        "LineRanges": [
            {
                "Start": 1,
                "End": 13
            }
        ]
    }
}

```

```

        },
        {
            "Count": 13826,
            "Type": "NameDetection",
            "Occurrences": {
                "Records": [
                    {
                        "RecordIndex": 1,
                        "JsonPath": "$.ssn.value"
                    }
                ]
            }
        },
        {
            "Count": 32,
            "Type": "AddressDetection"
        }
    ],
    "TotalCount": 32
}
],
"CustomDataIdentifiers": {
    "Detections": [
        {
            "Arn": "1712be25e7c7f53c731fe464f1c869b8",
            "Name": "1712be25e7c7f53c731fe464f1c869b8",
            "Count": 2
        }
    ],
    "TotalCount": 2
}
},
{
    "Type": "AwsEc2Instance",
    "Id": "arn:aws:ec2:us-west-2:123456789012:instance/i-abcdef01234567890",
    "Partition": "aws",
    "Region": "us-west-2",
    "ResourceRole": "Target",
    "Tags": {
        "billingCode": "Lotus-1-2-3",
        "needsPatching": true
    },
    "Details": {
        "IamInstanceProfileArn": "arn:aws:iam::123456789012:role/IamInstanceProfileArn",

```

```

    "ImageId": "ami-79fd7eee",
    "IPv4Addresses": ["1.1.1.1"],
    "IPv6Addresses": ["2001:db8:1234:1a2b::123"],
    "KeyName": "testkey",
    "LaunchedAt": "2018-09-29T01:25:54Z",
    "MetadataOptions": {
      "HttpEndpoint": "enabled",
      "HttpProtocolIpv6": "enabled",
      "HttpPutResponseHopLimit": 1,
      "HttpTokens": "optional",
      "InstanceMetadataTags": "disabled"
    },
    "NetworkInterfaces": [
      {
        "NetworkInterfaceId": "eni-e5aa89a3"
      }
    ],
    "SubnetId": "PublicSubnet",
    "Type": "i3.xlarge",
    "VirtualizationType": "hvm",
    "VpcId": "TestVPCIPv6"
  }
]

```

SchemaVersion

Versi skema yang diformat untuk temuan. Nilai bidang ini harus menjadi salah satu versi yang diterbitkan secara resmi yang diidentifikasi oleh AWS. Dalam rilis saat ini, versi skema AWS Security Finding Format adalah 2018-10-08.

Contoh

```
"SchemaVersion": "2018-10-08"
```

Kepelikan

Mendefinisikan pentingnya sebuah temuan. Untuk detail tentang objek ini, lihat [Severity](#) di Referensi API AWS Security Hub Cloud Security Posture Management (CSPM) Security Hub.

Severity adalah objek tingkat atas dalam temuan dan bersarang di bawah objek.

FindingProviderFields

Nilai Severity objek tingkat atas untuk temuan harus diperbarui hanya dengan menggunakan [BatchUpdateFindings](#) API.

Untuk memberikan informasi tingkat keparahan, penyedia pencarian harus memperbarui Severity objek di bawah FindingProviderFields saat membuat permintaan [BatchImportFindings](#) API. Jika BatchImportFindings permintaan untuk temuan baru hanya menyediakan Label atau hanya menyediakan Normalized, Security Hub CSPM secara otomatis mengisi nilai bidang lainnya. OriginalBidang Product dan juga dapat dihuni.

Jika Finding.Severity objek tingkat atas hadir tetapi tidak Finding.FindingProviderFields ada, Security Hub CSPM membuat FindingProviderFields.Severity objek dan menyalin keseluruhan Finding.Severity object ke dalamnya. Ini memastikan bahwa detail asli yang disediakan penyedia dipertahankan dalam FindingProviderFields.Severity struktur, bahkan jika objek tingkat atas Severity ditimpa.

Tingkat keparahan temuan tidak mempertimbangkan kekritisitas aset yang terlibat atau sumber daya yang mendasarinya. Kritikalitas didefinisikan sebagai tingkat kepentingan sumber daya yang terkait dengan temuan tersebut. Misalnya, sumber daya yang terkait dengan aplikasi kritis misi memiliki kekritisitas yang lebih tinggi daripada yang terkait dengan pengujian nonproduksi. Untuk menangkap informasi tentang kekritisitas sumber daya, gunakan Criticality bidang.

Sebaiknya gunakan panduan berikut saat menerjemahkan skor keparahan asli temuan ke nilai Severity.Label di ASFF.

- INFORMATIONAL Kategori ini dapat mencakup temuan untuk PASSED, WARNING, atau NOT AVAILABLE cek atau identifikasi data sensitif.
- LOW— Temuan yang dapat menghasilkan kompromi di masa depan. Misalnya, kategori ini mungkin mencakup kerentanan, kelemahan konfigurasi, dan kata sandi yang terbuka.
- MEDIUM— Temuan yang menunjukkan kompromi aktif, tetapi tidak ada indikasi bahwa musuh menyelesaikan tujuan mereka. Misalnya, kategori ini mungkin mencakup aktivitas malware, aktivitas peretasan, dan deteksi perilaku yang tidak biasa.
- HIGH atau CRITICAL — Temuan yang menunjukkan bahwa musuh menyelesaikan tujuan mereka, seperti kehilangan data aktif atau kompromi atau penolakan layanan.

Contoh


```
"Severity": {  
  "Label": "CRITICAL",  
  "Normalized": 90,  
  "Original": "CRITICAL"  
}
```

Judul

Judul temuan. Bidang ini dapat berisi teks boilerplate nonspesifik atau detail yang spesifik untuk contoh temuan ini.

Untuk temuan kontrol, bidang ini memberikan judul kontrol. Bidang ini tidak mereferensikan standar jika Anda mengaktifkan [temuan kontrol terkonsolidasi](#).

Contoh

```
"Title": "AWS Config should be enabled"
```

Tipe

Satu atau lebih jenis temuan dalam format *namespace/category/classifier* yang mengklasifikasikan temuan. Bidang ini tidak mereferensikan standar jika Anda mengaktifkan [temuan kontrol terkonsolidasi](#).

Types harus diperbarui hanya dengan menggunakan [BatchUpdateFindingsAPI](#).

Menemukan penyedia yang ingin memberikan nilai untuk Types harus menggunakan Types atribut di bawah [FindingProviderFields](#).

Dalam daftar berikut, peluru tingkat atas adalah ruang nama, peluru tingkat kedua adalah kategori, dan peluru tingkat ketiga adalah pengklasifikasi. Sebaiknya penyedia pencarian menggunakan ruang nama yang ditentukan untuk membantu mengurutkan dan mengelompokkan temuan. Kategori dan pengklasifikasi yang ditentukan juga dapat digunakan, tetapi tidak diperlukan. Hanya namespace Pemeriksaan Perangkat Lunak dan Konfigurasi yang telah menentukan pengklasifikasi.

Anda dapat menentukan jalur sebagian untuk namespace/category/classifier. Misalnya, jenis temuan berikut semuanya valid:

- TTPs

- TTPs/Penghindaran Pertahanan
- TTPs/Defense Evasion/CloudTrailStopped

Kategori taktik, teknik, dan prosedur (TTPs) dalam daftar berikut selaras dengan MatrixTM [MITRE ATT&CK](#). Namespace Perilaku Tidak Biasa mencerminkan perilaku umum yang tidak biasa, seperti anomali statistik umum, dan tidak selaras dengan TTP tertentu. Namun, Anda dapat mengklasifikasikan temuan dengan Perilaku Tidak Biasa dan tipe TTPs temuan.

Daftar ruang nama, kategori, dan pengklasifikasi:

- Pemeriksaan Perangkat Lunak dan Konfigurasi
 - Kerentanan
 - CVE
 - AWS Praktik Terbaik Keamanan
 - Keterjangkauan Jaringan
 - Analisis Perilaku Waktu Aktif
 - Standar Industri dan Regulasi
 - AWS Praktik Terbaik Keamanan Dasar
 - Tolok Ukur Pengerasan Host CIS
 - Tolok Ukur AWS Yayasan CIS
 - PCI-DSS
 - Kontrol Aliansi Keamanan Cloud
 - Kontrol ISO 90001
 - Kontrol ISO 27001
 - Kontrol ISO 27017
 - Kontrol ISO 27018
 - SOC 1
 - SOC 2
 - Kontrol HIPAA (AS)
 - NIST 800-53 Kontrol (AS)
 - Kontrol CSF NIST (AS)
 - Kontrol IRAP (Australia)

- Kontrol K-ISMS (Korea)
- Kontrol MTCS (Singapura)
- Kontrol FISC (Jepang)
- Kontrol Undang-Undang Nomor Saya (Jepang)
- ENS Controls (Spanyol)
- Kontrol Cyber Essentials Plus (Inggris)
- Kontrol G-Cloud (Inggris)
- Kontrol C5 (Jerman)
- Kontrol IT-Grundschutz (Jerman)
- Kontrol GDPR (Eropa)
- Kontrol TISAX (Eropa)
- Manajemen Patch
- TTPs
 - Akses Awal
 - Eksekusi
 - Tetap
 - Eskalasi Hak Istimewa
 - Penghindaran Pertahanan
 - Akses Kredensi
 - Penemuan
 - Gerakan Lateral
 - Koleksi
 - Perintah dan Kontrol
- Efek
 - Eksposur Data
 - Ekfiltrasi Data
 - Penghancuran Data
 - Penolakan Layanan
 - Konsumsi Sumber Daya
- Perilaku Tidak Biasa

- Aplikasi
- Aliran Jaringan
- Alamat IP
- Pengguna
- VM
- Kontainer
- Nirserver
- Proses
- Basis Data
- Data
- Identifikasi Data Sensitif
 - PII
 - Kata Sandi
 - Legal
 - Keuangan
 - Keamanan
 - Bisnis

Contoh

```
"Types": [  
  "Software and Configuration Checks/Vulnerabilities/CVE"  
]
```

UpdatedAt

Menunjukkan kapan penyedia temuan terakhir memperbarui catatan temuan.

Stempel waktu ini mencerminkan waktu ketika catatan temuan terakhir atau yang terbaru diperbarui. Akibatnya, ini dapat berbeda dari `LastObservedAt` stempel waktu, yang mencerminkan kapan peristiwa atau kerentanan terakhir atau yang terbaru diamati.

Saat memperbarui catatan temuan, Anda harus memperbarui stempel waktu ini ke stempel waktu saat ini. Setelah membuat catatan temuan, `CreatedAt` dan `UpdatedAt` stempel waktu harus sama.

Setelah pembaruan ke catatan temuan, nilai bidang ini harus lebih baru dari semua nilai sebelumnya yang terkandung di dalamnya.

Perhatikan bahwa `UpdatedAt` tidak dapat diperbarui dengan menggunakan [BatchUpdateFindings](#) operasi. Anda dapat memperbaruinya hanya dengan menggunakan [BatchImportFindings](#) operasi.

Contoh

```
"UpdatedAt": "2017-04-22T13:22:13.933Z"
```

Atribut ASFF tingkat atas opsional

Atribut tingkat atas berikut dalam AWS Security Finding Format (ASFF) adalah opsional untuk temuan di Security Hub CSPM. Untuk informasi selengkapnya tentang atribut ini, lihat [AwsSecurityFinding](#) di Referensi API AWS Security Hub.

Tindakan

[Action](#) Objek memberikan rincian tentang tindakan yang mempengaruhi atau diambil pada sumber daya.

Contoh

```
"Action": {
  "ActionType": "PORT_PROBE",
  "PortProbeAction": {
    "PortProbeDetails": [
      {
        "LocalPortDetails": {
          "Port": 80,
          "PortName": "HTTP"
        },
        "LocalIpDetails": {
          "IpAddressV4": "192.0.2.0"
        },
        "RemoteIpDetails": {
          "Country": {
            "CountryName": "Example Country"
          }
        }
      ]
    }
  }
}
```

```
        "City": {
            "CityName": "Example City"
        },
        "GeoLocation": {
            "Lon": 0,
            "Lat": 0
        },
        "Organization": {
            "AsnOrg": "ExampleASO",
            "Org": "ExampleOrg",
            "Isp": "ExampleISP",
            "Asn": 64496
        }
    },
    "Blocked": false
}
```

AwsAccountName

Akun AWS Nama yang digunakan untuk temuan itu.

Contoh

```
"AwsAccountName": "jane-doe-testaccount"
```

CompanyName

Nama perusahaan untuk produk yang menghasilkan temuan. Untuk temuan berbasis kontrol, perusahaan adalah. AWS

Security Hub CSPM mengisi atribut ini secara otomatis untuk setiap temuan. Anda tidak dapat memperbaruinya menggunakan [BatchImportFindings](#) atau [BatchUpdateFindings](#).

Pengecualian untuk ini adalah ketika Anda menggunakan integrasi khusus. Lihat [the section called "Integrasi produk khusus"](#).

Saat Anda menggunakan konsol CSPM Security Hub untuk memfilter temuan berdasarkan nama perusahaan, Anda menggunakan atribut ini. Bila Anda menggunakan Security Hub CSPM API untuk memfilter temuan berdasarkan nama perusahaan, Anda menggunakan `aws/securityhub/`

CompanyName atribut di bawah. ProductFields Security Hub CSPM tidak menyinkronkan kedua atribut tersebut.

Contoh

```
"CompanyName": "AWS"
```

Kepatuhan

[Compliance](#) Objek biasanya memberikan rincian tentang temuan kontrol, seperti standar yang berlaku dan status pemeriksaan kontrol.

Contoh

```
"Compliance": {
  "AssociatedStandards": [
    {"StandardsId": "standards/aws-foundational-security-best-practices/v/1.0.0"},
    {"StandardsId": "standards/service-managed-aws-control-tower/v/1.0.0"},
    {"StandardsId": "standards/nist-800-53/v/5.0.0"}
  ],
  "RelatedRequirements": [
    "NIST.800-53.r5 AC-4",
    "NIST.800-53.r5 AC-4(21)",
    "NIST.800-53.r5 SC-7",
    "NIST.800-53.r5 SC-7(11)",
    "NIST.800-53.r5 SC-7(16)",
    "NIST.800-53.r5 SC-7(21)",
    "NIST.800-53.r5 SC-7(4)",
    "NIST.800-53.r5 SC-7(5)"
  ],
  "SecurityControlId": "EC2.18",
  "SecurityControlParameters": [
    {
      "Name": "authorizedTcpPorts",
      "Value": ["80", "443"]
    },
    {
      "Name": "authorizedUdpPorts",
      "Value": ["427"]
    }
  ],
  "Status": "NOT_AVAILABLE",
```

```

    "StatusReasons": [
      {
        "ReasonCode": "CONFIG_RETURNS_NOT_APPLICABLE",
        "Description": "This finding has a compliance status of NOT AVAILABLE because AWS Config sent Security Hub CSPM a finding with a compliance state of Not Applicable. The potential reasons for a Not Applicable finding from Config are that (1) a resource has been moved out of scope of the Config rule; (2) the Config rule has been deleted; (3) the resource has been deleted; or (4) the logic of the Config rule itself includes scenarios where Not Applicable is returned. The specific reason why Not Applicable is returned is not available in the Config rule evaluation."
      }
    ]
  }
}

```

Kepercayaan

Kemungkinan bahwa temuan secara akurat mengidentifikasi perilaku atau masalah yang dimaksudkan untuk diidentifikasi.

Confidenceseharusnya hanya diperbarui menggunakan [BatchUpdateFindings](#).

Menemukan penyedia yang ingin memberikan nilai untuk Confidence harus menggunakan Confidence atribut di bawah `FindingProviderFields`. Lihat [the section called “Memperbarui temuan dengan FindingProviderFields”](#).

Confidencedinilai berdasarkan 0-100 menggunakan skala rasio. 0 berarti kepercayaan 0 persen, dan 100 berarti kepercayaan 100 persen. Misalnya, deteksi eksfiltrasi data berdasarkan penyimpangan statistik lalu lintas jaringan memiliki kepercayaan diri yang rendah karena eksfiltrasi aktual belum diverifikasi.

Contoh

```
"Confidence": 42
```

Kekritisan

Tingkat kepentingan yang ditetapkan untuk sumber daya yang terkait dengan temuan.

Criticalityseharusnya hanya diperbarui dengan memanggil operasi [BatchUpdateFindings](#) API. Jangan perbarui objek ini dengan [BatchImportFindings](#).

Menemukan penyedia yang ingin memberikan nilai untuk `Criticality` harus menggunakan `Criticality` atribut di bawah `FindingProviderFields`. Lihat [the section called “Memperbarui temuan dengan FindingProviderFields”](#).

`Criticality` diberi skor pada basis 0-100, menggunakan skala rasio yang hanya mendukung bilangan bulat penuh. Skor 0 berarti bahwa sumber daya yang mendasarinya tidak memiliki kekritisan, dan skor 100 dicadangkan untuk sumber daya yang paling kritis.

Untuk setiap sumber daya, pertimbangkan hal berikut saat menetapkan `Criticality`:

- Apakah sumber daya yang terpengaruh berisi data sensitif (misalnya, bucket S3 dengan PII)?
- Apakah sumber daya yang terpengaruh memungkinkan musuh untuk memperdalam akses mereka atau memperluas kemampuan mereka untuk melakukan aktivitas berbahaya tambahan (misalnya, akun sysadmin yang disusupi)?
- Apakah sumber daya merupakan aset penting bisnis (misalnya, sistem bisnis utama yang jika dikompromikan dapat memiliki dampak pendapatan yang signifikan)?

Anda dapat menggunakan pedoman berikut:

- Sumber daya yang menggerakkan sistem mission-critical atau berisi data yang sangat sensitif dapat dinilai dalam kisaran 75-100.
- Sumber daya yang memberi daya pada sistem penting (tetapi bukan sistem kritis) atau berisi data yang cukup penting dapat dinilai dalam kisaran 25-74.
- Sumber daya yang memberi daya pada sistem yang tidak penting atau berisi data yang tidak sensitif harus dinilai dalam kisaran 0-24.

Contoh

```
"Criticality": 99
```

Deteksi

`DetectionObjek` ini memberikan detail tentang temuan urutan serangan dari Amazon GuardDuty Extended Threat Detection. GuardDuty menghasilkan temuan urutan serangan ketika beberapa peristiwa sejajar dengan aktivitas yang berpotensi mencurigakan. Untuk menerima temuan urutan GuardDuty serangan di AWS Security Hub Cloud Security Posture Management (CSPM), Anda

harus GuardDuty mengaktifkan di akun Anda. Untuk informasi selengkapnya, lihat [Deteksi Ancaman GuardDuty Diperpanjang Amazon](#) di Panduan GuardDuty Pengguna Amazon.

Contoh

```
"Detection": {
  "Sequence": {
    "Uid": "111111111111-184ec3b9-cf8d-452d-9aad-f5bdb7afb010",
    "Actors": [{
      "Id": "USER:ARO987654321EXAMPLE:i-b188560f:1234567891",
      "Session": {
        "Uid": "1234567891",
        "MfAStatus": "DISABLED",
        "CreatedTime": "1716916944000",
        "Issuer": "arn:aws:s3:::amzn-s3-demo-destination-bucket"
      },
      "User": {
        "CredentialUid": "ASIAIOSFODNN7EXAMPLE",
        "Name": "ec2_instance_role_production",
        "Type": "AssumedRole",
        "Uid": "ARO987654321EXAMPLE:i-b188560f",
        "Account": {
          "Uid": "AccountId",
          "Name": "AccountName"
        }
      }
    }],
    "Endpoints": [{
      "Id": "EndpointId",
      "Ip": "203.0.113.1",
      "Domain": "example.com",
      "Port": 4040,
      "Location": {
        "City": "New York",
        "Country": "US",
        "Lat": 40.7123,
        "Lon": -74.0068
      },
      "AutonomousSystem": {
        "Name": "AnyCompany",
        "Number": 64496
      },
      "Connection": {
        "Direction": "INBOUND"
      }
    }]
```

```

    }
  ]],
  "Signals": [{
    "Id": "arn:aws:guardduty:us-east-1:123456789012:detector/
d0bfe135ab8b4dd8c3eaae7df9900073/finding/535a382b1bcc44d6b219517a29058fb7",
    "Title": "Someone ran a penetration test tool on your account.",
    "ActorIds": ["USER:AR0A987654321EXAMPLE:i-b188560f:1234567891"],
    "Count": 19,
    "FirstSeenAt": 1716916943000,
    "SignalIndicators": [
      {
        "Key": "ATTACK_TACTIC",
        "Title": "Attack Tactic",
        "Values": [
          "Impact"
        ]
      },
      {
        "Key": "HIGH_RISK_API",
        "Title": "High Risk Api",
        "Values": [
          "s3:DeleteObject"
        ]
      },
      {
        "Key": "ATTACK_TECHNIQUE",
        "Title": "Attack Technique",
        "Values": [
          "Data Destruction"
        ]
      }
    ],
    "LastSeenAt": 1716916944000,
    "Name": "Test:IAMUser/KaliLinux",
    "ResourceIds": [
      "arn:aws:s3:::amzn-s3-demo-destination-bucket"
    ],
    "Type": "FINDING"
  ]],
  "SequenceIndicators": [
    {
      "Key": "ATTACK_TACTIC",
      "Title": "Attack Tactic",
      "Values": [

```

```

        "Discovery",
        "Exfiltration",
        "Impact"
    ]
},
{
    "Key": "HIGH_RISK_API",
    "Title": "High Risk Api",
    "Values": [
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:ListBuckets",
        "s3:ListObjects"
    ]
},
{
    "Key": "ATTACK_TECHNIQUE",
    "Title": "Attack Technique",
    "Values": [
        "Cloud Service Discovery",
        "Data Destruction"
    ]
}
]
}
}

```

FindingProviderFields

FindingProviderFieldstermasuk atribut berikut:

- Confidence
- Criticality
- RelatedFindings
- Severity
- Types

Bidang sebelumnya bersarang di bawah FindingProviderFields objek, tetapi memiliki analog dengan nama yang sama dengan bidang ASFF tingkat atas. Ketika temuan baru dikirim ke Security

Hub CSPM oleh penyedia pencarian, Security Hub CSPM mengisi `FindingProviderFields` objek secara otomatis jika kosong berdasarkan bidang tingkat atas yang sesuai.

Penyedia pencarian dapat memperbarui `FindingProviderFields` dengan menggunakan [BatchImportFindings](#) pengoperasian Security Hub CSPM API. Menemukan penyedia tidak dapat memperbarui objek ini dengan [BatchUpdateFindings](#).

Untuk detail tentang cara Security Hub CSPM menangani pembaruan dari `BatchImportFindings` ke `FindingProviderFields` dan ke atribut tingkat atas yang sesuai, lihat. [the section called "Memperbarui temuan dengan FindingProviderFields"](#)

Pelanggan dapat memperbarui bidang tingkat atas dengan menggunakan `BatchUpdateFindings` operasi. Pelanggan tidak dapat memperbarui `FindingProviderFields`.

Contoh

```
"FindingProviderFields": {
  "Confidence": 42,
  "Criticality": 99,
  "RelatedFindings": [
    {
      "ProductArn": "arn:aws:securityhub:us-west-2::product/aws/guardduty",
      "Id": "123e4567-e89b-12d3-a456-426655440000"
    }
  ],
  "Severity": {
    "Label": "MEDIUM",
    "Original": "MEDIUM"
  },
  "Types": [ "Software and Configuration Checks/Vulnerabilities/CVE" ]
}
```

FirstObservedAt

Menunjukkan kapan potensi masalah keamanan atau peristiwa yang ditangkap oleh temuan pertama kali diamati.

Stempel waktu ini menentukan kapan peristiwa atau kerentanan pertama kali diamati. Akibatnya, ini dapat berbeda dari `CreatedAt` stempel waktu, yang mencerminkan kapan catatan temuan ini dibuat.

Stempel waktu ini harus tidak dapat diubah antara pembaruan catatan temuan tetapi dapat diperbarui jika stempel waktu yang lebih akurat ditentukan.

Contoh

```
"FirstObservedAt": "2017-03-22T13:22:13.933Z"
```

LastObservedAt

Menunjukkan kapan potensi masalah keamanan atau peristiwa yang ditangkap oleh temuan baru-baru ini diamati oleh produk temuan keamanan.

Stempel waktu ini menentukan kapan peristiwa atau kerentanan terakhir atau yang terbaru diamati. Akibatnya, ini dapat berbeda dari UpdatedAt stempel waktu, yang mencerminkan kapan catatan temuan ini terakhir atau yang terbaru diperbarui.

Anda dapat memberikan stempel waktu ini, tetapi tidak diperlukan pada pengamatan pertama. Jika Anda mengisi bidang ini pada pengamatan pertama, stempel waktu harus sama dengan stempel waktu. FirstObservedAt Anda harus memperbarui bidang ini untuk mencerminkan stempel waktu terakhir atau yang paling baru diamati setiap kali temuan diamati.

Contoh

```
"LastObservedAt": "2017-03-23T13:22:13.933Z"
```

Malware

[Malware](#) Objek menyediakan daftar malware yang terkait dengan temuan.

Contoh

```
"Malware": [  
  {  
    "Name": "Stringler",  
    "Type": "COIN_MINER",  
    "Path": "/usr/sbin/stringler",  
    "State": "OBSERVED"  
  }  
]
```

Jaringan (Pensiunan)

[Network](#) Objek menyediakan informasi terkait jaringan tentang temuan.

Objek ini sudah pensiun. Untuk menyediakan data ini, Anda dapat memetakan data ke sumber daya diResources, atau menggunakan Action objek.

Contoh

```
"Network": {
  "Direction": "IN",
  "OpenPortRange": {
    "Begin": 443,
    "End": 443
  },
  "Protocol": "TCP",
  "SourceIPv4": "1.2.3.4",
  "SourceIPv6": "FE80:CD00:0000:0CDE:1257:0000:211E:729C",
  "SourcePort": "42",
  "SourceDomain": "example1.com",
  "SourceMac": "00:0d:83:b1:c0:8e",
  "DestinationIPv4": "2.3.4.5",
  "DestinationIPv6": "FE80:CD00:0000:0CDE:1257:0000:211E:729C",
  "DestinationPort": "80",
  "DestinationDomain": "example2.com"
}
```

NetworkPath

[NetworkPath](#) Objek memberikan informasi tentang jalur jaringan yang terkait dengan temuan. Setiap entri di NetworkPath mewakili komponen jalur.

Contoh

```
"NetworkPath" : [
  {
    "ComponentId": "abc-01a234bc56d8901ee",
    "ComponentType": "AWS::EC2::InternetGateway",
    "Egress": {
      "Destination": {
        "Address": [ "192.0.2.0/24" ],
        "PortRanges": [
```

```

        {
            "Begin": 443,
            "End": 443
        }
    ]
},
"Protocol": "TCP",
"Source": {
    "Address": ["203.0.113.0/24"]
}
},
"Ingress": {
    "Destination": {
        "Address": [ "198.51.100.0/24" ],
        "PortRanges": [
            {
                "Begin": 443,
                "End": 443
            }
        ]
    },
    "Protocol": "TCP",
    "Source": {
        "Address": [ "203.0.113.0/24" ]
    }
}
}
]

```

Catatan

[Note](#) Objek menentukan catatan yang ditentukan pengguna yang dapat Anda tambahkan ke temuan.

Penyedia temuan dapat memberikan catatan awal untuk sebuah temuan, tetapi tidak dapat menambahkan catatan setelah itu. Anda hanya dapat memperbarui catatan menggunakan [BatchUpdateFindings](#).

Contoh

```

"Note": {
    "Text": "Don't forget to check under the mat.",
    "UpdatedBy": "jsmith",
    "UpdatedAt": "2018-08-31T00:15:09Z"
}

```



```
}
```

PatchSummary

[PatchSummary](#) Objek menyediakan ringkasan status kepatuhan patch untuk sebuah instance terhadap standar kepatuhan yang dipilih.

Contoh

```
"PatchSummary" : {
  "FailedCount" : 0,
  "Id" : "pb-123456789098",
  "InstalledCount" : 100,
  "InstalledOtherCount" : 1023,
  "InstalledPendingReboot" : 0,
  "InstalledRejectedCount" : 0,
  "MissingCount" : 100,
  "Operation" : "Install",
  "OperationEndTime" : "2018-09-27T23:39:31Z",
  "OperationStartTime" : "2018-09-27T23:37:31Z",
  "RebootOption" : "RebootIfNeeded"
}
```

Proses

[Process](#) Objek memberikan rincian terkait proses tentang temuan.

Contoh:

```
"Process": {
  "LaunchedAt": "2018-09-27T22:37:31Z",
  "Name": "syslogd",
  "ParentPid": 56789,
  "Path": "/usr/sbin/syslogd",
  "Pid": 12345,
  "TerminatedAt": "2018-09-27T23:37:31Z"
}
```

ProcessedAt

Menunjukkan kapan Security Hub CSPM menerima temuan dan mulai memprosesnya.

Ini berbeda dari `CreatedAt` dan `UpdatedAt`, yang merupakan stempel waktu yang diperlukan yang berhubungan dengan interaksi penyedia temuan dengan masalah keamanan dan temuan. `ProcessedAt` stempel waktu menunjukkan kapan Security Hub CSPM mulai memproses temuan. Temuan muncul di akun pengguna setelah pemrosesan selesai.

```
"ProcessedAt": "2023-03-23T13:22:13.933Z"
```

ProductFields

Tipe data di mana produk temuan keamanan dapat menyertakan detail spesifik solusi tambahan yang bukan merupakan bagian dari Format Pencarian AWS Keamanan yang ditentukan.

Untuk temuan yang dihasilkan oleh kontrol CSPM Security Hub, `ProductFields` termasuk informasi tentang kontrol. Lihat [the section called “Menghasilkan dan memperbarui temuan kontrol”](#).

Bidang ini tidak boleh berisi data yang berlebihan dan tidak boleh berisi data yang bertentangan dengan bidang Format Pencarian AWS Keamanan.

Awalan `aws/` mewakili namespace yang dicadangkan hanya untuk AWS produk dan layanan dan tidak boleh diserahkan dengan temuan dari integrasi pihak ketiga.

Meskipun tidak diperlukan, produk harus memformat nama bidang sebagai `company-id/product-id/field-name`, di mana `company-id` dan `product-id` cocok dengan yang `ProductArn` disediakan dalam temuan.

Referensi bidang `Archival` digunakan saat Security Hub CSPM mengarsipkan temuan yang ada. Misalnya, Security Hub CSPM mengarsipkan temuan yang ada saat Anda menonaktifkan kontrol atau standar dan saat Anda mengaktifkan atau menonaktifkan [temuan kontrol konsolidasi](#).

Bidang ini juga dapat mencakup informasi tentang standar yang mencakup kontrol yang menghasilkan temuan.

Contoh

```
"ProductFields": {
  "API", "DeleteTrail",
  "ArchivalReasons:0/Description": "The finding is in an ARCHIVED state because consolidated control findings has been turned on or off. This causes findings in the previous state to be archived when new findings are being generated.",
  "ArchivalReasons:0/ReasonCode": "CONSOLIDATED_CONTROL_FINDINGS_UPDATE",
  "aws/inspector/AssessmentTargetName": "My prod env",
```

```
"aws/inspector/AssessmentTemplateName": "My daily CVE assessment",  
"aws/inspector/RulesPackageName": "Common Vulnerabilities and Exposures",  
"generico/secure-pro/Action.Type", "AWS_API_CALL",  
"generico/secure-pro/Count": "6",  
"Service_Name": "cloudtrail.amazonaws.com"  
}
```

ProductName

Memberikan nama produk yang menghasilkan temuan. Untuk temuan berbasis kontrol, nama produknya adalah Security Hub CSPM.

Security Hub CSPM mengisi atribut ini secara otomatis untuk setiap temuan. Anda tidak dapat memperbaruinya menggunakan [BatchImportFindings](#) atau [BatchUpdateFindings](#). Pengecualian untuk ini adalah ketika Anda menggunakan integrasi khusus. Lihat [the section called "Integrasi produk khusus"](#).

Saat Anda menggunakan konsol CSPM Security Hub untuk memfilter temuan berdasarkan nama produk, Anda menggunakan atribut ini.

Bila Anda menggunakan Security Hub CSPM API untuk memfilter temuan berdasarkan nama produk, Anda menggunakan `aws/securityhub/ProductName` atribut di bawah `ProductFields`

Security Hub CSPM tidak menyinkronkan kedua atribut tersebut.

RecordState

Memberikan status catatan temuan.

Secara default, ketika awalnya dihasilkan oleh layanan, temuan dipertimbangkan `ACTIVE`.

`ARCHIVED` Negara menunjukkan bahwa temuan harus disembunyikan dari pandangan. Temuan yang diarsipkan tidak segera dihapus. Anda dapat mencari, meninjau, dan melaporkannya. Security Hub CSPM secara otomatis mengarsipkan temuan berbasis kontrol jika sumber daya terkait dihapus, sumber daya tidak ada, atau kontrol dinonaktifkan.

`RecordState` dimaksudkan untuk menemukan penyedia, dan dapat diperbarui hanya dengan menggunakan [BatchImportFindings](#) operasi. Anda tidak dapat memperbaruinya dengan menggunakan [BatchUpdateFindings](#) operasi.

Untuk melacak status penyelidikan Anda ke dalam sebuah temuan, gunakan [Workflow](#) sebagai gantinya `RecordState`.

Jika status rekaman berubah dari ARCHIVED ke ACTIVE, dan status alur kerja temuan adalah NOTIFIED atau RESOLVED, Security Hub CSPM secara otomatis mengubah status alur kerja menjadi NEW.

Contoh

```
"RecordState": "ACTIVE"
```

Wilayah

Menentukan Wilayah AWS dari mana temuan itu dihasilkan.

Security Hub CSPM mengisi atribut ini secara otomatis untuk setiap temuan. Anda tidak dapat memperbaruinya menggunakan [BatchImportFindings](#) atau [BatchUpdateFindings](#).

Contoh

```
"Region": "us-west-2"
```

RelatedFindings

Memberikan daftar temuan yang terkait dengan temuan saat ini.

RelatedFindings seharusnya hanya diperbarui dengan operasi [BatchUpdateFindings](#) API. Anda tidak harus memperbarui objek ini dengan [BatchImportFindings](#).

Untuk [BatchImportFindings](#) permintaan, penyedia pencarian harus menggunakan RelatedFindings objek di bawah [FindingProviderFields](#).

Untuk melihat deskripsi RelatedFindings atribut, lihat [RelatedFinding](#) di Referensi API AWS Security Hub Cloud Security Posture Management (CSPM) Security Hub.

Contoh

```
"RelatedFindings": [  
  {  
    "ProductArn": "arn:aws:securityhub:us-west-2::product/aws/guardduty",  
    "Id": "123e4567-e89b-12d3-a456-426655440000" },  
  {  
    "ProductArn": "arn:aws:securityhub:us-west-2::product/aws/guardduty",  
    "Id": "AcmeNerfHerder-111111111111-x189dx7824" }  
]
```

RiskAssessment

Contoh

```
"RiskAssessment": {
  "Posture": {
    "FindingTotal": 4,
    "Indicators": [
      {
        "Type": "Reachability",
        "Findings": [
          {
            "Id": "arn:aws:inspector2:us-east-2:123456789012:finding/1234567890abcdef0",
            "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/inspector",
            "Title": "Finding title"
          },
          {
            "Id": "arn:aws:inspector2:us-east-2:123456789012:finding/abcdef01234567890",
            "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/inspector",
            "Title": "Finding title"
          }
        ]
      },
      {
        "Type": "Vulnerability",
        "Findings": [
          {
            "Id": "arn:aws:inspector2:us-east-2:123456789012:finding/021345abcdef6789",
            "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/inspector",
            "Title": "Finding title"
          },
          {
            "Id": "arn:aws:inspector2:us-east-2:123456789012:finding/021345ghijkl6789",
            "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/inspector",
            "Title": "Finding title"
          }
        ]
      }
    ]
  }
}
```

```
    ]
  }
]
}
```

Remediasi

[Remediation](#) Objek memberikan informasi tentang langkah-langkah remediasi yang direkomendasikan untuk mengatasi temuan tersebut.

Contoh

```
"Remediation": {
  "Recommendation": {
    "Text": "For instructions on how to fix this issue, see the AWS Security Hub Cloud Security Posture Management (CSPM) documentation for EC2.2.",
    "Url": "https://docs.aws.amazon.com/console/securityhub/EC2.2/remediation"
  }
}
```

Sampel

Menentukan apakah temuan adalah temuan sampel.

```
"Sample": true
```

SourceUrl

[SourceUrl](#) Objek menyediakan URL yang menautkan ke halaman tentang temuan saat ini dalam produk pencarian.

```
"SourceUrl": "http://sourceurl.com"
```

ThreatIntelIndicators

[ThreatIntelIndicator](#) Objek tersebut memberikan rincian intelijen ancaman yang terkait dengan temuan.

Contoh

```
"ThreatIntelIndicators": [  
  {  
    "Category": "BACKDOOR",  
    "LastObservedAt": "2018-09-27T23:37:31Z",  
    "Source": "Threat Intel Weekly",  
    "SourceUrl": "http://threatintelweekly.org/backdoors/8888",  
    "Type": "IPV4_ADDRESS",  
    "Value": "8.8.8.8",  
  }  
]
```

Ancaman

[Threats](#) Objek memberikan rincian tentang ancaman yang terdeteksi oleh sebuah temuan.

Contoh

```
"Threats": [{  
  "FilePaths": [{  
    "FileName": "b.txt",  
    "FilePath": "/tmp/b.txt",  
    "Hash": "sha256",  
    "ResourceId": "arn:aws:ec2:us-west-2:123456789012:volume/vol-032f3bdd89aee112f"  
  }],  
  "ItemCount": 3,  
  "Name": "Iot.linux.mirai.vwisi",  
  "Severity": "HIGH"  
}]
```

UserDefinedFields

Menyediakan daftar pasangan string nama-nilai yang terkait dengan temuan. Ini adalah bidang khusus yang ditentukan pengguna yang ditambahkan ke temuan. Bidang ini dapat dihasilkan secara otomatis melalui konfigurasi spesifik Anda.

Penyedia pencarian tidak boleh menggunakan bidang ini untuk data yang dihasilkan produk. Sebagai gantinya, penyedia pencarian dapat menggunakan `ProductFields` bidang untuk data yang tidak dipetakan ke bidang Format Pencarian AWS Keamanan standar apa pun.

Bidang ini hanya dapat diperbarui menggunakan [BatchUpdateFindings](#).

Contoh

```
"UserDefinedFields": {
  "reviewedByCio": "true",
  "comeBackToLater": "Check this again on Monday"
}
```

VerificationState

Memberikan kebenaran temuan. Temuan produk dapat memberikan nilai UNKNOWN untuk bidang ini. Produk temuan harus memberikan nilai untuk bidang ini jika ada analog yang berarti dalam sistem produk temuan. Bidang ini biasanya diisi oleh penentuan atau tindakan pengguna setelah menyelidiki temuan.

Penyedia temuan dapat memberikan nilai awal untuk atribut ini, tetapi tidak dapat memperbaruinya setelah itu. Anda hanya dapat memperbarui atribut ini dengan menggunakan [BatchUpdateFindings](#).

```
"VerificationState": "Confirmed"
```

Kerentanan

[Vulnerabilities](#) Objek menyediakan daftar kerentanan yang terkait dengan temuan.

Contoh

```
"Vulnerabilities" : [
  {
    "CodeVulnerabilities": [{
      "Cwes": [
        "CWE-798",
        "CWE-799"
      ],
      "FilePath": {
        "EndLine": 421,
        "FileName": "package-lock.json",
        "FilePath": "package-lock.json",
        "StartLine": 420
      },
      "SourceArn": "arn:aws:lambda:us-east-1:123456789012:layer:AWS-AppConfig-Extension:114"
    }],
    "Cvss": [
      {
```



```

        "BaseScore": 4.7,
        "BaseVector": "AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N",
        "Version": "V3"
    },
    {
        "BaseScore": 4.7,
        "BaseVector": "AV:L/AC:M/Au:N/C:C/I:N/A:N",
        "Version": "V2"
    }
],
"EpssScore": 0.015,
"ExploitAvailable": "YES",
"FixAvailable": "YES",
"Id": "CVE-2020-12345",
"LastKnownExploitAt": "2020-01-16T00:01:35Z",
"ReferenceUrls": [
    "http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-12418",
    "http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-17563"
],
"RelatedVulnerabilities": ["CVE-2020-12345"],
"Vendor": {
    "Name": "Alas",
    "Url": "https://alas.aws.amazon.com/ALAS-2020-1337.html",
    "VendorCreatedAt": "2020-01-16T00:01:43Z",
    "VendorSeverity": "Medium",
    "VendorUpdatedAt": "2020-01-16T00:01:43Z"
},
"VulnerablePackages": [
    {
        "Architecture": "x86_64",
        "Epoch": "1",
        "FilePath": "/tmp",
        "FixedInVersion": "0.14.0",
        "Name": "openssl",
        "PackageManager": "OS",
        "Release": "16.amzn2.0.3",
        "Remediation": "Update aws-crt to 0.14.0",
        "SourceLayerArn": "arn:aws:lambda:us-west-2:123456789012:layer:id",
        "SourceLayerHash":
            "sha256:c1962c35b63a6ff6ce7df6e042ee82371a605ca9515569edec46ff14f926f001",
        "Version": "1.0.2k"
    }
]
}

```

]

Alur kerja

[Workflow](#) Objek memberikan informasi tentang status investigasi terhadap suatu temuan.

Bidang ini ditujukan bagi pelanggan untuk digunakan dengan alat remediasi, orkestrasi, dan tiket. Ini tidak dimaksudkan untuk menemukan penyedia.

Anda hanya dapat memperbarui Workflow bidang dengan [BatchUpdateFindings](#). Pelanggan juga dapat memperbaruinya dari konsol. Lihat [the section called “Mengatur status alur kerja temuan”](#).

Contoh

```
"Workflow": {  
  "Status": "NEW"  
}
```

WorkflowState (Pensiun)

Objek ini sudah pensiun dan telah digantikan oleh Status bidang Workflow objek.

Bidang ini menyediakan status alur kerja temuan. Temuan produk dapat memberikan nilai NEW untuk bidang ini. Produk temuan dapat memberikan nilai untuk bidang ini jika ada analog yang berarti dalam sistem produk temuan.

Contoh

```
"WorkflowState": "NEW"
```

ResourcesObjek ASFF

Dalam AWS Security Finding Format (ASFF), Resources objek memberikan informasi tentang sumber daya yang terlibat dalam temuan. Ini berisi array hingga 32 objek sumber daya. Untuk menentukan bagaimana nama sumber daya diformat, lihat [AWS Format Pencarian Keamanan \(ASFF\)](#). Untuk contoh setiap objek sumber daya, pilih sumber daya dari daftar berikut.

Topik

- [Atribut sumber daya di ASFF](#)
- [AwsAmazonMQsumber daya di ASFF](#)

- [AwsApiGatewaysumber daya di ASFF](#)
- [AwsAppSyncsumber daya di ASFF](#)
- [AwsAthenasumber daya di ASFF](#)
- [AwsAutoScalingsumber daya di ASFF](#)
- [AwsBackupsummary sumber daya di ASFF](#)
- [AwsCertificateManagersumber daya di ASFF](#)
- [AwsCloudFormationsumber daya di ASFF](#)
- [AwsCloudFrontsumber daya di ASFF](#)
- [AwsCloudTrailsummary sumber daya di ASFF](#)
- [AwsCloudWatchsummary sumber daya di ASFF](#)
- [AwsCodeBuildsummary sumber daya di ASFF](#)
- [AwsDmssummary sumber daya di ASFF](#)
- [AwsDynamoDBsummary sumber daya di ASFF](#)
- [AwsEc2summary sumber daya di ASFF](#)
- [AwsEcrsummary sumber daya di ASFF](#)
- [AwsEcssummary sumber daya di ASFF](#)
- [AwsEfssummary sumber daya di ASFF](#)
- [AwsEkssumber daya di ASFF](#)
- [AwsElasticBeanstalksummary sumber daya di ASFF](#)
- [AwsElasticSearchsummary sumber daya di ASFF](#)
- [AwsElbsumber daya di ASFF](#)
- [AwsEventBridgesumber daya di ASFF](#)
- [AwsGuardDutysumber daya di ASFF](#)
- [AwsIamsumber daya di ASFF](#)
- [AwsKinesissummary sumber daya di ASFF](#)
- [AwsKmssummary sumber daya di ASFF](#)
- [AwsLambda](#)
- [AwsMsksummary sumber daya di ASFF](#)
- [AwsNetworkFirewallsummary sumber daya di ASFF](#)
- [AwsOpenSearchServicesumber daya di ASFF](#)

- [AwsRdsSumber daya di ASFF](#)
- [AwsRedshiftsumber daya di ASFF](#)
- [AwsRoute53sumber daya di ASFF](#)
- [AwsS3sumber daya di ASFF](#)
- [AwsSageMakersumber daya di ASFF](#)
- [AwsSecretsManagersumber daya di ASFF](#)
- [AwsSnssumber daya di ASFF](#)
- [AwsSqssumber daya di ASFF](#)
- [AwsSmsumber daya di ASFF](#)
- [AwsStepFunctionssumber daya di ASFF](#)
- [AwsWafsumber daya di ASFF](#)
- [AwsXraysumber daya di ASFF](#)
- [ContainerObjek ASFF](#)
- [OtherObjek ASFF](#)

Atribut sumber daya di ASFF

Berikut adalah deskripsi dan contoh untuk Resources objek dalam AWS Security Finding Format (ASFF). Untuk informasi lebih lanjut tentang bidang ini, lihat [Sumber daya](#).

ApplicationArn

Mengidentifikasi Nama Sumber Daya Amazon (ARN) dari aplikasi yang terlibat dalam temuan.

Contoh

```
"ApplicationArn": "arn:aws:resource-groups:us-west-2:123456789012:group/SampleApp/1234567890abcdef0"
```

ApplicationName

Mengidentifikasi nama aplikasi yang terlibat dalam temuan.

Contoh

```
"ApplicationName": "SampleApp"
```

DataClassification

[DataClassification](#) Bidang ini memberikan informasi tentang data sensitif yang terdeteksi pada sumber daya.

Contoh

```
"DataClassification": {
  "DetailedResultsLocation": "Path_to_Folder_Or_File",
  "Result": {
    "MimeType": "text/plain",
    "SizeClassified": 2966026,
    "AdditionalOccurrences": false,
    "Status": {
      "Code": "COMPLETE",
      "Reason": "Unsupportedfield"
    },
  },
  "SensitiveData": [
    {
      "Category": "PERSONAL_INFORMATION",
      "Detections": [
        {
          "Count": 34,
          "Type": "GE_PERSONAL_ID",
          "Occurrences": {
            "LineRanges": [
              {
                "Start": 1,
                "End": 10,
                "StartColumn": 20
              }
            ],
            "Pages": [],
            "Records": [],
            "Cells": []
          }
        }
      ],
    },
    {
      "Count": 59,
      "Type": "EMAIL_ADDRESS",
      "Occurrences": {
        "Pages": [
          {
            "PageNumber": 1,
```

```

        "OffsetRange": {
            "Start": 1,
            "End": 100,
            "StartColumn": 10
        },
        "LineRange": {
            "Start": 1,
            "End": 100,
            "StartColumn": 10
        }
    }
}
},
{
    "Count": 2229,
    "Type": "URL",
    "Occurrences": {
        "LineRanges": [
            {
                "Start": 1,
                "End": 13
            }
        ]
    }
},
{
    "Count": 13826,
    "Type": "NameDetection",
    "Occurrences": {
        "Records": [
            {
                "RecordIndex": 1,
                "JsonPath": "$.ssn.value"
            }
        ]
    }
},
{
    "Count": 32,
    "Type": "AddressDetection"
}
],
"TotalCount": 32

```

```

    }
  ],
  "CustomDataIdentifiers": {
    "Detections": [
      {
        "Arn": "1712be25e7c7f53c731fe464f1c869b8",
        "Name": "1712be25e7c7f53c731fe464f1c869b8",
        "Count": 2,
      }
    ],
    "TotalCount": 2
  }
}

```

Detail

[Details](#) Bidang ini memberikan informasi tambahan tentang sumber daya tunggal menggunakan objek yang sesuai. Setiap sumber daya harus disediakan dalam objek sumber daya terpisah di Resources objek.

Perhatikan bahwa jika ukuran temuan melebihi maksimum 240 KB, maka Details objek dihapus dari temuan. Untuk temuan kontrol yang menggunakan AWS Config aturan, Anda dapat melihat detail sumber daya di AWS Config konsol.

Security Hub menyediakan serangkaian detail sumber daya yang tersedia untuk jenis sumber daya yang didukung. Detail ini sesuai dengan nilai Type objek. Gunakan jenis yang disediakan bila memungkinkan.

Misalnya, jika sumber daya adalah bucket S3, maka atur sumber daya Type ke `AwsS3Bucket` dan berikan detail sumber daya di [AwsS3Bucket](#) objek.

[Other](#) Objek memungkinkan Anda untuk memberikan bidang dan nilai khusus. Anda menggunakan Other objek dalam kasus berikut:

- Jenis sumber daya (nilai sumber dayaType) tidak memiliki objek detail yang sesuai. Untuk memberikan detail untuk sumber daya, Anda menggunakan [Other](#) objek.
- Objek untuk jenis sumber daya tidak menyertakan semua bidang yang ingin Anda isi. Dalam hal ini, gunakan objek detail untuk jenis sumber daya untuk mengisi bidang yang tersedia. Gunakan Other objek untuk mengisi bidang yang tidak ada di objek khusus tipe.

- Jenis sumber daya bukan salah satu jenis yang disediakan. Dalam hal ini, atur `Resource.Type` ke `Other`, dan gunakan `Other` objek untuk mengisi detail.

Contoh

```
"Details": {
  "AwsEc2Instance": {
    "IamInstanceProfileArn": "arn:aws:iam::123456789012:role/IamInstanceProfileArn",
    "ImageId": "ami-79fd7eee",
    "IPv4Addresses": ["1.1.1.1"],
    "IPv6Addresses": ["2001:db8:1234:1a2b::123"],
    "KeyName": "testkey",
    "LaunchedAt": "2018-09-29T01:25:54Z",
    "MetadataOptions": {
      "HttpEndpoint": "enabled",
      "HttpProtocolIpv6": "enabled",
      "HttpPutResponseHopLimit": 1,
      "HttpTokens": "optional",
      "InstanceMetadataTags": "disabled"
    },
    "NetworkInterfaces": [
      {
        "NetworkInterfaceId": "eni-e5aa89a3"
      }
    ],
    "SubnetId": "PublicSubnet",
    "Type": "i3.xlarge",
    "VirtualizationType": "hvm",
    "VpcId": "TestVPCIPv6"
  },
  "AwsS3Bucket": {
    "OwnerId": "da4d66eac431652a4d44d490a00500bde52c97d235b7b4752f9f688566fe6de",
    "OwnerName": "acmes3bucketowner"
  },
  "Other": { "LightPen": "blinky", "SerialNo": "1234abcd" }
}
```

Id

Pengidentifikasi untuk jenis sumber daya yang diberikan.

Untuk AWS sumber daya yang diidentifikasi oleh Amazon Resource Names (ARNs), ini adalah ARN.

Untuk AWS sumber daya yang kurang ARNs, ini adalah pengidentifikasi seperti yang didefinisikan oleh AWS layanan yang menciptakan sumber daya.

Untuk AWS non-sumber daya, ini adalah pengidentifikasi unik yang terkait dengan sumber daya.

Contoh

```
"Id": "arn:aws:s3:::amzn-s3-demo-bucket"
```

Partition

Partisi tempat sumber daya berada. Partisi adalah sekelompok Wilayah AWS. Masing-masing Akun AWS dicakup ke satu partisi.

Partisi berikut didukung:

- `aws` – Wilayah AWS
- `aws-cn`— Wilayah Tiongkok
- `aws-us-gov` – AWS GovCloud (US) Region

Contoh

```
"Partition": "aws"
```

Wilayah

Kode untuk Wilayah AWS tempat sumber daya ini berada. Untuk daftar kode Wilayah, lihat [Titik akhir Regional](#).

Contoh

```
"Region": "us-west-2"
```

ResourceRole

Mengidentifikasi peran sumber daya dalam temuan. Sumber daya adalah target aktivitas pencarian atau aktor yang melakukan aktivitas tersebut.

Contoh

```
"ResourceRole": "target"
```

Tanda

Bidang ini menyediakan kunci tag dan informasi nilai untuk sumber daya yang terlibat dalam temuan. Anda dapat menandai [sumber daya yang didukung](#) oleh GetResources pengoperasian API AWS Resource Groups Tagging. Security Hub memanggil operasi ini melalui [peran terkait layanan](#) dan mengambil tag sumber daya jika Resource.Id bidang AWS Security Finding Format (ASFF) diisi dengan ARN sumber daya. AWS Sumber daya yang tidak valid diabaikan IDs .

Anda dapat menambahkan tag sumber daya ke temuan yang dicerna Security Hub, termasuk temuan dari produk terintegrasi Layanan AWS dan pihak ketiga.

Menambahkan tag memberi tahu Anda tag yang dikaitkan dengan sumber daya pada saat temuan diproses. Anda dapat menyertakan Tags atribut hanya untuk sumber daya yang memiliki tag terkait. Jika sumber daya tidak memiliki tag terkait, jangan sertakan Tags atribut dalam temuan.

Dimasukkannya tag sumber daya dalam temuan menghilangkan kebutuhan untuk membangun jaringan pengayaan data atau secara manual memperkaya metadata temuan keamanan. Anda juga dapat menggunakan tag untuk mencari atau memfilter temuan dan wawasan dan membuat [aturan otomatisasi](#).

Untuk informasi tentang pembatasan yang berlaku untuk tag, lihat [Batas dan persyaratan penamaan tag](#).

Anda hanya dapat memberikan tag yang ada pada AWS sumber daya di bidang ini. Untuk menyediakan data yang tidak ditentukan dalam Format Pencarian AWS Keamanan, gunakan subbidang Other detail.

Contoh

```
"Tags": {  
  "billingCode": "Lotus-1-2-3",  
  "needsPatching": "true"  
}
```

Tipe

Jenis sumber daya yang Anda berikan detailnya.

Bila memungkinkan, gunakan salah satu jenis sumber daya yang disediakan, seperti `AwsEc2Instance` atau `AwsS3Bucket`.

Jika jenis sumber daya tidak cocok dengan salah satu jenis sumber daya yang disediakan, setelah sumber daya `Type` ke `Other`, dan gunakan subbidang `Other` detail untuk mengisi detailnya.

Nilai yang didukung tercantum di bawah [Sumber Daya](#).

Contoh

```
"Type": "AwsS3Bucket"
```

AwsAmazonMQ sumber daya di ASFF

Berikut ini adalah contoh sintaks AWS Security Finding Format (ASFF) untuk `AwsAmazonMQ` sumber daya.

AWS Security Hub menormalkan temuan dari berbagai sumber menjadi ASFF. Untuk informasi latar belakang tentang ASFF, lihat [AWS Format Pencarian Keamanan \(ASFF\)](#).

AwsAmazonMQBroker

`AwsAmazonMQBroker` memberikan informasi tentang broker Amazon MQ, yang merupakan lingkungan broker pesan yang berjalan di Amazon MQ.

Contoh berikut menunjukkan ASFF untuk `AwsAmazonMQBroker` objek. Untuk melihat deskripsi `AwsAmazonMQBroker` atribut, lihat [AwsAmazonMQBroker](#) di Referensi AWS Security Hub API.

Contoh

```
"AwsAmazonMQBroker": {
  "AutoMinorVersionUpgrade": true,
  "BrokerArn": "arn:aws:mq:us-east-1:123456789012:broker:TestBroker:b-
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "BrokerId": "b-a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "BrokerName": "TestBroker",
  "Configuration": {
    "Id": "c-a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
    "Revision": 1
  },
}
```

```

    "DeploymentMode": "ACTIVE_STANDBY_MULTI_AZ",
    "EncryptionOptions": {
        "UseAwsOwnedKey": true
    },
    "EngineType": "ActiveMQ",
    "EngineVersion": "5.17.2",
    "HostInstanceType": "mq.t2.micro",
    "Logs": {
        "Audit": false,
        "AuditLogGroup": "/aws/amazonmq/broker/b-a1b2c3d4-5678-90ab-cdef-EXAMPLE11111/audit",
        "General": false,
        "GeneralLogGroup": "/aws/amazonmq/broker/b-a1b2c3d4-5678-90ab-cdef-EXAMPLE11111/general"
    },
    "MaintenanceWindowStartTime": {
        "DayOfWeek": "MONDAY",
        "TimeOfDay": "22:00",
        "TimeZone": "UTC"
    },
    "PubliclyAccessible": true,
    "SecurityGroups": [
        "sg-021345abcdef6789"
    ],
    "StorageType": "efs",
    "SubnetIds": [
        "subnet-1234567890abcdef0",
        "subnet-abcdef01234567890"
    ],
    "Users": [
        {
            "Username": "admin"
        }
    ]
}

```

AwsApiGatewaysumber daya di ASFF

Berikut ini adalah contoh sintaks AWS Security Finding Format (ASFF) untuk AwsApiGateway sumber daya.

AWS Security Hub menormalkan temuan dari berbagai sumber menjadi ASFF. Untuk informasi latar belakang tentang ASFF, lihat [AWS Format Pencarian Keamanan \(ASFF\)](#).

AwsApiGatewayRestApi

AwsApiGatewayRestApiObjek berisi informasi tentang REST API di Amazon API Gateway versi 1.

Berikut ini adalah contoh AwsApiGatewayRestApi temuan dalam AWS Security Finding Format (ASFF). Untuk melihat deskripsi AwsApiGatewayRestApi atribut, lihat [AwsApiGatewayRestApiDetails](#) di Referensi AWS Security Hub API.

Contoh

```
AwsApiGatewayRestApi: {
  "Id": "exampleapi",
  "Name": "Security Hub",
  "Description": "AWS Security Hub",
  "CreateDate": "2018-11-18T10:20:05-08:00",
  "Version": "2018-10-26",
  "BinaryMediaTypes" : ["-*~1*"],
  "MinimumCompressionSize": 1024,
  "ApiKeySource": "AWS_ACCOUNT_ID",
  "EndpointConfiguration": {
    "Types": [
      "REGIONAL"
    ]
  }
}
```

AwsApiGatewayStage

AwsApiGatewayStageObjek menyediakan informasi tentang tahap Amazon API Gateway versi 1.

Berikut ini adalah contoh AwsApiGatewayStage temuan dalam AWS Security Finding Format (ASFF). Untuk melihat deskripsi AwsApiGatewayStage atribut, lihat [AwsApiGatewayStageDetails](#) di Referensi AWS Security Hub API.

Contoh

```
"AwsApiGatewayStage": {
  "DeploymentId": "n7hlmf",
  "ClientCertificateId": "a1b2c3",
  "StageName": "Prod",
  "Description" : "Stage Description",
  "CacheClusterEnabled": false,
  "CacheClusterSize" : "1.6",
```

```

"CacheClusterStatus": "NOT_AVAILABLE",
"MethodSettings": [
  {
    "MetricsEnabled": true,
    "LoggingLevel": "INFO",
    "DataTraceEnabled": false,
    "ThrottlingBurstLimit": 100,
    "ThrottlingRateLimit": 5.0,
    "CachingEnabled": false,
    "CacheTtlInSeconds": 300,
    "CacheDataEncrypted": false,
    "RequireAuthorizationForCacheControl": true,
    "UnauthorizedCacheControlHeaderStrategy": "SUCCEED_WITH_RESPONSE_HEADER",
    "HttpMethod": "POST",
    "ResourcePath": "/echo"
  }
],
"Variables": {"test": "value"},
"DocumentationVersion": "2.0",
"AccessLogSettings": {
  "Format": "{\"requestId\": \"${context.requestId}\", \"extendedRequestId\": \"${context.extendedRequestId}\", \"ownerAccountId\": \"${context.accountId}\", \"requestAccountId\": \"${context.identity.accountId}\", \"callerPrincipal\": \"${context.identity.caller}\", \"httpMethod\": \"${context.httpMethod}\", \"resourcePath\": \"${context.resourcePath}\", \"status\": \"${context.status}\", \"requestTime\": \"${context.requestTime}\", \"responseLatencyMs\": \"${context.responseLatency}\", \"errorMessage\": \"${context.error.message}\", \"errorResponseType\": \"${context.error.responseType}\", \"apiId\": \"${context.apiId}\", \"awsEndpointRequestId\": \"${context.awsEndpointRequestId}\", \"domainName\": \"${context.domainName}\", \"stage\": \"${context.stage}\", \"xrayTraceId\": \"${context.xrayTraceId}\", \"sourceIp\": \"${context.identity.sourceIp}\", \"user\": \"${context.identity.user}\", \"userAgent\": \"${context.identity.userAgent}\", \"userArn\": \"${context.identity.userArn}\", \"integrationLatency\": \"${context.integrationLatency}\", \"integrationStatus\": \"${context.integrationStatus}\", \"authorizerIntegrationLatency\": \"${context.authorizer.integrationLatency}\" }",
  "DestinationArn": "arn:aws:logs:us-west-2:111122223333:log-group:SecurityHubAPIAccessLog/Prod"
},
"CanarySettings": {
  "PercentTraffic": 0.0,
  "DeploymentId": "ul73s8",
  "StageVariableOverrides" : [
    "String" : "String"
  ]
},

```

```

    "UseStageCache": false
  },
  "TracingEnabled": false,
  "CreateDate": "2018-07-11T10:55:18-07:00",
  "LastUpdatedDate": "2020-08-26T11:51:04-07:00",
  "WebAclArn" : "arn:aws:waf-regional:us-west-2:111122223333:webacl/cb606bd8-5b0b-4f0b-830a-dd304e48a822"
}

```

AwsApiGatewayV2Api

AwsApiGatewayV2ApiObjek berisi informasi tentang API versi 2 di Amazon API Gateway.

Berikut ini adalah contoh AwsApiGatewayV2Api temuan dalam AWS Security Finding Format (ASFF). Untuk melihat deskripsi AwsApiGatewayV2Api atribut, lihat [AwsApiGatewayV2 ApiDetails](#) di Referensi AWS Security Hub API.

Contoh

```

"AwsApiGatewayV2Api": {
  "ApiEndpoint": "https://example.us-west-2.amazonaws.com",
  "ApiId": "a1b2c3d4",
  "ApiKeySelectionExpression": "$request.header.x-api-key",
  "CreateDate": "2020-03-28T00:32:37Z",
  "Description": "ApiGatewayV2 Api",
  "Version": "string",
  "Name": "my-api",
  "ProtocolType": "HTTP",
  "RouteSelectionExpression": "$request.method $request.path",
  "CorsConfiguration": {
    "AllowOrigins": [ "*" ],
    "AllowCredentials": true,
    "ExposeHeaders": [ "string" ],
    "MaxAge": 3000,
    "AllowMethods": [
      "GET",
      "PUT",
      "POST",
      "DELETE",
      "HEAD"
    ],
    "AllowHeaders": [ "*" ]
  }
}

```

}

AwsApiGatewayV2Panggung

AwsApiGatewayV2Stage berisi informasi tentang tahap versi 2 untuk Amazon API Gateway.

Berikut ini adalah contoh AwsApiGatewayV2Stage temuan dalam AWS Security Finding Format (ASFF). Untuk melihat deskripsi AwsApiGatewayV2Stage atribut, lihat [AwsApiGatewayV2StageDetails](#) di Referensi AWS Security Hub API.

Contoh

```
"AwsApiGatewayV2Stage": {
  "CreateDate": "2020-04-08T00:36:05Z",
  "Description" : "ApiGatewayV2",
  "DefaultRouteSettings": {
    "DetailedMetricsEnabled": false,
    "LoggingLevel": "INFO",
    "DataTraceEnabled": true,
    "ThrottlingBurstLimit": 100,
    "ThrottlingRateLimit": 50
  },
  "DeploymentId": "x1zwyv",
  "LastUpdatedDate": "2020-04-08T00:36:13Z",
  "RouteSettings": {
    "DetailedMetricsEnabled": false,
    "LoggingLevel": "INFO",
    "DataTraceEnabled": true,
    "ThrottlingBurstLimit": 100,
    "ThrottlingRateLimit": 50
  },
  "StageName": "prod",
  "StageVariables": [
    "function": "my-prod-function"
  ],
  "AccessLogSettings": {
    "Format": "{\"requestId\": \"${context.requestId}\", \"extendedRequestId\": \"${context.extendedRequestId}\", \"ownerAccountId\": \"${context.accountId}\", \"requestAccountId\": \"${context.identity.accountId}\", \"callerPrincipal\": \"${context.identity.caller}\", \"httpMethod\": \"${context.httpMethod}\", \"resourcePath\": \"${context.resourcePath}\", \"status\": \"${context.status}\", \"requestTime\": \"${context.requestTime}\", \"responseLatencyMs\": \"${context.responseLatency}\", \"errorMessage\": \"${context.error.message}\", \"errorResponseType\": \"
```



```

    \"$context.error.responseType\", \"$apiId\": \"$context.apiId\", \"$awsEndpointRequestId
\": \"$context.awsEndpointRequestId\", \"$domainName\": \"$context.domainName\", \"$stage
\": \"$context.stage\", \"$xrayTraceId\": \"$context.xrayTraceId\", \"$sourceIp\":
 \"$context.identity.sourceIp\", \"$user\": \"$context.identity.user\", \"$userAgent
\": \"$context.identity.userAgent\", \"$userArn\": \"$context.identity.userArn\",
 \"$integrationLatency\": \"$context.integrationLatency\", \"$integrationStatus
\": \"$context.integrationStatus\", \"$authorizerIntegrationLatency\":
 \"$context.authorizer.integrationLatency\" }\",
    \"DestinationArn\": \"arn:aws:logs:us-west-2:111122223333:log-
group:SecurityHubAPIAccessLog/Prod\"
  },
  \"AutoDeploy\": false,
  \"LastDeploymentStatusMessage\": \"Message\",
  \"ApiGatewayManaged\": true,
}

```

AwsAppSyncsumber daya di ASFF

Berikut ini adalah contoh sintaks AWS Security Finding Format (ASFF) untuk AwsAppSync sumber daya.

AWS Security Hub menormalkan temuan dari berbagai sumber menjadi ASFF. Untuk informasi latar belakang tentang ASFF, lihat [AWS Format Pencarian Keamanan \(ASFF\)](#).

AwsAppSyncGraphQLApi

AwsAppSyncGraphQLApi menyediakan informasi tentang AWS AppSync GraphQL API, yang merupakan konstruksi tingkat atas untuk aplikasi Anda.

Contoh berikut menunjukkan ASFF untuk AwsAppSyncGraphQLApi objek. Untuk melihat deskripsi AwsAppSyncGraphQLApi atribut, lihat [AwsAppSyncGraphQLApi](#) di Referensi AWS Security Hub API.

Contoh

```

"AwsAppSyncGraphQLApi": {
  "AdditionalAuthenticationProviders": [
    {
      "AuthenticationType": "AWS_LAMBDA",
      "LambdaAuthorizerConfig": {
        "AuthorizerResultTtlInSeconds": 300,
        "AuthorizerUri": "arn:aws:lambda:us-east-1:123456789012:function:mylambdafunc"
      }
    }
  ]
}

```

```

    },
    {
      "AuthenticationType": "AWS_IAM"
    }
  ],
  "ApiId": "021345abcdef6789",
  "Arn": "arn:aws:appsync:eu-central-1:123456789012:apis/021345abcdef6789",
  "AuthenticationType": "API_KEY",
  "Id": "021345abcdef6789",
  "LogConfig": {
    "CloudWatchLogsRoleArn": "arn:aws:iam::123456789012:role/service-role/appsync-graphqlapi-logs-eu-central-1",
    "ExcludeVerboseContent": true,
    "FieldLogLevel": "ALL"
  },
  "Name": "My AppSync App",
  "XrayEnabled": true,
}

```

AwsAthenasumber daya di ASFF

Berikut ini adalah contoh sintaks AWS Security Finding Format (ASFF) untuk AwsAthena sumber daya.

AWS Security Hub menormalkan temuan dari berbagai sumber menjadi ASFF. Untuk informasi latar belakang tentang ASFF, lihat [AWS Format Pencarian Keamanan \(ASFF\)](#).

AwsAthenaWorkGroup

AwsAthenaWorkGroup memberikan informasi tentang workgroup Amazon Athena. Workgroup membantu Anda memisahkan pengguna, tim, aplikasi, atau beban kerja. Ini juga membantu Anda menetapkan batasan pada pemrosesan data dan melacak biaya.

Contoh berikut menunjukkan ASFF untuk AwsAthenaWorkGroup objek. Untuk melihat deskripsi AwsAthenaWorkGroup atribut, lihat [AwsAthenaWorkGroup](#) di Referensi AWS Security Hub API.

Contoh

```

"AwsAthenaWorkGroup": {
  "Description": "My workgroup for prod workloads",
  "Name": "MyWorkgroup",
  "WorkgroupConfiguration" {
    "ResultConfiguration": {

```

```

      "EncryptionConfiguration": {
        "EncryptionOption": "SSE_KMS",
        "KmsKey": "arn:aws:kms:us-east-1:123456789012:key/a1b2c3d4-5678-90ab-
cdef-EXAMPLE11111"
      }
    },
    "State": "ENABLED"
  }
}

```

AwsAutoScaling sumber daya di ASFF

Berikut ini adalah contoh sintaks AWS Security Finding Format (ASFF) untuk `AwsAutoScaling` sumber daya.

AWS Security Hub menormalkan temuan dari berbagai sumber menjadi ASFF. Untuk informasi latar belakang tentang ASFF, lihat [AWS Format Pencarian Keamanan \(ASFF\)](#).

`AwsAutoScalingAutoScalingGroup`

`AwsAutoScalingAutoScalingGroup` objek memberikan rincian tentang grup penskalaan otomatis.

Berikut ini adalah contoh `AwsAutoScalingAutoScalingGroup` temuan dalam AWS Security Finding Format (ASFF). Untuk melihat deskripsi `AwsAutoScalingAutoScalingGroup` atribut, lihat [AwsAutoScalingAutoScalingGroupDetails](#) di Referensi AWS Security Hub API.

Contoh

```

"AwsAutoScalingAutoScalingGroup": {
  "CreatedTime": "2017-10-17T14:47:11Z",
  "HealthCheckGracePeriod": 300,
  "HealthCheckType": "EC2",
  "LaunchConfigurationName": "mylaunchconf",
  "LoadBalancerNames": [],
  "LaunchTemplate": {
    "LaunchTemplateId": "string",
    "LaunchTemplateName": "string",
    "Version": "string"
  },
  "MixedInstancesPolicy": {
    "InstancesDistribution": {

```

```

        "OnDemandAllocationStrategy": "prioritized",
        "OnDemandBaseCapacity": number,
        "OnDemandPercentageAboveBaseCapacity": number,
        "SpotAllocationStrategy": "lowest-price",
        "SpotInstancePools": number,
        "SpotMaxPrice": "string"
    },
    "LaunchTemplate": {
        "LaunchTemplateSpecification": {
            "LaunchTemplateId": "string",
            "LaunchTemplateName": "string",
            "Version": "string"
        },
        "CapacityRebalance": true,
        "Overrides": [
            {
                "InstanceType": "string",
                "WeightedCapacity": "string"
            }
        ]
    }
}
}
}
}
}

```

AwsAutoScalingLaunchConfiguration

`AwsAutoScalingLaunchConfiguration` Objek memberikan rincian tentang konfigurasi peluncuran.

Berikut ini adalah contoh `AwsAutoScalingLaunchConfiguration` temuan dalam AWS Security Finding Format (ASFF).

Untuk melihat deskripsi `AwsAutoScalingLaunchConfiguration` atribut, lihat [AwsAutoScalingLaunchConfigurationDetails](#) di Referensi AWS Security Hub API.

Contoh

```

AwsAutoScalingLaunchConfiguration: {
    "LaunchConfigurationName": "newtest",
    "ImageId": "ami-058a3739b02263842",
    "KeyName": "55hundredinstance",
    "SecurityGroups": [ "sg-01fce87ad6e019725" ],

```

```

"ClassicLinkVpcSecurityGroups": [],
"UserData": "...Base64-Encoded user data..."
"InstanceType": "a1.metal",
"KernelId": "",
"RamdiskId": "ari-a51cf9cc",
"BlockDeviceMappings": [
  {
    "DeviceName": "/dev/sdh",
    "Ebs": {
      "VolumeSize": 30,
      "VolumeType": "gp2",
      "DeleteOnTermination": false,
      "Encrypted": true,
      "SnapshotId": "snap-ffaa1e69",
      "VirtualName": "ephemeral1"
    }
  },
  {
    "DeviceName": "/dev/sdb",
    "NoDevice": true
  },
  {
    "DeviceName": "/dev/sda1",
    "Ebs": {
      "SnapshotId": "snap-02420cd3d2dea1bc0",
      "VolumeSize": 8,
      "VolumeType": "gp2",
      "DeleteOnTermination": true,
      "Encrypted": false
    }
  },
  {
    "DeviceName": "/dev/sdi",
    "Ebs": {
      "VolumeSize": 20,
      "VolumeType": "gp2",
      "DeleteOnTermination": false,
      "Encrypted": true
    }
  },
  {
    "DeviceName": "/dev/sdc",
    "NoDevice": true
  }
]

```

```

    ],
    "InstanceMonitoring": {
        "Enabled": false
    },
    "CreatedTime": 1620842933453,
    "EbsOptimized": false,
    "AssociatePublicIpAddress": true,
    "SpotPrice": "0.045"
}

```

AwsBackup sumber daya di ASFF

Berikut ini adalah contoh sintaks AWS Security Finding Format (ASFF) untuk AwsBackup sumber daya.

AWS Security Hub menormalkan temuan dari berbagai sumber menjadi ASFF. Untuk informasi latar belakang tentang ASFF, lihat [AWS Format Pencarian Keamanan \(ASFF\)](#).

AwsBackupBackupPlan

AwsBackupBackupPlanObjek memberikan informasi tentang rencana AWS Backup cadangan. Rencana AWS Backup cadangan adalah ekspresi kebijakan yang menentukan kapan dan bagaimana Anda ingin mencadangkan AWS sumber daya Anda.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk AwsBackupBackupPlan objek. Untuk melihat deskripsi AwsBackupBackupPlan atribut, lihat [AwsBackupBackupPlan](#) di Referensi AWS Security Hub API.

Contoh

```

"AwsBackupBackupPlan": {
  "BackupPlan": {
    "AdvancedBackupSettings": [{
      "BackupOptions": {
        "WindowsVSS": "enabled"
      },
      "ResourceType": "EC2"
    }],
    "BackupPlanName": "test",
    "BackupPlanRule": [{
      "CompletionWindowMinutes": 10080,
      "CopyActions": [{

```

```

    "DestinationBackupVaultArn": "arn:aws:backup:us-east-1:858726136373:backup-
vault:aws/efs/automatic-backup-vault",
    "Lifecycle": {
      "DeleteAfterDays": 365,
      "MoveToColdStorageAfterDays": 30
    }
  ]],
  "Lifecycle": {
    "DeleteAfterDays": 35
  },
  "RuleName": "DailyBackups",
  "ScheduleExpression": "cron(0 5 ? * * *)",
  "StartWindowMinutes": 480,
  "TargetBackupVault": "Default"
},
{
  "CompletionWindowMinutes": 10080,
  "CopyActions": [{
    "DestinationBackupVaultArn": "arn:aws:backup:us-east-1:858726136373:backup-
vault:aws/efs/automatic-backup-vault",
    "Lifecycle": {
      "DeleteAfterDays": 365,
      "MoveToColdStorageAfterDays": 30
    }
  ]],
  "Lifecycle": {
    "DeleteAfterDays": 35
  },
  "RuleName": "Monthly",
  "ScheduleExpression": "cron(0 5 1 * ? *)",
  "StartWindowMinutes": 480,
  "TargetBackupVault": "Default"
}]
},
"BackupPlanArn": "arn:aws:backup:us-east-1:858726136373:backup-
plan:b6d6b896-590d-4ee1-bf29-c5ccae63f4e7",
"BackupPlanId": "b6d6b896-590d-4ee1-bf29-c5ccae63f4e7",
"VersionId": "ZDVjNDIzMjItYTZiNS00NzczLTg4YzctNmExMWM2NjZhY2E1"
}

```

AwsBackupBackupVault

AwsBackupBackupVaultObjek memberikan informasi tentang brankas AWS Backup cadangan. Brankas AWS Backup cadangan adalah wadah yang menyimpan dan mengatur cadangan Anda.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk AwsBackupBackupVault objek. Untuk melihat deskripsi AwsBackupBackupVault atribut, lihat [AwsBackupBackupVault](#) di Referensi AWS Security Hub API.

Contoh

```
"AwsBackupBackupVault": {
  "AccessPolicy": {
    "Statement": [{
      "Action": [
        "backup:DeleteBackupVault",
        "backup:DeleteBackupVaultAccessPolicy",
        "backup:DeleteRecoveryPoint",
        "backup:StartCopyJob",
        "backup:StartRestoreJob",
        "backup:UpdateRecoveryPointLifecycle"
      ],
      "Effect": "Deny",
      "Principal": {
        "AWS": "*"
      },
      "Resource": "*"
    }],
    "Version": "2012-10-17"
  },
  "BackupVaultArn": "arn:aws:backup:us-east-1:123456789012:backup-vault:aws/efs/automatic-backup-vault",
  "BackupVaultName": "aws/efs/automatic-backup-vault",
  "EncryptionKeyArn": "arn:aws:kms:us-east-1:444455556666:key/72ba68d4-5e43-40b0-ba38-838bf8d06ca0",
  "Notifications": {
    "BackupVaultEvents": ["BACKUP_JOB_STARTED", "BACKUP_JOB_COMPLETED", "COPY_JOB_STARTED"],
    "SNSTopicArn": "arn:aws:sns:us-west-2:111122223333:MyVaultTopic"
  }
}
```


AwsBackupRecoveryPoint

AwsBackupRecoveryPointObjek memberikan informasi tentang AWS Backup cadangan, juga disebut sebagai titik pemulihan. Titik AWS Backup pemulihan mewakili konten sumber daya pada waktu tertentu.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk AwsBackupRecoveryPoint objek. Untuk melihat deskripsi AwsBackupBackupVault atribut, lihat [AwsBackupRecoveryPoint](#) di Referensi AWS Security Hub API.

Contoh

```
"AwsBackupRecoveryPoint": {
  "BackupSizeInBytes": 0,
  "BackupVaultName": "aws/efs/automatic-backup-vault",
  "BackupVaultArn": "arn:aws:backup:us-east-1:111122223333:backup-vault:aws/efs/automatic-backup-vault",
  "CalculatedLifecycle": {
    "DeleteAt": "2021-08-30T06:51:58.271Z",
    "MoveToColdStorageAt": "2020-08-10T06:51:58.271Z"
  },
  "CompletionDate": "2021-07-26T07:21:40.361Z",
  "CreatedBy": {
    "BackupPlanArn": "arn:aws:backup:us-east-1:111122223333:backup-plan:aws/efs/73d922fb-9312-3a70-99c3-e69367f9fdad",
    "BackupPlanId": "aws/efs/73d922fb-9312-3a70-99c3-e69367f9fdad",
    "BackupPlanVersion": "ZGM4YzY5YjktMWYxNC00ZTBmLWE5MjYtZmU5OWNiZmM5ZjIz",
    "BackupRuleId": "2a600c2-42ad-4196-808e-084923ebfd25"
  },
  "CreationDate": "2021-07-26T06:51:58.271Z",
  "EncryptionKeyArn": "arn:aws:kms:us-east-1:111122223333:key/72ba68d4-5e43-40b0-ba38-838bf8d06ca0",
  "IamRoleArn": "arn:aws:iam::111122223333:role/aws-service-role/backup.amazonaws.com/AWSServiceRoleForBackup",
  "IsEncrypted": true,
  "LastRestoreTime": "2021-07-26T06:51:58.271Z",
  "Lifecycle": {
    "DeleteAfterDays": 35,
    "MoveToColdStorageAfterDays": 15
  },
  "RecoveryPointArn": "arn:aws:backup:us-east-1:111122223333:recovery-point:151a59e4-f1d5-4587-a7fd-0774c6e91268",
```

```

    "ResourceArn": "arn:aws:elasticfilesystem:us-east-1:858726136373:file-system/
fs-15bd31a1",
    "ResourceType": "EFS",
    "SourceBackupVaultArn": "arn:aws:backup:us-east-1:111122223333:backup-vault:aws/
efs/automatic-backup-vault",
    "Status": "COMPLETED",
    "StatusMessage": "Failure message",
    "StorageClass": "WARM"
}

```

AwsCertificateManagersumber daya di ASFF

Berikut ini adalah contoh sintaks AWS Security Finding Format (ASFF) untuk `AwsCertificateManager` sumber daya.

AWS Security Hub menormalkan temuan dari berbagai sumber menjadi ASFF. Untuk informasi latar belakang tentang ASFF, lihat [AWS Format Pencarian Keamanan \(ASFF\)](#).

AwsCertificateManagerCertificate

`AwsCertificateManagerCertificate` objek memberikan rincian tentang sertifikat AWS Certificate Manager (ACM).

Berikut ini adalah contoh `AwsCertificateManagerCertificate` temuan dalam AWS Security Finding Format (ASFF). Untuk melihat deskripsi `AwsCertificateManagerCertificate` atribut, lihat [AwsCertificateManagerCertificateDetails](#) di Referensi AWS Security Hub API.

Contoh

```

"AwsCertificateManagerCertificate": {
  "CertificateAuthorityArn": "arn:aws:acm:us-west-2:444455556666:certificate-
authority/example",
  "CreatedAt": "2019-05-24T18:12:02.000Z",
  "DomainName": "example.amazondomains.com",
  "DomainValidationOptions": [
    {
      "DomainName": "example.amazondomains.com",
      "ResourceRecord": {
        "Name": "_1bacb61828d3a1020c40a560ceed08f7.example.amazondomains.com",
        "Type": "CNAME",
        "Value": "_example.acm-validations.aws."
      },
      "ValidationDomain": "example.amazondomains.com",
    }
  ]
}

```

```

        "ValidationEmails": [sample_email@sample.com],
        "ValidationMethod": "DNS",
        "ValidationStatus": "SUCCESS"
    }
],
"ExtendedKeyUsages": [
    {
        "Name": "TLS_WEB_SERVER_AUTHENTICATION",
        "OId": "1.3.6.1.5.5.7.3.1"
    },
    {
        "Name": "TLS_WEB_CLIENT_AUTHENTICATION",
        "OId": "1.3.6.1.5.5.7.3.2"
    }
],
"FailureReason": "",
"ImportedAt": "2018-08-17T00:13:00.000Z",
"InUseBy": ["arn:aws:amazondomains:us-west-2:444455556666:loadbalancer/example"],
"IssuedAt": "2020-04-26T00:41:17.000Z",
"Issuer": "Amazon",
"KeyAlgorithm": "RSA-1024",
"KeyUsages": [
    {
        "Name": "DIGITAL_SIGNATURE",
    },
    {
        "Name": "KEY_ENCIIPHERMENT",
    }
],
"NotAfter": "2021-05-26T12:00:00.000Z",
"NotBefore": "2020-04-26T00:00:00.000Z",
"Options": {
    "CertificateTransparencyLoggingPreference": "ENABLED",
}
"RenewalEligibility": "ELIGIBLE",
"RenewalSummary": {
    "DomainValidationOptions": [
        {
            "DomainName": "example.amazondomains.com",
            "ResourceRecord": {
                "Name":
"_1bacb61828d3a1020c40a560ceed08f7.example.amazondomains.com",
                "Type": "CNAME",
                "Value": "_example.acm-validations.aws.com",
            }
        }
    ]
}

```

```

    },
    "ValidationDomain": "example.amazondomains.com",
    "ValidationEmails": ["sample_email@sample.com"],
    "ValidationMethod": "DNS",
    "ValidationStatus": "SUCCESS"
  }
],
"RenewalStatus": "SUCCESS",
"RenewalStatusReason": "",
"UpdatedAt": "2020-04-26T00:41:35.000Z",
},
"Serial": "02:ac:86:b6:07:2f:0a:61:0e:3a:ac:fd:d9:ab:17:1a",
"SignatureAlgorithm": "SHA256WITHRSA",
"Status": "ISSUED",
"Subject": "CN=example.amazondomains.com",
"SubjectAlternativeNames": ["example.amazondomains.com"],
"Type": "AMAZON_ISSUED"
}

```

AwsCloudFormation sumber daya di ASFF

Berikut ini adalah contoh sintaks AWS Security Finding Format (ASFF) untuk `AwsCloudFormation` sumber daya.

AWS Security Hub menormalkan temuan dari berbagai sumber menjadi ASFF. Untuk informasi latar belakang tentang ASFF, lihat [AWS Format Pencarian Keamanan \(ASFF\)](#).

AwsCloudFormationStack

`AwsCloudFormationStack` objek memberikan rincian tentang AWS CloudFormation tumpukan yang bersarang sebagai sumber daya dalam template tingkat atas.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsCloudFormationStack` objek. Untuk melihat deskripsi `AwsCloudFormationStack` atribut, lihat [AwsCloudFormationStackDetails](#) di Referensi AWS Security Hub API.

Contoh

```

"AwsCloudFormationStack": {
  "Capabilities": [
    "CAPABILITY_IAM",
    "CAPABILITY_NAMED_IAM"
  ]
}

```

```

],
"CreationTime": "2022-02-18T15:31:53.161Z",
"Description": "AWS CloudFormation Sample",
"DisableRollback": true,
"DriftInformation": {
  "StackDriftStatus": "DRIFTED"
},
"EnableTerminationProtection": false,
"LastUpdatedTime": "2022-02-18T15:31:53.161Z",
"NotificationArns": [
  "arn:aws:sns:us-east-1:978084797471:sample-sns-cfn"
],
"Outputs": [{
  "Description": "URL for newly created LAMP stack",
  "OutputKey": "WebsiteUrl",
  "OutputValue": "http://ec2-44-193-18-241.compute-1.amazonaws.com"
}],
"RoleArn": "arn:aws:iam::012345678910:role/exampleRole",
"StackId": "arn:aws:cloudformation:us-east-1:978084797471:stack/sample-stack/e5d9f7e0-90cf-11ec-88c6-12ac1f91724b",
"StackName": "sample-stack",
"StackStatus": "CREATE_COMPLETE",
"StackStatusReason": "Success",
"TimeoutInMinutes": 1
}

```

AwsCloudFrontsumber daya di ASFF

Berikut ini adalah contoh sintaks AWS Security Finding Format (ASFF) untuk `AwsCloudFront` sumber daya.

AWS Security Hub menormalkan temuan dari berbagai sumber menjadi ASFF. Untuk informasi latar belakang tentang ASFF, lihat [AWS Format Pencarian Keamanan \(ASFF\)](#).

AwsCloudFrontDistribution

`AwsCloudFrontDistribution` Objek memberikan rincian tentang konfigurasi CloudFront distribusi Amazon.

Berikut ini adalah contoh `AwsCloudFrontDistribution` temuan dalam AWS Security Finding Format (ASFF). Untuk melihat deskripsi `AwsCloudFrontDistribution` atribut, lihat [AwsCloudFrontDistributionDetails](#) di Referensi AWS Security Hub API.

Contoh

```

"AwsCloudFrontDistribution": {
  "CacheBehaviors": {
    "Items": [
      {
        "ViewerProtocolPolicy": "https-only"
      }
    ]
  },
  "DefaultCacheBehavior": {
    "ViewerProtocolPolicy": "https-only"
  },
  "DefaultRootObject": "index.html",
  "DomainName": "d2wkuj2w9l34gt.cloudfront.net",
  "Etag": "E37H0T42DHPVYH",
  "LastModifiedTime": "2015-08-31T21:11:29.093Z",
  "Logging": {
    "Bucket": "myawslogbucket.s3.amazonaws.com",
    "Enabled": false,
    "IncludeCookies": false,
    "Prefix": "myawslog/"
  },
  "OriginGroups": {
    "Items": [
      {
        "FailoverCriteria": {
          "StatusCodes": {
            "Items": [
              200,
              301,
              404
            ]
          }
        }
      }
    ]
  },
  "Origins": {
    "Items": [
      {
        "CustomOriginConfig": {
          "HttpPort": 80,

```

```

        "HttpsPort": 443,
        "OriginKeepaliveTimeout": 60,
        "OriginProtocolPolicy": "match-viewer",
        "OriginReadTimeout": 30,
        "OriginSslProtocols": {
            "Items": ["SSLv3", "TLSv1"],
            "Quantity": 2
        }
    },
    ],
},
{
    "DomainName": "amzn-s3-demo-bucket.s3.amazonaws.com",
    "Id": "my-origin",
    "OriginPath": "/production",
    "S3OriginConfig": {
        "OriginAccessIdentity": "origin-access-identity/cloudfront/
E2YFS67H6VB6E4"
    }
},
],
},
"Status": "Deployed",
"ViewerCertificate": {
    "AcmCertificateArn": "arn:aws:acm::123456789012:AcmCertificateArn",
    "Certificate": "ASCAJRRE5XYF52TKRY5M4",
    "CertificateSource": "iam",
    "CloudFrontDefaultCertificate": true,
    "IamCertificateId": "ASCAJRRE5XYF52TKRY5M4",
    "MinimumProtocolVersion": "TLSv1.2_2021",
    "SslSupportMethod": "sni-only"
},
"WebAclId": "waf-1234567890"
}

```

AwsCloudTrail sumber data di ASFF

Berikut ini adalah contoh sintaks AWS Security Finding Format (ASFF) untuk `AwsCloudTrail` sumber data.

AWS Security Hub menormalkan temuan dari berbagai sumber menjadi ASFF. Untuk informasi latar belakang tentang ASFF, lihat [AWS Format Pencarian Keamanan \(ASFF\)](#).

AwsCloudTrailTrail

AwsCloudTrailTrailObjek tersebut memberikan detail tentang AWS CloudTrail jejak.

Berikut ini adalah contoh AwsCloudTrailTrail temuan dalam AWS Security Finding Format (ASFF). Untuk melihat deskripsi AwsCloudTrailTrail atribut, lihat [AwsCloudTrailTrailDetails](#) di Referensi AWS Security Hub API.

Contoh

```
"AwsCloudTrailTrail": {
  "CloudWatchLogsLogGroupArn": "arn:aws:logs:us-west-2:123456789012:log-group:CloudTrail/regression:*",
  "CloudWatchLogsRoleArn": "arn:aws:iam::866482105055:role/CloudTrail_CloudWatchLogs",
  "HasCustomEventSelectors": true,
  "HomeRegion": "us-west-2",
  "IncludeGlobalServiceEvents": true,
  "IsMultiRegionTrail": true,
  "IsOrganizationTrail": false,
  "KmsKeyId": "kmsKeyId",
  "LogFileValidationEnabled": true,
  "Name": "regression-trail",
  "S3BucketName": "cloudtrail-bucket",
  "S3KeyPrefix": "s3KeyPrefix",
  "SnsTopicArn": "arn:aws:sns:us-east-2:123456789012:MyTopic",
  "SnsTopicName": "snsTopicName",
  "TrailArn": "arn:aws:cloudtrail:us-west-2:123456789012:trail"
}
```

AwsCloudWatchsumber daya di ASFF

Berikut ini adalah contoh sintaks AWS Security Finding Format (ASFF) untuk AwsCloudWatch sumber daya.

AWS Security Hub menormalkan temuan dari berbagai sumber menjadi ASFF. Untuk informasi latar belakang tentang ASFF, lihat [AWS Format Pencarian Keamanan \(ASFF\)](#).

AwsCloudWatchAlarm

AwsCloudWatchAlarmObjek memberikan detail tentang CloudWatch alarm Amazon yang menonton metrik atau melakukan tindakan saat alarm berubah status.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsCloudWatchAlarm` objek. Untuk melihat deskripsi `AwsCloudWatchAlarm` atribut, lihat [AwsCloudWatchAlarmDetails](#) di Referensi AWS Security Hub API.

Contoh

```
"AwsCloudWatchAlarm": {
  "ActionsEnabled": true,
  "AlarmActions": [
    "arn:aws:automate:region:ec2:stop",
    "arn:aws:automate:region:ec2:terminate"
  ],
  "AlarmArn": "arn:aws:cloudwatch:us-west-2:012345678910:alarm:sampleAlarm",
  "AlarmConfigurationUpdatedTimestamp": "2022-02-18T15:31:53.161Z",
  "AlarmDescription": "Alarm Example",
  "AlarmName": "Example",
  "ComparisonOperator": "GreaterThanOrEqualToThreshold",
  "DatapointsToAlarm": 1,
  "Dimensions": [{
    "Name": "InstanceId",
    "Value": "i-1234567890abcdef0"
  }],
  "EvaluateLowSampleCountPercentile": "evaluate",
  "EvaluationPeriods": 1,
  "ExtendedStatistic": "p99.9",
  "InsufficientDataActions": [
    "arn:aws:automate:region:ec2:stop"
  ],
  "MetricName": "Sample Metric",
  "Namespace": "YourNamespace",
  "OkActions": [
    "arn:aws:swf:region:account-id:action/actions/AWS_EC2.InstanceId.Stop/1.0"
  ],
  "Period": 1,
  "Statistic": "SampleCount",
  "Threshold": 12.3,
  "ThresholdMetricId": "t1",
  "TreatMissingData": "notBreaching",
  "Unit": "Kilobytes/Second"
}
```

AwsCodeBuildsumber daya di ASFF

Berikut ini adalah contoh sintaks AWS Security Finding Format (ASFF) untuk AwsCodeBuild sumber daya.

AWS Security Hub menormalkan temuan dari berbagai sumber menjadi ASFF. Untuk informasi latar belakang tentang ASFF, lihat [AWS Format Pencarian Keamanan \(ASFF\)](#).

AwsCodeBuildProject

AwsCodeBuildProjectObjek memberikan informasi tentang suatu AWS CodeBuild proyek.

Berikut ini adalah contoh AwsCodeBuildProject temuan dalam AWS Security Finding Format (ASFF). Untuk melihat deskripsi AwsCodeBuildProject atribut, lihat [AwsCodeBuildProjectDetails](#) di Referensi AWS Security Hub API.

Contoh

```
"AwsCodeBuildProject": {
  "Artifacts": [
    {
      "ArtifactIdentifier": "string",
      "EncryptionDisabled": boolean,
      "Location": "string",
      "Name": "string",
      "NamespaceType": "string",
      "OverrideArtifactName": boolean,
      "Packaging": "string",
      "Path": "string",
      "Type": "string"
    }
  ],
  "SecondaryArtifacts": [
    {
      "ArtifactIdentifier": "string",
      "EncryptionDisabled": boolean,
      "Location": "string",
      "Name": "string",
      "NamespaceType": "string",
      "OverrideArtifactName": boolean,
      "Packaging": "string",
      "Path": "string",
      "Type": "string"
    }
  ]
}
```

```

    }
  ],
  "EncryptionKey": "string",
  "Certificate": "string",
  "Environment": {
    "Certificate": "string",
    "EnvironmentVariables": [
      {
        "Name": "string",
        "Type": "string",
        "Value": "string"
      }
    ]
  },
  "ImagePullCredentialsType": "string",
  "PrivilegedMode": boolean,
  "RegistryCredential": {
    "Credential": "string",
    "CredentialProvider": "string"
  },
  "Type": "string"
},
"LogsConfig": {
  "CloudWatchLogs": {
    "GroupName": "string",
    "Status": "string",
    "StreamName": "string"
  },
  "S3Logs": {
    "EncryptionDisabled": boolean,
    "Location": "string",
    "Status": "string"
  }
},
"Name": "string",
"ServiceRole": "string",
"Source": {
  "Type": "string",
  "Location": "string",
  "GitCloneDepth": integer
},
"VpcConfig": {
  "VpcId": "string",
  "Subnets": ["string"],
  "SecurityGroupIds": ["string"]
}

```

```
}
}
```

AwsDms sumber daya di ASFF

Berikut ini adalah contoh sintaks AWS Security Finding Format (ASFF) untuk AwsDms sumber daya.

AWS Security Hub menormalkan temuan dari berbagai sumber menjadi ASFF. Untuk informasi latar belakang tentang ASFF, lihat [AWS Format Pencarian Keamanan \(ASFF\)](#).

AwsDmsEndpoint

AwsDmsEndpointObjek memberikan informasi tentang titik akhir AWS Database Migration Service (AWS DMS). Endpoint menyediakan koneksi, tipe penyimpanan data, dan informasi lokasi tentang penyimpanan data Anda.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk AwsDmsEndpoint objek. Untuk melihat deskripsi AwsDmsEndpoint atribut, lihat [AwsDmsEndpointDetails](#) di Referensi AWS Security Hub API.

Contoh

```
"AwsDmsEndpoint": {
  "CertificateArn": "arn:aws:dms:us-east-1:123456789012:cert:EXAMPLEIGDURVZGVJQZDPWJ5A7F2YDJVSMTBWF1",
  "DatabaseName": "Test",
  "EndpointArn": "arn:aws:dms:us-east-1:123456789012:endpoint:EXAMPLEQB3CZY33F7XV253NAJVBPNPK6MJQVFVQA",
  "EndpointIdentifier": "target-db",
  "EndpointType": "TARGET",
  "EngineName": "mariadb",
  "KmsKeyId": "arn:aws:kms:us-east-1:123456789012:key/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "Port": 3306,
  "ServerName": "target-db.exampletafyu.us-east-1.rds.amazonaws.com",
  "SslMode": "verify-ca",
  "Username": "admin"
}
```

AwsDmsReplicationInstance

AwsDmsReplicationInstanceObjek memberikan informasi tentang contoh replikasi AWS Database Migration Service (AWS DMS). DMS menggunakan contoh replikasi untuk terhubung ke

penyimpanan data sumber Anda, membaca data sumber, dan memformat data untuk konsumsi oleh penyimpanan data target.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsDmsReplicationInstance` objek. Untuk melihat deskripsi `AwsDmsReplicationInstance` atribut, lihat [AwsDmsReplicationInstanceDetails](#) di Referensi AWS Security Hub API.

Contoh

```
"AwsDmsReplicationInstance": {
  "AllocatedStorage": 50,
  "AutoMinorVersionUpgrade": true,
  "AvailabilityZone": "us-east-1b",
  "EngineVersion": "3.5.1",
  "KmsKeyId": "arn:aws:kms:us-east-1:123456789012:key/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "MultiAZ": false,
  "PreferredMaintenanceWindow": "wed:08:08-wed:08:38",
  "PubliclyAccessible": true,
  "ReplicationInstanceClass": "dms.c5.xlarge",
  "ReplicationInstanceIdentifier": "second-replication-instance",
  "ReplicationSubnetGroup": {
    "ReplicationSubnetGroupIdentifier": "default-vpc-2344f44f"
  },
  "VpcSecurityGroups": [
    {
      "VpcSecurityGroupId": "sg-003a34e205138138b"
    }
  ]
}
```

AwsDmsReplicationTask

`AwsDmsReplicationTask` objek memberikan informasi tentang tugas replikasi AWS Database Migration Service (AWS DMS). Tugas replikasi memindahkan sekumpulan data dari titik akhir sumber ke titik akhir target.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsDmsReplicationInstance` objek. Untuk melihat deskripsi `AwsDmsReplicationInstance` atribut, lihat [AwsDmsReplicationInstance](#) di Referensi AWS Security Hub API.

Contoh

```

"AwsDmsReplicationTask": {
  "CdcStartPosition": "2023-08-28T14:26:22",
  "Id": "arn:aws:dms:us-east-1:123456789012:task:YDYUOHZIXWKQSUCBMUCQCN44SJW74VJNB5DFWQ",
  "MigrationType": "cdc",
  "ReplicationInstanceArn": "arn:aws:dms:us-east-1:123456789012:rep:T7V6RFDP23PYQWUL26N3PF5REKML4Y0UGIMYJUI",
  "ReplicationTaskIdentifier": "test-task",
  "ReplicationTaskSettings": "{\\"Logging\\":{\\"EnableLogging\\":false,\\"EnableLogContext\\":false,\\"LogComponents\\":[{\\"Severity\\":\\"LOGGER_SEVERITY_DEFAULT\\",\\"Id\\":\\"TRANSFORMATION\\"},{\\"Severity\\":\\"LOGGER_SEVERITY_DEFAULT\\",\\"Id\\":\\"SOURCE_UNLOAD\\"},{\\"Severity\\":\\"LOGGER_SEVERITY_DEFAULT\\",\\"Id\\":\\"IO\\"},{\\"Severity\\":\\"LOGGER_SEVERITY_DEFAULT\\",\\"Id\\":\\"TARGET_LOAD\\"},{\\"Severity\\":\\"LOGGER_SEVERITY_DEFAULT\\",\\"Id\\":\\"PERFORMANCE\\"},{\\"Severity\\":\\"LOGGER_SEVERITY_DEFAULT\\",\\"Id\\":\\"SOURCE_CAPTURE\\"},{\\"Severity\\":\\"LOGGER_SEVERITY_DEFAULT\\",\\"Id\\":\\"SORTER\\"},{\\"Severity\\":\\"LOGGER_SEVERITY_DEFAULT\\",\\"Id\\":\\"REST_SERVER\\"},{\\"Severity\\":\\"LOGGER_SEVERITY_DEFAULT\\",\\"Id\\":\\"VALIDATOR_EXT\\"},{\\"Severity\\":\\"LOGGER_SEVERITY_DEFAULT\\",\\"Id\\":\\"TARGET_APPLY\\"},{\\"Severity\\":\\"LOGGER_SEVERITY_DEFAULT\\",\\"Id\\":\\"TASK_MANAGER\\"},{\\"Severity\\":\\"LOGGER_SEVERITY_DEFAULT\\",\\"Id\\":\\"TABLES_MANAGER\\"},{\\"Severity\\":\\"LOGGER_SEVERITY_DEFAULT\\",\\"Id\\":\\"METADATA_MANAGER\\"},{\\"Severity\\":\\"LOGGER_SEVERITY_DEFAULT\\",\\"Id\\":\\"FILE_FACTORY\\"},{\\"Severity\\":\\"LOGGER_SEVERITY_DEFAULT\\",\\"Id\\":\\"COMMON\\"},{\\"Severity\\":\\"LOGGER_SEVERITY_DEFAULT\\",\\"Id\\":\\"ADDONS\\"},{\\"Severity\\":\\"LOGGER_SEVERITY_DEFAULT\\",\\"Id\\":\\"DATA_STRUCTURE\\"},{\\"Severity\\":\\"LOGGER_SEVERITY_DEFAULT\\",\\"Id\\":\\"COMMUNICATION\\"},{\\"Severity\\":\\"LOGGER_SEVERITY_DEFAULT\\",\\"Id\\":\\"FILE_TRANSFER\\"}],\\"CloudWatchLogGroup\\":null,\\"CloudWatchLogStream\\":null},\\"StreamBufferSettings\\":{\\"StreamBufferCount\\":3,\\"CtrlStreamBufferSizeInMB\\":5,\\"StreamBufferSizeInMB\\":8},\\"ErrorBehavior\\":{\\"FailOnNoTablesCaptured\\":true,\\"ApplyErrorUpdatePolicy\\":\\"LOG_ERROR\\",\\"FailOnTransactionConsistencyBreached\\":false,\\"RecoverableErrorThrottlingMax\\":1800,\\"DataErrorEscalationPolicy\\":\\"SUSPEND_TABLE\\",\\"ApplyErrorEscalationCount\\":0,\\"RecoverableErrorStopRetryAfterThrottlingMax\\":true,\\"RecoverableErrorThrottling\\":true,\\"ApplyErrorFailOnTruncationDdl\\":false,\\"DataTruncationErrorPolicy\\":\\"LOG_ERROR\\",\\"ApplyErrorInsertPolicy\\":\\"LOG_ERROR\\",\\"EventErrorPolicy\\":\\"IGNORE\\",\\"ApplyErrorEscalationPolicy\\":\\"LOG_ERROR\\",\\"RecoverableErrorCount\\":-1,\\"DataErrorEscalationCount\\":0,\\"TableErrorEscalationPolicy\\":\\"STOP_TASK\\",\\"RecoverableErrorInterval\\":5,\\"ApplyErrorDeletePolicy\\":\\"IGNORE_RECORD\\",\\"TableErrorEscalationCount\\":0,\\"FullLoadIgnoreConflicts\\":true,\\"DataErrorPolicy\\":\\"LOG_ERROR\\",\\"TableErrorPolicy\\":\\"SUSPEND_TABLE\\"},\\"TTSettings\\":{\\"TTS3Settings\\":null,\\"TTRecordSettings\\":null,\\"EnableTT\\":false},\\"FullLoadSettings\\":{\\"CommitRate\\":10000,\\"StopTaskCachedChangesApplied\\":false,\\"StopTaskCachedChangesNotApplied\\":false,\\"MaxFullLoadSubTasks\\":8,\\"TransactionConsistencyTimeout\\":600,\\"CreatePkAfterFullLoad\\":false,

```

```

\ "TargetTablePrepMode\":"\ "DO_NOTHING\"," , \ "TargetMetadata\":{ \ "ParallelApplyBufferSize
\":"0, \ "ParallelApplyQueuesPerThread\":"0, \ "ParallelApplyThreads\":"0, \ "TargetSchema
\":"\ " , \ "InlineLobMaxSize\":"0, \ "ParallelLoadQueuesPerThread\":"0, \ "SupportLobs
\":"true, \ "LobChunkSize\":"64, \ "TaskRecoveryTableEnabled\":"false, \ "ParallelLoadThreads
\":"0, \ "LobMaxSize\":"0, \ "BatchApplyEnabled\":"false, \ "FullLobMode\":"true,
\ "LimitedSizeLobMode\":"false, \ "LoadMaxFileSize\":"0, \ "ParallelLoadBufferSize\":"0},
\ "BeforeImageSettings\":"null, \ "ControlTablesSettings\":{ \ "historyTimeslotInMinutes
\":"5, \ "HistoryTimeslotInMinutes\":"5, \ "StatusTableEnabled\":"false,
\ "SuspendedTablesTableEnabled\":"false, \ "HistoryTableEnabled\":"false, \ "ControlSchema
\":"\ " , \ "FullLoadExceptionTableEnabled\":"false}, \ "LoopbackPreventionSettings
\":"null, \ "CharacterSetSettings\":"null, \ "FailTaskWhenCleanTaskResourceFailed
\":"false, \ "ChangeProcessingTuning\":{ \ "StatementCacheSize\":"50, \ "CommitTimeout
\":"1, \ "BatchApplyPreserveTransaction\":"true, \ "BatchApplyTimeoutMin\":"1,
\ "BatchSplitSize\":"0, \ "BatchApplyTimeoutMax\":"30, \ "MinTransactionSize\":"1000,
\ "MemoryKeepTime\":"60, \ "BatchApplyMemoryLimit\":"500, \ "MemoryLimitTotal\":"1024},
\ "ChangeProcessingDdlHandlingPolicy\":{ \ "HandleSourceTableDropped\":"true,
\ "HandleSourceTableTruncated\":"true, \ "HandleSourceTableAltered\":"true},
\ "PostProcessingRules\":"null}],
    "SourceEndpointArn": "arn:aws:dms:us-
east-1:123456789012:endpoint:TZPWV2VCXEGHY0KVKRNHAKJ4Q3RUXACNGFGYWRI",
    "TableMappings": "{ \ "rules\":"[{ \ "rule-type\":"\ "selection\"," , \ "rule-id\":"
\ "969761702\"," , \ "rule-name\":"\ "969761702\"," , \ "object-locator\":{ \ "schema-name\":"\ "%table
\ "," , \ "table-name\":"\ "%example\"," }, \ "rule-action\":"\ "exclude\"," , \ "filters\":"[[]]}]"}",
    "TargetEndpointArn": "arn:aws:dms:us-
east-1:123456789012:endpoint:ABR8LB0QB3CZY33F7XV253NAJVBPNPK6MJQVVFVQA"
}

```

AwsDynamoDBsumber daya di ASFF

Berikut ini adalah contoh sintaks AWS Security Finding Format (ASFF) untuk AwsDynamoDB sumber daya.

AWS Security Hub menormalkan temuan dari berbagai sumber menjadi ASFF. Untuk informasi latar belakang tentang ASFF, lihat [AWS Format Pencarian Keamanan \(ASFF\)](#).

AwsDynamoDbTable

AwsDynamoDbTableObjek memberikan rincian tentang tabel Amazon DynamoDB.

Berikut ini adalah contoh AwsDynamoDbTable temuan dalam AWS Security Finding Format (ASFF). Untuk melihat deskripsi AwsDynamoDbTable atribut, lihat [AwsDynamoDbTableDetails](#) di Referensi AWS Security Hub API.

Contoh

```

"AwsDynamoDbTable": {
  "AttributeDefinitions": [
    {
      "AttributeName": "attribute1",
      "AttributeType": "value 1"
    },
    {
      "AttributeName": "attribute2",
      "AttributeType": "value 2"
    },
    {
      "AttributeName": "attribute3",
      "AttributeType": "value 3"
    }
  ],
  "BillingModeSummary": {
    "BillingMode": "PAY_PER_REQUEST",
    "LastUpdateToPayPerRequestDateTime": "2019-12-03T15:23:10.323Z"
  },
  "CreationDateTime": "2019-12-03T15:23:10.248Z",
  "DeletionProtectionEnabled": true,
  "GlobalSecondaryIndexes": [
    {
      "Backfilling": false,
      "IndexArn": "arn:aws:dynamodb:us-west-2:111122223333:table/exampleTable/index/exampleIndex",
      "IndexName": "standardsControlArnIndex",
      "IndexSizeBytes": 1862513,
      "IndexStatus": "ACTIVE",
      "ItemCount": 20,
      "KeySchema": [
        {
          "AttributeName": "City",
          "KeyType": "HASH"
        },
        {
          "AttributeName": "Date",
          "KeyType": "RANGE"
        }
      ],
      "Projection": {
        "NonKeyAttributes": ["predictorName"],

```



```

        "ProjectionType": "ALL"
    },
    "ProvisionedThroughput": {
        "LastIncreaseDateTime": "2019-03-14T13:21:00.399Z",
        "LastDecreaseDateTime": "2019-03-14T12:47:35.193Z",
        "NumberOfDecreasesToday": 0,
        "ReadCapacityUnits": 100,
        "WriteCapacityUnits": 50
    },
}
],
"GlobalTableVersion": "V1",
"ItemCount": 2705,
"KeySchema": [
    {
        "AttributeName": "zipcode",
        "KeyType": "HASH"
    }
],
"LatestStreamArn": "arn:aws:dynamodb:us-west-2:111122223333:table/exampleTable/
stream/2019-12-03T23:23:10.248",
"LatestStreamLabel": "2019-12-03T23:23:10.248",
"LocalSecondaryIndexes": [
    {
        "IndexArn": "arn:aws:dynamodb:us-east-1:111122223333:table/exampleGroup/
index/exampleId",
        "IndexName": "CITY_DATE_INDEX_NAME",
        "KeySchema": [
            {
                "AttributeName": "zipcode",
                "KeyType": "HASH"
            }
        ],
        "Projection": {
            "NonKeyAttributes": ["predictorName"],
            "ProjectionType": "ALL"
        },
    }
],
"ProvisionedThroughput": {
    "LastIncreaseDateTime": "2019-03-14T13:21:00.399Z",
    "LastDecreaseDateTime": "2019-03-14T12:47:35.193Z",
    "NumberOfDecreasesToday": 0,
    "ReadCapacityUnits": 100,

```

```

    "WriteCapacityUnits": 50
  },
  "Replicas": [
    {
      "GlobalSecondaryIndexes": [
        {
          "IndexName": "CITY_DATE_INDEX_NAME",
          "ProvisionedThroughputOverride": {
            "ReadCapacityUnits": 10
          }
        }
      ],
      "KmsMasterKeyId" : "KmsKeyId"
      "ProvisionedThroughputOverride": {
        "ReadCapacityUnits": 10
      },
      "RegionName": "regionName",
      "ReplicaStatus": "CREATING",
      "ReplicaStatusDescription": "replicaStatusDescription"
    }
  ],
  "RestoreSummary" : {
    "SourceBackupArn": "arn:aws:dynamodb:us-west-2:111122223333:table/exampleTable/backup/backup1",
    "SourceTableArn": "arn:aws:dynamodb:us-west-2:111122223333:table/exampleTable",
    "RestoreDateTime": "2020-06-22T17:40:12.322Z",
    "RestoreInProgress": true
  },
  "SseDescription": {
    "InaccessibleEncryptionDateTime": "2018-01-26T23:50:05.000Z",
    "Status": "ENABLED",
    "SseType": "KMS",
    "KmsMasterKeyArn": "arn:aws:kms:us-east-1:111122223333:key/key1"
  },
  "StreamSpecification" : {
    "StreamEnabled": true,
    "StreamViewType": "NEW_IMAGE"
  },
  "TableId": "example-table-id-1",
  "TableName": "example-table",
  "TableSizeBytes": 1862513,
  "TableStatus": "ACTIVE"
}

```

AwsEc2sumber daya di ASFF

Berikut ini adalah contoh sintaks AWS Security Finding Format (ASFF) untuk AwsEc2 sumber daya.

AWS Security Hub menormalkan temuan dari berbagai sumber menjadi ASFF. Untuk informasi latar belakang tentang ASFF, lihat [AWS Format Pencarian Keamanan \(ASFF\)](#).

AwsEc2ClientVpnEndpoint

AwsEc2ClientVpnEndpointObjek memberikan informasi tentang AWS Client VPN titik akhir. Titik akhir Client VPN adalah sumber daya yang Anda buat dan konfigurasi untuk mengaktifkan dan mengelola sesi VPN klien. Ini adalah titik terminasi untuk semua sesi VPN klien.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk AwsEc2ClientVpnEndpoint objek. Untuk melihat deskripsi AwsEc2ClientVpnEndpoint atribut, lihat [AwsEc2 ClientVpnEndpointDetails](#) di Referensi AWS Security Hub API.

Contoh

```
"AwsEc2ClientVpnEndpoint": {
  "AuthenticationOptions": [
    {
      "MutualAuthentication": {
        "ClientRootCertificateChainArn": "arn:aws:acm:us-east-1:123456789012:certificate/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
      },
      "Type": "certificate-authentication"
    }
  ],
  "ClientCidrBlock": "10.0.0.0/22",
  "ClientConnectOptions": {
    "Enabled": false
  },
  "ClientLoginBannerOptions": {
    "Enabled": false
  },
  "ClientVpnEndpointId": "cvpn-endpoint-00c5d11fc4729f2a5",
  "ConnectionLogOptions": {
    "Enabled": false
  },
  "Description": "test",
  "DnsServer": ["10.0.0.0"],
```

```

    "ServerCertificateArn": "arn:aws:acm:us-east-1:123456789012:certificate/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "SecurityGroupIdSet": [
        "sg-0f7a177b82b443691"
    ],
    "SelfServicePortalUrl": "https://self-service.clientvpn.amazonaws.com/endpoints/
cvpn-endpoint-00c5d11fc4729f2a5",
    "SessionTimeoutHours": 24,
    "SplitTunnel": false,
    "TransportProtocol": "udp",
    "VpcId": "vpc-1a2b3c4d5e6f1a2b3",
    "VpnPort": 443
}

```

AwsEc2Eip

AwsEc2EipObjek memberikan informasi tentang alamat IP Elastis.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk AwsEc2Eip objek. Untuk melihat deskripsi AwsEc2Eip atribut, lihat [AwsEc2 EipDetails](#) di Referensi AWS Security Hub API.

Contoh

```

"AwsEc2Eip": {
    "InstanceId": "instance1",
    "PublicIp": "192.0.2.04",
    "AllocationId": "eipalloc-example-id-1",
    "AssociationId": "eipassoc-example-id-1",
    "Domain": "vpc",
    "PublicIpv4Pool": "anycompany",
    "NetworkBorderGroup": "eu-central-1",
    "NetworkInterfaceId": "eni-example-id-1",
    "NetworkInterfaceOwnerId": "777788889999",
    "PrivateIpAddress": "192.0.2.03"
}

```

AwsEc2Instance

AwsEc2InstanceObjek memberikan rincian tentang EC2 instance Amazon.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk AwsEc2Instance objek. Untuk melihat deskripsi AwsEc2Instance atribut, lihat [AwsEc2 InstanceDetails](#) di Referensi AWS Security Hub API.

Contoh

```
"AwsEc2Instance": {
  "IamInstanceProfileArn": "arn:aws:iam::123456789012:instance-profile/AdminRole",
  "ImageId": "ami-1234",
  "IPv4Addresses": [ "1.1.1.1" ],
  "IPv6Addresses": [ "2001:db8:1234:1a2b::123" ],
  "KeyName": "my_keypair",
  "LaunchedAt": "2018-05-08T16:46:19.000Z",
  "MetadataOptions": {
    "HttpEndpoint": "enabled",
    "HttpProtocolIpv6": "enabled",
    "HttpPutResponseHopLimit": 1,
    "HttpTokens": "optional",
    "InstanceMetadataTags": "disabled",
  },
  "Monitoring": {
    "State": "disabled"
  },
  "NetworkInterfaces": [
    {
      "NetworkInterfaceId": "eni-e5aa89a3"
    }
  ],
  "SubnetId": "subnet-123",
  "Type": "i3.xlarge",
  "VpcId": "vpc-123"
}
```

AwsEc2LaunchTemplate

AwsEc2LaunchTemplateObjek berisi detail tentang template peluncuran Amazon Elastic Compute Cloud yang menentukan informasi konfigurasi instans.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk AwsEc2LaunchTemplate objek. Untuk melihat deskripsi AwsEc2LaunchTemplate atribut, lihat [AwsEc2LaunchTemplateDetails](#) di Referensi AWS Security Hub API.

Contoh

```
"AwsEc2LaunchTemplate": {
  "DefaultVersionNumber": "1",
  "ElasticGpuSpecifications": ["string"],
```

```

    "ElasticInferenceAccelerators": ["string"],
    "Id": "lt-0a16e9802800bdd85",
    "ImageId": "ami-0d5eff06f840b45e9",
    "LatestVersionNumber": "1",
    "LaunchTemplateData": {
      "BlockDeviceMappings": [{
        "DeviceName": "/dev/xvda",
        "Ebs": {
          "DeleteonTermination": true,
          "Encrypted": true,
          "SnapshotId": "snap-01047646ec075f543",
          "VolumeSize": 8,
          "VolumeType": "gp2"
        }
      }],
      "MetadataOptions": {
        "HttpTokens": "enabled",
        "HttpPutResponseHopLimit" : 1
      },
      "Monitoring": {
        "Enabled": true,
      },
      "NetworkInterfaces": [{
        "AssociatePublicIpAddress" : true,
      }],
      "LaunchTemplateName": "string",
      "LicenseSpecifications": ["string"],
      "SecurityGroupIds": ["sg-01fce87ad6e019725"],
      "SecurityGroups": ["string"],
      "TagSpecifications": ["string"]
    }
  }
}

```

AwsEc2NetworkAcl

AwsEc2NetworkAclObjek berisi rincian tentang daftar kontrol akses EC2 jaringan Amazon (ACL).

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk AwsEc2NetworkAcl objek. Untuk melihat deskripsi AwsEc2NetworkAcl atribut, lihat [AwsEc2 NetworkAclDetails](#) di Referensi AWS Security Hub API.

Contoh

```

"AwsEc2NetworkAcl": {
  "IsDefault": false,

```

```

    "NetworkAclId": "acl-1234567890abcdef0",
    "OwnerId": "123456789012",
    "VpcId": "vpc-1234abcd",
    "Associations": [{
      "NetworkAclAssociationId": "aclassoc-abcd1234",
      "NetworkAclId": "acl-021345abcdef6789",
      "SubnetId": "subnet-abcd1234"
    }],
    "Entries": [{
      "CidrBlock": "10.24.34.0/23",
      "Egress": true,
      "IcmpTypeCode": {
        "Code": 10,
        "Type": 30
      },
      "Ipv6CidrBlock": "2001:DB8::/32",
      "PortRange": {
        "From": 20,
        "To": 40
      },
      "Protocol": "tcp",
      "RuleAction": "allow",
      "RuleNumber": 100
    }]
  }
}

```

AwsEc2NetworkInterface

AwsEc2NetworkInterfaceObjek menyediakan informasi tentang antarmuka EC2 jaringan Amazon.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk AwsEc2NetworkInterface objek. Untuk melihat deskripsi AwsEc2NetworkInterface atribut, lihat [AwsEc2 NetworkInterfaceDetails](#) di Referensi AWS Security Hub API.

Contoh

```

"AwsEc2NetworkInterface": {
  "Attachment": {
    "AttachTime": "2019-01-01T03:03:21Z",
    "AttachmentId": "eni-attach-43348162",
    "DeleteOnTermination": true,
    "DeviceIndex": 123,

```

```

    "InstanceId": "i-1234567890abcdef0",
    "InstanceOwnerId": "123456789012",
    "Status": 'ATTACHED'
  },
  "SecurityGroups": [
    {
      "GroupName": "my-security-group",
      "GroupId": "sg-903004f8"
    },
  ],
  "NetworkInterfaceId": 'eni-686ea200',
  "SourceDestCheck": false
}

```

AwsEc2RouteTable

AwsEc2RouteTableObjek memberikan informasi tentang tabel EC2 rute Amazon.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk AwsEc2RouteTable objek. Untuk melihat deskripsi AwsEc2RouteTable atribut, lihat [AwsEc2 RouteTableDetails](#) di Referensi AWS Security Hub API.

Contoh

```

"AwsEc2RouteTable": {
  "AssociationSet": [{
    "AssociationSet": {
      "State": "associated"
    },
    "Main": true,
    "RouteTableAssociationId": "rtbassoc-08e706c45de9f7512",
    "RouteTableId": "rtb-0a59bde9cf2548e34",
  }],
  "PropogatingVgwSet": [],
  "RouteTableId": "rtb-0a59bde9cf2548e34",
  "RouteSet": [
    {
      "DestinationCidrBlock": "10.24.34.0/23",
      "GatewayId": "local",
      "Origin": "CreateRouteTable",
      "State": "active"
    },
    {

```



```

    "DestinationCidrBlock": "10.24.34.0/24",
    "GatewayId": "igw-0242c2d7d513fc5d3",
    "Origin": "CreateRoute",
    "State": "active"
  }
],
  "VpcId": "vpc-0c250a5c33f51d456"
}

```

AwsEc2SecurityGroup

AwsEc2SecurityGroupObjek tersebut menggambarkan grup EC2 keamanan Amazon.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk AwsEc2SecurityGroup objek. Untuk melihat deskripsi AwsEc2SecurityGroup atribut, lihat [AwsEc2 SecurityGroupDetails](#) di Referensi AWS Security Hub API.

Contoh

```

"AwsEc2SecurityGroup": {
  "GroupName": "MySecurityGroup",
  "GroupId": "sg-903004f8",
  "OwnerId": "123456789012",
  "VpcId": "vpc-1a2b3c4d",
  "IpPermissions": [
    {
      "IpProtocol": "-1",
      "IpRanges": [],
      "UserIdGroupPairs": [
        {
          "UserId": "123456789012",
          "GroupId": "sg-903004f8"
        }
      ],
      "PrefixListIds": [
        {"PrefixListId": "pl-63a5400a"}
      ]
    },
    {
      "PrefixListIds": [],
      "FromPort": 22,
      "IpRanges": [
        {

```

```

        "CidrIp": "203.0.113.0/24"
      }
    ],
    "ToPort": 22,
    "IpProtocol": "tcp",
    "UserIdGroupPairs": []
  }
]
}

```

AwsEc2Subnet

AwsEc2SubnetObjek memberikan informasi tentang subnet di Amazon EC2.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk AwsEc2Subnet objek. Untuk melihat deskripsi AwsEc2Subnet atribut, lihat [AwsEc2 SubnetDetails](#) di Referensi AWS Security Hub API.

Contoh

```

AwsEc2Subnet: {
  "AssignIpv6AddressOnCreation": false,
  "AvailabilityZone": "us-west-2c",
  "AvailabilityZoneId": "usw2-az3",
  "AvailableIpAddressCount": 8185,
  "CidrBlock": "10.0.0.0/24",
  "DefaultForAz": false,
  "MapPublicIpOnLaunch": false,
  "OwnerId": "123456789012",
  "State": "available",
  "SubnetArn": "arn:aws:ec2:us-west-2:123456789012:subnet/subnet-d5436c93",
  "SubnetId": "subnet-d5436c93",
  "VpcId": "vpc-153ade70",
  "Ipv6CidrBlockAssociationSet": [{
    "AssociationId": "subnet-cidr-assoc-EXAMPLE",
    "Ipv6CidrBlock": "2001:DB8::/32",
    "CidrBlockState": "associated"
  }]
}

```

AwsEc2TransitGateway

AwsEc2TransitGatewayObjek ini memberikan detail tentang gateway EC2 transit Amazon yang menghubungkan cloud pribadi virtual (VPCs) dan jaringan lokal Anda.

Berikut ini adalah contoh AwsEc2TransitGateway temuan dalam AWS Security Finding Format (ASFF). Untuk melihat deskripsi AwsEc2TransitGateway atribut, lihat [AwsEc2 TransitGatewayDetails](#) di Referensi AWS Security Hub API.

Contoh

```
"AwsEc2TransitGateway": {
  "AmazonSideAsn": 65000,
  "AssociationDefaultRouteTableId": "tgw-rtb-099ba47cbbea837cc",
  "AutoAcceptSharedAttachments": "disable",
  "DefaultRouteTableAssociation": "enable",
  "DefaultRouteTablePropagation": "enable",
  "Description": "sample transit gateway",
  "DnsSupport": "enable",
  "Id": "tgw-042ae6bf7a5c126c3",
  "MulticastSupport": "disable",
  "PropagationDefaultRouteTableId": "tgw-rtb-099ba47cbbea837cc",
  "TransitGatewayCidrBlocks": ["10.0.0.0/16"],
  "VpnEcmpSupport": "enable"
}
```

AwsEc2Volume

AwsEc2VolumeObjek memberikan detail tentang EC2 volume Amazon.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk AwsEc2Volume objek. Untuk melihat deskripsi AwsEc2Volume atribut, lihat [AwsEc2 VolumeDetails](#) di Referensi AWS Security Hub API.

Contoh

```
"AwsEc2Volume": {
  "Attachments": [
    {
      "AttachTime": "2017-10-17T14:47:11Z",
      "DeleteOnTermination": true,
```

```

      "InstanceId": "i-123abc456def789g",
      "Status": "attached"
    }
  ],
  "CreateTime": "2020-02-24T15:54:30Z",
  "Encrypted": true,
  "KmsKeyId": "arn:aws:kms:us-east-1:111122223333:key/wJalrXUtnFEMI/K7MDENG/
bPxRfiCYEXAMPLEKEY",
  "Size": 80,
  "SnapshotId": "",
  "Status": "available"
}

```

AwsEc2Vpc

AwsEc2VpcObjek tersebut memberikan detail tentang EC2 VPC Amazon.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk AwsEc2Vpc objek. Untuk melihat deskripsi AwsEc2Vpc atribut, lihat [AwsEc2 VpcDetails](#) di Referensi AWS Security Hub API.

Contoh

```

"AwsEc2Vpc": {
  "CidrBlockAssociationSet": [
    {
      "AssociationId": "vpc-cidr-assoc-0dc4c852f52abda97",
      "CidrBlock": "192.0.2.0/24",
      "CidrBlockState": "associated"
    }
  ],
  "DhcpOptionsId": "dopt-4e42ce28",
  "Ipv6CidrBlockAssociationSet": [
    {
      "AssociationId": "vpc-cidr-assoc-0dc4c852f52abda97",
      "CidrBlockState": "associated",
      "Ipv6CidrBlock": "192.0.2.0/24"
    }
  ],
  "State": "available"
}

```

AwsEc2VpcEndpointService

AwsEc2VpcEndpointServiceObjek berisi rincian tentang konfigurasi layanan untuk layanan titik akhir VPC.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk AwsEc2VpcEndpointService objek. Untuk melihat deskripsi AwsEc2VpcEndpointService atribut, lihat [AwsEc2 VpcEndpointServiceDetails](#) di Referensi AWS Security Hub API.

Contoh

```
"AwsEc2VpcEndpointService": {
  "ServiceType": [
    {
      "ServiceType": "Interface"
    }
  ],
  "ServiceId": "vpce-svc-example1",
  "ServiceName": "com.amazonaws.vpce.us-east-1.vpce-svc-example1",
  "ServiceState": "Available",
  "AvailabilityZones": [
    "us-east-1"
  ],
  "AcceptanceRequired": true,
  "ManagesVpcEndpoints": false,
  "NetworkLoadBalancerArns": [
    "arn:aws:elasticloadbalancing:us-east-1:444455556666:loadbalancer/net/my-network-load-balancer/example1"
  ],
  "GatewayLoadBalancerArns": [],
  "BaseEndpointDnsNames": [
    "vpce-svc-04eec859668b51c34.us-east-1.vpce.amazonaws.com"
  ],
  "PrivateDnsName": "my-private-dns"
}
```

AwsEc2VpcPeeringConnection

AwsEc2VpcPeeringConnectionObjek memberikan rincian tentang koneksi jaringan antara dua VPCs.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk AwsEc2VpcPeeringConnection objek. Untuk melihat deskripsi

AwsEc2VpcPeeringConnection atribut, lihat [AwsEc2 VpcPeeringConnectionDetails](#) di Referensi AWS Security Hub API.

Contoh

```
"AwsEc2VpcPeeringConnection": {
  "AcceptorVpcInfo": {
    "CidrBlock": "10.0.0.0/28",
    "CidrBlockSet": [{
      "CidrBlock": "10.0.0.0/28"
    }],
    "Ipv6CidrBlockSet": [{
      "Ipv6CidrBlock": "2002::1234:abcd:ffff:c0a8:101/64"
    }],
    "OwnerId": "012345678910",
    "PeeringOptions": {
      "AllowDnsResolutionFromRemoteVpc": true,
      "AllowEgressFromLocalClassicLinkToRemoteVpc": false,
      "AllowEgressFromLocalVpcToRemoteClassicLink": true
    },
    "Region": "us-west-2",
    "VpcId": "vpc-i123456"
  },
  "ExpirationTime": "2022-02-18T15:31:53.161Z",
  "RequesterVpcInfo": {
    "CidrBlock": "192.168.0.0/28",
    "CidrBlockSet": [{
      "CidrBlock": "192.168.0.0/28"
    }],
    "Ipv6CidrBlockSet": [{
      "Ipv6CidrBlock": "2002::1234:abcd:ffff:c0a8:101/64"
    }],
    "OwnerId": "012345678910",
    "PeeringOptions": {
      "AllowDnsResolutionFromRemoteVpc": true,
      "AllowEgressFromLocalClassicLinkToRemoteVpc": false,
      "AllowEgressFromLocalVpcToRemoteClassicLink": true
    },
    "Region": "us-west-2",
    "VpcId": "vpc-i123456"
  },
  "Status": {
    "Code": "initiating-request",
    "Message": "Active"
  }
}
```

```

},
"VpcPeeringConnectionId": "pcx-1a2b3c4d"
}

```

AwsEcrsumber daya di ASFF

Berikut ini adalah contoh sintaks AWS Security Finding Format (ASFF) untuk `AwsEcr` sumber daya.

AWS Security Hub menormalkan temuan dari berbagai sumber menjadi ASFF. Untuk informasi latar belakang tentang ASFF, lihat [AWS Format Pencarian Keamanan \(ASFF\)](#).

AwsEcrContainerImage

`AwsEcrContainerImage` objek memberikan informasi tentang gambar Amazon ECR.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsEcrContainerImage` objek. Untuk melihat deskripsi `AwsEcrContainerImage` atribut, lihat [AwsEcrContainerImageDetails](#) di Referensi AWS Security Hub API.

Contoh

```

"AwsEcrContainerImage": {
  "RegistryId": "123456789012",
  "RepositoryName": "repository-name",
  "Architecture": "amd64"
  "ImageDigest":
    "sha256:a568e5c7a953fbeaa2904ac83401f93e4a076972dc1bae527832f5349cd2fb10",
  "ImageTags": ["00000000-0000-0000-0000-000000000000"],
  "ImagePublishedAt": "2019-10-01T20:06:12Z"
}

```

AwsEcrRepository

`AwsEcrRepository` objek memberikan informasi tentang repositori Amazon Elastic Container Registry.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsEcrRepository` objek. Untuk melihat deskripsi `AwsEcrRepository` atribut, lihat [AwsEcrRepositoryDetails](#) di Referensi AWS Security Hub API.

Contoh

```

"AwsEcrRepository": {

```

```

    "LifecyclePolicy": {
      "RegistryId": "123456789012",
    },
    "RepositoryName": "sample-repo",
    "Arn": "arn:aws:ecr:us-west-2:111122223333:repository/sample-repo",
    "ImageScanningConfiguration": {
      "ScanOnPush": true
    },
    "ImageTagMutability": "IMMUTABLE"
  }

```

AwsEcs sumber daya di ASFF

Berikut ini adalah contoh sintaks AWS Security Finding Format (ASFF) untuk AwsEcs sumber daya.

AWS Security Hub menormalkan temuan dari berbagai sumber menjadi ASFF. Untuk informasi latar belakang tentang ASFF, lihat [AWS Format Pencarian Keamanan \(ASFF\)](#).

AwsEcsCluster

AwsEcsClusterObjek ini memberikan detail tentang kluster Amazon Elastic Container Service.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk AwsEcsCluster objek. Untuk melihat deskripsi AwsEcsCluster atribut, lihat [AwsEcsClusterDetails](#) di Referensi AWS Security Hub API.

Contoh

```

"AwsEcsCluster": {
  "CapacityProviders": [],
  "ClusterSettings": [
    {
      "Name": "containerInsights",
      "Value": "enabled"
    }
  ],
  "Configuration": {
    "ExecuteCommandConfiguration": {
      "KmsKeyId": "kmsKeyId",
      "LogConfiguration": {
        "CloudWatchEncryptionEnabled": true,
        "CloudWatchLogGroupName": "cloudWatchLogGroupName",
        "S3BucketName": "s3BucketName",

```



```

        "S3EncryptionEnabled": true,
        "S3KeyPrefix": "s3KeyPrefix"
    },
    "Logging": "DEFAULT"
}
}
"DefaultCapacityProviderStrategy": [
    {
        "Base": 0,
        "CapacityProvider": "capacityProvider",
        "Weight": 1
    }
]
}

```

AwsEcsContainer

AwsEcsContainerObjek berisi detail tentang wadah Amazon ECS.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk AwsEcsContainer objek. Untuk melihat deskripsi AwsEcsContainer atribut, lihat [AwsEcsContainerDetails](#) di Referensi AWS Security Hub API.

Contoh

```

"AwsEcsContainer": {
    "Image": "1111111/
knotejs@sha256:356131c9fef111111111111115f4ed8de5f9dce4dc3bd34bg21846588a3",
    "MountPoints": [{
        "ContainerPath": "/mnt/etc",
        "SourceVolume": "vol-03909e9"
    }],
    "Name": "knote",
    "Privileged": true
}

```

AwsEcsService

AwsEcsServiceObjek memberikan rincian tentang layanan dalam cluster Amazon ECS.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk AwsEcsService objek. Untuk melihat deskripsi AwsEcsService atribut, lihat [AwsEcsServiceDetails](#) di Referensi AWS Security Hub API.

Contoh

```
"AwsEcsService": {
  "CapacityProviderStrategy": [
    {
      "Base": 12,
      "CapacityProvider": "",
      "Weight": ""
    }
  ],
  "Cluster": "arn:aws:ecs:us-east-1:111122223333:cluster/example-ecs-cluster",
  "DeploymentConfiguration": {
    "DeploymentCircuitBreaker": {
      "Enable": false,
      "Rollback": false
    },
    "MaximumPercent": 200,
    "MinimumHealthyPercent": 100
  },
  "DeploymentController": "",
  "DesiredCount": 1,
  "EnableEcsManagedTags": false,
  "EnableExecuteCommand": false,
  "HealthCheckGracePeriodSeconds": 1,
  "LaunchType": "FARGATE",
  "LoadBalancers": [
    {
      "ContainerName": "",
      "ContainerPort": 23,
      "LoadBalancerName": "",
      "TargetGroupArn": ""
    }
  ],
  "Name": "sample-app-service",
  "NetworkConfiguration": {
    "AwsVpcConfiguration": {
      "Subnets": [
        "Subnet-example1",
        "Subnet-example2"
      ],
      "SecurityGroups": [
        "Sg-0ce48e9a6e5b457f5"
      ],
      "AssignPublicIp": "ENABLED"
    }
  }
}
```

```

    }
  },
  "PlacementConstraints": [
    {
      "Expression": "",
      "Type": ""
    }
  ],
  "PlacementStrategies": [
    {
      "Field": "",
      "Type": ""
    }
  ],
  "PlatformVersion": "LATEST",
  "PropagateTags": "",
  "Role": "arn:aws:iam::111122223333:role/aws-servicerole/ecs.amazonaws.com/ServiceRoleForECS",
  "SchedulingStrategy": "REPLICA",
  "ServiceName": "sample-app-service",
  "ServiceArn": "arn:aws:ecs:us-east-1:111122223333:service/example-ecs-cluster/sample-app-service",
  "ServiceRegistries": [
    {
      "ContainerName": "",
      "ContainerPort": 1212,
      "Port": 1221,
      "RegistryArn": ""
    }
  ],
  "TaskDefinition": "arn:aws:ecs:us-east-1:111122223333:task-definition/example-taskdef:1"
}

```

AwsEcsTask

AwsEcsTaskObjek memberikan detail tentang tugas Amazon ECS.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk AwsEcsTask objek. Untuk melihat deskripsi AwsEcsTask atribut, lihat [AwsEcsTask](#) di Referensi AWS Security Hub API.

Contoh

```
"AwsEcsTask": {
```

```

"ClusterArn": "arn:aws:ecs:us-west-2:123456789012:task/MyCluster/1234567890123456789",
"CreatedAt": "1557134011644",
"Group": "service:fargate-service",
"StartedAt": "1557134011644",
"StartedBy": "ecs-svc/1234567890123456789",
"TaskDefinitionArn": "arn:aws:ecs:us-west-2:123456789012:task-definition/sample-
fargate:2",
"Version": 3,
"Volumes": [{
  "Name": "string",
  "Host": {
    "SourcePath": "string"
  }
}],
"Containers": {
  "Image": "11111111/
knotejs@sha256:356131c9fef111111111111115f4ed8de5f9dce4dc3bd34bg21846588a3",
  "MountPoints": [{
    "ContainerPath": "/mnt/etc",
    "SourceVolume": "vol-03909e9"
  }],
  "Name": "knote",
  "Privileged": true
}
}

```

AwsEcsTaskDefinition

AwsEcsTaskDefinitionObjek berisi rincian tentang definisi tugas. Definisi tugas menjelaskan definisi kontainer dan volume tugas Amazon Elastic Container Service.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk AwsEcsTaskDefinition objek. Untuk melihat deskripsi AwsEcsTaskDefinition atribut, lihat [AwsEcsTaskDefinitionDetails](#) di Referensi AWS Security Hub API.

Contoh

```

"AwsEcsTaskDefinition": {
  "ContainerDefinitions": [
    {
      "Command": ['ruby', 'hi.rb'],
      "Cpu": 128,
      "Essential": true,

```

```
    "HealthCheck": {
      "Command": ["CMD-SHELL", "curl -f http://localhost/ || exit 1"],
      "Interval": 10,
      "Retries": 3,
      "StartPeriod": 5,
      "Timeout": 20
    },
    "Image": "tongueroo/sinatra:latest",
    "Interactive": true,
    "Links": [],
    "LogConfiguration": {
      "LogDriver": "awslogs",
      "Options": {
        "awslogs-group": "/ecs/sinatra-hi",
        "awslogs-region": "ap-southeast-1",
        "awslogs-stream-prefix": "ecs"
      },
      "SecretOptions": []
    },
    "MemoryReservation": 128,
    "Name": "web",
    "PortMappings": [
      {
        "ContainerPort": 4567,
        "HostPort": 4567,
        "Protocol": "tcp"
      }
    ],
    "Privileged": true,
    "StartTimeout": 10,
    "StopTimeout": 100,
  }
],
"Family": "sinatra-hi",
"NetworkMode": "host",
"RequiresCompatibilities": ["EC2"],
"Status": "ACTIVE",
"TaskRoleArn": "arn:aws:iam::111122223333:role/ecsTaskExecutionRole",
}
```

AwsEfs sumber daya di ASFF

Berikut ini adalah contoh sintaks AWS Security Finding Format (ASFF) untuk AwsEfs sumber daya.

AWS Security Hub menormalkan temuan dari berbagai sumber menjadi ASFF. Untuk informasi latar belakang tentang ASFF, lihat [AWS Format Pencarian Keamanan \(ASFF\)](#).

AwsEfsAccessPoint

AwsEfsAccessPointObjek memberikan detail tentang file yang disimpan di Amazon Elastic File System.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk AwsEfsAccessPoint objek. Untuk melihat deskripsi AwsEfsAccessPoint atribut, lihat [AwsEfsAccessPointDetails](#) di Referensi AWS Security Hub API.

Contoh

```
"AwsEfsAccessPoint": {
  "AccessPointId": "fsap-05c4c0e79ba0b118a",
  "Arn": "arn:aws:elasticfilesystem:us-east-1:863155670886:access-point/fsap-05c4c0e79ba0b118a",
  "ClientToken": "AccessPointCompliant-ASk06ZZSXsEp",
  "FileSystemId": "fs-0f8137f731cb32146",
  "PosixUser": {
    "Gid": "1000",
    "SecondaryGids": ["0", "4294967295"],
    "Uid": "1234"
  },
  "RootDirectory": {
    "CreationInfo": {
      "OwnerGid": "1000",
      "OwnerUid": "1234",
      "Permissions": "777"
    },
    "Path": "/tmp/example"
  }
}
```

AwsEkssumber daya di ASFF

Berikut ini adalah contoh sintaks AWS Security Finding Format (ASFF) untuk AwsEks sumber daya.

AWS Security Hub menormalkan temuan dari berbagai sumber menjadi ASFF. Untuk informasi latar belakang tentang ASFF, lihat [AWS Format Pencarian Keamanan \(ASFF\)](#).

AwsEksCluster

AwsEksClusterObjek tersebut memberikan detail tentang cluster Amazon EKS.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk AwsEksCluster objek. Untuk melihat deskripsi AwsEksCluster atribut, lihat [AwsEksClusterDetails](#) di Referensi AWS Security Hub API.

Contoh

```
{
  "AwsEksCluster": {
    "Name": "example",
    "Arn": "arn:aws:eks:us-west-2:222222222222:cluster/example",
    "CreatedAt": 1565804921.901,
    "Version": "1.12",
    "RoleArn": "arn:aws:iam::222222222222:role/example-cluster-ServiceRole-1XWBQWYSFRE2Q",
    "ResourcesVpcConfig": {
      "EndpointPublicAccess": false,
      "SubnetIds": [
        "subnet-021345abcdef6789",
        "subnet-abcdef01234567890",
        "subnet-1234567890abcdef0"
      ],
      "SecurityGroupIds": [
        "sg-abcdef01234567890"
      ]
    },
    "Logging": {
      "ClusterLogging": [
        {
          "Types": [
            "api",
            "audit",
            "authenticator",
            "controllerManager",
            "scheduler"
          ],
          "Enabled": true
        }
      ]
    }
  }
}
```

```

    ]
  },
  "Status": "CREATING",
  "CertificateAuthorityData": {},
}
}

```

AwsElasticBeanstalk sumber daya di ASFF

Berikut ini adalah contoh sintaks AWS Security Finding Format (ASFF) untuk `AwsElasticBeanstalk` sumber daya.

AWS Security Hub menormalkan temuan dari berbagai sumber menjadi ASFF. Untuk informasi latar belakang tentang ASFF, lihat [AWS Format Pencarian Keamanan \(ASFF\)](#).

AwsElasticBeanstalkEnvironment

`AwsElasticBeanstalkEnvironment` Objek berisi rincian tentang AWS Elastic Beanstalk lingkungan.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsElasticBeanstalkEnvironment` objek. Untuk melihat deskripsi `AwsElasticBeanstalkEnvironment` atribut, lihat [AwsElasticBeanstalkEnvironmentDetails](#) di Referensi AWS Security Hub API.

Contoh

```

"AwsElasticBeanstalkEnvironment": {
  "ApplicationName": "MyApplication",
  "Cname": "myexampleapp-env.devo-2.elasticbeanstalk-internal.com",
  "DateCreated": "2021-04-30T01:38:01.090Z",
  "DateUpdated": "2021-04-30T01:38:01.090Z",
  "Description": "Example description of my awesome application",
  "EndpointUrl": "eb-dv-e-p-AWSEBLoa-abcdef01234567890-021345abcdef6789.us-east-1.elb.amazonaws.com",
  "EnvironmentArn": "arn:aws:elasticbeanstalk:us-east-1:123456789012:environment/MyApplication/myapplication-env",
  "EnvironmentId": "e-abcd1234",
  "EnvironmentLinks": [
    {
      "EnvironmentName": "myexampleapp-env",
      "LinkName": "myapplicationLink"
    }
  ]
}

```



```

],
"EnvironmentName": "myapplication-env",
"OptionSettings": [
  {
    "Namespace": "aws:elasticbeanstalk:command",
    "OptionName": "BatchSize",
    "Value": "100"
  },
  {
    "Namespace": "aws:elasticbeanstalk:command",
    "OptionName": "Timeout",
    "Value": "600"
  },
  {
    "Namespace": "aws:elasticbeanstalk:command",
    "OptionName": "BatchSizeType",
    "Value": "Percentage"
  },
  {
    "Namespace": "aws:elasticbeanstalk:command",
    "OptionName": "IgnoreHealthCheck",
    "Value": "false"
  },
  {
    "Namespace": "aws:elasticbeanstalk:application",
    "OptionName": "Application Healthcheck URL",
    "Value": "TCP:80"
  }
],
"PlatformArn": "arn:aws:elasticbeanstalk:us-east-1::platform/Tomcat 8 with Java 8
running on 64bit Amazon Linux/2.7.7",
"SolutionStackName": "64bit Amazon Linux 2017.09 v2.7.7 running Tomcat 8 Java 8",
"Status": "Ready",
"Tier": {
  "Name": "WebServer"
  "Type": "Standard"
  "Version": "1.0"
},
"VersionLabel": "Sample Application"
}

```

AwsElasticSearchsumber daya di ASFF

Berikut ini adalah contoh sintaks AWS Security Finding Format (ASFF) untuk AwsElasticSearch sumber daya.

AWS Security Hub menormalkan temuan dari berbagai sumber menjadi ASFF. Untuk informasi latar belakang tentang ASFF, lihat [AWS Format Pencarian Keamanan \(ASFF\)](#).

AwsElasticSearchDomain

AwsElasticSearchDomainObjek memberikan detail tentang domain OpenSearch Layanan Amazon.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk AwsElasticSearchDomain objek. Untuk melihat deskripsi AwsElasticSearchDomain atribut, lihat [AwsElasticSearchDomainDetails](#) di Referensi AWS Security Hub API.

Contoh

```
"AwsElasticSearchDomain": {
  "AccessPolicies": "string",
  "DomainStatus": {
    "DomainId": "string",
    "DomainName": "string",
    "Endpoint": "string",
    "Endpoints": {
      "string": "string"
    }
  },
  "DomainEndpointOptions": {
    "EnforceHTTPS": boolean,
    "TLSSecurityPolicy": "string"
  },
  "ElasticsearchClusterConfig": {
    "DedicatedMasterCount": number,
    "DedicatedMasterEnabled": boolean,
    "DedicatedMasterType": "string",
    "InstanceCount": number,
    "InstanceType": "string",
    "ZoneAwarenessConfig": {
      "AvailabilityZoneCount": number
    },
    "ZoneAwarenessEnabled": boolean
  }
}
```

```
{,
"ElasticsearchVersion": "string",
"EncryptionAtRestOptions": {
    "Enabled": boolean,
    "KmsKeyId": "string"
},
"LogPublishingOptions": {
    "AuditLogs": {
        "CloudWatchLogsLogGroupArn": "string",
        "Enabled": boolean
    },
    "IndexSlowLogs": {
        "CloudWatchLogsLogGroupArn": "string",
        "Enabled": boolean
    },
    "SearchSlowLogs": {
        "CloudWatchLogsLogGroupArn": "string",
        "Enabled": boolean
    }
},
"NodeToNodeEncryptionOptions": {
    "Enabled": boolean
},
"ServiceSoftwareOptions": {
    "AutomatedUpdateDate": "string",
    "Cancellable": boolean,
    "CurrentVersion": "string",
    "Description": "string",
    "NewVersion": "string",
    "UpdateAvailable": boolean,
    "UpdateStatus": "string"
},
"VPCOptions": {
    "AvailabilityZones": [
        "string"
    ],
    "SecurityGroupIds": [
        "string"
    ],
    "SubnetIds": [
        "string"
    ],
    "VPCId": "string"
}
```

```
}
```

AwsElb sumber daya di ASFF

Berikut ini adalah contoh sintaks AWS Security Finding Format (ASFF) untuk AwsElb sumber daya.

AWS Security Hub menormalkan temuan dari berbagai sumber menjadi ASFF. Untuk informasi latar belakang tentang ASFF, lihat [AWS Format Pencarian Keamanan \(ASFF\)](#).

AwsElbLoadBalancer

AwsElbLoadBalancerObjek berisi rincian tentang Classic Load Balancer.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk AwsElbLoadBalancer objek. Untuk melihat deskripsi AwsElbLoadBalancer atribut, lihat [AwsElbLoadBalancerDetails](#) di Referensi AWS Security Hub API.

Contoh

```
"AwsElbLoadBalancer": {
  "AvailabilityZones": ["us-west-2a"],
  "BackendServerDescriptions": [
    {
      "InstancePort": 80,
      "PolicyNames": ["doc-example-policy"]
    }
  ],
  "CanonicalHostedZoneName": "Z3DZXE0EXAMPLE",
  "CanonicalHostedZoneNameID": "my-load-balancer-444455556666.us-
west-2.elb.amazonaws.com",
  "CreatedTime": "2020-08-03T19:22:44.637Z",
  "DnsName": "my-load-balancer-444455556666.us-west-2.elb.amazonaws.com",
  "HealthCheck": {
    "HealthyThreshold": 2,
    "Interval": 30,
    "Target": "HTTP:80/png",
    "Timeout": 3,
    "UnhealthyThreshold": 2
  },
  "Instances": [
    {
      "InstanceId": "i-example"
    }
  ],
}
```

```

"ListenerDescriptions": [
  {
    "Listener": {
      "InstancePort": 443,
      "InstanceProtocol": "HTTPS",
      "LoadBalancerPort": 443,
      "Protocol": "HTTPS",
      "SslCertificateId": "arn:aws:iam::444455556666:server-certificate/my-
server-cert"
    },
    "PolicyNames": ["ELBSecurityPolicy-TLS-1-2-2017-01"]
  }
],
"LoadBalancerAttributes": {
  "AccessLog": {
    "EmitInterval": 60,
    "Enabled": true,
    "S3BucketName": "amzn-s3-demo-bucket",
    "S3BucketPrefix": "doc-example-prefix"
  },
  "ConnectionDraining": {
    "Enabled": false,
    "Timeout": 300
  },
  "ConnectionSettings": {
    "IdleTimeout": 30
  },
  "CrossZoneLoadBalancing": {
    "Enabled": true
  },
  "AdditionalAttributes": [{
    "Key": "elb.http.desyncmitigationmode",
    "Value": "strictest"
  }]
},
"LoadBalancerName": "example-load-balancer",
"Policies": {
  "AppCookieStickinessPolicies": [
    {
      "CookieName": "",
      "PolicyName": ""
    }
  ],

```

```

    "LbCookieStickinessPolicies": [
      {
        "CookieExpirationPeriod": 60,
        "PolicyName": "my-example-cookie-policy"
      }
    ],
    "OtherPolicies": [
      "my-PublicKey-policy",
      "my-authentication-policy",
      "my-SSLNegotiation-policy",
      "my-ProxyProtocol-policy",
      "ELBSecurityPolicy-2015-03"
    ]
  },
  "Scheme": "internet-facing",
  "SecurityGroups": ["sg-example"],
  "SourceSecurityGroup": {
    "GroupName": "my-elb-example-group",
    "OwnerAlias": "444455556666"
  },
  "Subnets": ["subnet-example"],
  "VpcId": "vpc-a01106c2"
}

```

AwsElbv2LoadBalancer

AwsElbv2LoadBalancerObjek memberikan informasi tentang penyeimbang beban.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk AwsElbv2LoadBalancer objek. Untuk melihat deskripsi AwsElbv2LoadBalancer atribut, lihat [AwsElbv2LoadBalancerDetails](#) di Referensi AWS Security Hub API.

Contoh

```

"AwsElbv2LoadBalancer": {
  "AvailabilityZones": {
    "SubnetId": "string",
    "ZoneName": "string"
  },
  "CanonicalHostedZoneId": "string",
  "CreatedTime": "string",
  "DNSName": "string",
  "IpAddressType": "string",

```

```

        "LoadBalancerAttributes": [
            {
                "Key": "string",
                "Value": "string"
            }
        ],
        "Scheme": "string",
        "SecurityGroups": [ "string" ],
        "State": {
            "Code": "string",
            "Reason": "string"
        },
        "Type": "string",
        "VpcId": "string"
    }

```

AwsEventBridgesumber daya di ASFF

Berikut ini adalah contoh sintaks AWS Security Finding Format (ASFF) untuk `AwsEventBridge` sumber daya.

AWS Security Hub menormalkan temuan dari berbagai sumber menjadi ASFF. Untuk informasi latar belakang tentang ASFF, lihat [AWS Format Pencarian Keamanan \(ASFF\)](#).

AwsEventSchemasRegistry

`AwsEventSchemasRegistry` objek memberikan informasi tentang registri EventBridge skema Amazon. Skema mendefinisikan struktur peristiwa yang dikirim ke EventBridge Registries skema adalah wadah yang mengumpulkan dan secara logis mengelompokkan skema Anda.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsEventSchemasRegistry` objek. Untuk melihat deskripsi `AwsEventSchemasRegistry` atribut, lihat [AwsEventSchemasRegistry](#) di Referensi AWS Security Hub API.

Contoh

```

"AwsEventSchemasRegistry": {
    "Description": "This is an example event schema registry.",
    "RegistryArn": "arn:aws:schemas:us-east-1:123456789012:registry/schema-registry",
    "RegistryName": "schema-registry"
}

```

AwsEventsEndpoint

AwsEventsEndpointObjek memberikan informasi tentang titik akhir EventBridge global Amazon. Titik akhir dapat meningkatkan ketersediaan aplikasi Anda dengan membuatnya toleran terhadap kesalahan regional.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk AwsEventsEndpoint objek. Untuk melihat deskripsi AwsEventsEndpoint atribut, lihat [AwsEventsEndpointDetails](#) di Referensi AWS Security Hub API.

Contoh

```
"AwsEventsEndpoint": {
  "Arn": "arn:aws:events:us-east-1:123456789012:endpoint/my-endpoint",
  "Description": "This is a sample endpoint.",
  "EndpointId": "04k1exajoy.veo",
  "EndpointUrl": "https://04k1exajoy.veo.endpoint.events.amazonaws.com",
  "EventBuses": [
    {
      "EventBusArn": "arn:aws:events:us-east-1:123456789012:event-bus/default"
    },
    {
      "EventBusArn": "arn:aws:events:us-east-2:123456789012:event-bus/default"
    }
  ],
  "Name": "my-endpoint",
  "ReplicationConfig": {
    "State": "ENABLED"
  },
  "RoleArn": "arn:aws:iam::123456789012:role/service-role/Amazon_EventBridge_Invoke_Event_Bus_1258925394",
  "RoutingConfig": {
    "FailoverConfig": {
      "Primary": {
        "HealthCheck": "arn:aws:route53:::healthcheck/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
      },
      "Secondary": {
        "Route": "us-east-2"
      }
    }
  },
  "State": "ACTIVE"
}
```


}

AwsEventsEventbus

AwsEventsEventbusObjek memberikan informasi tentang titik akhir EventBridge global Amazon. Titik akhir dapat meningkatkan ketersediaan aplikasi Anda dengan membuatnya toleran terhadap kesalahan regional.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk AwsEventsEventbus objek. Untuk melihat deskripsi AwsEventsEventbus atribut, lihat [AwsEventsEventbusDetails](#) di Referensi AWS Security Hub API.

Contoh

```
"AwsEventsEventbus":
  "Arn": "arn:aws:events:us-east-1:123456789012:event-bus/my-event-bus",
  "Name": "my-event-bus",
  "Policy": "{\n  \"Version\": \"2012-10-17\",\n  \"Statement\": [\n    {\n      \"Sid\":\n        \"AllowAllAccountsFromOrganizationToPutEvents\",\n      \"Effect\": \"Allow\",\n      \"Principal\": \"*\",\n      \"Action\": \"events:PutEvents\",\n      \"Resource\":\n        \"arn:aws:events:us-east-1:123456789012:event-bus/my-event-bus\",\n      \"Condition\": {\n        \"StringEquals\": {\n          \"aws:PrincipalOrgID\": \"o-ki7yjt看5\"\n        }\n      },\n      \"Sid\":\n        \"AllowAccountToManageRulesTheyCreated\",\n      \"Effect\": \"Allow\",\n      \"Principal\": {\n        \"AWS\":\n          \"arn:aws:iam::123456789012:root\"\n      },\n      \"Action\": [\n        \"events:PutRule\",\n        \"events:PutTargets\",\n        \"events>DeleteRule\",\n        \"events:RemoveTargets\",\n        \"events:DisableRule\",\n        \"events:EnableRule\",\n        \"events:TagResource\",\n        \"events:UntagResource\",\n        \"events:DescribeRule\",\n        \"events>ListTargetsByRule\",\n        \"events>ListTagsForResource\"\n      ],\n      \"Resource\": \"arn:aws:events:us-east-1:123456789012:rule/my-event-bus\",\n      \"Condition\": {\n        \"StringEqualsIfExists\": {\n          \"events:creatorAccount\": \"123456789012\"\n        }\n      }\n    }\n  ]\n}"
```

AwsGuardDutysumber daya di ASFF

Berikut ini adalah contoh sintaks AWS Security Finding Format (ASFF) untuk AwsGuardDuty sumber daya.

AWS Security Hub menormalkan temuan dari berbagai sumber menjadi ASFF. Untuk informasi latar belakang tentang ASFF, lihat [AWS Format Pencarian Keamanan \(ASFF\)](#).

AwsGuardDutyDetector

AwsGuardDutyDetectorObjek tersebut memberikan informasi tentang GuardDuty detektor Amazon. Detektor adalah objek yang mewakili GuardDuty layanan. Detektor diperlukan GuardDuty untuk menjadi operasional.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk AwsGuardDutyDetector objek. Untuk melihat deskripsi AwsGuardDutyDetector atribut, lihat [AwsGuardDutyDetector](#) di Referensi AWS Security Hub API.

Contoh

```
"AwsGuardDutyDetector": {
  "FindingPublishingFrequency": "SIX_HOURS",
  "ServiceRole": "arn:aws:iam::123456789012:role/aws-service-role/
guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty",
  "Status": "ENABLED",
  "DataSources": {
    "CloudTrail": {
      "Status": "ENABLED"
    },
    "DnsLogs": {
      "Status": "ENABLED"
    },
    "FlowLogs": {
      "Status": "ENABLED"
    },
    "S3Logs": {
      "Status": "ENABLED"
    },
    "Kubernetes": {
      "AuditLogs": {
        "Status": "ENABLED"
      }
    },
    "MalwareProtection": {
      "ScanEc2InstanceWithFindings": {
        "EbsVolumes": {
          "Status": "ENABLED"
        }
      },
      "ServiceRole": "arn:aws:iam::123456789012:role/aws-service-role/malware-
protection.guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDutyMalwareProtection"
```

```

    }
  }
}

```

AwsIam sumber daya di ASFF

Berikut ini adalah contoh sintaks AWS Security Finding Format (ASFF) untuk `AwsIam` sumber daya.

AWS Security Hub menormalkan temuan dari berbagai sumber menjadi ASFF. Untuk informasi latar belakang tentang ASFF, lihat [AWS Format Pencarian Keamanan \(ASFF\)](#).

AwsIamAccessKey

`AwsIamAccessKey` objek berisi rincian tentang kunci akses IAM yang terkait dengan temuan.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsIamAccessKey` objek. Untuk melihat deskripsi `AwsIamAccessKey` atribut, lihat [AwsIamAccessKeyDetails](#) di Referensi AWS Security Hub API.

Contoh

```

"AwsIamAccessKey": {
    "AccessKeyId": "string",
    "AccountId": "string",
    "CreatedAt": "string",
    "PrincipalId": "string",
    "PrincipalName": "string",
    "PrincipalType": "string",
    "SessionContext": {
        "Attributes": {
            "CreationDate": "string",
            "MfaAuthenticated": boolean
        },
        "SessionIssuer": {
            "AccountId": "string",
            "Arn": "string",
            "PrincipalId": "string",
            "Type": "string",
            "UserName": "string"
        }
    },
    "Status": "string"
}

```

```
}
```

AwsIamGroup

AwsIamGroupObjek berisi rincian tentang grup IAM.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk AwsIamGroup objek. Untuk melihat deskripsi AwsIamGroup atribut, lihat [AwslamGroupDetails](#) di Referensi AWS Security Hub API.

Contoh

```
"AwsIamGroup": {
  "AttachedManagedPolicies": [
    {
      "PolicyArn": "arn:aws:iam::aws:policy/ExampleManagedAccess",
      "PolicyName": "ExampleManagedAccess",
    }
  ],
  "CreateDate": "2020-04-28T14:08:37.000Z",
  "GroupId": "AGPA4TPS3VLP7QEXAMPLE",
  "GroupName": "Example_User_Group",
  "GroupPolicyList": [
    {
      "PolicyName": "ExampleGroupPolicy"
    }
  ],
  "Path": "/"
}
```

AwsIamPolicy

AwsIamPolicyObjek mewakili kebijakan izin IAM.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk AwsIamPolicy objek. Untuk melihat deskripsi AwsIamPolicy atribut, lihat [AwslamPolicyDetails](#) di Referensi AWS Security Hub API.

Contoh

```
"AwsIamPolicy": {
```

```

    "AttachmentCount": 1,
    "CreateDate": "2017-09-14T08:17:29.000Z",
    "DefaultVersionId": "v1",
    "Description": "Example IAM policy",
    "IsAttachable": true,
    "Path": "/",
    "PermissionsBoundaryUsageCount": 5,
    "PolicyId": "ANPAJ2UCCR6DPCEXAMPLE",
    "PolicyName": "EXAMPLE-MANAGED-POLICY",
    "PolicyVersionList": [
      {
        "VersionId": "v1",
        "IsDefaultVersion": true,
        "CreateDate": "2017-09-14T08:17:29.000Z"
      }
    ],
    "UpdateDate": "2017-09-14T08:17:29.000Z"
  }
}

```

AwsIamRole

AwsIamRoleObjek berisi informasi tentang peran IAM, termasuk semua kebijakan peran.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk AwsIamRole objek. Untuk melihat deskripsi AwsIamRole atribut, lihat [AwsIamRoleDetails](#) di Referensi AWS Security Hub API.

Contoh

```

"AwsIamRole": {
  "AssumeRolePolicyDocument": "{ 'Version': '2012-10-17', 'Statement': [{ 'Effect': 'Allow', 'Action': 'sts:AssumeRole' } ] }",
  "AttachedManagedPolicies": [
    {
      "PolicyArn": "arn:aws:iam::aws:policy/ExamplePolicy1",
      "PolicyName": "Example policy 1"
    },
    {
      "PolicyArn": "arn:aws:iam::444455556666:policy/ExamplePolicy2",
      "PolicyName": "Example policy 2"
    }
  ],
  "CreateDate": "2020-03-14T07:19:14.000Z",
  "InstanceProfileList": [

```

```

    {
      "Arn": "arn:aws:iam::333333333333:ExampleProfile",
      "CreateDate": "2020-03-11T00:02:27Z",
      "InstanceProfileId": "AIPAIXEU4NUHUPEXAMPLE",
      "InstanceProfileName": "ExampleInstanceProfile",
      "Path": "/",
      "Roles": [
        {
          "Arn": "arn:aws:iam::444455556666:role/example-role",
          "AssumeRolePolicyDocument": "",
          "CreateDate": "2020-03-11T00:02:27Z",
          "Path": "/",
          "RoleId": "AR0AJ520TH4H7LEXAMPLE",
          "RoleName": "example-role",
        }
      ]
    },
    "MaxSessionDuration": 3600,
    "Path": "/",
    "PermissionsBoundary": {
      "PermissionsBoundaryArn": "arn:aws:iam::aws:policy/AdministratorAccess",
      "PermissionsBoundaryType": "PermissionsBoundaryPolicy"
    },
    "RoleId": "AR0A4TPS3VLEXAMPLE",
    "RoleName": "BONESBootstrapHydra-OverbridgeOpsFunctionsLambda",
    "RolePolicyList": [
      {
        "PolicyName": "Example role policy"
      }
    ]
  }
}

```

AwsIamUser

`AwsIamUser` objek memberikan informasi tentang pengguna.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsIamUser` objek. Untuk melihat deskripsi `AwsIamUser` atribut, lihat [AwsIamUserDetails](#) di Referensi AWS Security Hub API.

Contoh

```
"AwsIamUser": {
```

```

    "AttachedManagedPolicies": [
      {
        "PolicyName": "ExamplePolicy",
        "PolicyArn": "arn:aws:iam::aws:policy/ExampleAccess"
      }
    ],
    "CreateDate": "2018-01-26T23:50:05.000Z",
    "GroupList": [],
    "Path": "/",
    "PermissionsBoundary" : {
      "PermissionsBoundaryArn" : "arn:aws:iam::aws:policy/AdministratorAccess",
      "PermissionsBoundaryType" : "PermissionsBoundaryPolicy"
    },
    "UserId": "AIDACKCEVSQ6C2EXAMPLE",
    "UserName": "ExampleUser",
    "UserPolicyList": [
      {
        "PolicyName": "InstancePolicy"
      }
    ]
  }
}

```

AwsKinesis sumber daya di ASFF

Berikut ini adalah contoh sintaks AWS Security Finding Format (ASFF) untuk AwsKinesis sumber daya.

AWS Security Hub menormalkan temuan dari berbagai sumber menjadi ASFF. Untuk informasi latar belakang tentang ASFF, lihat [AWS Format Pencarian Keamanan \(ASFF\)](#).

AwsKinesisStream

AwsKinesisStreamObjek ini memberikan detail tentang Amazon Kinesis Data Streams.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk AwsKinesisStream objek. Untuk melihat deskripsi AwsKinesisStream atribut, lihat [AwsKinesisStreamDetails](#) di Referensi AWS Security Hub API.

Contoh

```

"AwsKinesisStream": {
  "Name": "test-vir-kinesis-stream",

```

```

"Arn": "arn:aws:kinesis:us-east-1:293279581038:stream/test-vir-kinesis-stream",
"RetentionPeriodHours": 24,
"ShardCount": 2,
"StreamEncryption": {
  "EncryptionType": "KMS",
  "KeyId": "arn:aws:kms:us-east-1:293279581038:key/849cf029-4143-4c59-91f8-
ea76007247eb"
}
}

```

AwsKms sumber daya di ASFF

Berikut ini adalah contoh sintaks AWS Security Finding Format (ASFF) untuk AwsKms sumber daya.

AWS Security Hub menormalkan temuan dari berbagai sumber menjadi ASFF. Untuk informasi latar belakang tentang ASFF, lihat [AWS Format Pencarian Keamanan \(ASFF\)](#).

AwsKmsKey

AwsKmsKeyObjek memberikan rincian tentang file AWS KMS key.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk AwsKmsKey objek. Untuk melihat deskripsi AwsKmsKey atribut, lihat [AwsKmsKeyDetails](#) di Referensi AWS Security Hub API.

Contoh

```

"AwsKmsKey": {
  "AWSAccountId": "string",
  "CreationDate": "string",
  "Description": "string",
  "KeyId": "string",
  "KeyManager": "string",
  "KeyRotationStatus": boolean,
  "KeyState": "string",
  "Origin": "string"
}

```

AwsLambda

Berikut ini adalah contoh sintaks AWS Security Finding Format (ASFF) untuk AwsLambda sumber daya.

AWS Security Hub menormalkan temuan dari berbagai sumber menjadi ASFF. Untuk informasi latar belakang tentang ASFF, lihat [AWS Format Pencarian Keamanan \(ASFF\)](#).

AwsLambdaFunction

AwsLambdaFunctionObjek memberikan rincian tentang konfigurasi fungsi Lambda.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsLambdaFunction` objek. Untuk melihat deskripsi `AwsLambdaFunction` atribut, lihat [AwsLambdaFunctionDetails](#) di Referensi AWS Security Hub API.

Contoh

```
"AwsLambdaFunction": {
  "Architectures": [
    "x86_64"
  ],
  "Code": {
    "S3Bucket": "amzn-s3-demo-bucket",
    "S3Key": "samplekey",
    "S3ObjectVersion": "2",
    "ZipFile": "myzip.zip"
  },
  "CodeSha256": "1111111111111111abcdef",
  "DeadLetterConfig": {
    "TargetArn": "arn:aws:lambda:us-east-2:123456789012:queue:myqueue:2"
  },
  "Environment": {
    "Variables": {
      "Stage": "foobar"
    },
    "Error": {
      "ErrorCode": "Sample-error-code",
      "Message": "Caller principal is a manager."
    }
  },
  "FunctionName": "CheckOut",
  "Handler": "main.py:lambda_handler",
  "KmsKeyArn": "arn:aws:kms:us-west-2:123456789012:key/mykey",
  "LastModified": "2001-09-11T09:00:00Z",
  "Layers": {
    "Arn": "arn:aws:lambda:us-east-2:123456789012:layer:my-layer:3",
    "CodeSize": 169
  }
}
```

```

    },
    "PackageType": "Zip",
    "RevisionId": "23",
    "Role": "arn:aws:iam::123456789012:role/Accounting-Role",
    "Runtime": "go1.7",
    "Timeout": 15,
    "TracingConfig": {
        "Mode": "Active"
    },
    },
    "Version": "$LATEST",
    "VpcConfig": {
        "SecurityGroupIds": ["sg-085912345678492fb", "sg-08591234567bdgdc"],
        "SubnetIds": ["subnet-071f712345678e7c8", "subnet-07fd123456788a036"]
    },
    },
    "MasterArn": "arn:aws:lambda:us-east-2:123456789012:\$LATEST",
    "MemorySize": 2048
}

```

AwsLambdaLayerVersion

AwsLambdaLayerVersionObjek memberikan rincian tentang versi lapisan Lambda.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk AwsLambdaLayerVersion objek. Untuk melihat deskripsi AwsLambdaLayerVersion atribut, lihat [AwsLambdaLayerVersionDetails](#) di Referensi AWS Security Hub API.

Contoh

```

"AwsLambdaLayerVersion": {
    "Version": 2,
    "CompatibleRuntimes": [
        "java8"
    ],
    "CreateDate": "2019-10-09T22:02:00.274+0000"
}

```

AwsMsk sumber daya di ASFF

Berikut ini adalah contoh sintaks AWS Security Finding Format (ASFF) untuk AwsMsk sumber daya.

AWS Security Hub menormalkan temuan dari berbagai sumber menjadi ASFF. Untuk informasi latar belakang tentang ASFF, lihat [AWS Format Pencarian Keamanan \(ASFF\)](#).

AwsMskCluster

`AwsMskClusterObjek` tersebut memberikan informasi tentang cluster Amazon Managed Streaming for Apache Kafka (Amazon MSK).

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsMskCluster` objek. Untuk melihat deskripsi `AwsMskCluster` atribut, lihat [AwsMskClusterDetails](#) di Referensi AWS Security Hub API.

Contoh

```
"AwsMskCluster": {
  "ClusterInfo": {
    "ClientAuthentication": {
      "Sasl": {
        "Scram": {
          "Enabled": true
        },
        "Iam": {
          "Enabled": true
        }
      },
      "Tls": {
        "CertificateAuthorityArnList": [],
        "Enabled": false
      },
      "Unauthenticated": {
        "Enabled": false
      }
    },
    "ClusterName": "my-cluster",
    "CurrentVersion": "K2PWKAKR8XB7XF",
    "EncryptionInfo": {
      "EncryptionAtRest": {
        "DataVolumeKMSKeyId": "arn:aws:kms:us-east-1:123456789012:key/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
      },
      "EncryptionInTransit": {
        "ClientBroker": "TLS",
        "InCluster": true
      }
    },
    "EnhancedMonitoring": "PER_TOPIC_PER_BROKER",
```

```

      "NumberOfBrokerNodes": 3
    }
  }
}

```

AwsNetworkFirewall sumber daya di ASFF

Berikut ini adalah contoh sintaks AWS Security Finding Format (ASFF) untuk `AwsNetworkFirewall` sumber daya.

AWS Security Hub menormalkan temuan dari berbagai sumber menjadi ASFF. Untuk informasi latar belakang tentang ASFF, lihat [AWS Format Pencarian Keamanan \(ASFF\)](#).

AwsNetworkFirewallFirewall

`AwsNetworkFirewallFirewallObjek` berisi rincian tentang AWS Network Firewall firewall.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsNetworkFirewallFirewall` objek. Untuk melihat deskripsi `AwsNetworkFirewallFirewall` atribut, lihat [AwsNetworkFirewallFirewallDetails](#) di Referensi AWS Security Hub API.

Contoh

```

"AwsNetworkFirewallFirewall": {
  "DeleteProtection": false,
  "FirewallArn": "arn:aws:network-firewall:us-east-1:024665936331:firewall/testfirewall",
  "FirewallPolicyArn": "arn:aws:network-firewall:us-east-1:444455556666:firewall-policy/InitialFirewall",
  "FirewallId": "dea7d8e9-ae38-4a8a-b022-672a830a99fa",
  "FirewallName": "testfirewall",
  "FirewallPolicyChangeProtection": false,
  "SubnetChangeProtection": false,
  "SubnetMappings": [
    {
      "SubnetId": "subnet-0183481095e588cdc"
    },
    {
      "SubnetId": "subnet-01f518fad1b1c90b0"
    }
  ],
  "VpcId": "vpc-40e83c38"
}

```

```
}
```

AwsNetworkFirewallFirewallPolicy

AwsNetworkFirewallFirewallPolicyObjek memberikan rincian tentang kebijakan firewall. Kebijakan firewall mendefinisikan perilaku firewall jaringan.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk AwsNetworkFirewallFirewallPolicy objek. Untuk melihat deskripsi AwsNetworkFirewallFirewallPolicy atribut, lihat [AwsNetworkFirewallFirewallPolicyDetails](#) di Referensi AWS Security Hub API.

Contoh

```
"AwsNetworkFirewallFirewallPolicy": {
  "FirewallPolicy": {
    "StatefulRuleGroupReferences": [
      {
        "ResourceArn": "arn:aws:network-firewall:us-east-1:444455556666:stateful-
rulegroup/PatchesOnly"
      }
    ],
    "StatelessDefaultActions": [ "aws:forward_to_sfe" ],
    "StatelessFragmentDefaultActions": [ "aws:forward_to_sfe" ],
    "StatelessRuleGroupReferences": [
      {
        "Priority": 1,
        "ResourceArn": "arn:aws:network-firewall:us-east-1:444455556666:stateless-
rulegroup/Stateless-1"
      }
    ]
  },
  "FirewallPolicyArn": "arn:aws:network-firewall:us-east-1:444455556666:firewall-
policy/InitialFirewall",
  "FirewallPolicyId": "9ceeda22-6050-4048-a0ca-50ce47f0cc65",
  "FirewallPolicyName": "InitialFirewall",
  "Description": "Initial firewall"
}
```

AwsNetworkFirewallRuleGroup

AwsNetworkFirewallRuleGroupObjek memberikan rincian tentang kelompok AWS Network Firewall aturan. Kelompok aturan digunakan untuk memeriksa dan mengontrol lalu lintas jaringan.

Kelompok aturan stateless berlaku untuk paket individu. Kelompok aturan stateful berlaku untuk paket dalam konteks arus lalu lintas mereka.

Grup aturan direferensikan dalam kebijakan firewall.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsNetworkFirewallRuleGroup` objek. Untuk melihat deskripsi `AwsNetworkFirewallRuleGroup` atribut, lihat [AwsNetworkFirewallRuleGroupDetails](#) di Referensi AWS Security Hub API.

Contoh - kelompok aturan tanpa kewarganegaraan

```
"AwsNetworkFirewallRuleGroup": {
  "Capacity": 600,
  "RuleGroupArn": "arn:aws:network-firewall:us-east-1:444455556666:stateless-
rulegroup/Stateless-1",
  "RuleGroupId": "fb13c4df-b6da-4c1e-91ec-84b7a5487493",
  "RuleGroupName": "Stateless-1"
  "Description": "Example of a stateless rule group",
  "Type": "STATELESS",
  "RuleGroup": {
    "RulesSource": {
      "StatelessRulesAndCustomActions": {
        "CustomActions": [],
        "StatelessRules": [
          {
            "Priority": 1,
            "RuleDefinition": {
              "Actions": [
                "aws:pass"
              ],
              "MatchAttributes": {
                "DestinationPorts": [
                  {
                    "FromPort": 443,
                    "ToPort": 443
                  }
                ],
                "Destinations": [
                  {
                    "AddressDefinition": "192.0.2.0/24"
                  }
                ]
              }
            }
          }
        ]
      }
    }
  }
}
```

```
        "Protocols": [
            6
        ],
        "SourcePorts": [
            {
                "FromPort": 0,
                "ToPort": 65535
            }
        ],
        "Sources": [
            {
                "AddressDefinition": "198.51.100.0/24"
            }
        ]
    }
}
}
```

Contoh - kelompok aturan stateful

```
"AwsNetworkFirewallRuleGroup": {
  "Capacity": 100,
  "RuleGroupArn": "arn:aws:network-firewall:us-east-1:444455556666:stateful-
rulegroup/tupletest",
  "RuleGroupId": "38b71c12-da80-4643-a6c5-03337f8933e0",
  "RuleGroupName": "ExampleRuleGroup",
  "Description": "Example of a stateful rule group",
  "Type": "STATEFUL",
  "RuleGroup": {
    "RuleSource": {
      "StatefulRules": [
        {
          "Action": "PASS",
          "Header": {
            "Destination": "Any",
            "DestinationPort": "443",
            "Direction": "ANY",
            "Protocol": "TCP",
```

```

        "Source": "Any",
        "SourcePort": "Any"
      },
      "RuleOptions": [
        {
          "Keyword": "sid:1"
        }
      ]
    }
  ]
}

```

Berikut ini adalah daftar contoh nilai yang valid untuk `AwsNetworkFirewallRuleGroup` atribut:

- **Action**

Nilai yang valid: PASS | DROP | ALERT

- **Protocol**

Nilai yang valid: IP TCP | UDP | ICMP | HTTP | FTP | TLS SMB | DNS | DCERPC | SSH | SMTP | IMAP | MSN | KRB5 | IKEV2 | TFTP | NTP | DHCP

- **Flags**

Nilai yang valid: FIN SYN | RST | PSH | ACK | URG | ECE | CWR

- **Masks**

Nilai yang valid: FIN SYN | RST | PSH | ACK | URG | ECE | CWR

AwsOpenSearchServicesumber daya di ASFF

Berikut ini adalah contoh sintaks AWS Security Finding Format (ASFF) untuk `AwsOpenSearchService` sumber daya.

AWS Security Hub menormalkan temuan dari berbagai sumber menjadi ASFF. Untuk informasi latar belakang tentang ASFF, lihat [AWS Format Pencarian Keamanan \(ASFF\)](#).

AwsOpenSearchServiceDomain

AwsOpenSearchServiceDomainObjek berisi informasi tentang domain OpenSearch Layanan Amazon.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk AwsOpenSearchServiceDomain objek. Untuk melihat deskripsi AwsOpenSearchServiceDomain atribut, lihat [AwsOpenSearchServiceDomainDetails](#) di Referensi AWS Security Hub API.

Contoh

```
"AwsOpenSearchServiceDomain": {
  "AccessPolicies": "IAM_Id",
  "AdvancedSecurityOptions": {
    "Enabled": true,
    "InternalUserDatabaseEnabled": true,
    "MasterUserOptions": {
      "MasterUserArn": "arn:aws:iam::123456789012:user/third-master-use",
      "MasterUserName": "third-master-use",
      "MasterUserPassword": "some-password"
    }
  },
  "Arn": "arn:aws:Opensearch:us-east-1:111122223333:somedomain",
  "ClusterConfig": {
    "InstanceType": "c5.large.search",
    "InstanceCount": 1,
    "DedicatedMasterEnabled": true,
    "ZoneAwarenessEnabled": false,
    "ZoneAwarenessConfig": {
      "AvailabilityZoneCount": 2
    },
    "DedicatedMasterType": "c5.large.search",
    "DedicatedMasterCount": 3,
    "WarmEnabled": true,
    "WarmCount": 3,
    "WarmType": "ultrawarm1.large.search"
  },
  "DomainEndpoint": "https://es-2021-06-23t17-04-qowmgghud5vofgb5e4wmi.eu-central-1.es.amazonaws.com",
  "DomainEndpointOptions": {
    "EnforceHTTPS": false,
    "TLSSecurityPolicy": "Policy-Min-TLS-1-0-2019-07",
```

```

    "CustomEndpointCertificateArn": "arn:aws:acm:us-east-1:111122223333:certificate/bda1bff1-79c0-49d0-abe6-50a15a7477d4",
    "CustomEndpointEnabled": true,
    "CustomEndpoint": "example.com"
  },
  "DomainEndpoints": {
    "vpc": "vpc-endpoint-h2dsd34efgyghrtguk5gt6j2foh4.us-east-1.es.amazonaws.com"
  },
  "DomainName": "my-domain",
  "EncryptionAtRestOptions": {
    "Enabled": false,
    "KmsKeyId": "1a2a3a4-1a2a-3a4a-5a6a-1a2a3a4a5a6a"
  },
  "EngineVersion": "7.1",
  "Id": "123456789012",
  "LogPublishingOptions": {
    "IndexSlowLogs": {
      "CloudWatchLogsLogGroupArn": "arn:aws:logs:us-east-1:111122223333:log-group:/aws/aes/domains/es-index-slow-logs",
      "Enabled": true
    },
    "SearchSlowLogs": {
      "CloudWatchLogsLogGroupArn": "arn:aws:logs:us-east-1:111122223333:log-group:/aws/aes/domains/es-slow-logs",
      "Enabled": true
    },
    "AuditLogs": {
      "CloudWatchLogsLogGroupArn": "arn:aws:logs:us-east-1:111122223333:log-group:/aws/aes/domains/es-slow-logs",
      "Enabled": true
    }
  },
  "NodeToNodeEncryptionOptions": {
    "Enabled": true
  },
  "ServiceSoftwareOptions": {
    "AutomatedUpdateDate": "2022-04-28T14:08:37.000Z",
    "Cancellable": false,
    "CurrentVersion": "R20210331",
    "Description": "There is no software update available for this domain.",
    "NewVersion": "OpenSearch_1.0",
    "UpdateAvailable": false,
    "UpdateStatus": "COMPLETED",
    "OptionalDeployment": false
  }
}

```

```

    },
    "VpcOptions": {
      "SecurityGroupIds": [
        "sg-2a3a4a5a"
      ],
      "SubnetIds": [
        "subnet-1a2a3a4a"
      ],
    }
  }
}

```

AwsRds sumber daya di ASFF

Berikut ini adalah contoh sintaks AWS Security Finding Format (ASFF) untuk AwsRds sumber daya.

AWS Security Hub menormalkan temuan dari berbagai sumber menjadi ASFF. Untuk informasi latar belakang tentang ASFF, lihat [AWS Format Pencarian Keamanan \(ASFF\)](#).

AwsRdsDbCluster

AwsRdsDbClusterObjek memberikan rincian tentang cluster database Amazon RDS.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk AwsRdsDbCluster objek. Untuk melihat deskripsi AwsRdsDbCluster atribut, lihat [AwsRdsDbClusterDetails](#) di Referensi AWS Security Hub API.

Contoh

```

"AwsRdsDbCluster": {
  "ActivityStreamStatus": "stopped",
  "AllocatedStorage": 1,
  "AssociatedRoles": [
    {
      "RoleArn": "arn:aws:iam::777788889999:role/aws-service-role/rds.amazonaws.com/AWSServiceRoleForRDS",
      "Status": "PENDING"
    }
  ],
  "AutoMinorVersionUpgrade": true,
  "AvailabilityZones": [
    "us-east-1a",
    "us-east-1c",
    "us-east-1e"
  ],

```

```

"BackupRetentionPeriod": 1,
"ClusterCreateTime": "2020-06-22T17:40:12.322Z",
"CopyTagsToSnapshot": true,
"CrossAccountClone": false,
"CustomEndpoints": [],
"DatabaseName": "Sample name",
"DbClusterIdentifier": "database-3",
"DbClusterMembers": [
  {
    "DbClusterParameterGroupStatus": "in-sync",
    "DbInstanceIdentifier": "database-3-instance-1",
    "IsClusterWriter": true,
    "PromotionTier": 1,
  }
],
"DbClusterOptionGroupMemberships": [],
"DbClusterParameterGroup": "cluster-parameter-group",
"DbClusterResourceId": "cluster-example",
"DbSubnetGroup": "subnet-group",
"DeletionProtection": false,
"DomainMemberships": [],
"Status": "modifying",
"EnabledCloudwatchLogsExports": [
  "audit",
  "error",
  "general",
  "slowquery"
],
"Endpoint": "database-3.cluster-example.us-east-1.rds.amazonaws.com",
"Engine": "aurora-mysql",
"EngineMode": "provisioned",
"EngineVersion": "5.7.mysql_aurora.2.03.4",
"HostedZoneId": "ZONE1",
"HttpEndpointEnabled": false,
"IamDatabaseAuthenticationEnabled": false,
"KmsKeyId": "arn:aws:kms:us-east-1:777788889999:key/key1",
"MasterUsername": "admin",
"MultiAz": false,
"Port": 3306,
"PreferredBackupWindow": "04:52-05:22",
"PreferredMaintenanceWindow": "sun:09:32-sun:10:02",
"ReaderEndpoint": "database-3.cluster-ro-example.us-east-1.rds.amazonaws.com",
"ReadReplicaIdentifiers": [],
"Status": "Modifying",

```

```
"StorageEncrypted": true,
"VpcSecurityGroups": [
  {
    "Status": "active",
    "VpcSecurityGroupId": "sg-example-1"
  }
],
}
```

AwsRdsDbClusterSnapshot

AwsRdsDbClusterSnapshotObjek berisi informasi tentang snapshot cluster Amazon RDS DB.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk AwsRdsDbClusterSnapshot objek. Untuk melihat deskripsi AwsRdsDbClusterSnapshot atribut, lihat [AwsRdsDbClusterSnapshotDetails](#) di Referensi AWS Security Hub API.

Contoh

```
"AwsRdsDbClusterSnapshot": {
  "AllocatedStorage": 0,
  "AvailabilityZones": [
    "us-east-1a",
    "us-east-1d",
    "us-east-1e"
  ],
  "ClusterCreateTime": "2020-06-12T13:23:15.577Z",
  "DbClusterIdentifier": "database-2",
  "DbClusterSnapshotAttributes": [{
    "AttributeName": "restore",
    "AttributeValues": ["123456789012"]
  }],
  "DbClusterSnapshotIdentifier": "rds:database-2-2020-06-23-03-52",
  "Engine": "aurora",
  "EngineVersion": "5.6.10a",
  "IamDatabaseAuthenticationEnabled": false,
  "KmsKeyId": "arn:aws:kms:us-east-1:777788889999:key/key1",
  "LicenseModel": "aurora",
  "MasterUsername": "admin",
  "PercentProgress": 100,
  "Port": 0,
  "SnapshotCreateTime": "2020-06-22T17:40:12.322Z",
  "SnapshotType": "automated",
```

```
"Status": "available",  
"StorageEncrypted": true,  
"VpcId": "vpc-faf7e380"  
}
```

AwsRdsDbInstance

AwsRdsDbInstanceObjek memberikan detail tentang instans Amazon RDS DB.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk AwsRdsDbInstance objek. Untuk melihat deskripsi AwsRdsDbInstance atribut, lihat [AwsRdsDbInstanceDetails](#) di Referensi AWS Security Hub API.

Contoh

```
"AwsRdsDbInstance": {  
  "AllocatedStorage": 20,  
  "AssociatedRoles": [],  
  "AutoMinorVersionUpgrade": true,  
  "AvailabilityZone": "us-east-1d",  
  "BackupRetentionPeriod": 7,  
  "CaCertificateIdentifier": "certificate1",  
  "CharacterSetName": "",  
  "CopyTagsToSnapshot": true,  
  "DbClusterIdentifier": "",  
  "DbInstanceArn": "arn:aws:rds:us-east-1:111122223333:db:database-1",  
  "DbInstanceClass": "db.t2.micro",  
  "DbInstanceIdentifier": "database-1",  
  "DbInstancePort": 0,  
  "DbInstanceStatus": "available",  
  "DbiResourceId": "db-EXAMPLE123",  
  "DbName": "",  
  "DbParameterGroups": [  
    {  
      "DbParameterGroupName": "default.mysql5.7",  
      "ParameterApplyStatus": "in-sync"  
    }  
  ],  
  "DbSecurityGroups": [],  
  
  "DbSubnetGroup": {  
    "DbSubnetGroupName": "my-group-123abc",
```

```

    "DbSubnetGroupDescription": "My subnet group",
    "VpcId": "vpc-example1",
    "SubnetGroupStatus": "Complete",
    "Subnets": [
      {
        "SubnetIdentifier": "subnet-123abc",
        "SubnetAvailabilityZone": {
          "Name": "us-east-1d"
        },
        "SubnetStatus": "Active"
      },
      {
        "SubnetIdentifier": "subnet-456def",
        "SubnetAvailabilityZone": {
          "Name": "us-east-1c"
        },
        "SubnetStatus": "Active"
      }
    ],
    "DbSubnetGroupArn": "",
  },
  "DeletionProtection": false,
  "DomainMemberships": [],
  "EnabledCloudWatchLogsExports": [],
  "Endpoint": {
    "address": "database-1.example.us-east-1.rds.amazonaws.com",
    "port": 3306,
    "hostedZoneId": "ZONEID1"
  },
  "Engine": "mysql",
  "EngineVersion": "5.7.22",
  "EnhancedMonitoringResourceArn": "arn:aws:logs:us-east-1:111122223333:log-
group:Example:log-stream:db-EXAMPLE1",
  "IamDatabaseAuthenticationEnabled": false,
  "InstanceCreateTime": "2020-06-22T17:40:12.322Z",
  "Iops": "",
  "KmsKeyId": "",
  "LatestRestorableTime": "2020-06-24T05:50:00.000Z",
  "LicenseModel": "general-public-license",
  "ListenerEndpoint": "",
  "MasterUsername": "admin",
  "MaxAllocatedStorage": 1000,
  "MonitoringInterval": 60,
  "MonitoringRoleArn": "arn:aws:iam::111122223333:role/rds-monitoring-role",

```

```

"MultiAz": false,
"OptionGroupMemberships": [
  {
    "OptionGroupName": "default:mysql-5-7",
    "Status": "in-sync"
  }
],
"PreferredBackupWindow": "03:57-04:27",
"PreferredMaintenanceWindow": "thu:10:13-thu:10:43",
"PendingModifiedValues": {
  "DbInstanceClass": "",
  "AllocatedStorage": "",
  "MasterUserPassword": "",
  "Port": "",
  "BackupRetentionPeriod": "",
  "MultiAZ": "",
  "EngineVersion": "",
  "LicenseModel": "",
  "Iops": "",
  "DbInstanceIdentifier": "",
  "StorageType": "",
  "CaCertificateIdentifier": "",
  "DbSubnetGroupName": "",
  "PendingCloudWatchLogsExports": "",
  "ProcessorFeatures": []
},
"PerformanceInsightsEnabled": false,
"PerformanceInsightsKmsKeyId": "",
"PerformanceInsightsRetentionPeriod": "",
"ProcessorFeatures": [],
"PromotionTier": "",
"PubliclyAccessible": false,
"ReadReplicaDBClusterIdentifiers": [],
"ReadReplicaDBInstanceIdentifiers": [],
"ReadReplicaSourceDBInstanceIdentifier": "",
"SecondaryAvailabilityZone": "",
"StatusInfos": [],
"StorageEncrypted": false,
"StorageType": "gp2",
"TdeCredentialArn": "",
"Timezone": "",
"VpcSecurityGroups": [
  {
    "VpcSecurityGroupId": "sg-example1",

```



```

        "Status": "active"
      }
    ]
  }

```

AwsRdsDbSecurityGroup

AwsRdsDbSecurityGroupObjek berisi informasi tentang Amazon Relational Database Service

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk AwsRdsDbSecurityGroup objek. Untuk melihat deskripsi AwsRdsDbSecurityGroup atribut, lihat [AwsRdsDbSecurityGroupDetails](#) di Referensi AWS Security Hub API.

Contoh

```

"AwsRdsDbSecurityGroup": {
  "DbSecurityGroupArn": "arn:aws:rds:us-west-1:111122223333:secgrp:default",
  "DbSecurityGroupDescription": "default",
  "DbSecurityGroupName": "mysecgroup",
  "Ec2SecurityGroups": [
    {
      "Ec2SecurityGrouppuId": "myec2group",
      "Ec2SecurityGroupName": "default",
      "Ec2SecurityGroupOwnerId": "987654321021",
      "Status": "authorizing"
    }
  ],
  "IpRanges": [
    {
      "CidrIp": "0.0.0.0/0",
      "Status": "authorizing"
    }
  ],
  "OwnerId": "123456789012",
  "VpcId": "vpc-1234567f"
}

```

AwsRdsDbSnapshot

AwsRdsDbSnapshotObjek berisi detail tentang snapshot cluster Amazon RDS DB.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsRdsDbSnapshot` objek. Untuk melihat deskripsi `AwsRdsDbSnapshot` atribut, lihat [AwsRdsDbSnapshotDetails](#) di Referensi AWS Security Hub API.

Contoh

```
"AwsRdsDbSnapshot": {
  "DbSnapshotIdentifier": "rds:database-1-2020-06-22-17-41",
  "DbInstanceIdentifier": "database-1",
  "SnapshotCreateTime": "2020-06-22T17:41:29.967Z",
  "Engine": "mysql",
  "AllocatedStorage": 20,
  "Status": "available",
  "Port": 3306,
  "AvailabilityZone": "us-east-1d",
  "VpcId": "vpc-example1",
  "InstanceCreateTime": "2020-06-22T17:40:12.322Z",
  "MasterUsername": "admin",
  "EngineVersion": "5.7.22",
  "LicenseModel": "general-public-license",
  "SnapshotType": "automated",
  "Iops": null,
  "OptionGroupName": "default:mysql-5-7",
  "PercentProgress": 100,
  "SourceRegion": null,
  "SourceDbSnapshotIdentifier": "",
  "StorageType": "gp2",
  "TdeCredentialArn": "",
  "Encrypted": false,
  "KmsKeyId": "",
  "Timezone": "",
  "IamDatabaseAuthenticationEnabled": false,
  "ProcessorFeatures": [],
  "DbiResourceId": "db-resourceexample1"
}
```

AwsRdsEventSubscription

`AwsRdsEventSubscription` berisi rincian tentang langganan pemberitahuan acara RDS. Langganan memungkinkan RDS untuk memposting acara ke topik SNS.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsRdsEventSubscription` objek. Untuk melihat deskripsi `AwsRdsEventSubscription` atribut, lihat [AwsRdsEventSubscriptionDetails](#) di Referensi AWS Security Hub API.

Contoh

```
"AwsRdsEventSubscription": {
  "CustSubscriptionId": "myawsuser-secgrp",
  "CustomerAwsId": "111111111111",
  "Enabled": true,
  "EventCategoriesList": [
    "configuration change",
    "failure"
  ],
  "EventSubscriptionArn": "arn:aws:rds:us-east-1:111111111111:es:my-instance-events",
  "SnsTopicArn": "arn:aws:sns:us-east-1:111111111111:myawsuser-RDS",
  "SourceIdsList": [
    "si-sample",
    "mysqlldb-rr"
  ],
  "SourceType": "db-security-group",
  "Status": "creating",
  "SubscriptionCreationTime": "2021-06-27T01:38:01.090Z"
}
```

AwsRedshiftsumber daya di ASFF

Berikut ini adalah contoh sintaks AWS Security Finding Format (ASFF) untuk `AwsRedshift` sumber daya.

AWS Security Hub menormalkan temuan dari berbagai sumber menjadi ASFF. Untuk informasi latar belakang tentang ASFF, lihat [AWS Format Pencarian Keamanan \(ASFF\)](#).

AwsRedshiftCluster

`AwsRedshiftCluster` objek berisi detail tentang cluster Amazon Redshift.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsRedshiftCluster` objek. Untuk melihat deskripsi `AwsRedshiftCluster` atribut, lihat [AwsRedshiftClusterDetails](#) di Referensi AWS Security Hub API.

Contoh

```

"AwsRedshiftCluster": {
  "AllowVersionUpgrade": true,
  "AutomatedSnapshotRetentionPeriod": 1,
  "AvailabilityZone": "us-west-2d",
  "ClusterAvailabilityStatus": "Unavailable",
  "ClusterCreateTime": "2020-08-03T19:22:44.637Z",
  "ClusterIdentifier": "redshift-cluster-1",
  "ClusterNodes": [
    {
      "NodeRole": "LEADER",
      "PrivateIPAddress": "192.0.2.108",
      "PublicIPAddress": "198.51.100.29"
    },
    {
      "NodeRole": "COMPUTE-0",
      "PrivateIPAddress": "192.0.2.22",
      "PublicIPAddress": "198.51.100.63"
    },
    {
      "NodeRole": "COMPUTE-1",
      "PrivateIPAddress": "192.0.2.224",
      "PublicIPAddress": "198.51.100.226"
    }
  ],
  "ClusterParameterGroups": [
    {
      "ClusterParameterStatusList": [
        {
          "ParameterName": "max_concurrency_scaling_clusters",
          "ParameterApplyStatus": "in-sync",
          "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
        },
        {
          "ParameterName": "enable_user_activity_logging",
          "ParameterApplyStatus": "in-sync",
          "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
        },
        {
          "ParameterName": "auto_analyze",
          "ParameterApplyStatus": "in-sync",
          "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
        },
        {

```

```

        "ParameterName": "query_group",
        "ParameterApplyStatus": "in-sync",
        "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
    },
    {
        "ParameterName": "datestyle",
        "ParameterApplyStatus": "in-sync",
        "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
    },
    {
        "ParameterName": "extra_float_digits",
        "ParameterApplyStatus": "in-sync",
        "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
    },
    {
        "ParameterName": "search_path",
        "ParameterApplyStatus": "in-sync",
        "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
    },
    {
        "ParameterName": "statement_timeout",
        "ParameterApplyStatus": "in-sync",
        "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
    },
    {
        "ParameterName": "wlm_json_configuration",
        "ParameterApplyStatus": "in-sync",
        "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
    },
    {
        "ParameterName": "require_ssl",
        "ParameterApplyStatus": "in-sync",
        "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
    },
    {
        "ParameterName": "use_fips_ssl",
        "ParameterApplyStatus": "in-sync",
        "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
    }
    ],
    "ParameterApplyStatus": "in-sync",
    "ParameterGroupName": "temp"
}
],

```

```

"ClusterPublicKey": "JalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY Amazon-Redshift",
"ClusterRevisionNumber": 17498,
"ClusterSecurityGroups": [
  {
    "ClusterSecurityGroupName": "default",
    "Status": "active"
  }
],
"ClusterSnapshotCopyStatus": {
  "DestinationRegion": "us-west-2",
  "ManualSnapshotRetentionPeriod": -1,
  "RetentionPeriod": 1,
  "SnapshotCopyGrantName": "snapshotCopyGrantName"
},
"ClusterStatus": "available",
"ClusterSubnetGroupName": "default",
"ClusterVersion": "1.0",
"DBName": "dev",
"DeferredMaintenanceWindows": [
  {
    "DeferMaintenanceEndTime": "2020-10-07T20:34:01.000Z",
    "DeferMaintenanceIdentifier": "deferMaintenanceIdentifier",
    "DeferMaintenanceStartTime": "2020-09-07T20:34:01.000Z"
  }
],
"ElasticIpStatus": {
  "ElasticIp": "203.0.113.29",
  "Status": "active"
},
"ElasticResizeNumberOfNodeOptions": "4",
"Encrypted": false,
"Endpoint": {
  "Address": "redshift-cluster-1.example.us-west-2.redshift.amazonaws.com",
  "Port": 5439
},
"EnhancedVpcRouting": false,
"ExpectedNextSnapshotScheduleTime": "2020-10-13T20:34:01.000Z",
"ExpectedNextSnapshotScheduleTimeStatus": "OnTrack",
"HsmStatus": {
  "HsmClientCertificateIdentifier": "hsmClientCertificateIdentifier",
  "HsmConfigurationIdentifier": "hsmConfigurationIdentifier",
  "Status": "applying"
},
"IamRoles": [

```

```

    {
      "ApplyStatus": "in-sync",
      "IamRoleArn": "arn:aws:iam::111122223333:role/RedshiftCopyUnload"
    }
  ],
  "KmsKeyId": "kmsKeyId",
  "LoggingStatus": {
    "BucketName": "amzn-s3-demo-bucket",
    "LastFailureMessage": "test message",
    "LastFailureTime": "2020-08-09T13:00:00.000Z",
    "LastSuccessfulDeliveryTime": "2020-08-08T13:00:00.000Z",
    "LoggingEnabled": true,
    "S3KeyPrefix": "/"
  },
  "MaintenanceTrackName": "current",
  "ManualSnapshotRetentionPeriod": -1,
  "MasterUsername": "awsuser",
  "NextMaintenanceWindowStartTime": "2020-08-09T13:00:00.000Z",
  "NodeType": "dc2.large",
  "NumberOfNodes": 2,
  "PendingActions": [],
  "PendingModifiedValues": {
    "AutomatedSnapshotRetentionPeriod": 0,
    "ClusterIdentifier": "clusterIdentifier",
    "ClusterType": "clusterType",
    "ClusterVersion": "clusterVersion",
    "EncryptionType": "None",
    "EnhancedVpcRouting": false,
    "MaintenanceTrackName": "maintenanceTrackName",
    "MasterUserPassword": "masterUserPassword",
    "NodeType": "dc2.large",
    "NumberOfNodes": 1,
    "PubliclyAccessible": true
  },
  "PreferredMaintenanceWindow": "sun:13:00-sun:13:30",
  "PubliclyAccessible": true,
  "ResizeInfo": {
    "AllowCancelResize": true,
    "ResizeType": "ClassicResize"
  },
  "RestoreStatus": {
    "CurrentRestoreRateInMegaBytesPerSecond": 15,
    "ElapsedTimeInSeconds": 120,
    "EstimatedTimeToCompletionInSeconds": 100,

```

```

    "ProgressInMegaBytes": 10,
    "SnapshotSizeInMegaBytes": 1500,
    "Status": "restoring"
  },
  "SnapshotScheduleIdentifier": "snapshotScheduleIdentifier",
  "SnapshotScheduleState": "ACTIVE",
  "VpcId": "vpc-example",
  "VpcSecurityGroups": [
    {
      "Status": "active",
      "VpcSecurityGroupId": "sg-example"
    }
  ]
}

```

AwsRoute53 sumber daya di ASFF

Berikut ini adalah contoh sintaks AWS Security Finding Format (ASFF) untuk `AwsRoute53` sumber daya.

AWS Security Hub menormalkan temuan dari berbagai sumber menjadi ASFF. Untuk informasi latar belakang tentang ASFF, lihat [AWS Format Pencarian Keamanan \(ASFF\)](#).

AwsRoute53HostedZone

`AwsRoute53HostedZone` objek memberikan informasi tentang zona yang dihosting Amazon Route 53, termasuk empat server nama yang ditetapkan ke zona yang dihosting. Zona yang dihosting mewakili kumpulan catatan yang dapat dikelola bersama, milik nama domain induk tunggal.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsRoute53HostedZone` objek. Untuk melihat deskripsi `AwsRoute53HostedZone` atribut, lihat [AwsRoute53 HostedZoneDetails](#) di Referensi AWS Security Hub API.

Contoh

```

"AwsRoute53HostedZone": {
  "HostedZone": {
    "Id": "Z06419652JEMG09TA2XKL",
    "Name": "asff.testing",
    "Config": {
      "Comment": "This is an example comment."
    }
  }
}

```



```

    }
  },
  "NameServers": [
    "ns-470.awsdns-32.net",
    "ns-1220.awsdns-12.org",
    "ns-205.awsdns-13.com",
    "ns-1960.awsdns-51.co.uk"
  ],
  "QueryLoggingConfig": {
    "CloudWatchLogsLogGroupArn": {
      "CloudWatchLogsLogGroupArn": "arn:aws:logs:us-east-1:123456789012:log-
group:asfftesting:*",
      "Id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
      "HostedZoneId": "Z00932193AF5H180PPNZD"
    }
  },
  "Vpcs": [
    {
      "Id": "vpc-05d7c6e36bc03ea76",
      "Region": "us-east-1"
    }
  ]
}

```

AwsS3sumber daya di ASFF

Berikut ini adalah contoh sintaks AWS Security Finding Format (ASFF) untuk AwsS3 sumber daya.

AWS Security Hub menormalkan temuan dari berbagai sumber menjadi ASFF. Untuk informasi latar belakang tentang ASFF, lihat [AWS Format Pencarian Keamanan \(ASFF\)](#).

AwsS3AccessPoint

AwsS3AccessPoint memberikan informasi tentang jalur akses Amazon S3. Titik akses S3 diberi nama titik akhir jaringan yang dilampirkan ke bucket S3 yang dapat Anda gunakan untuk melakukan operasi objek S3.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk AwsS3AccessPoint objek. Untuk melihat deskripsi *AwsS3AccessPoint* atribut, lihat [AWSS3 AccessPointDetails](#) di Referensi API.AWS Security Hub

Contoh

```

"AwsS3AccessPoint": {
  "AccessPointArn": "arn:aws:s3:us-east-1:123456789012:accesspoint/asff-access-point",
  "Alias": "asff-access-point-hrzrlukc5m36ft7okagglf3gmwluquse1b-s3alias",
  "Bucket": "amzn-s3-demo-bucket",
  "BucketAccountId": "123456789012",
  "Name": "asff-access-point",
  "NetworkOrigin": "VPC",
  "PublicAccessBlockConfiguration": {
    "BlockPublicAcls": true,
    "BlockPublicPolicy": true,
    "IgnorePublicAcls": true,
    "RestrictPublicBuckets": true
  },
  "VpcConfiguration": {
    "VpcId": "vpc-1a2b3c4d5e6f1a2b3"
  }
}

```

AwsS3AccountPublicAccessBlock

AwsS3AccountPublicAccessBlock memberikan informasi tentang konfigurasi Blok Akses Publik Amazon S3 untuk akun.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk AwsS3AccountPublicAccessBlock objek. Untuk melihat deskripsi *AwsS3AccountPublicAccessBlock* atribut, lihat [AWSS3 AccountPublicAccessBlockDetails](#) di Referensi API.AWS Security Hub

Contoh

```

"AwsS3AccountPublicAccessBlock": {
  "BlockPublicAcls": true,
  "BlockPublicPolicy": true,
  "IgnorePublicAcls": false,
  "RestrictPublicBuckets": true
}

```

AwsS3Bucket

AwsS3BucketObjek tersebut memberikan detail tentang bucket Amazon S3.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsS3Bucket` objek. Untuk melihat deskripsi `AwsS3Bucket` atribut, lihat [AWSS3 BucketDetails](#) di Referensi API.AWS Security Hub

Contoh

```
"AwsS3Bucket": {
  "AccessControlList": "{\"grantSet\":null,\"grantList\": [{\"grantee\":{\"id\": \"4df55416215956920d9d056aa8b99803a294ea221222bb668b55a8c6bca81094\"}, \"displayName\": null}, {\"permission\": \"FullControl\"}, {\"grantee\": \"AllUsers\"}, {\"permission\": \"ReadAcp\"}, {\"grantee\": \"AuthenticatedUsers\"}, {\"permission\": \"ReadAcp\"}], ,",
  "BucketLifecycleConfiguration": {
    "Rules": [
      {
        "AbortIncompleteMultipartUpload": {
          "DaysAfterInitiation": 5
        },
        "ExpirationDate": "2021-11-10T00:00:00.000Z",
        "ExpirationInDays": 365,
        "ExpiredObjectDeleteMarker": false,
        "Filter": {
          "Predicate": {
            "Operands": [
              {
                "Prefix": "tmp/",
                "Type": "LifecyclePrefixPredicate"
              },
              {
                "Tag": {
                  "Key": "ArchiveAge",
                  "Value": "9m"
                },
                "Type": "LifecycleTagPredicate"
              }
            ],
            "Type": "LifecycleAndOperator"
          }
        },
        "ID": "Move rotated logs to Glacier",
        "NoncurrentVersionExpirationInDays": -1,
        "NoncurrentVersionTransitions": [
          {
            "Days": 2,
```

```

        "StorageClass": "GLACIER"
      }
    ],
    "Prefix": "rotated/",
    "Status": "Enabled",
    "Transitions": [
      {
        "Date": "2020-11-10T00:00:00.000Z",
        "Days": 100,
        "StorageClass": "GLACIER"
      }
    ]
  }
]
},
"BucketLoggingConfiguration": {
  "DestinationBucketName": "s3serversideloggingbucket-123456789012",
  "LogFilePrefix": "buckettestreadwrite23435/"
},
"BucketName": "amzn-s3-demo-bucket",
"BucketNotificationConfiguration": {
  "Configurations": [{
    "Destination": "arn:aws:lambda:us-east-1:123456789012:function:s3_public_write",
    "Events": [
      "s3:ObjectCreated:Put"
    ],
    "Filter": {
      "S3KeyFilter": {
        "FilterRules": [
          {
            "Name": "AffS3BucketNotificationConfigurationS3KeyFilterRuleName.PREFIX",
            "Value": "pre"
          },
          {
            "Name": "AffS3BucketNotificationConfigurationS3KeyFilterRuleName.SUFFIX",
            "Value": "suf"
          }
        ]
      }
    }
  ]
},
"Type": "LambdaConfiguration"
]]
},
"BucketVersioningConfiguration": {

```

```
"IsMfaDeleteEnabled": true,
"Status": "Off"
},
"BucketWebsiteConfiguration": {
  "ErrorDocument": "error.html",
  "IndexDocumentSuffix": "index.html",
  "RedirectAllRequestsTo": {
    "HostName": "example.com",
    "Protocol": "http"
  },
  "RoutingRules": [{
    "Condition": {
      "HttpErrorCodeReturnedEquals": "Redirected",
      "KeyPrefixEquals": "index"
    },
    "Redirect": {
      "HostName": "example.com",
      "HttpRedirectCode": "401",
      "Protocol": "HTTP",
      "ReplaceKeyPrefixWith": "string",
      "ReplaceKeyWith": "string"
    }
  }]
},
"CreatedAt": "2007-11-30T01:46:56.000Z",
"ObjectLockConfiguration": {
  "ObjectLockEnabled": "Enabled",
  "Rule": {
    "DefaultRetention": {
      "Days": null,
      "Mode": "GOVERNANCE",
      "Years": 12
    }
  },
},
},
"OwnerId": "AIDACKCEVSQ6C2EXAMPLE",
"OwnerName": "s3bucketowner",
"PublicAccessBlockConfiguration": {
  "BlockPublicAcls": true,
  "BlockPublicPolicy": true,
  "IgnorePublicAcls": true,
  "RestrictPublicBuckets": true,
},
"ServerSideEncryptionConfiguration": {
```

```

    "Rules": [
      {
        "ApplyServerSideEncryptionByDefault": {
          "SSEAlgorithm": "AES256",
          "KMSMasterKeyID": "12345678-abcd-abcd-abcd-123456789012"
        }
      }
    ]
  }
}

```

AwsS3Object

AwsS3ObjectObjek memberikan informasi tentang objek Amazon S3.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk AwsS3Object objek. Untuk melihat deskripsi *AwsS3Object* atribut, lihat [AWSS3 ObjectDetails](#) di Referensi API.AWS Security Hub

Contoh

```

"AwsS3Object": {
  "ContentType": "text/html",
  "ETag": "\"30a6ec7e1a9ad79c203d05a589c8b400\"",
  "LastModified": "2012-04-23T18:25:43.511Z",
  "ServerSideEncryption": "aws:kms",
  "SSEKMSKeyId": "arn:aws:kms:us-west-2:123456789012:key/4dff8393-e225-4793-a9a0-608ec069e5a7",
  "VersionId": "ws310urg00jH_HH1lIxPE35P.MELYaYh"
}

```

AwsSageMaker sumber daya di ASFF

Berikut ini adalah contoh sintaks AWS Security Finding Format (ASFF) untuk AwsSageMaker sumber daya.

AWS Security Hub menormalkan temuan dari berbagai sumber menjadi ASFF. Untuk informasi latar belakang tentang ASFF, lihat [AWS Format Pencarian Keamanan \(ASFF\)](#).

AwsSageMakerNotebookInstance

AwsSageMakerNotebookInstanceObjek menyediakan informasi tentang instance notebook Amazon SageMaker AI, yang merupakan instance komputasi pembelajaran mesin yang menjalankan Aplikasi Notebook Jupyter.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk AwsSageMakerNotebookInstance objek. Untuk melihat deskripsi AwsSageMakerNotebookInstance atribut, lihat [AwsSageMakerNotebookInstanceDetails](#) di Referensi AWS Security Hub API.

Contoh

```
"AwsSageMakerNotebookInstance": {
  "DirectInternetAccess": "Disabled",
  "InstanceMetadataServiceConfiguration": {
    "MinimumInstanceMetadataServiceVersion": "1",
  },
  "InstanceType": "ml.t2.medium",
  "LastModifiedTime": "2022-09-09 22:48:32.012000+00:00",
  "NetworkInterfaceId": "eni-06c09ac2541a1bed3",
  "NotebookInstanceArn": "arn:aws:sagemaker:us-east-1:001098605940:notebook-instance/
sagemakernotebookinstancerootaccessdisabledcomplia-8myjcyofzixm",
  "NotebookInstanceName":
"SagemakerNotebookInstanceRootAccessDisabledComplia-8MYjcyofZiXm",
  "NotebookInstanceStatus": "InService",
  "PlatformIdentifier": "notebook-all-v1",
  "RoleArn": "arn:aws:iam::001098605940:role/sechub-SageMaker-1-scenar-
SageMakerCustomExecution-1R0X32HGC38IW",
  "RootAccess": "Disabled",
  "SecurityGroups": [
    "sg-06b347359ab068745"
  ],
  "SubnetId": "subnet-02c0deea5fa64578e",
  "Url":
"sagemakernotebookinstancerootaccessdisabledcomplia-8myjcyofzixm.notebook.us-
east-1.sagemaker.aws",
  "VolumeSizeInGB": 5
}
```

AwsSecretsManagersumber daya di ASFF

Berikut ini adalah contoh sintaks AWS Security Finding Format (ASFF) untuk AwsSecretsManager sumber daya.

AWS Security Hub menormalkan temuan dari berbagai sumber menjadi ASFF. Untuk informasi latar belakang tentang ASFF, lihat [AWS Format Pencarian Keamanan \(ASFF\)](#).

AwsSecretsManagerSecret

AwsSecretsManagerSecretObjek memberikan rincian tentang rahasia Secrets Manager.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk AwsSecretsManagerSecret objek. Untuk melihat deskripsi AwsSecretsManagerSecret atribut, lihat [AwsSecretsManagerSecretDetails](#) di Referensi AWS Security Hub API.

Contoh

```
"AwsSecretsManagerSecret": {
  "RotationRules": {
    "AutomaticallyAfterDays": 30
  },
  "RotationOccurredWithinFrequency": true,
  "KmsKeyId": "kmsKeyId",
  "RotationEnabled": true,
  "RotationLambdaArn": "arn:aws:lambda:us-west-2:777788889999:function:MyTestRotationLambda",
  "Deleted": false,
  "Name": "MyTestDatabaseSecret",
  "Description": "My test database secret"
}
```

AwsSnssumber daya di ASFF

Berikut ini adalah contoh sintaks AWS Security Finding Format (ASFF) untuk AwsSns sumber daya.

AWS Security Hub menormalkan temuan dari berbagai sumber menjadi ASFF. Untuk informasi latar belakang tentang ASFF, lihat [AWS Format Pencarian Keamanan \(ASFF\)](#).

AwsSnsTopic

AwsSnsTopicObjek berisi rincian tentang topik Amazon Simple Notification Service.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsSnsTopic` objek. Untuk melihat deskripsi `AwsSnsTopic` atribut, lihat [AwsSnsTopicDetails](#) di Referensi AWS Security Hub API.

Contoh

```
"AwsSnsTopic": {
  "ApplicationSuccessFeedbackRoleArn": "arn:aws:iam::123456789012:role/
ApplicationSuccessFeedbackRoleArn",
  "FirehoseFailureFeedbackRoleArn": "arn:aws:iam::123456789012:role/
FirehoseFailureFeedbackRoleArn",
  "FirehoseSuccessFeedbackRoleArn": "arn:aws:iam::123456789012:role/
FirehoseSuccessFeedbackRoleArn",
  "HttpFailureFeedbackRoleArn": "arn:aws:iam::123456789012:role/
HttpFailureFeedbackRoleArn",
  "HttpSuccessFeedbackRoleArn": "arn:aws:iam::123456789012:role/
HttpSuccessFeedbackRoleArn",
  "KmsMasterKeyId": "alias/ExampleAlias",
  "Owner": "123456789012",
  "SqsFailureFeedbackRoleArn": "arn:aws:iam::123456789012:role/
SqsFailureFeedbackRoleArn",
  "SqsSuccessFeedbackRoleArn": "arn:aws:iam::123456789012:role/
SqsSuccessFeedbackRoleArn",
  "Subscription": {
    "Endpoint": "http://sampleendpoint.com",
    "Protocol": "http"
  },
  "TopicName": "SampleTopic"
}
```

AwsSqs sumber daya di ASFF

Berikut ini adalah contoh sintaks AWS Security Finding Format (ASFF) untuk `AwsSqs` sumber daya.

AWS Security Hub menormalkan temuan dari berbagai sumber menjadi ASFF. Untuk informasi latar belakang tentang ASFF, lihat [AWS Format Pencarian Keamanan \(ASFF\)](#).

AwsSqsQueue

`AwsSqsQueueObjek` berisi informasi tentang antrian Amazon Simple Queue Service.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsSqsQueue` objek. Untuk melihat deskripsi `AwsSqsQueue` atribut, lihat [AwsSqsQueueDetails](#) di Referensi AWS Security Hub API.

Contoh

```
"AwsSqsQueue": {
  "DeadLetterTargetArn": "arn:aws:sqs:us-west-2:123456789012:queue/target",
  "KmsDataKeyReusePeriodSeconds": 60,,
  "KmsMasterKeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
  "QueueName": "sample-queue"
}
```

AwsSsm sumber daya di ASFF

Berikut ini adalah contoh sintaks AWS Security Finding Format (ASFF) untuk `AwsSsm` sumber daya.

AWS Security Hub menormalkan temuan dari berbagai sumber menjadi ASFF. Untuk informasi latar belakang tentang ASFF, lihat [AWS Format Pencarian Keamanan \(ASFF\)](#).

AwsSsmPatchCompliance

`AwsSsmPatchCompliance` Objek memberikan informasi tentang status patch pada instance berdasarkan baseline patch yang digunakan untuk menambal instance.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsSsmPatchCompliance` objek. Untuk melihat deskripsi `AwsSsmPatchCompliance` atribut, lihat [AwsSsmPatchComplianceDetails](#) di Referensi AWS Security Hub API.

Contoh

```
"AwsSsmPatchCompliance": {
  "Patch": {
    "ComplianceSummary": {
      "ComplianceType": "Patch",
      "CompliantCriticalCount": 0,
      "CompliantHighCount": 0,
      "CompliantInformationalCount": 0,
      "CompliantLowCount": 0,
      "CompliantMediumCount": 0,
      "CompliantUnspecifiedCount": 461,
    }
  }
}
```

```

    "ExecutionType": "Command",
    "NonCompliantCriticalCount": 0,
    "NonCompliantHighCount": 0,
    "NonCompliantInformationalCount": 0,
    "NonCompliantLowCount": 0,
    "NonCompliantMediumCount": 0,
    "NonCompliantUnspecifiedCount": 0,
    "OverallSeverity": "UNSPECIFIED",
    "PatchBaselineId": "pb-0c5b2769ef7cbe587",
    "PatchGroup": "ExamplePatchGroup",
    "Status": "COMPLIANT"
  }
}

```

AwsStepFunctionssumber daya di ASFF

Berikut ini adalah contoh sintaks AWS Security Finding Format (ASFF) untuk `AwsStepFunctions` sumber daya.

AWS Security Hub menormalkan temuan dari berbagai sumber menjadi ASFF. Untuk informasi latar belakang tentang ASFF, lihat [AWS Format Pencarian Keamanan \(ASFF\)](#).

AwsStepFunctionStateMachine

`AwsStepFunctionStateMachine` objek memberikan informasi tentang mesin AWS Step Functions negara, yang merupakan alur kerja yang terdiri dari serangkaian langkah yang digerakkan oleh peristiwa.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsStepFunctionStateMachine` objek. Untuk melihat deskripsi `AwsStepFunctionStateMachine` atribut, lihat [AwsStepFunctionStateMachine](#) di Referensi AWS Security Hub API.

Contoh

```

"AwsStepFunctionStateMachine": {
  "StateMachineArn": "arn:aws:states:us-
east-1:123456789012:stateMachine:StepFunctionsLogDisableNonCompliantResource-
fQLujTeXvwsb",
  "Name": "StepFunctionsLogDisableNonCompliantResource-fQLujTeXvwsb",
  "Status": "ACTIVE",

```

```

    "RoleArn": "arn:aws:iam::123456789012:role/teststepfunc-
StatesExecutionRole-1PNM71RV01UKT",
    "Type": "STANDARD",
    "LoggingConfiguration": {
        "Level": "OFF",
        "IncludeExecutionData": false
    },
    "TracingConfiguration": {
        "Enabled": false
    }
}

```

AwsWaf sumber daya di ASFF

Berikut ini adalah contoh sintaks AWS Security Finding Format (ASFF) untuk AwsWaf sumber daya.

AWS Security Hub menormalkan temuan dari berbagai sumber menjadi ASFF. Untuk informasi latar belakang tentang ASFF, lihat [AWS Format Pencarian Keamanan \(ASFF\)](#).

AwsWafRateBasedRule

AwsWafRateBasedRule objek berisi rincian tentang aturan AWS WAF berbasis tarif untuk sumber daya global. Aturan AWS WAF berbasis tarif menyediakan pengaturan untuk menunjukkan kapan harus mengizinkan, memblokir, atau menghitung permintaan. Aturan berbasis tarif mencakup jumlah permintaan yang tiba selama periode waktu tertentu.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk AwsWafRateBasedRule objek. Untuk melihat deskripsi AwsWafRateBasedRule atribut, lihat [AwsWafRateBasedRuleDetails](#) di Referensi AWS Security Hub API.

Contoh

```

"AwsWafRateBasedRule":{
  "MatchPredicates" : [{
    "DataId" : "391b7a7e-5f00-40d2-b114-3f27ceacbbb0",
    "Negated" : "True",
    "Type" : "IPMatch" ,
  }],
  "MetricName" : "MetricName",
  "Name" : "Test",
  "RateKey" : "IP",
  "RateLimit" : 235000,
  "RuleId" : "5dfb4085-f103-4ec6-b39a-d4a0dae5f47f"
}

```

```
}

```

AwsWafRegionalRateBasedRule

`AwsWafRegionalRateBasedRule` objek berisi rincian tentang aturan berbasis tarif untuk sumber daya Regional. Aturan berbasis tarif menyediakan pengaturan untuk menunjukkan kapan harus mengizinkan, memblokir, atau menghitung permintaan. Aturan berbasis tarif mencakup jumlah permintaan yang tiba selama periode waktu tertentu.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsWafRegionalRateBasedRule` objek. Untuk melihat deskripsi `AwsWafRegionalRateBasedRule` atribut, lihat [AwsWafRegionalRateBasedRuleDetails](#) di Referensi AWS Security Hub API.

Contoh

```
"AwsWafRegionalRateBasedRule":{
  "MatchPredicates" : [{
    "DataId" : "391b7a7e-5f00-40d2-b114-3f27ceacbbb0",
    "Negated" : "True",
    "Type" : "IPMatch" ,
  }],
  "MetricName" : "MetricName",
  "Name" : "Test",
  "RateKey" : "IP",
  "RateLimit" : 235000,
  "RuleId" : "5dfb4085-f103-4ec6-b39a-d4a0dae5f47f"
}
```

AwsWafRegionalRule

`AwsWafRegionalRule` objek memberikan rincian tentang aturan AWS WAF Regional. Aturan ini mengidentifikasi permintaan web yang ingin Anda izinkan, blokir, atau hitung.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsWafRegionalRule` objek. Untuk melihat deskripsi `AwsWafRegionalRule` atribut, lihat [AwsWafRegionalRuleDetails](#) di Referensi AWS Security Hub API.

Contoh

```
"AwsWafRegionalRule": {
```

```

    "MetricName": "SampleWAF_Rule__Metric_1",
    "Name": "bb-waf-regional-rule-not-empty-conditions-compliant",
    "RuleId": "8f651760-24fa-40a6-a9ed-4b60f1de95fe",
    "PredicateList": [{
      "DataId": "127d9346-e607-4e93-9286-c1296fb5445a",
      "Negated": false,
      "Type": "GeoMatch"
    }]
  }
}

```

AwsWafRegionalRuleGroup

`AwsWafRegionalRuleGroup` objek memberikan rincian tentang kelompok aturan AWS WAF Regional. Grup aturan adalah kumpulan aturan yang telah ditentukan sebelumnya yang Anda tambahkan ke daftar kontrol akses web (web ACL).

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsWafRegionalRuleGroup` objek. Untuk melihat deskripsi `AwsWafRegionalRuleGroup` atribut, lihat [AwsWafRegionalRuleGroupDetails](#) di Referensi AWS Security Hub API.

Contoh

```

"AwsWafRegionalRuleGroup": {
  "MetricName": "SampleWAF_Metric_1",
  "Name": "bb-WAFClassicRuleGroupWithRuleCompliant",
  "RuleGroupId": "2012ca6d-e66d-4d9b-b766-bfb03ad77cfb",
  "Rules": [{
    "Action": {
      "Type": "ALLOW"
    }
  }],
  "Priority": 1,
  "RuleId": "cdd225da-32cf-4773-8dc5-3bca3ed9c19c",
  "Type": "REGULAR"
}

```

AwsWafRegionalWebAcl

`AwsWafRegionalWebAcl` memberikan rincian tentang daftar kontrol akses web AWS WAF Regional (web ACL). ACL web berisi aturan yang mengidentifikasi permintaan yang ingin Anda izinkan, blokir, atau hitung.

Berikut ini adalah contoh `AwsWafRegionalWebAcl` temuan dalam AWS Security Finding Format (ASFF). Untuk melihat deskripsi `AwsApiGatewayV2Stage` atribut, lihat [AwsWafRegionalWebAclDetails](#) di Referensi AWS Security Hub API.

Contoh

```
"AwsWafRegionalWebAcl": {
  "DefaultAction": "ALLOW",
  "MetricName" : "web-regional-webacl-metric-1",
  "Name": "WebACL_123",
  "RulesList": [
    {
      "Action": {
        "Type": "Block"
      },
      "Priority": 3,
      "RuleId": "24445857-852b-4d47-bd9c-61f05e4d223c",
      "Type": "REGULAR",
      "ExcludedRules": [
        {
          "ExclusionType": "Exclusion",
          "RuleId": "Rule_id_1"
        }
      ],
      "OverrideAction": {
        "Type": "OVERRIDE"
      }
    }
  ],
  "WebAclId": "443c76f4-2e72-4c89-a2ee-389d501c1f67"
}
```

AwsWafRule

`AwsWafRule` memberikan informasi tentang suatu AWS WAF aturan. AWS WAF Aturan mengidentifikasi permintaan web yang ingin Anda izinkan, blokir, atau hitung.

Berikut ini adalah contoh `AwsWafRule` temuan dalam AWS Security Finding Format (ASFF). Untuk melihat deskripsi `AwsApiGatewayV2Stage` atribut, lihat [AwsWafRuleDetails](#) di Referensi AWS Security Hub API.

Contoh

```

"AwsWafRule": {
  "MetricName": "AwsWafRule_Metric_1",
  "Name": "AwsWafRule_Name_1",
  "PredicateList": [{
    "DataId": "cdd225da-32cf-4773-1dc2-3bca3ed9c19c",
    "Negated": false,
    "Type": "GeoMatch"
  }],
  "RuleId": "8f651760-24fa-40a6-a9ed-4b60f1de953e"
}

```

AwsWafRuleGroup

`AwsWafRuleGroup` memberikan informasi tentang kelompok AWS WAF aturan. Grup AWS WAF aturan adalah kumpulan aturan yang telah ditentukan sebelumnya yang Anda tambahkan ke daftar kontrol akses web (web ACL).

Berikut ini adalah contoh `AwsWafRuleGroup` temuan dalam AWS Security Finding Format (ASFF). Untuk melihat deskripsi `AwsApiGatewayV2Stage` atribut, lihat [AwsWafRuleGroupDetails](#) di Referensi AWS Security Hub API.

Contoh

```

"AwsWafRuleGroup": {
  "MetricName": "SampleWAF_Metric_1",
  "Name": "bb-WAFRuleGroupWithRuleCompliant",
  "RuleGroupId": "2012ca6d-e66d-4d9b-b766-bfb03ad77cfb",
  "Rules": [{
    "Action": {
      "Type": "ALLOW",
    },
    "Priority": 1,
    "RuleId": "cdd225da-32cf-4773-8dc5-3bca3ed9c19c",
    "Type": "REGULAR"
  ]
}

```

AwsWafv2RuleGroup

`AwsWafv2RuleGroup` objek memberikan rincian tentang grup aturan AWS WAF V2.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsWafv2RuleGroup` objek. Untuk melihat deskripsi `AwsWafv2RuleGroup` atribut, lihat [AwsWafv2 RuleGroupDetails](#) di Referensi AWS Security Hub API.

Contoh

```
"AwsWafv2RuleGroup": {
  "Arn": "arn:aws:wafv2:us-east-1:123456789012:global/rulegroup/wafv2rulegroupasff/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "Capacity": 1000,
  "Description": "Resource for ASFF",
  "Id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "Name": "wafv2rulegroupasff",
  "Rules": [{
    "Action": {
      "Allow": {
        "CustomRequestHandling": {
          "InsertHeaders": [
            {
              "Name": "AllowActionHeader1Name",
              "Value": "AllowActionHeader1Value"
            },
            {
              "Name": "AllowActionHeader2Name",
              "Value": "AllowActionHeader2Value"
            }
          ]
        }
      }
    },
    "Name": "RuleOne",
    "Priority": 1,
    "VisibilityConfig": {
      "CloudWatchMetricsEnabled": true,
      "MetricName": "rulegroupasff",
      "SampledRequestsEnabled": false
    }
  }],
  "VisibilityConfig": {
    "CloudWatchMetricsEnabled": true,
    "MetricName": "rulegroupasff",
    "SampledRequestsEnabled": false
  }
}
```

AwsWafWebAcl

AwsWafWebAclObjek memberikan rincian tentang ACL AWS WAF web.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk AwsWafWebAcl objek. Untuk melihat deskripsi AwsWafWebAcl atribut, lihat [AwsWafWebAclDetails](#) di Referensi AWS Security Hub API.

Contoh

```
"AwsWafWebAcl": {
  "DefaultAction": "ALLOW",
  "Name": "MyWafAcl",
  "Rules": [
    {
      "Action": {
        "Type": "ALLOW"
      },
      "ExcludedRules": [
        {
          "RuleId": "5432a230-0113-5b83-bbb2-89375c5bfa98"
        }
      ],
      "OverrideAction": {
        "Type": "NONE"
      },
      "Priority": 1,
      "RuleId": "5432a230-0113-5b83-bbb2-89375c5bfa98",
      "Type": "REGULAR"
    }
  ],
  "WebAclId": "waf-1234567890"
}
```

AwsWafv2WebAcl

AwsWafv2WebAclObjek memberikan rincian tentang ACL web AWS WAF V2.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk AwsWafv2WebAcl objek. Untuk melihat deskripsi AwsWafv2WebAcl atribut, lihat [AwsWafv2 WebAclDetails](#) di Referensi AWS Security Hub API.

Contoh

```

"AwsWafv2WebAcl": {
  "Arn": "arn:aws:wafv2:us-east-1:123456789012:regional/webacl/WebACL-RoaD4QexqSxG/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "Capacity": 1326,
  "CaptchaConfig": {
    "ImmunityTimeProperty": {
      "ImmunityTime": 500
    }
  },
  "DefaultAction": {
    "Block": {}
  },
  "Description": "Web ACL for JsonBody testing",
  "ManagedbyFirewallManager": false,
  "Name": "WebACL-RoaD4QexqSxG",
  "Rules": [{
    "Action": {
      "RuleAction": {
        "Block": {}
      }
    },
    "Name": "TestJsonBodyRule",
    "Priority": 1,
    "VisibilityConfig": {
      "SampledRequestsEnabled": true,
      "CloudWatchMetricsEnabled": true,
      "MetricName": "JsonBodyMatchMetric"
    }
  }],
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "TestingJsonBodyMetric"
  }
}

```

AwsXraysumber daya di ASFF

Berikut ini adalah contoh sintaks AWS Security Finding Format (ASFF) untuk AwsXray sumber daya.

AWS Security Hub menormalkan temuan dari berbagai sumber menjadi ASFF. Untuk informasi latar belakang tentang ASFF, lihat [AWS Format Pencarian Keamanan \(ASFF\)](#).

AwsXrayEncryptionConfig

AwsXrayEncryptionConfigObjek berisi informasi tentang konfigurasi enkripsi untuk AWS X-Ray.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk AwsXrayEncryptionConfig objek. Untuk melihat deskripsi AwsXrayEncryptionConfig atribut, lihat [AwsXrayEncryptionConfigDetails](#) di Referensi AWS Security Hub API.

Contoh

```
"AwsXRayEncryptionConfig":{
  "KeyId": "arn:aws:kms:us-east-2:222222222222:key/example-key",
  "Status": "UPDATING",
  "Type":"KMS"
}
```

ContainerObjek ASFF

Contoh berikut menunjukkan sintaks AWS Security Finding Format (ASFF) untuk objek. Container Untuk melihat deskripsi Container atribut, lihat [ContainerDetails](#) di Referensi AWS Security Hub API. Untuk informasi latar belakang tentang ASFF, lihat [AWS Format Pencarian Keamanan \(ASFF\)](#).

Contoh

```
"Container": {
  "ContainerRuntime": "docker",
  "ImageId": "image12",
  "ImageName": "11111111/
knotejs@sha256:372131c9fef1111111111111115f4ed3ea5f9dce4dc3bd34ce21846588a3",
  "LaunchedAt": "2018-09-29T01:25:54Z",
  "Name": "knote",
  "Privileged": true,
  "VolumeMounts": [{
    "Name": "vol-03909e9",
    "MountPath": "/mnt/etc"
  }]
}
```

OtherObjek ASFF

Contoh berikut menunjukkan sintaks AWS Security Finding Format (ASFF) untuk objek. Other Untuk informasi latar belakang tentang ASFF, lihat [AWS Format Pencarian Keamanan \(ASFF\)](#).

`Other`Objek memungkinkan Anda untuk memberikan bidang dan nilai khusus. Anda menggunakan `Other` objek dalam kasus berikut.

- Jenis sumber daya tidak memiliki `Details` objek yang sesuai. Untuk memberikan detail untuk sumber daya, Anda menggunakan `Other` objek.
- `Details`Objek untuk tipe sumber daya tidak menyertakan semua atribut yang ingin Anda isi. Dalam hal ini, gunakan `Details` objek untuk jenis sumber daya untuk mengisi atribut yang tersedia. Gunakan `Other` objek untuk mengisi atribut yang tidak ada dalam objek tipe-spesifik.
- Jenis sumber daya bukan salah satu jenis yang disediakan. Dalam hal ini, Anda mengatur `Resource.Type` ke`Other`, dan menggunakan `Other` objek untuk mengisi rincian.

Jenis: Peta hingga 50 pasangan nilai kunci

Setiap pasangan kunci-nilai harus memenuhi persyaratan berikut.

- Kunci harus berisi kurang dari 128 karakter.
- Nilai harus mengandung kurang dari 1.024 karakter.

Melihat wawasan di Security Hub CSPM

Dalam AWS Security Hub Cloud Security Posture Management (CSPM), wawasan adalah kumpulan temuan terkait. Wawasan dapat mengidentifikasi area keamanan tertentu yang membutuhkan perhatian dan intervensi. Misalnya, wawasan mungkin menunjukkan EC2 contoh yang menjadi subjek temuan yang mendeteksi praktik keamanan yang buruk. Wawasan menyatukan temuan dari seluruh penyedia pencarian.

Setiap wawasan didefinisikan oleh grup berdasarkan pernyataan dan filter opsional. Kelompok berdasarkan pernyataan menunjukkan bagaimana mengelompokkan temuan yang cocok, dan mengidentifikasi jenis item yang diterapkan wawasan tersebut. Misalnya, jika wawasan dikelompokkan berdasarkan pengidentifikasi sumber daya, maka wawasan menghasilkan daftar pengidentifikasi sumber daya. Filter opsional mengidentifikasi temuan yang cocok untuk wawasan. Misalnya, Anda mungkin ingin hanya melihat temuan dari penyedia atau temuan tertentu yang terkait dengan jenis sumber daya tertentu.

Security Hub CSPM menawarkan beberapa wawasan terkelola bawaan. Anda tidak dapat mengubah atau menghapus wawasan terkelola. Untuk melacak masalah keamanan yang unik untuk AWS lingkungan dan penggunaan Anda, Anda dapat membuat wawasan khusus.

Halaman Wawasan di konsol AWS Security Hub Cloud Security Posture Management (CSPM) Security Hub menampilkan daftar wawasan yang tersedia.

Secara default, daftar menampilkan wawasan terkelola dan kustom. Untuk memfilter daftar wawasan berdasarkan jenis wawasan, pilih jenis wawasan dari menu tarik-turun yang berada di sebelah bidang filter.

- Untuk menampilkan semua wawasan yang tersedia, pilih Semua wawasan. Ini adalah pilihan default.
- Untuk hanya menampilkan wawasan terkelola, pilih wawasan terkelola CSPM Security Hub.
- Untuk hanya menampilkan wawasan khusus, pilih Wawasan khusus.

Anda juga dapat memfilter daftar wawasan berdasarkan nama wawasan. Untuk melakukannya, di bidang filter, ketikkan teks yang akan digunakan untuk memfilter daftar. Filter tidak peka huruf besar/kecil. Filter mencari wawasan yang berisi teks di mana saja dalam nama wawasan.

Wawasan hanya mengembalikan hasil jika Anda telah mengaktifkan integrasi atau standar yang menghasilkan temuan yang cocok. Misalnya, wawasan terkelola 29. Sumber daya teratas

berdasarkan jumlah pemeriksaan CIS yang gagal hanya mengembalikan hasil jika Anda mengaktifkan versi standar Tolok Ukur AWS Yayasan Center for Internet Security (CIS).

Meninjau dan bertindak berdasarkan wawasan di Security Hub CSPM

Untuk setiap wawasan, AWS Security Hub Cloud Security Posture Management (CSPM) pertama-tama menentukan temuan yang cocok dengan kriteria filter, dan kemudian menggunakan atribut pengelompokan untuk mengelompokkan temuan yang cocok.

Dari halaman Wawasan di konsol, Anda dapat melihat dan mengambil tindakan atas hasil dan temuan.

Jika Anda mengaktifkan agregasi lintas wilayah, hasil untuk wawasan terkelola (saat Anda masuk ke Wilayah agregasi) menyertakan temuan dari Wilayah agregasi dan Wilayah tertaut. Hasil untuk wawasan khusus, jika wawasan tidak difilter menurut Wilayah, juga menyertakan temuan dari Wilayah agregasi dan Wilayah tertaut (saat Anda masuk ke Wilayah agregasi). Di Wilayah lain, hasil wawasan hanya untuk Wilayah tersebut.

Untuk informasi tentang mengonfigurasi agregasi lintas wilayah, lihat [Menggabungkan data CSPM di seluruh Wilayah](#)

Melihat dan mengambil tindakan pada hasil wawasan

Hasil wawasan terdiri dari daftar hasil yang dikelompokkan untuk wawasan. Misalnya, jika wawasan dikelompokkan berdasarkan pengidentifikasi sumber daya, maka hasil wawasan adalah daftar pengidentifikasi sumber daya. Setiap item dalam daftar hasil menunjukkan jumlah temuan yang cocok untuk item tersebut.

Jika temuan dikelompokkan berdasarkan pengidentifikasi sumber daya atau jenis sumber daya, hasilnya mencakup semua sumber daya dalam temuan yang cocok. Ini termasuk sumber daya yang memiliki tipe berbeda dari jenis sumber daya yang ditentukan dalam kriteria filter. Misalnya, wawasan mengidentifikasi temuan yang terkait dengan ember S3. Jika temuan yang cocok berisi sumber daya bucket S3 dan sumber daya kunci akses IAM, hasil wawasan menyertakan kedua sumber daya tersebut.

Di konsol CSPM Security Hub, daftar hasil diurutkan dari sebagian besar hingga paling sedikit temuan pencocokan. Security Hub CSPM hanya dapat menampilkan 100 hasil. Jika ada lebih dari 100 nilai pengelompokan, Anda hanya melihat 100 yang pertama.

Selain daftar hasil, hasil wawasan menampilkan serangkaian bagan yang merangkum jumlah temuan yang cocok untuk atribut berikut.

- Label keparahan — Jumlah temuan untuk setiap label keparahan
- Akun AWS ID - Lima akun teratas IDs untuk temuan yang cocok
- Jenis sumber daya - Lima jenis sumber daya teratas untuk temuan yang cocok
- ID Sumber Daya — Lima sumber daya teratas IDs untuk temuan yang cocok
- Nama produk - Lima penyedia temuan teratas untuk temuan yang cocok

Jika Anda telah mengonfigurasi tindakan kustom, maka Anda dapat mengirim hasil yang dipilih ke tindakan kustom. Tindakan harus dikaitkan dengan CloudWatch aturan Amazon untuk jenis Security Hub Insight Results acara. Untuk informasi selengkapnya, lihat [the section called “Respon dan remediasi otomatis”](#). Jika Anda belum mengonfigurasi tindakan khusus, menu Tindakan dinonaktifkan.

Security Hub CSPM console

Untuk melihat dan mengambil tindakan pada hasil wawasan (konsol)

1. Buka konsol AWS Security Hub Cloud Security Posture Management (CSPM) di <https://console.aws.amazon.com/securityhub/>
2. Pada panel navigasi, silakan pilih Wawasan.
3. Untuk menampilkan daftar hasil insight, pilih nama insight.
4. Pilih kotak centang untuk setiap hasil untuk dikirim ke tindakan kustom.
5. Dari menu Tindakan, pilih tindakan kustom.

Security Hub CSPM API, AWS CLI

Untuk melihat dan mengambil tindakan pada hasil wawasan (API, AWS CLI)

Untuk melihat hasil insight, gunakan [>GetInsightResults](#) pengoperasian Security Hub CSPM API. Jika Anda menggunakan AWS CLI, jalankan [get-insight-results](#) perintah.

Untuk mengidentifikasi wawasan untuk mengembalikan hasil, Anda memerlukan wawasan ARN. Untuk mendapatkan wawasan ARNs untuk wawasan kustom, gunakan operasi [GetInsights](#) API atau [get-insight-results](#) perintah.

Contoh berikut mengambil hasil untuk wawasan yang ditentukan. Contoh ini diformat untuk Linux, macOS, atau Unix, dan menggunakan karakter garis miring terbalik (\) untuk meningkatkan keterbacaan.

```
$ aws securityhub get-insight-results --insight-arn "arn:aws:securityhub:us-west-1:123456789012:insight/123456789012/custom/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

Untuk informasi tentang cara membuat tindakan kustom secara terprogram, lihat. [Menggunakan tindakan khusus untuk mengirim temuan dan hasil wawasan ke EventBridge](#)

Melihat dan mengambil tindakan atas temuan hasil wawasan (konsol)

Dari daftar hasil wawasan di konsol CSPM Security Hub, Anda dapat menampilkan daftar temuan untuk setiap hasil.

Untuk menampilkan dan mengambil tindakan pada temuan wawasan (konsol)

1. Buka konsol AWS Security Hub Cloud Security Posture Management (CSPM) di. <https://console.aws.amazon.com/securityhub/>
2. Pada panel navigasi, silakan pilih Wawasan.
3. Untuk menampilkan daftar hasil insight, pilih nama insight.
4. Untuk menampilkan daftar temuan untuk hasil wawasan, pilih item dari daftar hasil. Daftar temuan menunjukkan temuan aktif untuk hasil wawasan yang dipilih yang memiliki status alur kerja NEW atau NOTIFIED.

Dari daftar temuan, Anda dapat melakukan tindakan berikut:

- [Penyaringan temuan di Security Hub CSPM](#)
- [Meninjau detail dan riwayat penemuan](#)
- [Menetapkan status alur kerja temuan di Security Hub CSPM](#)
- [Mengirim temuan ke tindakan CSPM Security Hub kustom](#)

Wawasan terkelola di Security Hub CSPM

AWS Security Hub Cloud Security Posture Management (CSPM) memberikan beberapa wawasan terkelola.

Anda tidak dapat mengedit atau menghapus wawasan terkelola CSPM Security Hub. Anda dapat [melihat dan mengambil tindakan atas hasil dan temuan wawasan](#). Anda juga dapat [menggunakan wawasan terkelola sebagai dasar untuk wawasan kustom baru](#).

Seperti semua wawasan, wawasan terkelola hanya mengembalikan hasil jika Anda telah mengaktifkan integrasi produk atau standar keamanan yang dapat menghasilkan temuan yang cocok.

Untuk wawasan yang dikelompokkan berdasarkan pengenalan sumber daya, hasilnya mencakup pengidentifikasi semua sumber daya dalam temuan yang cocok. Ini termasuk sumber daya yang memiliki tipe berbeda dari jenis sumber daya dalam kriteria filter. Misalnya, wawasan 2 dalam daftar berikut mengidentifikasi temuan yang terkait dengan bucket Amazon S3. Jika temuan yang cocok berisi sumber daya bucket S3 dan sumber daya kunci akses IAM, hasil wawasan menyertakan kedua sumber daya tersebut.

Security Hub CSPM saat ini menawarkan wawasan terkelola berikut:

1. AWS sumber daya dengan temuan terbanyak

ARN: `arn:aws:securityhub:::insight/securityhub/default/1`

Dikelompokkan berdasarkan: Pengenal sumber daya

Menemukan filter:

- Record state adalah ACTIVE
- Status alur kerja adalah NEW atau NOTIFIED

2. Bucket S3 dengan izin tulis atau baca publik

ARN: `arn:aws:securityhub:::insight/securityhub/default/10`

Dikelompokkan berdasarkan: Pengenal sumber daya

Menemukan filter:

- Jenis dimulai dengan Effects/Data Exposure

- Jenis sumber daya adalah AwsS3Bucket
- Record state adalah ACTIVE
- Status alur kerja adalah NEW atau NOTIFIED

3. AMIs yang menghasilkan temuan terbanyak

ARN: `arn:aws:securityhub:::insight/securityhub/default/3`

Dikelompokkan berdasarkan: EC2 contoh ID gambar

Menemukan filter:

- Jenis sumber daya adalah AwsEc2Instance
- Record state adalah ACTIVE
- Status alur kerja adalah NEW atau NOTIFIED

4. EC2 contoh yang terlibat dalam Taktik, Teknik, dan Prosedur yang diketahui () TTPs

ARN: `arn:aws:securityhub:::insight/securityhub/default/14`

Dikelompokkan berdasarkan: ID Sumber Daya

Menemukan filter:

- Jenis dimulai dengan TTPs
- Jenis sumber daya adalah AwsEc2Instance
- Record state adalah ACTIVE
- Status alur kerja adalah NEW atau NOTIFIED

5. AWS kepala sekolah dengan aktivitas kunci akses yang mencurigakan

ARN: `arn:aws:securityhub:::insight/securityhub/default/9`

Dikelompokkan berdasarkan: Nama utama kunci akses IAM

Menemukan filter:

- Jenis sumber daya adalah AwsIamAccessKey
- Record state adalah ACTIVE
- Status alur kerja adalah NEW atau NOTIFIED

6. AWS contoh sumber daya yang tidak memenuhi standar keamanan/praktik terbaik

ARN: `arn:aws:securityhub:::insight/securityhub/default/6`

Dikelompokkan berdasarkan: ID Sumber Daya

Menemukan filter:

- Tipe adalah Software and Configuration Checks/Industry and Regulatory Standards/AWS Security Best Practices
- Record state adalah ACTIVE
- Status alur kerja adalah NEW atau NOTIFIED

7. AWS sumber daya yang terkait dengan eksfiltrasi data potensial

ARN: `arn:aws:securityhub:::insight/securityhub/default/7`

Dikelompokkan berdasarkan: Resource ID

Menemukan filter:

- Jenis dimulai dengan Effects/Data Eksfiltrasi/
- Record state adalah ACTIVE
- Status alur kerja adalah NEW atau NOTIFIED

8. AWS sumber daya yang terkait dengan konsumsi sumber daya yang tidak sah

ARN: `arn:aws:securityhub:::insight/securityhub/default/8`

Dikelompokkan berdasarkan: ID Sumber Daya

Menemukan filter:

- Jenis dimulai dengan Effects/Resource Consumption
- Record state adalah ACTIVE
- Status alur kerja adalah NEW atau NOTIFIED

9. Bucket S3 yang tidak memenuhi standar keamanan/praktik terbaik

ARN: `arn:aws:securityhub:::insight/securityhub/default/11`

Dikelompokkan berdasarkan: ID Sumber Daya

Menemukan filter:

- Jenis sumber daya adalah AwsS3Bucket
- Tipe adalah Software and Configuration Checks/Industry and Regulatory Standards/AWS Security Best Practices
- Record state adalah ACTIVE
- Status alur kerja adalah NEW atau NOTIFIED

10. Bucket S3 dengan data sensitif

ARN: `arn:aws:securityhub:::insight/securityhub/default/12`

Dikelompokkan berdasarkan: ID Sumber Daya

Menemukan filter:

- Jenis sumber daya adalah AwsS3Bucket
- Jenis dimulai dengan Sensitive Data Identifications/
- Record state adalah ACTIVE
- Status alur kerja adalah NEW atau NOTIFIED

11. Kredensial yang mungkin bocor

ARN: `arn:aws:securityhub:::insight/securityhub/default/13`

Dikelompokkan berdasarkan: ID Sumber Daya

Menemukan filter:

- Jenis dimulai dengan Sensitive Data Identifications/Passwords/
- Record state adalah ACTIVE
- Status alur kerja adalah NEW atau NOTIFIED

12. EC2 contoh yang memiliki patch keamanan yang hilang untuk kerentanan penting

ARN: `arn:aws:securityhub:::insight/securityhub/default/16`

Dikelompokkan berdasarkan: ID Sumber Daya

Menemukan filter:

- Jenis dimulai dengan Software and Configuration Checks/Vulnerabilities/CVE

- Jenis sumber daya adalah `AwsEc2Instance`
- Record state adalah `ACTIVE`
- Status alur kerja adalah `NEW` atau `NOTIFIED`

13. EC2 contoh dengan perilaku umum yang tidak biasa

ARN: `arn:aws:securityhub:::insight/securityhub/default/17`

Dikelompokkan berdasarkan: ID Sumber Daya

Menemukan filter:

- Jenis dimulai dengan `Unusual Behaviors`
- Jenis sumber daya adalah `AwsEc2Instance`
- Record state adalah `ACTIVE`
- Status alur kerja adalah `NEW` atau `NOTIFIED`

14. EC2 contoh yang memiliki port yang dapat diakses dari Internet

ARN: `arn:aws:securityhub:::insight/securityhub/default/18`

Dikelompokkan berdasarkan: ID Sumber Daya

Menemukan filter:

- Jenis dimulai dengan `Software and Configuration Checks/AWS Security Best Practices/Network Reachability`
- Jenis sumber daya adalah `AwsEc2Instance`
- Record state adalah `ACTIVE`
- Status alur kerja adalah `NEW` atau `NOTIFIED`

15. EC2 contoh yang tidak memenuhi standar keamanan/praktik terbaik

ARN: `arn:aws:securityhub:::insight/securityhub/default/19`

Dikelompokkan berdasarkan: ID Sumber Daya

Menemukan filter:

- Jenis dimulai dengan salah satu dari berikut ini:
 - `Software and Configuration Checks/Industry and Regulatory Standards/`

- Software and Configuration Checks/AWS Security Best Practices
- Jenis sumber daya adalah AwsEc2Instance
- Record state adalah ACTIVE
- Status alur kerja adalah NEW atau NOTIFIED

16. EC2 contoh yang terbuka untuk Internet

ARN: `arn:aws:securityhub:::insight/securityhub/default/21`

Dikelompokkan berdasarkan: ID Sumber Daya

Menemukan filter:

- Jenis dimulai dengan Software and Configuration Checks/AWS Security Best Practices/Network Reachability
- Jenis sumber daya adalah AwsEc2Instance
- Record state adalah ACTIVE
- Status alur kerja adalah NEW atau NOTIFIED

17. EC2 contoh yang terkait dengan pengintaian musuh

ARN: `arn:aws:securityhub:::insight/securityhub/default/22`

Dikelompokkan berdasarkan: ID Sumber Daya

Menemukan filter:

- Jenis dimulai TTPs dengan/Discovery/Recon
- Jenis sumber daya adalah AwsEc2Instance
- Record state adalah ACTIVE
- Status alur kerja adalah NEW atau NOTIFIED

18. AWS sumber daya yang terkait dengan malware

ARN: `arn:aws:securityhub:::insight/securityhub/default/23`

Dikelompokkan berdasarkan: ID Sumber Daya

Menemukan filter:

- Jenis dimulai dengan salah satu dari berikut ini:
 - Effects/Data Exfiltration/Trojan
 - TTPs/Initial Access/Trojan
 - TTPs/Command and Control/Backdoor
 - TTPs/Command and Control/Trojan
 - Software and Configuration Checks/Backdoor
 - Unusual Behaviors/VM/Backdoor
- Record state adalah ACTIVE
- Status alur kerja adalah NEW atau NOTIFIED

19. AWS sumber daya yang terkait dengan masalah cryptocurrency

ARN: `arn:aws:securityhub:::insight/securityhub/default/24`

Dikelompokkan berdasarkan: ID Sumber Daya

Menemukan filter:

- Jenis dimulai dengan salah satu dari berikut ini:
 - Effects/Resource Consumption/Cryptocurrency
 - TTPs/Command and Control/CryptoCurrency
- Record state adalah ACTIVE
- Status alur kerja adalah NEW atau NOTIFIED

20. AWS sumber daya dengan upaya akses yang tidak sah

ARN: `arn:aws:securityhub:::insight/securityhub/default/25`

Dikelompokkan berdasarkan: ID Sumber Daya

Menemukan filter:

- Jenis dimulai dengan salah satu dari berikut ini:
 - TTPs/Command and Control/UnauthorizedAccess
 - TTPs/Initial Access/UnauthorizedAccess
 - Effects/Data Exfiltration/UnauthorizedAccess
 - Unusual Behaviors/User/UnauthorizedAccess

- Effects/Resource Consumption/UnauthorizedAccess
- Record state adalah ACTIVE
- Status alur kerja adalah NEW atau NOTIFIED

21. Indikator Ancaman Intel dengan hit terbanyak dalam seminggu terakhir

ARN: `arn:aws:securityhub:::insight/securityhub/default/26`

Menemukan filter:

- Dibuat dalam 7 hari terakhir

22. Akun teratas berdasarkan jumlah temuan

ARN: `arn:aws:securityhub:::insight/securityhub/default/27`

Dikelompokkan berdasarkan: ID Akun AWS

Menemukan filter:

- Record state adalah ACTIVE
- Status alur kerja adalah NEW atau NOTIFIED

23. Produk teratas berdasarkan jumlah temuan

ARN: `arn:aws:securityhub:::insight/securityhub/default/28`

Dikelompokkan berdasarkan: Nama produk

Menemukan filter:

- Record state adalah ACTIVE
- Status alur kerja adalah NEW atau NOTIFIED

24. Keparahan berdasarkan jumlah temuan

ARN: `arn:aws:securityhub:::insight/securityhub/default/29`

Dikelompokkan berdasarkan: Label keparahan

Menemukan filter:

- Record state adalah ACTIVE
- Status alur kerja adalah NEW atau NOTIFIED

25. Ember S3 teratas berdasarkan jumlah temuan

ARN: `arn:aws:securityhub:::insight/securityhub/default/30`

Dikelompokkan berdasarkan: ID Sumber Daya

Menemukan filter:

- Jenis sumber daya adalah `AwsS3Bucket`
- Record state adalah `ACTIVE`
- Status alur kerja adalah `NEW` atau `NOTIFIED`

26. EC2 Contoh teratas berdasarkan jumlah temuan

ARN: `arn:aws:securityhub:::insight/securityhub/default/31`

Dikelompokkan berdasarkan: ID Sumber Daya

Menemukan filter:

- Jenis sumber daya adalah `AwsEc2Instance`
- Record state adalah `ACTIVE`
- Status alur kerja adalah `NEW` atau `NOTIFIED`

27. Teratas AMIs dengan jumlah temuan

ARN: `arn:aws:securityhub:::insight/securityhub/default/32`

Dikelompokkan berdasarkan: EC2 contoh ID gambar

Menemukan filter:

- Jenis sumber daya adalah `AwsEc2Instance`
- Record state adalah `ACTIVE`
- Status alur kerja adalah `NEW` atau `NOTIFIED`

28. Pengguna IAM teratas berdasarkan jumlah temuan

ARN: `arn:aws:securityhub:::insight/securityhub/default/33`

Dikelompokkan berdasarkan: ID kunci akses IAM

Menemukan filter:

- Jenis sumber daya adalah `AwsIamAccessKey`
- Record state adalah `ACTIVE`
- Status alur kerja adalah `NEW` atau `NOTIFIED`

29. Sumber daya teratas berdasarkan jumlah pemeriksaan CIS yang gagal

ARN: `arn:aws:securityhub:::insight/securityhub/default/34`

Dikelompokkan berdasarkan: ID Sumber Daya

Menemukan filter:

- Generator ID dimulai dengan `arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule`
- Diperbarui di hari terakhir
- Status kepatuhan adalah `FAILED`
- Record state adalah `ACTIVE`
- Status alur kerja adalah `NEW` atau `NOTIFIED`

30. Integrasi teratas berdasarkan jumlah temuan

ARN: `arn:aws:securityhub:::insight/securityhub/default/35`

Dikelompokkan berdasarkan: Produk ARN

Menemukan filter:

- Record state adalah `ACTIVE`
- Status alur kerja adalah `NEW` atau `NOTIFIED`

31. Sumber daya dengan pemeriksaan keamanan paling gagal

ARN: `arn:aws:securityhub:::insight/securityhub/default/36`

Dikelompokkan berdasarkan: ID Sumber Daya

Menemukan filter:

- Diperbarui di hari terakhir
- Status kepatuhan adalah `FAILED`
- Record state adalah `ACTIVE`

- Status alur kerja adalah NEW atau NOTIFIED

32. Pengguna IAM dengan aktivitas mencurigakan

ARN: `arn:aws:securityhub:::insight/securityhub/default/37`

Dikelompokkan berdasarkan: Pengguna IAM

Menemukan filter:

- Jenis sumber daya adalah `AwsIamUser`
- Record state adalah `ACTIVE`
- Status alur kerja adalah NEW atau NOTIFIED

33. Sumber daya dengan AWS Health temuan terbanyak

ARN: `arn:aws:securityhub:::insight/securityhub/default/38`

Dikelompokkan berdasarkan: ID Sumber Daya

Menemukan filter:

- `ProductNamesama Health`

34. Sumber daya dengan AWS Config temuan terbanyak

ARN: `arn:aws:securityhub:::insight/securityhub/default/39`

Dikelompokkan berdasarkan: ID Sumber Daya

Menemukan filter:

- `ProductNamesama Config`

35. Aplikasi dengan temuan terbanyak

ARN: `arn:aws:securityhub:::insight/securityhub/default/40`

Dikelompokkan berdasarkan: `ResourceApplicationArn`

Menemukan filter:

- `RecordStatesama ACTIVE`
- `Workflow.Statussama NEW atau NOTIFIED`

Memahami wawasan khusus di Security Hub CSPM

Selain wawasan terkelola AWS Security Hub Cloud Security Posture Management (CSPM), Anda dapat membuat wawasan khusus di Security Hub CSPM untuk melacak masalah yang spesifik untuk lingkungan Anda. Wawasan khusus membantu Anda melacak subset masalah yang dikuratori.

Berikut adalah beberapa contoh wawasan khusus yang mungkin berguna untuk disiapkan:

- Jika Anda memiliki akun administrator, Anda dapat menyiapkan wawasan khusus untuk melacak temuan kritis dan tingkat keparahan tinggi yang memengaruhi akun anggota.
- Jika Anda mengandalkan [AWS layanan terintegrasi](#) tertentu, Anda dapat menyiapkan wawasan khusus untuk melacak temuan kritis dan tingkat keparahan tinggi dari layanan tersebut.
- Jika Anda mengandalkan [integrasi pihak ketiga](#), Anda dapat menyiapkan wawasan khusus untuk melacak temuan kritis dan tingkat keparahan tinggi dari produk terintegrasi tersebut.

Anda dapat membuat wawasan kustom yang benar-benar baru, atau mulai dari wawasan kustom atau terkelola yang ada.

Setiap wawasan dapat dikonfigurasi dengan opsi berikut:

- Atribut pengelompokan - Atribut pengelompokan menentukan item mana yang ditampilkan dalam daftar hasil wawasan. Misalnya, jika atribut pengelompokan adalah Nama Produk, hasil wawasan menampilkan jumlah temuan yang terkait dengan setiap penyedia temuan.
- Filter opsional — Filter mempersempit temuan yang cocok untuk wawasan.

Temuan disertakan dalam hasil wawasan hanya jika cocok dengan semua filter yang disediakan. Misalnya, jika filter adalah “Nama produk adalah GuardDuty” dan “Jenis sumber daya adalah AwsS3Bucket”, temuan yang cocok harus cocok dengan kedua kriteria ini.

Namun, Security Hub CSPM menerapkan logika BOOLEAN OR ke filter yang menggunakan atribut yang sama tetapi nilainya berbeda. Misalnya, jika filter adalah “Nama produk adalah GuardDuty” dan “Nama produk adalah Amazon Inspector”, temuan cocok jika dihasilkan oleh Amazon GuardDuty atau Amazon Inspector.

Jika Anda menggunakan pengenal sumber daya atau tipe sumber daya sebagai atribut pengelompokan, hasil wawasan mencakup semua sumber daya yang ada dalam temuan yang cocok. Daftar ini tidak terbatas pada sumber daya yang cocok dengan filter jenis sumber daya.

Misalnya, wawasan mengidentifikasi temuan yang terkait dengan ember S3, dan mengelompokkan temuan tersebut berdasarkan pengidentifikasi sumber daya. Temuan yang cocok berisi sumber daya bucket S3 dan sumber daya kunci akses IAM. Hasil wawasan mencakup kedua sumber daya.

Jika Anda mengaktifkan [agregasi lintas wilayah](#) dan kemudian membuat wawasan khusus, wawasan tersebut berlaku untuk temuan yang cocok di Wilayah agregasi dan Wilayah tertaut. Pengecualiannya adalah jika wawasan Anda menyertakan filter Wilayah.

Membuat wawasan khusus

Di AWS Security Hub Cloud Security Posture Management (CSPM), wawasan khusus dapat digunakan untuk mengumpulkan serangkaian temuan tertentu dan melacak masalah yang unik bagi lingkungan Anda. Untuk informasi latar belakang tentang wawasan khusus, lihat [Memahami wawasan khusus di Security Hub CSPM](#).

Pilih metode pilihan Anda, dan ikuti langkah-langkah untuk membuat wawasan khusus di Security Hub CSPM

Security Hub CSPM console

Untuk membuat wawasan khusus (konsol)

1. Buka konsol AWS Security Hub Cloud Security Posture Management (CSPM) di <https://console.aws.amazon.com/securityhub/>
2. Pada panel navigasi, silakan pilih Wawasan.
3. Pilih Buat wawasan.
4. Untuk memilih atribut pengelompokan untuk wawasan:
 - a. Pilih kotak pencarian untuk menampilkan opsi filter.
 - b. Pilih Grup berdasarkan.
 - c. Pilih atribut yang akan digunakan untuk mengelompokkan temuan yang terkait dengan wawasan ini.
 - d. Pilih Terapkan.
5. Secara opsional, pilih filter tambahan apa pun yang akan digunakan untuk wawasan ini. Untuk setiap filter, tentukan kriteria filter, lalu pilih Terapkan.
6. Pilih Buat wawasan.
7. Masukkan nama Insight, lalu pilih Create insight.

Security Hub CSPM API

Untuk membuat wawasan khusus (API)

1. Untuk membuat wawasan khusus, gunakan [CreateInsight](#) pengoperasian Security Hub CSPM API. Jika Anda menggunakan AWS CLI, jalankan [create-insight](#) perintah.
2. Isi Name parameter dengan nama untuk wawasan kustom Anda.
3. Isi Filters parameter untuk menentukan temuan mana yang akan dimasukkan dalam wawasan.
4. Isi GroupByAttribute parameter untuk menentukan atribut mana yang digunakan untuk mengelompokkan temuan yang termasuk dalam wawasan.
5. Secara opsional, isi SortCriteria parameter untuk mengurutkan temuan berdasarkan bidang tertentu.

Contoh berikut menciptakan wawasan khusus yang mencakup temuan penting dengan jenis AwsIamRole sumber daya. Contoh ini diformat untuk Linux, macOS, atau Unix, dan menggunakan karakter garis miring terbalik (\) untuk meningkatkan keterbacaan.

```
$ aws securityhub create-insight --name "Critical role findings" --filters  
'{"ResourceType": [{ "Comparison": "EQUALS", "Value": "AwsIamRole" }],  
"SeverityLabel": [{"Comparison": "EQUALS", "Value": "CRITICAL"}]}' --group-by-  
attribute "ResourceId"
```

PowerShell

Untuk membuat wawasan khusus (PowerShell)

1. Gunakan New-SHUBInsight cmdlet.
2. Isi Name parameter dengan nama untuk wawasan kustom Anda.
3. Isi Filter parameter untuk menentukan temuan mana yang akan dimasukkan dalam wawasan.
4. Isi GroupByAttribute parameter untuk menentukan atribut mana yang digunakan untuk mengelompokkan temuan yang termasuk dalam wawasan.

Jika Anda telah mengaktifkan [agregasi lintas wilayah](#) dan menggunakan cmdlet ini dari Wilayah agregasi, wawasan berlaku untuk temuan yang cocok dari agregasi dan Wilayah tertaut.

Contoh

```
$Filter = @{
    AwsAccountId = [Amazon.SecurityHub.Model.StringFilter]@{
        Comparison = "EQUALS"
        Value = "XXX"
    }
    ComplianceStatus = [Amazon.SecurityHub.Model.StringFilter]@{
        Comparison = "EQUALS"
        Value = 'FAILED'
    }
}
New-SHUBInsight -Filter $Filter -Name TestInsight -GroupByAttribute ResourceId
```

Membuat wawasan khusus dari wawasan terkelola (hanya konsol)

Anda tidak dapat menyimpan perubahan atau menghapus wawasan terkelola. Namun, Anda dapat menggunakan wawasan terkelola sebagai dasar untuk wawasan khusus. Ini adalah opsi di konsol CSPM Security Hub saja.

Untuk membuat wawasan khusus dari wawasan terkelola (konsol)

1. Buka konsol AWS Security Hub Cloud Security Posture Management (CSPM) di <https://console.aws.amazon.com/securityhub/>
2. Pada panel navigasi, silakan pilih Wawasan.
3. Pilih wawasan terkelola untuk bekerja.
4. Edit konfigurasi wawasan sesuai kebutuhan.
 - Untuk mengubah atribut yang digunakan untuk mengelompokkan temuan dalam wawasan:
 - a. Untuk menghapus pengelompokan yang ada, pilih X di sebelah Grup dengan pengaturan.
 - b. Pilih kotak pencarian.
 - c. Pilih atribut yang akan digunakan untuk pengelompokan.
 - d. Pilih Terapkan.
 - Untuk menghapus filter dari wawasan, pilih X yang dilingkari di sebelah filter.
 - Untuk menambahkan filter ke wawasan:
 - a. Pilih kotak pencarian.
 - b. Pilih atribut dan nilai yang akan digunakan sebagai filter.

c. Pilih Terapkan.

5. Saat pembaruan Anda selesai, pilih Buat wawasan.
6. Saat diminta, masukkan nama Insight, lalu pilih Buat wawasan.

Mengedit wawasan khusus

Anda dapat mengedit wawasan kustom yang ada untuk mengubah nilai pengelompokan dan filter. Setelah Anda membuat perubahan, Anda dapat menyimpan pembaruan ke wawasan asli, atau menyimpan versi yang diperbarui sebagai wawasan baru.

Di AWS Security Hub Cloud Security Posture Management (CSPM), wawasan khusus dapat digunakan untuk mengumpulkan serangkaian temuan tertentu dan melacak masalah yang unik bagi lingkungan Anda. Untuk informasi latar belakang tentang wawasan khusus, lihat [Memahami wawasan khusus di Security Hub CSPM](#).

Untuk mengedit wawasan khusus, pilih metode pilihan Anda, dan ikuti petunjuknya.

Security Hub CSPM console

Untuk mengedit wawasan khusus (konsol)

1. Buka konsol AWS Security Hub Cloud Security Posture Management (CSPM) di <https://console.aws.amazon.com/securityhub/>
2. Pada panel navigasi, silakan pilih Wawasan.
3. Pilih wawasan khusus untuk dimodifikasi.
4. Edit konfigurasi wawasan sesuai kebutuhan.
 - Untuk mengubah atribut yang digunakan untuk mengelompokkan temuan dalam wawasan:
 - a. Untuk menghapus pengelompokan yang ada, pilih X di sebelah Grup dengan pengaturan.
 - b. Pilih kotak pencarian.
 - c. Pilih atribut yang akan digunakan untuk pengelompokan.
 - d. Pilih Terapkan.
 - Untuk menghapus filter dari wawasan, pilih X yang dilingkari di sebelah filter.
 - Untuk menambahkan filter ke wawasan:
 - a. Pilih kotak pencarian.

- b. Pilih atribut dan nilai yang akan digunakan sebagai filter.
 - c. Pilih Terapkan.
5. Saat Anda menyelesaikan pembaruan, pilih Simpan wawasan.
6. Saat diminta, lakukan salah satu hal berikut:
 - Untuk memperbarui wawasan yang ada untuk mencerminkan perubahan Anda, pilih Perbarui, *<Insight_Name>* lalu pilih Simpan wawasan.
 - Untuk membuat wawasan baru dengan pembaruan, pilih Simpan wawasan baru. Masukkan nama Insight, lalu pilih Simpan wawasan.

Security Hub CSPM API

Untuk mengedit wawasan kustom (API)

1. Gunakan [UpdateInsight](#) pengoperasian Security Hub CSPM API. Jika Anda menggunakan [update-insight](#) perintah AWS CLI run.
2. Untuk mengidentifikasi wawasan khusus yang ingin Anda perbarui, berikan Amazon Resource Name (ARN) insight tersebut. Untuk mendapatkan ARN dari wawasan khusus, gunakan [GetInsights](#) operasi atau perintah. [get-insights](#)
3. PerbaruiName, Filters, dan GroupByAttribute parameter sesuai kebutuhan.

Contoh berikut memperbarui wawasan yang ditentukan. Contoh ini diformat untuk Linux, macOS, atau Unix, dan menggunakan karakter garis miring terbalik (\) untuk meningkatkan keterbacaan.

```
$ aws securityhub update-insight --insight-arn "arn:aws:securityhub:us-west-1:123456789012:insight/123456789012/custom/a1b2c3d4-5678-90ab-cdef-EXAMPLE1111" --filters '{"ResourceType": [{ "Comparison": "EQUALS", "Value": "AwsIamRole"}], "SeverityLabel": [{"Comparison": "EQUALS", "Value": "HIGH"}]}' --name "High severity role findings"
```

PowerShell

Untuk mengedit wawasan khusus (PowerShell)

1. Gunakan Update-SHUBInsight cmdlet.

2. Untuk mengidentifikasi wawasan khusus, berikan Amazon Resource Name (ARN) wawasan tersebut. Untuk mendapatkan ARN dari wawasan khusus, gunakan cmdlet. `Get-SHUBInsight`
3. Perbarui `Name`, `Filter`, dan `GroupByAttribute` parameter sesuai kebutuhan.

Contoh

```
$Filter = @{
    ResourceType = [Amazon.SecurityHub.Model.StringFilter]@{
        Comparison = "EQUALS"
        Value = "AwsIamRole"
    }
    SeverityLabel = [Amazon.SecurityHub.Model.StringFilter]@{
        Comparison = "EQUALS"
        Value = "HIGH"
    }
}

Update-SHUBInsight -InsightArn "arn:aws:securityhub:us-west-1:123456789012:insight/123456789012/custom/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111" -Filter $Filter -Name "High severity role findings"
```

Menghapus wawasan khusus

Di AWS Security Hub Cloud Security Posture Management (CSPM), wawasan khusus dapat digunakan untuk mengumpulkan serangkaian temuan tertentu dan melacak masalah yang unik bagi lingkungan Anda. Untuk informasi latar belakang tentang wawasan khusus, lihat [Memahami wawasan khusus di Security Hub CSPM](#).

Untuk menghapus wawasan khusus, pilih metode pilihan Anda, dan ikuti petunjuknya. Anda tidak dapat menghapus wawasan terkelola.

Security Hub CSPM console

Untuk menghapus wawasan khusus (konsol)

1. Buka konsol AWS Security Hub Cloud Security Posture Management (CSPM) di <https://console.aws.amazon.com/securityhub/>
2. Pada panel navigasi, silakan pilih Wawasan.

3. Temukan wawasan khusus untuk dihapus.
4. Untuk wawasan itu, pilih ikon opsi lainnya (tiga titik di sudut kanan atas kartu).
5. Pilih Hapus.

Security Hub CSPM API

Untuk menghapus wawasan kustom (API)

1. Gunakan [DeleteInsight](#) pengoperasian Security Hub CSPM API. Jika Anda menggunakan [delete-insight](#) perintah AWS CLI run.
2. Untuk mengidentifikasi wawasan khusus yang akan dihapus, berikan ARN wawasan. Untuk mendapatkan ARN dari wawasan khusus, gunakan [GetInsights](#) operasi atau [get-insights](#) perintah.

Contoh berikut menghapus wawasan yang ditentukan. Contoh ini diformat untuk Linux, macOS, atau Unix, dan menggunakan karakter garis miring terbalik (\) untuk meningkatkan keterbacaan.

```
$ aws securityhub delete-insight --insight-arn "arn:aws:securityhub:us-west-1:123456789012:insight/123456789012/custom/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

PowerShell

Untuk menghapus wawasan kustom (PowerShell)

1. Gunakan `Remove-SHUBInsight` cmdlet.
2. Untuk mengidentifikasi wawasan khusus, berikan ARN wawasan. Untuk mendapatkan ARN dari wawasan khusus, gunakan cmdlet `Get-SHUBInsight`

Contoh

```
-InsightArn "arn:aws:securityhub:us-west-1:123456789012:insight/123456789012/custom/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

Secara otomatis memodifikasi dan bertindak atas temuan di Security Hub CSPM

AWS Security Hub Cloud Security Posture Management (CSPM) memiliki fitur yang secara otomatis memodifikasi dan mengambil tindakan atas temuan berdasarkan spesifikasi Anda.

Security Hub CSPM saat ini mendukung dua jenis otomatisasi:

- Aturan otomatisasi — Memperbarui dan menekan temuan secara otomatis dalam waktu dekat berdasarkan kriteria yang Anda tentukan.
- Respons dan remediasi otomatis — Buat EventBridge aturan Amazon khusus yang menentukan tindakan otomatis yang harus diambil terhadap temuan dan wawasan tertentu.

Aturan otomatisasi sangat membantu saat Anda ingin memperbarui bidang pencarian secara otomatis di AWS Security Finding Format (ASFF). Misalnya, Anda dapat menggunakan aturan otomatisasi untuk memperbarui tingkat keparahan atau status alur kerja temuan dari integrasi pihak ketiga tertentu. Menggunakan aturan otomatisasi menghilangkan kebutuhan untuk memperbarui tingkat keparahan atau status alur kerja secara manual dari setiap temuan dari produk pihak ketiga ini.

EventBridge aturan sangat membantu ketika Anda ingin mengambil tindakan di luar CSPM Security Hub sehubungan dengan temuan spesifik atau mengirimkan temuan spesifik ke alat pihak ketiga untuk remediasi atau penyelidikan tambahan. Aturan dapat digunakan untuk memicu tindakan yang didukung, seperti menjalankan AWS Lambda fungsi atau memberi tahu topik Amazon Simple Notification Service (Amazon SNS) tentang temuan tertentu.

Aturan otomatisasi berlaku sebelum EventBridge aturan diterapkan. Artinya, aturan otomatisasi dipicu dan memperbarui temuan sebelum EventBridge menerima temuan. EventBridge aturan kemudian berlaku untuk temuan yang diperbarui.

Saat menyiapkan otomatisasi untuk kontrol keamanan, sebaiknya filter berdasarkan ID kontrol daripada judul atau deskripsi. Sedangkan Security Hub CSPM terkadang memperbarui judul dan deskripsi kontrol, kontrol IDs tetap sama.

Topik

- [Memahami aturan otomatisasi di Security Hub CSPM](#)
- [Menggunakan EventBridge untuk respon otomatis dan remediasi](#)

Memahami aturan otomatisasi di Security Hub CSPM

Anda dapat menggunakan aturan otomatisasi untuk memperbarui temuan secara otomatis di AWS Security Hub Cloud Security Posture Management (CSPM). Saat menyerap temuan, Security Hub CSPM dapat menerapkan berbagai tindakan aturan, seperti menekan temuan, mengubah tingkat keparahannya, dan menambahkan catatan. Tindakan aturan tersebut mengubah temuan yang sesuai dengan kriteria yang Anda tentukan.

Contoh kasus penggunaan untuk aturan otomatisasi meliputi:

- Meningkatkan keparahan temuan CRITICAL jika ID sumber daya temuan mengacu pada sumber daya bisnis yang penting.
- Meningkatkan keparahan temuan dari HIGH CRITICAL jika temuan tersebut memengaruhi sumber daya dalam akun produksi tertentu.
- Menetapkan temuan spesifik yang memiliki tingkat keparahan status INFORMATIONAL SUPPRESSED alur kerja.

Anda dapat membuat dan mengelola aturan otomatisasi hanya dari akun administrator CSPM Security Hub.

Aturan berlaku untuk temuan baru dan temuan terbaru. Anda dapat membuat aturan kustom dari awal, atau menggunakan templat aturan yang disediakan oleh Security Hub CSPM. Anda juga dapat memulai dengan template dan memodifikasinya sesuai kebutuhan.

Mendefinisikan kriteria aturan dan tindakan aturan

Dari akun administrator CSPM Security Hub, Anda dapat membuat aturan otomatisasi dengan menentukan satu atau beberapa kriteria aturan dan satu atau beberapa tindakan aturan. Ketika temuan cocok dengan kriteria yang ditentukan, Security Hub CSPM menerapkan tindakan aturan untuk itu. Untuk informasi selengkapnya tentang kriteria dan tindakan yang tersedia, lihat [Kriteria aturan dan tindakan aturan yang tersedia](#).

Security Hub CSPM saat ini mendukung maksimal 100 aturan otomatisasi untuk setiap akun administrator.

Akun administrator CSPM Security Hub juga dapat mengedit, melihat, dan menghapus aturan otomatisasi. Aturan berlaku untuk pencocokan temuan di akun administrator dan semua akun anggotanya. Dengan menyediakan akun anggota IDs sebagai kriteria aturan, administrator CSPM

Security Hub juga dapat menggunakan aturan otomatisasi untuk memperbarui atau menekan temuan di akun anggota tertentu.

Aturan otomatisasi hanya berlaku Wilayah AWS di tempat pembuatannya. Untuk menerapkan aturan di beberapa Wilayah, administrator harus membuat aturan di setiap Wilayah. Ini dapat dilakukan melalui konsol CSPM Security Hub, Security Hub CSPM API, atau [AWS CloudFormation](#). Anda juga dapat menggunakan skrip [penyebaran Multi-wilayah](#).

Kriteria aturan dan tindakan aturan yang tersedia

Bidang AWS Security Finding Format (ASFF) berikut saat ini didukung sebagai kriteria untuk aturan otomatisasi:

Kriteria aturan	Operator filter	Jenis bidang
AwsAccountId	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
AwsAccountName	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
CompanyName	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
ComplianceAssociatedStandardsId	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
ComplianceSecurityControlId	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS,	String

Kriteria aturan	Operator filter	Jenis bidang
	NOT_EQUALS, PREFIX_NOT_EQUALS	
ComplianceStatus	Is, Is Not	Pilih: [FAILED,NOT_AVAILABLE ,PASSED,WARNING]
Confidence	Eq (equal-to), Gte (greater-than-equal), Lte (less-than-equal)	Bilangan
CreatedAt	Start, End, DateRange	Tanggal (diformat sebagai 2022-12-01T 21:47:39.269 Z)
Criticality	Eq (equal-to), Gte (greater-than-equal), Lte (less-than-equal)	Bilangan
Description	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
FirstObservedAt	Start, End, DateRange	Tanggal (diformat sebagai 2022-12-01T 21:47:39.269 Z)
GeneratorId	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
Id	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String

Kriteria aturan	Operator filter	Jenis bidang
LastObservedAt	Start, End, DateRange	Tanggal (diformat sebagai 2022-12-01T 21:47:39.269 Z)
NoteText	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
NoteUpdatedAt	Start, End, DateRange	Tanggal (diformat sebagai 2022-12-01T 21:47:39.269 Z)
NoteUpdatedBy	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
ProductArn	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
ProductName	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
RecordState	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
RelatedFindingsId	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String

Kriteria aturan	Operator filter	Jenis bidang
RelatedFindingsProductArn	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
ResourceApplicationArn	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
ResourceApplicationName	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
ResourceDetailsOther	CONTAINS, EQUALS, NOT_CONTAINS, NOT_EQUALS	Peta
ResourceId	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
ResourcePartition	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
ResourceRegion	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String

Kriteria aturan	Operator filter	Jenis bidang
ResourceTags	CONTAINS, EQUALS, NOT_CONTAINS, NOT_EQUALS	Peta
ResourceType	Is, Is Not	Pilih (lihat Sumber yang didukung oleh ASFF)
SeverityLabel	Is, Is Not	Pilih: [CRITICAL,HIGH,MEDIUM,LOW,INFORMATIONAL]
SourceUrl	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
Title	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
Type	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
UpdatedAt	Start, End, DateRange	Tanggal (diformat sebagai 2022-12-01T 21:47:39.269 Z)
UserDefinedFields	CONTAINS, EQUALS, NOT_CONTAINS, NOT_EQUALS	Peta

Kriteria aturan	Operator filter	Jenis bidang
VerificationState	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
WorkflowStatus	Is, Is Not	Pilih: [NEW,NOTIFIED,RESOLVED,SUPPRESSED]

Untuk kriteria yang diberi label sebagai bidang string, menggunakan operator filter yang berbeda pada bidang yang sama memengaruhi logika evaluasi. Untuk informasi selengkapnya, lihat [StringFilter](#) di Referensi API AWS Security Hub Cloud Security Posture Management (CSPM) Security Hub.

Setiap kriteria mendukung jumlah maksimum nilai yang dapat digunakan untuk menyaring temuan yang cocok. Untuk batasan pada setiap kriteria, lihat [AutomationRulesFindingFilters](#) di Referensi API AWS Security Hub Cloud Security Posture Management (CSPM) Security Hub.

Bidang ASFF berikut saat ini didukung sebagai tindakan untuk aturan otomatisasi:

- Confidence
- Criticality
- Note
- RelatedFindings
- Severity
- Types
- UserDefinedFields
- VerificationState
- Workflow

Untuk informasi selengkapnya tentang bidang ASFF tertentu, lihat sintaks [AWS Security Finding Format \(ASFF\)](#).

 Tip

Jika Anda ingin Security Hub CSPM berhenti menghasilkan temuan untuk kontrol tertentu, sebaiknya nonaktifkan kontrol daripada menggunakan aturan otomatisasi. Ketika Anda menonaktifkan kontrol, Security Hub CSPM berhenti menjalankan pemeriksaan keamanan di atasnya dan berhenti menghasilkan temuan untuk itu, sehingga Anda tidak akan dikenakan biaya untuk kontrol itu. Sebaiknya gunakan aturan otomatisasi untuk mengubah nilai bidang ASFF tertentu untuk temuan yang sesuai dengan kriteria yang ditentukan. Untuk informasi selengkapnya tentang menonaktifkan kontrol, lihat [Menonaktifkan kontrol di Security Hub CSPM](#)

Temuan yang dievaluasi oleh aturan otomatisasi

Aturan otomatisasi mengevaluasi temuan baru dan terbaru yang dihasilkan atau diserap oleh Security Hub CSPM melalui [BatchImportFindings](#) operasi setelah Anda membuat aturan. Security Hub CSPM memperbarui temuan kontrol setiap 12-24 jam atau ketika sumber daya terkait berubah status. Untuk informasi selengkapnya, lihat [Jadwal untuk menjalankan pemeriksaan keamanan](#).

Aturan otomatisasi mengevaluasi temuan asli yang disediakan penyedia. Penyedia dapat menyediakan temuan baru dan memperbarui temuan yang ada melalui `BatchImportFindings` pengoperasian Security Hub CSPM API. Aturan tidak dipicu saat Anda memperbarui bidang pencarian setelah pembuatan aturan melalui [BatchUpdateFindings](#) operasi. Jika Anda membuat aturan otomatisasi dan membuat `BatchUpdateFindings` pembaruan yang memengaruhi bidang temuan yang sama, pembaruan terakhir akan menetapkan nilai untuk bidang tersebut. Ambil contoh berikut:

1. Anda gunakan `BatchUpdateFindings` untuk memperbarui `Workflow.Status` bidang temuan dari `NEW` ke `NOTIFIED`.
2. Jika Anda menelepon `GetFindings`, `Workflow.Status` bidang sekarang memiliki nilai `NOTIFIED`.
3. Anda membuat aturan otomatisasi yang mengubah `Workflow.Status` bidang temuan dari `NEW` ke `SUPPRESSED` (ingat bahwa aturan mengabaikan pembaruan yang dibuat dengan `BatchUpdateFindings`).
4. Penyedia pencarian menggunakan `BatchImportFindings` untuk memperbarui temuan dan mengubah `Workflow.Status` bidang menjadi `NEW`.

5. Jika Anda menelepon `GetFindings`, `Workflow.Status` bidang sekarang memiliki nilai `SUPPRESSED` karena aturan otomatisasi diterapkan, dan aturan adalah tindakan terakhir yang diambil pada temuan.

Saat Anda membuat atau mengedit aturan di konsol CSPM Security Hub, konsol akan menampilkan beta temuan yang sesuai dengan kriteria aturan. Sementara aturan otomatisasi mengevaluasi temuan asli yang dikirim oleh penyedia temuan, beta konsol mencerminkan temuan dalam keadaan akhir mereka karena akan ditampilkan dalam respons terhadap operasi [GetFindingsAPI](#) (yaitu, setelah tindakan aturan atau pembaruan lain diterapkan pada temuan).

Cara kerja urutan aturan

Saat membuat aturan otomatisasi, Anda menetapkan setiap aturan pesanan. Ini menentukan urutan di mana Security Hub CSPM menerapkan aturan otomatisasi Anda, dan menjadi penting ketika beberapa aturan terkait dengan bidang temuan atau pencarian yang sama.

Ketika beberapa tindakan aturan berhubungan dengan bidang temuan atau pencarian yang sama, aturan dengan nilai numerik tertinggi untuk urutan aturan berlaku terakhir dan memiliki efek akhir.

Saat Anda membuat aturan di konsol CSPM Security Hub, Security Hub CSPM secara otomatis menetapkan urutan aturan berdasarkan urutan pembuatan aturan. Aturan yang paling baru dibuat memiliki nilai numerik terendah untuk urutan aturan dan oleh karena itu berlaku terlebih dahulu. Security Hub CSPM menerapkan aturan berikutnya dalam urutan menaik.

Bila Anda membuat aturan melalui Security Hub CSPM API atau AWS CLI, Security Hub CSPM menerapkan aturan dengan nilai numerik terendah untuk pertama. `RuleOrder` Ini kemudian menerapkan aturan selanjutnya dalam urutan menaik. Jika beberapa temuan memiliki hal yang sama `RuleOrder`, Security Hub CSPM menerapkan aturan dengan nilai sebelumnya untuk `UpdatedAt` bidang terlebih dahulu (yaitu, aturan yang terakhir diedit berlaku terakhir).

Anda dapat mengubah urutan aturan kapan saja.

Contoh urutan aturan:

Aturan A (urutan aturan adalah **1**):

- Kriteria Aturan A
 - `ProductName = Security Hub CSPM`

- `Resources.Type` adalah S3 Bucket
- `Compliance.Status` = FAILED
- `RecordState` adalah NEW
- `Workflow.Status` = ACTIVE
- Aturan A tindakan
 - Perbarui Confidence ke 95
 - Perbarui Severity ke CRITICAL

Aturan B (urutan aturan adalah 2):

- Kriteria aturan B
 - `AwsAccountId` = 123456789012
- Tindakan aturan B
 - Perbarui Severity ke INFORMATIONAL

Aturan Tindakan diterapkan terlebih dahulu pada temuan CSPM Security Hub yang cocok dengan kriteria Aturan A. Selanjutnya, tindakan Aturan B berlaku untuk temuan CSPM Security Hub dengan ID akun yang ditentukan. Dalam contoh ini, karena Aturan B berlaku terakhir, nilai akhir Severity dalam temuan dari ID akun yang ditentukan adalah INFORMATIONAL. Berdasarkan tindakan Aturan A, nilai akhir dari temuan Confidence yang cocok adalah 95.

Membuat aturan otomatisasi

Aturan otomatisasi dapat digunakan untuk memperbarui temuan secara otomatis di AWS Security Hub Cloud Security Posture Management (CSPM). Anda dapat membuat aturan otomatisasi kustom dari awal atau, di konsol CSPM Security Hub, gunakan templat aturan yang telah diisi sebelumnya. Untuk informasi latar belakang tentang cara kerja aturan otomatisasi, lihat [Memahami aturan otomatisasi di Security Hub CSPM](#).

Anda hanya dapat membuat satu aturan otomatisasi pada satu waktu. Untuk membuat beberapa aturan otomatisasi, ikuti prosedur konsol beberapa kali, atau panggil API atau perintah beberapa kali dengan parameter yang Anda inginkan.

Anda harus membuat aturan otomatisasi di setiap Wilayah dan akun di mana Anda ingin aturan tersebut diterapkan pada temuan.

Saat Anda membuat aturan otomatisasi di konsol CSPM Security Hub, Security Hub CSPM menunjukkan versi beta dari temuan yang diterapkan aturan Anda. Beta saat ini tidak didukung jika kriteria aturan Anda menyertakan filter CONTAINS atau NOT_CONTAINS. Anda dapat memilih filter ini untuk jenis bidang peta dan string.

 Important

AWS merekomendasikan agar Anda tidak menyertakan informasi identitas pribadi, rahasia, atau sensitif dalam nama aturan, deskripsi, atau bidang lainnya.

Membuat aturan otomatisasi khusus

Pilih metode pilihan Anda, dan selesaikan langkah-langkah berikut untuk membuat aturan otomatisasi kustom.

Console

Untuk membuat aturan otomatisasi kustom (konsol)

1. Menggunakan kredensi administrator CSPM Security Hub, buka konsol Security Hub AWS Cloud Security Posture Management (CSPM) di <https://console.aws.amazon.com/securityhub/>
2. Di panel navigasi, pilih Otomatisasi.
3. Pilih Buat aturan. Untuk Jenis Aturan, pilih Buat aturan khusus.
4. Di bagian Aturan, berikan nama aturan unik dan deskripsi untuk aturan Anda.
5. Untuk Kriteria, gunakan menu drop-down Kunci, Operator, dan Nilai untuk menentukan kriteria aturan Anda. Anda harus menentukan setidaknya satu kriteria aturan.

Jika didukung untuk kriteria yang Anda pilih, konsol akan menampilkan beta temuan yang sesuai dengan kriteria Anda.

6. Untuk tindakan Otomatis, gunakan menu tarik-turun untuk menentukan bidang pencarian mana yang akan diperbarui saat temuan cocok dengan kriteria aturan Anda. Anda harus menentukan setidaknya satu tindakan aturan.
7. Untuk status Aturan, pilih apakah Anda ingin aturan Diaktifkan atau Dinonaktifkan setelah dibuat.

8. (Opsional) Perluas bagian Pengaturan tambahan. Pilih Abaikan aturan berikutnya untuk temuan yang cocok dengan kriteria ini jika Anda ingin aturan ini menjadi aturan terakhir yang diterapkan pada temuan yang cocok dengan kriteria aturan.
9. (Opsional) Untuk Tag, tambahkan tag sebagai pasangan nilai kunci untuk membantu Anda mengidentifikasi aturan dengan mudah.
10. Pilih Buat aturan.

API

Untuk membuat aturan otomatisasi kustom (API)

1. Jalankan [CreateAutomationRule](#) dari akun administrator CSPM Security Hub. API ini membuat aturan dengan Amazon Resource Name (ARN) tertentu.
2. Sediakan nama dan deskripsi untuk aturan.
3. Tetapkan `IsTerminal` parameter ke `true` jika Anda ingin aturan ini menjadi aturan terakhir yang diterapkan pada temuan yang cocok dengan kriteria aturan.
4. Untuk `RuleOrder` parameter, berikan urutan aturan. Security Hub CSPM menerapkan aturan dengan nilai numerik yang lebih rendah untuk parameter ini terlebih dahulu.
5. Untuk `RuleStatus` parameter, tentukan apakah Anda ingin CSPM Security Hub mengaktifkan dan mulai menerapkan aturan ke temuan setelah pembuatan. Jika tidak ada nilai yang ditentukan, nilai defaultnya adalah `ENABLED`. Nilai `DISABLED` berarti bahwa aturan dijeda setelah penciptaan.
6. Untuk `Criteria` parameter, berikan kriteria yang ingin digunakan CSPM Security Hub untuk memfilter temuan Anda. Tindakan aturan akan berlaku untuk temuan yang sesuai dengan kriteria. Untuk daftar kriteria yang didukung, lihat [Kriteria aturan dan tindakan aturan yang tersedia](#).
7. Untuk `Actions` parameter, berikan tindakan yang ingin dilakukan CSPM Security Hub saat ada kecocokan antara temuan dan kriteria yang ditentukan. Untuk daftar tindakan yang didukung, lihat [Kriteria aturan dan tindakan aturan yang tersedia](#).

Contoh AWS CLI perintah berikut membuat aturan otomatisasi memperbarui status alur kerja dan catatan temuan yang cocok. Contoh ini diformat untuk Linux, macOS, atau Unix, dan menggunakan karakter garis miring terbalik (\) untuk meningkatkan keterbacaan.

```
$ aws securityhub create-automation-rule \
```

```
--actions '[{
  "Type": "FINDING_FIELDS_UPDATE",
  "FindingFieldsUpdate": {
    "Severity": {
      "Label": "HIGH"
    },
    "Note": {
      "Text": "Known issue that is a risk. Updated by automation rules",
      "UpdatedBy": "sechub-automation"
    }
  }
}]' \
--criteria '{
  "SeverityLabel": [{
    "Value": "INFORMATIONAL",
    "Comparison": "EQUALS"
  }]
}' \
--description "A sample rule" \
--no-is-terminal \
--rule-name "sample rule" \
--rule-order 1 \
--rule-status "ENABLED" \
--region us-east-1
```

Membuat aturan otomatisasi dari template (hanya konsol)

Template aturan mencerminkan kasus penggunaan umum untuk aturan otomatisasi. Saat ini, hanya konsol CSPM Security Hub yang mendukung template aturan. Selesaikan langkah-langkah berikut untuk membuat aturan otomatisasi dari templat di konsol.

Untuk membuat aturan otomatisasi dari template (konsol)

1. Menggunakan kredensi administrator CSPM Security Hub, buka konsol Security Hub AWS Cloud Security Posture Management (CSPM) di <https://console.aws.amazon.com/securityhub/>
2. Di panel navigasi, pilih Otomatisasi.
3. Pilih Buat aturan. Untuk Jenis Aturan, pilih Buat aturan dari templat.
4. Pilih template aturan dari menu drop-down.
5. (Opsional) Jika perlu untuk kasus penggunaan Anda, ubah bagian Aturan, Kriteria, dan Tindakan Otomatis. Anda harus menentukan setidaknya satu kriteria aturan dan satu tindakan aturan.

Jika didukung untuk kriteria yang Anda pilih, konsol akan menampilkan beta temuan yang sesuai dengan kriteria Anda.

6. Untuk status Aturan, pilih apakah Anda ingin aturan Diaktifkan atau Dinonaktifkan setelah dibuat.
7. (Opsional) Perluas bagian Pengaturan tambahan. Pilih Abaikan aturan berikutnya untuk temuan yang cocok dengan kriteria ini jika Anda ingin aturan ini menjadi aturan terakhir yang diterapkan pada temuan yang cocok dengan kriteria aturan.
8. (Opsional) Untuk Tag, tambahkan tag sebagai pasangan nilai kunci untuk membantu Anda mengidentifikasi aturan dengan mudah.
9. Pilih Buat aturan.

Melihat aturan otomatisasi

Aturan otomatisasi dapat digunakan untuk memperbarui temuan secara otomatis di AWS Security Hub Cloud Security Posture Management (CSPM). Untuk informasi latar belakang tentang cara kerja aturan otomatisasi, lihat [Memahami aturan otomatisasi di Security Hub CSPM](#).

Pilih metode pilihan Anda, dan ikuti langkah-langkah untuk melihat aturan otomatisasi yang ada dan detail setiap aturan.

Untuk melihat riwayat bagaimana aturan otomatisasi telah mengubah temuan Anda, lihat [Meninjau detail dan riwayat penemuan di Security Hub CSPM](#).

Console

Untuk melihat aturan otomatisasi (konsol)

1. Menggunakan kredensi administrator CSPM Security Hub, buka konsol Security Hub AWS Cloud Security Posture Management (CSPM) di <https://console.aws.amazon.com/securityhub/>
2. Di panel navigasi, pilih Otomatisasi.
3. Pilih nama aturan. Atau, pilih aturan.
4. Pilih Tindakan dan Tampilan.

API

Untuk melihat aturan otomatisasi (API)

1. Untuk melihat aturan otomatisasi akun Anda, jalankan [ListAutomationRules](#) dari akun administrator CSPM Security Hub. API ini mengembalikan aturan ARNs dan metadata lainnya untuk aturan Anda. Tidak ada parameter input yang diperlukan untuk API ini, tetapi Anda dapat secara opsional menyediakan `MaxResults` untuk membatasi jumlah hasil dan `NextToken` sebagai parameter pagination. Nilai awal `NextToken` harus `NULL`.
2. Untuk detail aturan tambahan, termasuk kriteria dan tindakan untuk aturan, jalankan [BatchGetAutomationRules](#) dari akun administrator CSPM Security Hub. Berikan aturan ARNs otomatisasi yang Anda inginkan detailnya.

Contoh berikut mengambil rincian untuk aturan otomatisasi yang ditentukan. Contoh ini diformat untuk Linux, macOS, atau Unix, dan menggunakan karakter garis miring terbalik (\) untuk meningkatkan keterbacaan.

```
$ aws securityhub batch-get-automation-rules \
--automation-rules-arns '["arn:aws:securityhub:us-
east-1:123456789012:automation-rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
"arn:aws:securityhub:us-east-1:123456789012:automation-rule/a1b2c3d4-5678-90ab-
cdef-EXAMPLE22222"]' \
--region us-east-1
```

Mengedit aturan otomatisasi

Aturan otomatisasi dapat digunakan untuk memperbarui temuan secara otomatis di AWS Security Hub Cloud Security Posture Management (CSPM). Untuk informasi latar belakang tentang cara kerja aturan otomatisasi, lihat [Memahami aturan otomatisasi di Security Hub CSPM](#).

Setelah membuat aturan otomatisasi, administrator CSPM Security Hub yang didelegasikan dapat mengedit aturan. Saat Anda mengedit aturan otomatisasi, perubahan berlaku untuk temuan baru dan terbaru yang dihasilkan atau diserap oleh Security Hub CSPM setelah aturan diedit.

Pilih metode pilihan Anda, dan ikuti langkah-langkah untuk mengedit konten aturan otomatisasi. Anda dapat mengedit satu atau beberapa aturan dengan satu permintaan. Untuk petunjuk tentang urutan aturan pengeditan, lihat [Mengedit urutan aturan otomatisasi](#).

Console

Untuk mengedit aturan otomatisasi (konsol)

1. Menggunakan kredensi administrator CSPM Security Hub, buka konsol Security Hub AWS Cloud Security Posture Management (CSPM) di <https://console.aws.amazon.com/securityhub/>
2. Di panel navigasi, pilih Otomatisasi.
3. Pilih aturan yang ingin Anda edit. Pilih Tindakan dan Edit.
4. Ubah aturan sesuai keinginan, dan pilih Simpan perubahan.

API

Untuk mengedit aturan otomatisasi (API)

1. Jalankan [BatchUpdateAutomationRules](#) dari akun administrator CSPM Security Hub.
2. Untuk RuleArn parameter, berikan ARN dari aturan yang ingin Anda edit.
3. Berikan nilai baru untuk parameter yang ingin Anda edit. Anda dapat mengedit parameter apa pun kecuali RuleArn.

Contoh berikut memperbarui aturan otomatisasi yang ditentukan. Contoh ini diformat untuk Linux, macOS, atau Unix, dan menggunakan karakter garis miring terbalik (\) untuk meningkatkan keterbacaan.

```
$ aws securityhub batch-update-automation-rules \
--update-automation-rules-request-items '[
  {
    "Actions": [{
      "Type": "FINDING_FIELDS_UPDATE",
      "FindingFieldsUpdate": {
        "Note": {
          "Text": "Known issue that is a risk",
          "UpdatedBy": "sechub-automation"
        },
        "Workflow": {
          "Status": "NEW"
        }
      }
    }
  ]],
```

```
"Criteria": {
  "SeverityLabel": [{
    "Value": "LOW",
    "Comparison": "EQUALS"
  }]
},
"RuleArn": "arn:aws:securityhub:us-east-1:123456789012:automation-
rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
"RuleOrder": 14,
"RuleStatus": "DISABLED",
}
]' \
--region us-east-1
```

Mengedit urutan aturan otomatisasi

Aturan otomatisasi dapat digunakan untuk memperbarui temuan secara otomatis di AWS Security Hub Cloud Security Posture Management (CSPM). Untuk informasi latar belakang tentang cara kerja aturan otomatisasi, lihat [Memahami aturan otomatisasi di Security Hub CSPM](#).

Setelah membuat aturan otomatisasi, administrator CSPM Security Hub yang didelegasikan dapat mengedit aturan.

Jika Anda ingin menjaga kriteria aturan dan tindakan tetap sama, tetapi mengubah urutan di mana Security Hub CSPM menerapkan aturan otomatisasi, Anda dapat mengedit hanya urutan aturan. Pilih metode pilihan Anda, dan ikuti langkah-langkah untuk mengedit urutan aturan.

Untuk petunjuk tentang mengedit kriteria atau tindakan aturan otomatisasi, lihat [Mengedit aturan otomatisasi](#).

Console

Untuk mengedit urutan aturan otomatisasi (konsol)

1. Menggunakan kredensi administrator CSPM Security Hub, buka konsol Security Hub AWS Cloud Security Posture Management (CSPM) di <https://console.aws.amazon.com/securityhub/>
2. Di panel navigasi, pilih Otomatisasi.
3. Pilih aturan yang urutannya ingin Anda ubah. Pilih Edit prioritas.

4. Pilih Pindah ke atas untuk meningkatkan prioritas aturan dengan satu unit. Pilih Pindah ke bawah untuk mengurangi prioritas aturan sebanyak satu unit. Pilih Pindah ke atas untuk menetapkan aturan urutan 1 (ini memberikan aturan lebih diutamakan daripada aturan lain yang ada).

 Note

Saat Anda membuat aturan di konsol CSPM Security Hub, Security Hub CSPM secara otomatis menetapkan urutan aturan berdasarkan urutan pembuatan aturan. Aturan yang paling baru dibuat memiliki nilai numerik terendah untuk urutan aturan dan oleh karena itu berlaku terlebih dahulu.

API

Untuk mengedit urutan aturan otomatisasi (API)

1. Gunakan [BatchUpdateAutomationRules](#) operasi dari akun administrator CSPM Security Hub.
2. Untuk `RuleArn` parameter, berikan ARN dari aturan yang urutannya ingin Anda edit.
3. Ubah nilai `RuleOrder` bidang.

 Note

Jika beberapa aturan memiliki hal yang sama `RuleOrder`, Security Hub CSPM menerapkan aturan dengan nilai sebelumnya untuk `UpdatedAt` bidang terlebih dahulu (yaitu, aturan yang terakhir diedit berlaku terakhir).

Menghapus atau menonaktifkan aturan otomatisasi

Aturan otomatisasi dapat digunakan untuk memperbarui temuan secara otomatis di AWS Security Hub Cloud Security Posture Management (CSPM). Untuk informasi latar belakang tentang cara kerja aturan otomatisasi, lihat [Memahami aturan otomatisasi di Security Hub CSPM](#).

Saat Anda menghapus aturan otomatisasi, Security Hub CSPM menghapusnya dari akun Anda dan tidak lagi menerapkan aturan tersebut pada temuan. Sebagai alternatif untuk penghapusan, Anda

dapat menonaktifkan aturan. Ini mempertahankan aturan untuk penggunaan di masa mendatang, tetapi CSPM Security Hub tidak akan menerapkan aturan tersebut pada temuan yang cocok sampai Anda mengaktifkannya.

Pilih metode pilihan Anda, dan ikuti langkah-langkah untuk menghapus aturan otomatisasi. Anda dapat menghapus satu atau beberapa aturan dalam satu permintaan.

Console

Untuk menghapus atau menonaktifkan aturan otomatisasi (konsol)

1. Menggunakan kredensi administrator CSPM Security Hub, buka konsol Security Hub AWS Cloud Security Posture Management (CSPM) di <https://console.aws.amazon.com/securityhub/>
2. Di panel navigasi, pilih Otomatisasi.
3. Pilih aturan yang ingin Anda hapus. Pilih Tindakan dan Hapus (untuk mempertahankan aturan, tetapi nonaktifkan sementara, pilih Nonaktifkan).
4. Konfirmasikan pilihan Anda, dan pilih Hapus.

API

Untuk menghapus atau menonaktifkan aturan otomatisasi (API)

1. Gunakan [BatchDeleteAutomationRules](#) operasi dari akun administrator CSPM Security Hub.
2. Untuk `AutomationRulesArns` parameter, berikan ARN aturan yang ingin Anda hapus (untuk mempertahankan aturan, tetapi nonaktifkan sementara, sediakan `DISABLED RuleStatus` parameteranya).

Contoh berikut menghapus aturan otomatisasi yang ditentukan. Contoh ini diformat untuk Linux, macOS, atau Unix, dan menggunakan karakter garis miring terbalik (\) untuk meningkatkan keterbacaan.

```
$ aws securityhub batch-delete-automation-rules \
--automation-rules-arns '["arn:aws:securityhub:us-east-1:123456789012:automation-
rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE1111"]' \
--region us-east-1
```


Contoh aturan otomatisasi

Bagian ini memberikan contoh aturan otomatisasi untuk kasus penggunaan CSPM Security Hub umum. Contoh-contoh ini sesuai dengan template aturan yang tersedia di konsol CSPM Security Hub.

Tingkatkan tingkat keparahan menjadi Kritis saat sumber daya tertentu seperti bucket S3 berisiko

Dalam contoh ini, kriteria aturan dicocokkan ketika ResourceId dalam temuan adalah bucket Amazon Simple Storage Service (Amazon S3) tertentu. Tindakan aturannya adalah mengubah tingkat keparahan temuan yang cocok menjadi CRITICAL. Anda dapat memodifikasi template ini untuk diterapkan ke sumber daya lain.

Contoh permintaan API:

```
{
  "IsTerminal": true,
  "RuleName": "Elevate severity of findings that relate to important resources",
  "RuleOrder": 1,
  "RuleStatus": "ENABLED",
  "Description": "Elevate finding severity to CRITICAL when specific resource such as an S3 bucket is at risk",
  "Criteria": {
    "ProductName": [{
      "Value": "Security Hub CSPM",
      "Comparison": "EQUALS"
    }],
    "ComplianceStatus": [{
      "Value": "FAILED",
      "Comparison": "EQUALS"
    }],
    "RecordState": [{
      "Value": "ACTIVE",
      "Comparison": "EQUALS"
    }],
    "WorkflowStatus": [{
      "Value": "NEW",
      "Comparison": "EQUALS"
    }],
    "ResourceId": [{
      "Value": "arn:aws:s3:::amzn-s3-demo-bucket/developers/design_info.doc",
```

```

        "Comparison": "EQUALS"
    }
  ],
  "Actions": [{
    "Type": "FINDING_FIELDS_UPDATE",
    "FindingFieldsUpdate": {
      "Severity": {
        "Label": "CRITICAL"
      },
      "Note": {
        "Text": "This is a critical resource. Please review ASAP.",
        "UpdatedBy": "sechub-automation"
      }
    }
  ]
}

```

Contoh perintah CLI:

```

$
aws securityhub create-automation-rule \
--is-terminal \
--rule-name "Elevate severity of findings that relate to important resources" \
--rule-order 1 \
--rule-status "ENABLED" \

--description "Elevate finding severity to CRITICAL when specific resource such as an
S3 bucket is at risk" \
--criteria '{
  "ProductName": [{
    "Value": "Security Hub CSPM",
    "Comparison": "EQUALS"
  }],
  "ComplianceStatus": [{
    "Value": "FAILED",
    "Comparison": "EQUALS"
  }],
  "RecordState": [{
    "Value": "ACTIVE",
    "Comparison": "EQUALS"
  }],
  "WorkflowStatus": [{
    "Value": "NEW",

```

```

"Comparison": "EQUALS"
}],
"ResourceId": [{
"Value": "arn:aws:s3:::amzn-s3-demo-bucket/developers/design_info.doc",
"Comparison": "EQUALS"
}]
}' \
--actions '[{
"Type": "FINDING_FIELDS_UPDATE",
"FindingFieldsUpdate": {
"Severity": {
"Label": "CRITICAL"
},
"Note": {
"Text": "This is a critical resource. Please review ASAP.",
"UpdatedBy": "sechub-automation"
}
}
}]' \
--region us-east-1

```

Meningkatkan keparahan temuan yang berhubungan dengan sumber daya dalam akun produksi

Dalam contoh ini, kriteria aturan dicocokkan ketika temuan HIGH tingkat keparahan dihasilkan di akun produksi tertentu. Tindakan aturannya adalah mengubah tingkat keparahan temuan yang cocok menjadi CRITICAL.

Contoh permintaan API:

```

{
  "IsTerminal": false,
  "RuleName": "Elevate severity for production accounts",
  "RuleOrder": 1,
  "RuleStatus": "ENABLED",
  "Description": "Elevate finding severity from HIGH to CRITICAL for findings that relate to resources in specific production accounts",
  "Criteria": {
    "ProductName": [{
      "Value": "Security Hub CSPM",
      "Comparison": "EQUALS"
    }],
    "ComplianceStatus": [{

```

```

        "Value": "FAILED",
        "Comparison": "EQUALS"
    ]],
    "RecordState": [{
        "Value": "ACTIVE",
        "Comparison": "EQUALS"
    }],
    "WorkflowStatus": [{
        "Value": "NEW",
        "Comparison": "EQUALS"
    }],
    "SeverityLabel": [{
        "Value": "HIGH",
        "Comparison": "EQUALS"
    }],
    "AwsAccountId": [
        {
            "Value": "111122223333",
            "Comparison": "EQUALS"
        },
        {
            "Value": "123456789012",
            "Comparison": "EQUALS"
        }
    ],
},
"Actions": [{
    "Type": "FINDING_FIELDS_UPDATE",
    "FindingFieldsUpdate": {
        "Severity": {
            "Label": "CRITICAL"
        },
        "Note": {
            "Text": "A resource in production accounts is at risk. Please review
ASAP.",
            "UpdatedBy": "sechub-automation"
        }
    }
}]
}

```

Contoh perintah CLI:

```
aws securityhub create-automation-rule \
--no-is-terminal \
--rule-name "Elevate severity of findings that relate to resources in production accounts" \
--rule-order 1 \
--rule-status "ENABLED" \
--description "Elevate finding severity from HIGH to CRITICAL for findings that relate to resources in specific production accounts" \
--criteria '{
  "ProductName": [{
    "Value": "Security Hub CSPM",
    "Comparison": "EQUALS"
  }],
  "ComplianceStatus": [{
    "Value": "FAILED",
    "Comparison": "EQUALS"
  }],
  "RecordState": [{
    "Value": "ACTIVE",
    "Comparison": "EQUALS"
  }],
  "SeverityLabel": [{
    "Value": "HIGH",
    "Comparison": "EQUALS"
  }],
  "AwsAccountId": [
    {
      "Value": "111122223333",
      "Comparison": "EQUALS"
    },
    {
      "Value": "123456789012",
      "Comparison": "EQUALS"
    }
  ]
}' \
--actions '[{
  "Type": "FINDING_FIELDS_UPDATE",
  "FindingFieldsUpdate": {
    "Severity": {
      "Label": "CRITICAL"
    },
    "Note": {
      "Text": "A resource in production accounts is at risk. Please review ASAP.",
      "UpdatedBy": "sechub-automation"
    }
  }
}]'
```

```

}
}
]]' \
--region us-east-1

```

Menekan temuan informasi

Dalam contoh ini, kriteria aturan dicocokkan untuk temuan INFORMATIONAL tingkat keparahan yang dikirim ke Security Hub CSPM dari Amazon. GuardDuty Tindakan aturannya adalah mengubah status alur kerja dari temuan yang cocok menjadi. SUPPRESSED

Contoh permintaan API:

```

{
  "IsTerminal": false,
  "RuleName": "Suppress informational findings",
  "RuleOrder": 1,
  "RuleStatus": "ENABLED",
  "Description": "Suppress GuardDuty findings with INFORMATIONAL severity",
  "Criteria": {
    "ProductName": [{
      "Value": "GuardDuty",
      "Comparison": "EQUALS"
    }],
    "RecordState": [{
      "Value": "ACTIVE",
      "Comparison": "EQUALS"
    }],
    "WorkflowStatus": [{
      "Value": "NEW",
      "Comparison": "EQUALS"
    }],
    "SeverityLabel": [{
      "Value": "INFORMATIONAL",
      "Comparison": "EQUALS"
    }]
  },
  "Actions": [{
    "Type": "FINDING_FIELDS_UPDATE",
    "FindingFieldsUpdate": {
      "Workflow": {
        "Status": "SUPPRESSED"
      }
    }
  ],

```

```

        "Note": {
            "Text": "Automatically suppress GuardDuty findings with INFORMATIONAL
severity",
            "UpdatedBy": "sechub-automation"
        }
    }
}
]]
}

```

Contoh perintah CLI:

```

aws securityhub create-automation-rule \
--no-is-terminal \
--rule-name "Suppress informational findings" \
--rule-order 1 \
--rule-status "ENABLED" \
--description "Suppress GuardDuty findings with INFORMATIONAL severity" \
--criteria '{
"ProductName": [{
"Value": "GuardDuty",
"Comparison": "EQUALS"
}],
"ComplianceStatus": [{
"Value": "FAILED",
"Comparison": "EQUALS"
}],
"RecordState": [{
"Value": "ACTIVE",
"Comparison": "EQUALS"
}],
"WorkflowStatus": [{
"Value": "NEW",
"Comparison": "EQUALS"
}],
"SeverityLabel": [{
"Value": "INFORMATIONAL",
"Comparison": "EQUALS"
}]
}' \
--actions '[{
"Type": "FINDING_FIELDS_UPDATE",
"FindingFieldsUpdate": {

```

```
"Workflow": {  
  "Status": "SUPPRESSED"  
},  
"Note": {  
  "Text": "Automatically suppress GuardDuty findings with INFORMATIONAL severity",  
  "UpdatedBy": "sechub-automation"  
}  
}  
}]' \  
--region us-east-1
```

Menggunakan EventBridge untuk respon otomatis dan remediasi

Dengan membuat aturan di Amazon EventBridge, Anda dapat merespons secara otomatis temuan AWS Security Hub Cloud Security Posture Management (CSPM) Security Hub. Security Hub CSPM mengirimkan temuan sebagai peristiwa EventBridge dalam waktu nyaris nyata. Anda dapat menulis aturan sederhana untuk menunjukkan acara mana yang Anda minati dan tindakan otomatis apa yang harus diambil ketika suatu acara cocok dengan aturan. Tindakan yang dapat dipicu secara otomatis meliputi hal-hal berikut:

- Memanggil fungsi AWS Lambda
- Memanggil perintah Amazon EC2 run
- Mengirim peristiwa ke Amazon Kinesis Data Streams
- Mengaktifkan mesin AWS Step Functions negara
- Memberi tahu topik Amazon SNS atau antrean Amazon SQS
- Mengirim temuan ke tiket pihak ketiga, obrolan, SIEM, atau alat manajemen dan respons insiden

Security Hub CSPM secara otomatis mengirimkan semua temuan baru dan semua pembaruan temuan yang ada ke EventBridge sebagai EventBridge peristiwa. Anda juga dapat membuat tindakan kustom yang memungkinkan Anda mengirim temuan dan hasil wawasan yang dipilih EventBridge.

Anda kemudian mengonfigurasi EventBridge aturan untuk merespons setiap jenis acara.

Untuk informasi selengkapnya tentang penggunaan EventBridge, lihat [Panduan EventBridge Pengguna Amazon](#).

Note

Sebagai praktik terbaik, pastikan bahwa izin yang diberikan kepada pengguna Anda untuk mengakses EventBridge menggunakan kebijakan least-privilege AWS Identity and Access Management (IAM) yang hanya memberikan izin yang diperlukan. Untuk informasi selengkapnya, lihat [Identitas dan manajemen akses di Amazon EventBridge](#).

Satu set templat untuk respons dan remediasi otomatis lintas akun juga tersedia di AWS Solusi. Template memanfaatkan aturan EventBridge acara dan fungsi Lambda. Anda menerapkan solusi menggunakan AWS CloudFormation dan AWS Systems Manager. Solusinya dapat membuat respons dan tindakan remediasi yang sepenuhnya otomatis. Hal ini juga dapat menggunakan Security Hub CSPM tindakan kustom untuk membuat respon yang dipicu pengguna dan tindakan remediasi. Untuk detail tentang cara mengonfigurasi dan menggunakan solusi, lihat [halaman AWS Solusi Respons Keamanan Otomatis](#).

Topik

- [Jenis acara CSPM Security Hub di EventBridge](#)
- [EventBridge format acara untuk Security Hub CSPM](#)
- [Mengkonfigurasi EventBridge aturan untuk temuan CSPM Security Hub](#)
- [Menggunakan tindakan khusus untuk mengirim temuan dan hasil wawasan ke EventBridge](#)

Jenis acara CSPM Security Hub di EventBridge

Security Hub CSPM menggunakan jenis EventBridge acara Amazon berikut untuk diintegrasikan. EventBridge

Di EventBridge dasbor untuk Security Hub CSPM, Semua Acara mencakup semua jenis acara ini.

Semua temuan (Security Hub Findings - Imported)

Security Hub CSPM secara otomatis mengirimkan semua temuan baru dan semua pembaruan temuan yang ada ke EventBridge sebagai Security Hub Findings - Imported peristiwa. Setiap Security Hub Findings - Imported peristiwa berisi satu temuan.

Setiap [BatchUpdateFindings](#) permintaan [BatchImportFindings](#) dan memicu suatu Security Hub Findings - Imported peristiwa.

Untuk akun administrator, feed acara EventBridge termasuk peristiwa untuk temuan dari akun mereka dan dari akun anggota mereka.

Di Wilayah agregasi, umpan acara mencakup peristiwa untuk temuan dari Wilayah agregasi dan Wilayah terkait. Temuan Lintas Wilayah dimasukkan dalam umpan acara dalam waktu dekat. Untuk informasi tentang cara mengonfigurasi agregasi pencarian, lihat [Menggabungkan data CSPM di seluruh Wilayah](#).

Anda dapat menentukan aturan EventBridge yang secara otomatis merutekan temuan ke alur kerja remediasi, alat pihak ketiga, atau target [lain yang didukung EventBridge](#). Aturan dapat mencakup filter yang hanya menerapkan aturan jika temuan memiliki nilai atribut tertentu.

Anda menggunakan metode ini untuk secara otomatis mengirim semua temuan, atau semua temuan yang memiliki karakteristik spesifik, ke alur kerja respons atau remediasi.

Lihat [the section called “Mengkonfigurasi aturan EventBridge”](#).

Temuan untuk tindakan kustom (Security Hub Findings - Custom Action)

Security Hub CSPM juga mengirimkan temuan yang terkait dengan tindakan kustom ke EventBridge as Security Hub Findings - Custom Action events.

Ini berguna bagi analis yang bekerja dengan konsol CSPM Security Hub yang ingin mengirim temuan tertentu, atau serangkaian kecil temuan, ke alur kerja respons atau remediasi. Anda dapat memilih tindakan kustom hingga 20 temuan sekaligus. Setiap temuan dikirim EventBridge sebagai EventBridge acara terpisah.

Saat membuat tindakan kustom, Anda menentukannya ID tindakan kustom. Anda dapat menggunakan ID ini untuk membuat EventBridge aturan yang mengambil tindakan tertentu setelah menerima temuan yang terkait dengan ID tindakan kustom tersebut.

Lihat [the section called “Mengkonfigurasi dan menggunakan tindakan kustom”](#).

Misalnya, Anda dapat membuat tindakan kustom di Security Hub CSPM yang dipanggil `send_to_ticketing`. Kemudian EventBridge, Anda membuat aturan yang dipicu saat EventBridge menerima temuan yang menyertakan ID tindakan `send_to_ticketing` kustom. Aturannya mencakup logika untuk mengirim temuan ke sistem tiket Anda. Anda kemudian dapat memilih temuan dalam Security Hub CSPM dan menggunakan tindakan kustom di Security Hub CSPM untuk mengirim temuan secara manual ke sistem tiket Anda.

Untuk contoh cara mengirim temuan CSPM Security Hub EventBridge untuk diproses lebih lanjut, lihat [Cara Mengintegrasikan AWS Security Hub Cloud Security Posture Management \(CSPM\) Custom Actions dengan PagerDuty dan Cara Mengaktifkan Tindakan Kustom di Security Hub AWS Cloud Security Posture Management \(CSPM\) di Blog AWS Partner Network \(APN\)](#).

Hasil wawasan untuk tindakan kustom (Security Hub Insight Results)

Anda juga dapat menggunakan tindakan kustom untuk mengirim kumpulan hasil wawasan ke EventBridge sebagai Security Hub Insight Results peristiwa. Hasil wawasan adalah sumber daya yang cocok dengan wawasan. Perhatikan bahwa ketika Anda mengirim hasil wawasan ke EventBridge, Anda tidak mengirimkan temuan ke EventBridge. Anda hanya mengirimkan pengenalan sumber daya yang terkait dengan hasil wawasan. Anda dapat mengirim hingga 100 pengidentifikasi sumber daya sekaligus.

Mirip dengan tindakan kustom untuk temuan, pertama-tama Anda membuat tindakan kustom di Security Hub CSPM, lalu membuat aturan di EventBridge

Lihat [the section called “Mengkonfigurasi dan menggunakan tindakan kustom”](#).

Misalnya, Anda melihat hasil wawasan tertentu yang menarik yang ingin Anda bagikan dengan rekan kerja. Dalam hal ini, Anda dapat menggunakan tindakan khusus untuk mengirimkan hasil wawasan tersebut ke kolega melalui sistem obrolan atau tiket.

EventBridge format acara untuk Security Hub CSPM

Jenis Security Hub Findings - ImportedSecurity Findings - Custom Action,, dan Security Hub Insight Resultsacara menggunakan format acara berikut.

Format acara adalah format yang digunakan saat Security Hub CSPM mengirimkan acara ke EventBridge

Security Hub Findings - Imported

Security Hub Findings - Importedperistiwa yang dikirim dari Security Hub CSPM untuk EventBridge menggunakan format berikut.

```
{
  "version": "0",
  "id": "CWE-event-id",
```

```

    "detail-type": "Security Hub Findings - Imported",
    "source": "aws.securityhub",
    "account": "111122223333",
    "time": "2019-04-11T21:52:17Z",
    "region": "us-west-2",
    "resources": [
        "arn:aws:securityhub:us-west-2::product/aws/macie/arn:aws:macie:us-west-2:111122223333:integtest/trigger/6294d71b927c41cbab915159a8f326a3/alert/f2893b211841"
    ],
    "detail": {
        "findings": [
            <finding content>
        ]
    }
}

```

<finding content> adalah konten, dalam format JSON, dari temuan yang dikirim oleh acara. Setiap peristiwa mengirimkan satu temuan.

Untuk daftar lengkap menemukan atribut, lihat [AWS Format Pencarian Keamanan \(ASFF\)](#).

Untuk informasi tentang cara mengonfigurasi EventBridge aturan yang dipicu oleh peristiwa ini, lihat [the section called “Mengkonfigurasi aturan EventBridge”](#).

Security Hub Findings - Custom Action

Security Hub Findings - Custom Action peristiwa yang dikirim dari Security Hub CSPM untuk EventBridge menggunakan format berikut. Setiap temuan dikirim dalam acara terpisah.

```

{
    "version": "0",
    "id": "1a1111a1-b22b-3c33-444d-5555e5ee5555",
    "detail-type": "Security Hub Findings - Custom Action",
    "source": "aws.securityhub",
    "account": "111122223333",
    "time": "2019-04-11T18:43:48Z",
    "region": "us-west-1",
    "resources": [
        "arn:aws:securityhub:us-west-1:111122223333:action/custom/custom-action-name"
    ],
    "detail": {

```

```

    "actionName": "custom-action-name",
    "actionDescription": "description of the action",
    "findings": [
      {
        <finding content>
      }
    ]
  }
}

```

<finding content> adalah konten, dalam format JSON, dari temuan yang dikirim oleh acara. Setiap peristiwa mengirimkan satu temuan.

Untuk daftar lengkap menemukan atribut, lihat [AWS Format Pencarian Keamanan \(ASFF\)](#).

Untuk informasi tentang cara mengonfigurasi EventBridge aturan yang dipicu oleh peristiwa ini, lihat [the section called “Mengkonfigurasi dan menggunakan tindakan kustom”](#).

Security Hub Insight Results

Security Hub Insight Results peristiwa yang dikirim dari Security Hub CSPM untuk EventBridge menggunakan format berikut.

```

{
  "version": "0",
  "id": "1a1111a1-b22b-3c33-444d-5555e5ee5555",
  "detail-type": "Security Hub Insight Results",
  "source": "aws.securityhub",
  "account": "111122223333",
  "time": "2017-12-22T18:43:48Z",
  "region": "us-west-1",
  "resources": [
    "arn:aws:securityhub:us-west-1:111122223333::product/aws/maciek:us-west-1:222233334444:test/trigger/1ec9cf700ef6be062b19584e0b7d84ec/alert/f2893b211841"
  ],
  "detail": {
    "actionName": "name of the action",
    "actionDescription": "description of the action",
    "insightArn": "ARN of the insight",
    "insightName": "Name of the insight",
    "resultType": "ResourceAwsIamAccessKeyUserName",
    "number of results": "number of results, max of 100",
  }
}

```

```
"insightResults": [  
  {"result 1": 5},  
  {"result 2": 6}  
]  
}
```

Untuk informasi tentang cara membuat EventBridge aturan yang dipicu oleh peristiwa ini, lihat [the section called “Mengkonfigurasi dan menggunakan tindakan kustom”](#).

Mengkonfigurasi EventBridge aturan untuk temuan CSPM Security Hub

Anda dapat membuat aturan di Amazon EventBridge yang menentukan tindakan yang harus diambil saat Security Hub Findings - Imported acara diterima. Security Hub Findings - Imported peristiwa dipicu oleh pembaruan dari kedua [BatchImportFindings](#) dan [BatchUpdateFindings](#) operasi.

Setiap aturan berisi pola peristiwa, yang mengidentifikasi peristiwa yang memicu aturan. Pola acara selalu berisi sumber peristiwa (`aws.securityhub`) dan jenis acara (Temuan Security Hub - Imported). Pola peristiwa juga dapat menentukan filter untuk mengidentifikasi temuan yang berlaku aturan tersebut.

Aturan acara kemudian mengidentifikasi target aturan. Targetnya adalah tindakan yang harus diambil saat EventBridge menerima Temuan Security Hub - Acara yang diimpor dan temuannya cocok dengan filter.

Instruksi yang diberikan di sini menggunakan EventBridge konsol. Saat Anda menggunakan konsol, EventBridge secara otomatis membuat kebijakan berbasis sumber daya yang diperlukan yang memungkinkan untuk EventBridge menulis ke Amazon Logs. CloudWatch

Anda juga dapat menggunakan [PutRule](#) pengoperasian EventBridge API. Namun, jika Anda menggunakan EventBridge API, Anda harus membuat kebijakan berbasis sumber daya. Untuk informasi tentang kebijakan yang diperlukan, lihat [Izin CloudWatch log](#) di Panduan EventBridge Pengguna Amazon.

Format pola acara

Format pola acara untuk Temuan Security Hub - Peristiwa yang diimpor adalah sebagai berikut:

```
{
```

```

"source": [
  "aws.securityhub"
],
"detail-type": [
  "Security Hub Findings - Imported"
],
"detail": {
  "findings": {
    <attribute filter values>
  }
}
}

```

- `source` mengidentifikasi Security Hub CSPM sebagai layanan yang menghasilkan acara.
- `detail-type` mengidentifikasi jenis acara.
- `detail` bersifat opsional dan memberikan nilai filter untuk pola acara. Jika pola peristiwa tidak mengandung detail bidang, maka semua temuan memicu aturan.

Anda dapat memfilter temuan berdasarkan atribut temuan apa pun. Untuk setiap atribut, Anda menyediakan array dipisahkan koma dari satu atau lebih nilai.

```
"<attribute name>": [ "<value1>", "<value2>" ]
```

Jika Anda memberikan lebih dari satu nilai untuk atribut, maka nilai-nilai tersebut digabungkan oleh OR. Temuan cocok dengan filter untuk atribut individual jika temuan memiliki salah satu nilai yang terdaftar. Misalnya, jika Anda memberikan keduanya `INFORMATIONAL` dan `LOW` sebagai nilai untuk `Severity.Label`, maka temuan tersebut cocok jika memiliki label keparahan salah satu `INFORMATIONAL` atau `LOW`.

Atribut bergabung dengan AND. Temuan cocok jika cocok dengan kriteria filter untuk semua atribut yang disediakan.

Ketika Anda memberikan nilai atribut, itu harus mencerminkan lokasi atribut tersebut dalam struktur AWS Security Finding Format (ASFF).

Tip

Saat memfilter temuan kontrol, sebaiknya gunakan [bidang `SecurityControlId` atau `SecurityControlArn` ASFF](#) sebagai filter, bukan `Title` atau `Description` Bidang

yang terakhir dapat berubah sesekali, sedangkan ID kontrol dan ARN adalah pengidentifikasi statis.

Dalam contoh berikut, pola peristiwa memberikan nilai filter untuk `ProductArn` dan `Severity.Label`, sehingga temuan cocok jika dihasilkan oleh Amazon Inspector dan memiliki label keparahan salah satu atau `INFORMATIONAL`. `LOW`

```
{
  "source": [
    "aws.securityhub"
  ],
  "detail-type": [
    "Security Hub Findings - Imported"
  ],
  "detail": {
    "findings": {
      "ProductArn": ["arn:aws:securityhub:us-east-1::product/aws/inspector"],
      "Severity": {
        "Label": ["INFORMATIONAL", "LOW"]
      }
    }
  }
}
```

Membuat aturan acara

Anda dapat menggunakan pola peristiwa yang telah ditentukan atau pola acara khusus untuk membuat aturan di EventBridge. Jika Anda memilih pola yang telah ditentukan, EventBridge secara otomatis mengisi `source` `detail-type` EventBridge juga menyediakan bidang untuk menentukan nilai filter untuk atribut temuan berikut:

- `AwsAccountId`
- `Compliance.Status`
- `Criticality`
- `ProductArn`
- `RecordState`
- `ResourceId`

- `ResourceType`
- `Severity.Label`
- `Types`
- `Workflow.Status`

Untuk membuat EventBridge aturan (konsol)

1. Buka EventBridge konsol Amazon di <https://console.aws.amazon.com/events/>.
2. Dengan menggunakan nilai berikut, buat EventBridge aturan yang memantau penemuan peristiwa:
 - Untuk Tipe aturan, pilih Aturan dengan pola peristiwa.
 - Pilih cara membangun pola acara.

Untuk membangun pola acara dengan...	Lakukan ini...	
Template	Di bagian Pola acara, pilih opsi berikut: • Untuk Sumber peristiwa, pilih Layanan AWS . • Untuk AWS layanan, pilih Security Hub. • Untuk jenis Acara, pilih Temuan Security Hub - Imported. • (Opsional) Untuk membuat aturan lebih spesifik, tambahkan nilai filter. Misalnya, untuk membatasi aturan pada temuan dengan status rekaman aktif, untuk status Rekaman Khusus, pilih Aktif.	

Untuk membangun pola acara dengan...	Lakukan ini...	
Pola acara khusus (Gunakan pola kustom jika Anda ingin memfilter temuan berdasarkan atribut yang tidak muncul di EventBridge konsol.)	- Di bagian Pola acara, pilih Pola kustom (editor JSON), lalu tempelkan pola acara berikut ke area teks: <pre data-bbox="690 535 1063 1333"> { "source": ["aws.secu rityhub"], "detail-type": ["Security Hub Findings - Imported"], "detail": { "findings": { "<attribut e name> ": ["<value1>", "<value2>"] } } }</pre> - Perbarui pola acara untuk menyertakan atribut dan nilai atribut yang ingin Anda gunakan sebagai filter. Misalnya, untuk menerapkan aturan pada temuan yang memiliki status verifikasi TRUE_POSITIVE ,	

Untuk membangun pola acara dengan...	Lakukan ini...	
	gunakan contoh pola berikut: <pre data-bbox="690 380 1062 1136"> { "source": ["aws.secu rityhub"], "detail-type": ["Security Hub Findings - Imported"], "detail": { "findings": { "Verifica tionState": ["TRUE_POSITIVE"] } } }</pre>	

- Untuk jenis Target, pilih AWS layanan, dan untuk Pilih target, pilih target seperti topik atau AWS Lambda fungsi Amazon SNS. Target terpicu saat peristiwa diterima yang sesuai dengan pola peristiwa yang ditentukan dalam aturan.

Untuk detail tentang membuat aturan, lihat [Membuat EventBridge aturan Amazon yang bereaksi terhadap peristiwa](#) di Panduan EventBridge Pengguna Amazon.

Menggunakan tindakan khusus untuk mengirim temuan dan hasil wawasan ke EventBridge

Untuk menggunakan tindakan kustom AWS Security Hub Cloud Security Posture Management (CSPM) untuk mengirim temuan atau hasil wawasan ke Amazon EventBridge, Anda terlebih dahulu

membuat tindakan kustom di Security Hub CSPM. Kemudian, Anda dapat menentukan aturan EventBridge yang berlaku untuk tindakan kustom Anda.

Anda dapat membuat hingga 50 tindakan kustom.

Jika Anda mengaktifkan agregasi lintas wilayah, dan mengelola temuan dari Wilayah agregasi, maka buat tindakan kustom di Wilayah agregasi.

Aturan dalam EventBridge menggunakan Amazon Resource Name (ARN) dari tindakan kustom.

Membuat tindakan kustom

Saat membuat tindakan kustom di AWS Security Hub Cloud Security Posture Management (CSPM), Anda menentukan nama, deskripsi, dan pengenalan uniknya.

Tindakan kustom menentukan tindakan mana yang harus diambil saat EventBridge acara cocok dengan EventBridge aturan. Security Hub CSPM mengirimkan setiap temuan EventBridge sebagai sebuah acara.

Pilih metode pilihan Anda, dan ikuti langkah-langkah untuk membuat tindakan kustom.

Console

Untuk membuat tindakan kustom di Security Hub CSPM (konsol)

1. Buka konsol AWS Security Hub Cloud Security Posture Management (CSPM) di <https://console.aws.amazon.com/securityhub/>
2. Di panel navigasi, pilih Pengaturan dan kemudian pilih Tindakan kustom.
3. Pilih Buat tindakan kustom.
4. Berikan Nama, Deskripsi, dan ID tindakan Kustom untuk tindakan tersebut.

Nama harus kurang dari 20 karakter.

ID tindakan kustom harus unik untuk setiap AWS akun.

5. Pilih Buat tindakan kustom.
6. Catat ARN tindakan Kustom. Anda perlu menggunakan ARN saat membuat aturan untuk dikaitkan dengan tindakan ini di EventBridge

API

Untuk membuat tindakan kustom (API)

Gunakan [CreateActionTarget](#) operasi. Jika Anda menggunakan AWS CLI, jalankan [create-action-target](#) perintah.

Contoh berikut membuat tindakan kustom untuk mengirim temuan ke alat remediasi. Contoh ini diformat untuk Linux, macOS, atau Unix, dan menggunakan karakter garis miring terbalik (\) untuk meningkatkan keterbacaan.

```
$ aws securityhub create-action-target --name "Send to remediation" --description "Action to send the finding for remediation tracking" --id "Remediation"
```

Mendefinisikan aturan di EventBridge

Untuk memicu tindakan kustom di Amazon EventBridge, Anda harus membuat aturan yang sesuai di EventBridge. Definisi aturan mencakup Nama Sumber Daya Amazon (ARN) dari tindakan kustom.

Pola acara untuk Temuan Security Hub - peristiwa Tindakan Kustom memiliki format berikut:

```
{
  "source": [
    "aws.securityhub"
  ],
  "detail-type": [
    "Security Hub Findings - Custom Action"
  ],
  "resources": [ "<custom action ARN>" ]
}
```

Pola acara untuk acara Hasil Wawasan Security Hub memiliki format berikut:

```
{
  "source": [
    "aws.securityhub"
  ],
  "detail-type": [
    "Security Hub Insight Results"
  ],
  "resources": [ "<custom action ARN>" ]
}
```

```
}
```

Dalam kedua pola, *<custom action ARN>* adalah ARN dari tindakan khusus. Anda dapat mengonfigurasi aturan yang berlaku untuk lebih dari satu tindakan kustom.

Instruksi yang diberikan di sini adalah untuk EventBridge konsol. Saat Anda menggunakan konsol, EventBridge secara otomatis membuat kebijakan berbasis sumber daya yang diperlukan yang memungkinkan EventBridge untuk menulis ke Log. CloudWatch

Anda juga dapat menggunakan operasi [PutRule](#) API EventBridge API. Namun, jika Anda menggunakan EventBridge API, Anda harus membuat kebijakan berbasis sumber daya. Untuk detail tentang kebijakan yang diperlukan, lihat [Izin CloudWatch log](#) di Panduan EventBridge Pengguna Amazon.

Untuk menentukan aturan di EventBridge (EventBridge konsol)

1. Buka EventBridge konsol Amazon di <https://console.aws.amazon.com/events/>.
2. Di panel navigasi, pilih Aturan.
3. Pilih Buat aturan.
4. Masukkan nama dan deskripsi aturan.
5. Untuk bus acara, pilih bus acara yang ingin Anda kaitkan dengan aturan ini. Jika Anda ingin aturan ini cocok dengan peristiwa yang berasal dari akun Anda, pilih default. Saat layanan AWS di akun Anda menghasilkan kejadian, layanan tersebut akan selalu masuk ke bus kejadian default akun Anda.
6. Untuk Tipe aturan, pilih Aturan dengan pola peristiwa.
7. Pilih Selanjutnya.
8. Untuk sumber Acara, pilih AWS acara.
9. Untuk pola Acara, pilih Formulir pola acara.
10. Untuk Sumber peristiwa, pilih Layanan AWS .
11. Untuk AWS layanan, pilih Security Hub.
12. Untuk Jenis peristiwa, lakukan salah satu hal berikut:
 - Untuk membuat aturan yang akan diterapkan saat Anda mengirim temuan ke tindakan kustom, pilih Temuan Security Hub - Tindakan Kustom.
 - Untuk membuat aturan yang akan diterapkan saat Anda mengirim hasil wawasan ke tindakan kustom, pilih Hasil Wawasan Security Hub.

13. Pilih Tindakan khusus khusus ARNs, tambahkan ARN tindakan kustom.

Jika aturan berlaku untuk beberapa tindakan kustom, pilih Tambah untuk menambahkan lebih banyak tindakan kustom ARNs.

14. Pilih Berikutnya.

15. Di bawah Pilih target, pilih dan konfigurasi target yang akan dipanggil saat aturan ini cocok.

16. Pilih Berikutnya.

17. (Opsional) Masukkan satu atau lebih tanda untuk aturan. Untuk informasi selengkapnya, lihat [EventBridge tag Amazon](#) di Panduan EventBridge Pengguna Amazon.

18. Pilih Berikutnya.

19. Tinjau detail aturan dan pilih Buat aturan.

Saat Anda melakukan tindakan kustom pada hasil temuan atau wawasan di akun Anda, peristiwa akan dihasilkan EventBridge.

Memilih tindakan khusus untuk temuan dan hasil wawasan

Setelah membuat tindakan kustom AWS Security Hub Cloud Security Posture Management (CSPM) dan EventBridge aturan Amazon, Anda dapat mengirimkan hasil temuan dan wawasan EventBridge untuk pengelolaan dan pemrosesan otomatis.

Acara dikirim ke EventBridge hanya di akun di mana mereka dilihat. Jika Anda melihat temuan menggunakan akun administrator, acara dikirim ke EventBridge akun administrator.

Agar panggilan AWS API efektif, implementasi kode target harus beralih peran ke akun anggota. Ini juga berarti bahwa peran yang Anda alihkan harus diterapkan ke setiap anggota di mana tindakan diperlukan.

Untuk mengirim temuan ke EventBridge (konsol)

1. Buka konsol AWS Security Hub Cloud Security Posture Management (CSPM) di <https://console.aws.amazon.com/securityhub/>
2. Menampilkan daftar temuan:
 - Dari Temuan, Anda dapat melihat temuan dari semua integrasi dan kontrol produk yang diaktifkan.

- Dari standar Keamanan, Anda dapat menavigasi ke daftar temuan yang dihasilkan dari kontrol tertentu. Untuk informasi selengkapnya, lihat [Meninjau rincian kontrol di Security Hub CSPM](#).
 - Dari Integrasi, Anda dapat menavigasi ke daftar temuan yang dihasilkan oleh integrasi yang diaktifkan. Untuk informasi selengkapnya, lihat [Melihat temuan dari integrasi CSPM Security Hub](#).
 - Dari Wawasan, Anda dapat menavigasi ke daftar temuan untuk hasil wawasan. Untuk informasi selengkapnya, lihat [Meninjau dan bertindak berdasarkan wawasan di Security Hub CSPM](#).
3. Pilih temuan yang akan dikirim EventBridge. Anda dapat memilih hingga 20 temuan sekaligus.
 4. Dari Tindakan, pilih tindakan kustom yang selaras dengan EventBridge aturan yang akan diterapkan.

Security Hub CSPM mengirimkan temuan Security Hub terpisah - peristiwa Tindakan Kustom untuk setiap temuan.

Untuk mengirim hasil wawasan ke EventBridge (konsol)

1. Buka konsol AWS Security Hub Cloud Security Posture Management (CSPM) di <https://console.aws.amazon.com/securityhub/>
2. Pada panel navigasi, silakan pilih Wawasan.
3. Pada halaman Wawasan, pilih wawasan yang menyertakan hasil untuk EventBridge dikirim.
4. Pilih hasil wawasan yang akan dikirim EventBridge. Anda dapat memilih hingga 20 hasil sekaligus.
5. Dari Tindakan, pilih tindakan kustom yang selaras dengan EventBridge aturan yang akan diterapkan.

Bekerja dengan dasbor di Security Hub CSPM

Halaman Ringkasan di konsol Security Hub menampilkan ringkasan risiko, urutan serangan, dan cakupan keamanan Anda. Halaman ini membantu Anda mengidentifikasi risiko dan urutan serangan berdasarkan tingkat keparahannya dan cakupan akun untuk berbagai kemampuan keamanan. Anda dapat menyesuaikan halaman ini dengan menambahkan dan menghapus widget keamanan yang berbeda dan menetapkan kriteria filter untuk mengambil jenis data tertentu.

Kustomisasi ke halaman ini disimpan untuk digunakan di masa mendatang. Jika pengguna di akun Anda menyesuaikan halaman ini, preferensi penyesuaian mereka disimpan secara independen dari preferensi penyesuaian Anda.

Jika akun Anda adalah akun administrator yang didelegasikan untuk suatu organisasi, data tersebut mencakup temuan untuk akun dan akun anggota Anda. Jika akun Anda adalah akun anggota atau akun mandiri, data hanya mencakup temuan untuk akun Anda.

Jika Anda mengonfigurasi agregasi lintas wilayah di CSPM Security Hub, halaman ini menampilkan temuan dari agregasi Anda

Note

Setiap kali Anda membuka halaman ini, halaman ini secara otomatis menyegarkan. Namun, skor keamanan dan status kontrol disegarkan setiap 24 jam.

Widget ringkasan risiko

Widget ini menunjukkan semua risiko Anda berdasarkan tingkat keparahan. Risiko dengan tingkat keparahan yang lebih besar muncul lebih dulu. Risiko didasarkan pada analisis temuan dan sifat dari Security Hub CSPM dan lainnya. Layanan AWS

Widget ringkasan ancaman

Widget ini menunjukkan semua urutan serangan Anda berdasarkan tingkat keparahan. Urutan serangan dengan tingkat keparahan yang lebih besar muncul lebih dulu. Urutan serangan terkait dengan serangkaian peristiwa dan mengidentifikasi potensi ancaman di lingkungan Anda. Mereka juga berasal. GuardDuty

Widget cakupan keamanan

Widget yang tersedia untuk dasbor Ringkasan

Dasbor Ringkasan mencakup widget yang mencerminkan lanskap ancaman keamanan cloud modern, dipandu oleh operasi keamanan dan pengalaman AWS pelanggan. Beberapa widget ditampilkan secara default sementara yang lain tidak. Anda dapat menyesuaikan tampilan dasbor dengan menambahkan atau menghapus widget.

Untuk menambahkannya, pilih Tambah widget di kanan atas halaman Ringkasan. Di bilah pencarian, masukkan judul widget. Seret dan jatuhkan widget ke dasbor.

Widget ditampilkan secara default

Secara default, dasbor Ringkasan mencakup widget berikut:

Urutan ancaman teratas

Menampilkan urutan ancaman tingkat keparahan tertinggi. Temuan urutan ancaman, yang dikenal sebagai temuan urutan serangan di Amazon GuardDuty, mengkorelasikan beberapa peristiwa untuk mengidentifikasi potensi ancaman terhadap AWS lingkungan Anda. Urutan ancaman dapat mencakup perilaku serangan yang sedang berlangsung atau baru-baru ini (dalam jangka waktu 24 jam) di lingkungan Anda, yang pada gilirannya dapat menyebabkan kompromi lebih lanjut. Anda harus memiliki GuardDuty dan Perlindungan GuardDuty S3 diaktifkan untuk menerima temuan urutan ancaman di Security Hub CSPM.

Risiko teratas

Menampilkan ringkasan risiko teratas di lingkungan Anda. Bagian atas widget menunjukkan jumlah risiko pada setiap tingkat keparahan. Anda dapat memilih tingkat keparahan untuk membuka halaman Risiko dengan risiko yang disaring ke tingkat keparahan yang dipilih. Risiko yang paling banyak terjadi di lingkungan Anda muncul terlebih dahulu. Widget ini membantu Anda memprioritaskan risiko mana yang harus dikurangi.

Cakupan keamanan

Merangkum sejauh mana cakupan keamanan Anda, berdasarkan temuan kontrol cakupan. Kontrol cakupan memeriksa apakah spesifik Layanan AWS dan kemampuannya diaktifkan (misalnya, [\[Macie.1\] Amazon Macie harus diaktifkan](#)). Widget ini membantu Anda memastikan bahwa Anda memiliki PASSED temuan untuk kontrol cakupan. Konsol CSPM Security Hub

menyediakan tautan dari widget ini untuk membantu Anda mengaktifkan kemampuan keamanan yang hilang. Kami merekomendasikan penggunaan konfigurasi pusat untuk mengaktifkan kemampuan keamanan yang hilang di beberapa Akun AWS dan Wilayah AWS. Untuk informasi selengkapnya, lihat [Memahami konfigurasi pusat di Security Hub CSPM](#).

Standar keamanan

Menampilkan skor keamanan ringkasan terbaru Anda dan skor keamanan untuk setiap standar CSPM Security Hub. Skor keamanan, yang berkisar antara 0-100 persen, mewakili proporsi kontrol yang diteruskan relatif terhadap semua kontrol yang Anda aktifkan. Untuk informasi lebih lanjut tentang skor ini, lihat [Metode penghitungan skor keamanan](#). Widget ini membantu Anda memahami postur keamanan Anda secara keseluruhan.

Standar keamanan

Menampilkan skor keamanan ringkasan terbaru Anda dan skor keamanan untuk setiap standar CSPM Security Hub. Skor keamanan, yang berkisar antara 0-100 persen, mewakili proporsi kontrol yang diteruskan relatif terhadap semua kontrol yang Anda aktifkan. Untuk informasi lebih lanjut tentang skor ini, lihat [Metode penghitungan skor keamanan](#). Widget ini membantu Anda memahami postur keamanan Anda secara keseluruhan.

Aset dengan temuan terbanyak

Memberikan gambaran umum tentang sumber daya, akun, dan aplikasi yang memiliki temuan paling banyak. Daftar ini diurutkan dalam urutan menurun berdasarkan jumlah temuan. Di widget, setiap tab menampilkan enam item teratas dalam kategori itu, dikelompokkan berdasarkan tingkat keparahan dan jenis sumber daya. Jika Anda memilih nomor di kolom Total temuan, Security Hub CSPM membuka halaman yang menunjukkan temuan untuk aset tersebut. Widget ini membantu Anda dengan cepat mengidentifikasi aset inti mana yang memiliki potensi ancaman keamanan.

Temuan berdasarkan Wilayah

Menunjukkan jumlah total temuan, dikelompokkan berdasarkan tingkat keparahan, Wilayah AWS di masing-masing tempat CSPM Security Hub diaktifkan. Widget ini membantu Anda mengidentifikasi masalah keamanan yang berpotensi memengaruhi Wilayah tertentu. Jika Anda membuka dasbor di Wilayah agregasi Anda, widget ini membantu Anda memantau potensi masalah keamanan di setiap Wilayah yang ditautkan.

Jenis ancaman yang paling umum

Memberikan rincian dari 10 jenis ancaman paling umum di AWS lingkungan Anda. Ini termasuk ancaman seperti eskalasi hak istimewa, penggunaan kredensial yang terbuka, atau komunikasi dengan alamat IP berbahaya.

Untuk melihat data ini, [Amazon GuardDuty](#) harus diaktifkan. Jika ya, pilih jenis ancaman di widget ini untuk membuka GuardDuty konsol dan meninjau temuan yang terkait dengan ancaman ini. Widget ini membantu Anda mengevaluasi potensi ancaman dalam konteks masalah keamanan lainnya.

Kerentanan perangkat lunak dengan eksploitasi

Menyediakan ringkasan kerentanan perangkat lunak yang ada di AWS lingkungan Anda dan telah diketahui eksploitasi. Anda juga dapat meninjau rincian kerentanan yang melakukan dan tidak memiliki perbaikan yang tersedia.

Untuk melihat data ini, [Amazon Inspector](#) harus diaktifkan. Jika ya, pilih statistik di widget ini untuk membuka konsol Amazon Inspector dan tinjau detail lebih lanjut tentang kerentanan. Widget ini membantu Anda mengevaluasi kerentanan perangkat lunak dalam konteks masalah keamanan lainnya.

Temuan baru dari waktu ke waktu

Menunjukkan tren dalam jumlah temuan harian baru selama 90 hari terakhir. Anda dapat memecah data berdasarkan tingkat keparahan atau oleh penyedia untuk konteks tambahan. Widget ini membantu Anda memahami jika menemukan volume melonjak atau turun pada waktu tertentu selama 90 hari terakhir.

Sumber daya dengan temuan terbanyak

Memberikan ringkasan sumber daya yang paling banyak menghasilkan temuan, dipecah berdasarkan jenis sumber daya berikut: Bucket Amazon Simple Storage Service (Amazon S3), instans Amazon Elastic Compute Cloud (EC2Amazon), dan fungsi. AWS Lambda

Di widget, setiap tab berfokus pada salah satu jenis sumber daya sebelumnya, mencantumkan 10 contoh sumber daya yang menghasilkan temuan terbanyak. Untuk meninjau temuan untuk sumber daya tertentu, pilih contoh sumber daya. Widget ini membantu Anda melakukan triase temuan keamanan yang terkait dengan AWS sumber daya umum.

Widget tersembunyi secara default

Widget berikut juga tersedia untuk dasbor Ringkasan, tetapi mereka disembunyikan secara default:

AMIs dengan temuan terbanyak

Menyediakan daftar 10 Amazon Machine Images (AMIs) yang telah menghasilkan temuan terbanyak. Data ini hanya tersedia jika Amazon EC2 diaktifkan untuk akun Anda. Ini membantu Anda mengidentifikasi mana yang AMIs menimbulkan risiko keamanan potensial.

Prinsipal IAM dengan temuan terbanyak

Menyediakan daftar 10 AWS Identity and Access Management (IAM) pengguna yang telah menghasilkan temuan terbanyak. Widget ini membantu Anda melakukan tugas administratif dan penagihan. Ini menunjukkan kepada Anda pengguna mana yang paling berkontribusi pada penggunaan CSPM Security Hub.

Akun dengan temuan terbanyak (berdasarkan tingkat keparahan)

Menunjukkan grafik dari 10 akun yang telah menghasilkan temuan terbanyak, dikelompokkan berdasarkan tingkat keparahan. Widget ini membantu Anda menentukan akun mana yang akan memfokuskan upaya analisis dan remediasi.

Akun dengan temuan terbanyak (berdasarkan jenis sumber daya)

Menampilkan grafik dari 10 akun yang telah menghasilkan temuan terbanyak, dikelompokkan berdasarkan jenis sumber daya. Widget ini membantu Anda menentukan jenis akun dan sumber daya mana yang akan diprioritaskan untuk analisis dan remediasi.

Wawasan

Daftar lima [wawasan terkelola CSPM Security Hub](#) dan jumlah temuan yang mereka hasilkan. Wawasan mengidentifikasi area keamanan tertentu yang membutuhkan perhatian.

Temuan terbaru dari AWS integrasi

[Menunjukkan jumlah temuan yang Anda terima di Security Hub CSPM dari terintegrasi. Layanan AWS](#) Ini juga menunjukkan kapan Anda baru-baru ini menerima temuan dari setiap layanan terintegrasi. Widget ini menyediakan data temuan terkonsolidasi dari beberapa Layanan AWS. Untuk menelusuri, pilih layanan terintegrasi. Security Hub CSPM kemudian membuka konsol untuk layanan itu.

Memfilter dasbor Ringkasan di Security Hub CSPM

Anda dapat mengkurasi dasbor Ringkasan di konsol AWS Security Hub Cloud Security Posture Management (CSPM) sehingga hanya menyertakan data keamanan yang paling relevan bagi Anda.

Misalnya, jika Anda anggota tim aplikasi, Anda dapat membuat tampilan khusus untuk aplikasi penting di lingkungan produksi Anda. Jika Anda anggota tim keamanan, Anda dapat membuat tampilan khusus yang membantu Anda fokus pada temuan tingkat keparahan tinggi.

Untuk membuat tampilan yang dikuratori ini, Anda memasukkan kriteria filter di kotak filter di atas dasbor. Jika Anda menerapkan kriteria filter, kriteria berlaku untuk semua data dan widget di dasbor, kecuali data dalam widget standar Wawasan dan Keamanan. Untuk daftar widget yang tersedia di dasbor, lihat [Widget yang tersedia untuk dasbor Ringkasan](#).

Anda dapat memfilter data dengan menggunakan bidang berikut:

- Nama akun
- account-id
- Aplikasi Nama Sumber Daya Amazon (ARN)
- Nama aplikasi
- Nama produk (untuk produk Layanan AWS atau pihak ketiga yang mengirimkan temuan ke Security Hub CSPM)
- Rekam keadaan
- Wilayah
- Tanda sumber daya
- Kepelikan
- Status alur kerja

Secara default, data dasbor disaring menggunakan kriteria berikut: `Workflow.Status is NOTIFIED or NEW`, and `RecordState is ACTIVE`. Kriteria ini muncul di atas dasbor, di bawah kotak filter. Untuk menghapus kriteria ini, pilih X di token filter untuk kriteria yang ingin Anda hapus.

Jika Anda menerapkan kriteria filter yang ingin Anda gunakan lagi, Anda dapat menyimpannya sebagai set filter. Kumpulan filter adalah sekumpulan kriteria filter yang Anda buat dan simpan untuk diterapkan kembali saat Anda meninjau data di dasbor Ringkasan.

Note

Bidang berikut tidak dapat disimpan sebagai bagian dari kumpulan filter: ARN aplikasi, nama aplikasi, dan tag sumber daya.

Membuat dan menyimpan set filter

Ikuti langkah-langkah ini untuk membuat dan menyimpan set filter.

Untuk membuat dan menyimpan set filter

1. Buka konsol AWS Security Hub Cloud Security Posture Management (CSPM) di <https://console.aws.amazon.com/securityhub/>
2. Di panel navigasi, pilih Ringkasan.
3. Pada kotak filter di atas dasbor Ringkasan, masukkan kriteria filter untuk set filter.
4. Pada menu Hapus filter, pilih Simpan set filter baru.
5. Dalam kotak dialog Simpan set filter, masukkan nama untuk set filter.
6. (Opsional) Untuk menggunakan filter yang ditetapkan secara default setiap kali Anda membuka halaman Ringkasan, pilih opsi untuk mengaturnya sebagai tampilan default.
7. Pilih Simpan.

Untuk beralih di antara set filter yang telah Anda buat dan simpan, gunakan menu Pilih set filter di atas dasbor Ringkasan. Saat Anda memilih set filter, Security Hub CSPM menerapkan kriteria filter yang disetel ke data di dasbor.

Memperbarui atau menghapus set filter

Ikuti langkah-langkah ini untuk memperbarui atau menghapus set filter yang ada. Jika Anda menghapus kumpulan filter yang saat ini ditetapkan sebagai tampilan default dasbor Ringkasan, tampilan default Anda disetel ulang ke tampilan CSPM Security Hub default.

Untuk memperbarui atau menghapus set filter

1. Buka konsol AWS Security Hub Cloud Security Posture Management (CSPM) di <https://console.aws.amazon.com/securityhub/>
2. Di panel navigasi, pilih Ringkasan.
3. Dalam menu Pilih set filter di atas halaman Ringkasan, pilih set filter.
4. Pada menu Hapus filter, lakukan salah satu hal berikut:
 - Untuk memperbarui set filter, pilih Perbarui set filter saat ini. Kemudian, masukkan perubahan Anda di kotak dialog yang muncul.

- Untuk menghapus set filter pilih Hapus set filter saat ini. Kemudian, pilih Hapus di kotak dialog yang muncul.

Menyesuaikan dasbor Ringkasan di Security Hub CSPM

Anda dapat menyesuaikan dasbor Ringkasan di konsol AWS Security Hub Cloud Security Posture Management (CSPM) dengan beberapa cara. Misalnya, Anda dapat menambah dan menghapus widget dari dasbor. Anda juga dapat mengatur ulang dan mengubah ukuran widget di dasbor. Untuk daftar widget yang tersedia di dasbor, lihat [Widget yang tersedia untuk dasbor Ringkasan](#).

Jika Anda menyesuaikan dasbor, Security Hub CSPM segera menerapkan perubahan Anda dan menyimpan pengaturan dasbor baru Anda. Perubahan Anda berlaku untuk tampilan dasbor Anda di semua Wilayah AWS dan browser.

Untuk menyesuaikan dasbor Ringkasan

1. Buka konsol AWS Security Hub Cloud Security Posture Management (CSPM) di <https://console.aws.amazon.com/securityhub/>
2. Di panel navigasi, pilih Ringkasan.
3. Lakukan salah satu langkah berikut ini:
 - Untuk menambahkan widget, pilih Tambahkan widget di sudut kanan atas halaman. Di bilah pencarian, masukkan judul widget yang akan ditambahkan. Kemudian, seret widget ke lokasi yang Anda inginkan.
 - Untuk menghapus widget, pilih tiga titik di sudut kanan atas widget.
 - Untuk memindahkan widget, pilih pegangan di sudut kiri atas widget, lalu seret widget ke lokasi yang Anda inginkan.
 - Untuk mengubah ukuran widget, pilih pegangan pengubahan ukuran di sudut kanan bawah widget. Seret tepi widget hingga widget adalah ukuran pilihan Anda.

Untuk selanjutnya mengembalikan pengaturan asli, pilih Atur ulang ke tata letak default di bagian atas halaman.

Batas regional untuk Security Hub CSPM

Beberapa fitur AWS Security Hub Cloud Security Posture Management (CSPM) hanya tersedia dalam beberapa hal tertentu. Wilayah AWS Bagian berikut menentukan batas Regional ini. Untuk daftar lengkap semua Wilayah di mana Security Hub CSPM saat ini tersedia, lihat [titik akhir dan kuota AWS Security Hub Cloud Security Posture Management \(CSPM\)](#) Security Hub di. Referensi Umum AWS

Pembatasan agregasi Lintas Wilayah

Di AWS GovCloud (US) Wilayah, [agregasi lintas wilayah](#) tersedia untuk temuan, menemukan pembaruan, dan wawasan di seluruh AWS GovCloud (US) Wilayah saja. Secara khusus, Anda hanya dapat mengumpulkan temuan, menemukan pembaruan, dan wawasan antara AWS GovCloud (AS-Timur) dan AWS GovCloud (AS-Barat).

Di Wilayah Tiongkok, agregasi lintas wilayah tersedia untuk temuan, menemukan pembaruan, dan wawasan di seluruh Wilayah Tiongkok saja. Secara khusus, Anda hanya dapat mengumpulkan temuan, menemukan pembaruan, dan wawasan antara Tiongkok (Beijing) dan Tiongkok (Ningxia).

Anda tidak dapat menggunakan Wilayah yang dinonaktifkan secara default sebagai Wilayah agregasi Anda. Untuk daftar Wilayah yang dinonaktifkan secara default, lihat [Mengaktifkan atau menonaktifkan Wilayah AWS di akun Anda](#) di Panduan AWS Account Management Referensi.

Ketersediaan integrasi menurut Wilayah

Beberapa integrasi tidak tersedia di semua Wilayah. Jika integrasi tidak tersedia di Wilayah tertentu, integrasi tidak tercantum di halaman Integrasi konsol CSPM Security Hub saat Anda memilih Wilayah tersebut.

Integrasi yang didukung di Wilayah Tiongkok (Beijing) dan Tiongkok (Ningxia)

Wilayah Tiongkok (Beijing) dan Tiongkok (Ningxia) hanya mendukung [integrasi AWS berikut dengan layanan:](#)

- AWS Firewall Manager
- Amazon GuardDuty

- AWS Identity and Access Management Access Analyzer
- Amazon Inspector
- AWS IoT Device Defender
- AWS Systems Manager Explorer
- AWS Systems Manager OpsCenter
- AWS Systems Manager Manager Patch

Wilayah Tiongkok (Beijing) dan Tiongkok (Ningxia) hanya mendukung integrasi pihak ketiga [berikut](#):

- Cloud Custodian
- FireEye Helix
- Helecloud
- IBM QRadar
- PagerDuty
- Palo Alto Networks Cortex XSOAR
- Palo Alto Networks VM-Series
- Prowler
- RSA Archer
- Splunk Enterprise
- Splunk Phantom
- ThreatModeler

Integrasi yang didukung di Wilayah AWS GovCloud (AS-Timur) dan AWS GovCloud (AS-Barat)

Wilayah AWS GovCloud (AS-Timur) dan AWS GovCloud (AS-Barat) hanya mendukung [integrasi](#) berikut dengan layanan: AWS

- AWS Config
- Amazon Detective
- AWS Firewall Manager
- Amazon GuardDuty

- AWS Health
- IAM Access Analyzer
- Amazon Inspector
- AWS IoT Device Defender

Wilayah AWS GovCloud (AS-Timur) dan AWS GovCloud (AS-Barat) hanya mendukung integrasi pihak [ketiga](#) berikut:

- Atlassian Jira Service Management
- Atlassian Jira Service Management Cloud
- Atlassian OpsGenie
- Caveonix Cloud
- Cloud Custodian
- Cloud Storage Security Antivirus for Amazon S3
- CrowdStrike Falcon
- FireEye Helix
- Forcepoint CASB
- Forcepoint DLP
- Forcepoint NGFW
- Fugue
- Kion
- MicroFocus ArcSight
- NETSCOUT Cyber Investigator
- PagerDuty
- Palo Alto Networks – Prisma Cloud Compute
- Palo Alto Networks – Prisma Cloud Enterprise
- Palo Alto Networks – VM-Series(hanya tersedia di AWS GovCloud (AS-Barat))
- Prowler
- Rackspace Technology – Cloud Native Security
- Rapid7 InsightConnect
- RSA Archer

- SecureCloudDb
- ServiceNow ITSM
- Slack
- ThreatModeler
- Vectra AI Cognito Detect

Ketersediaan standar menurut Wilayah

Standar yang AWS Control Tower dikelola layanan hanya tersedia di Wilayah yang AWS Control Tower mendukung, termasuk AWS GovCloud (US) Wilayah. Untuk daftar Wilayah yang AWS Control Tower saat ini mendukung, lihat [Cara Wilayah AWS Bekerja Dengan AWS Control Tower](#) di Panduan AWS Control Tower Pengguna.

Standar Penandaan AWS Sumber Daya tidak tersedia di Kanada Barat (Calgary), Tiongkok, dan Wilayah. AWS GovCloud (US)

Standar keamanan lainnya tersedia di semua Wilayah di mana Security Hub CSPM saat ini tersedia.

Ketersediaan kontrol berdasarkan Wilayah

Beberapa kontrol CSPM Security Hub tidak tersedia di semua Wilayah. Untuk daftar kontrol yang tidak tersedia di setiap Wilayah, lihat [Batas regional pada kontrol CSPM Security Hub](#).

Di konsol CSPM Security Hub, kontrol tidak akan muncul di daftar kontrol jika tidak tersedia di Wilayah tempat Anda masuk saat ini. Pengecualian adalah Wilayah agregasi. Jika Anda menyetel Wilayah agregasi dan masuk ke Wilayah tersebut, konsol akan menampilkan kontrol yang tersedia di Wilayah agregasi atau satu atau beberapa Wilayah tertaut.

Batas regional pada kontrol CSPM Security Hub

Beberapa kontrol AWS Security Hub Cloud Security Posture Management (CSPM) tidak tersedia di semua. Wilayah AWS Halaman ini menentukan kontrol mana yang tidak tersedia di Wilayah tertentu.

Di konsol CSPM Security Hub, kontrol tidak akan muncul di daftar kontrol jika tidak tersedia di Wilayah tempat Anda masuk saat ini. Pengecualian adalah Wilayah agregasi. Jika Anda menyetel Wilayah agregasi dan masuk ke Wilayah tersebut, konsol akan menampilkan kontrol yang tersedia di Wilayah agregasi atau satu atau beberapa Wilayah tertaut.

Wilayah AWS

- [AS Timur \(Virginia Utara\)](#)
- [AS Timur \(Ohio\)](#)
- [AS Barat \(California Utara\)](#)
- [AS Barat \(Oregon\)](#)
- [Afrika \(Cape Town\)](#)
- [Asia Pasifik \(Hong Kong\)](#)
- [Asia Pasifik \(Hyderabad\)](#)
- [Asia Pasifik \(Jakarta\)](#)
- [Asia Pasifik \(Malaysia\)](#)
- [Asia Pasifik \(Melbourne\)](#)
- [Asia Pasifik \(Mumbai\)](#)
- [Asia Pasifik \(Osaka\)](#)
- [Asia Pasifik \(Seoul\)](#)
- [Asia Pasifik \(Singapura\)](#)
- [Asia Pasifik \(Sydney\)](#)
- [Asia Pasifik \(Thailand\)](#)
- [Asia Pasifik \(Tokyo\)](#)
- [Kanada \(Pusat\)](#)
- [Kanada Barat \(Calgary\)](#)
- [Tiongkok \(Beijing\)](#)
- [Tiongkok \(Ningxia\)](#)
- [Eropa \(Frankfurt\)](#)
- [Eropa \(Irlandia\)](#)
- [Eropa \(London\)](#)
- [Eropa \(Milan\)](#)
- [Eropa \(Paris\)](#)
- [Eropa \(Spanyol\)](#)
- [Eropa \(Stockholm\)](#)
- [Eropa \(Zürich\)](#)

- [Israel \(Tel Aviv\)](#)
- [Meksiko \(Tengah\)](#)
- [Timur Tengah \(Bahrain\)](#)
- [Timur Tengah \(UEA\)](#)
- [Amerika Selatan \(Sao Paulo\)](#)
- [AWS GovCloud \(AS-Timur\)](#)
- [AWS GovCloud \(AS-Barat\)](#)

AS Timur (Virginia Utara)

Kontrol berikut tidak didukung di Wilayah AS Timur (Virginia N.).

- [\[ElastiCache.4\]](#) grup ElastiCache replikasi harus dienkripsi saat istirahat
- [\[ElastiCache.5\]](#) grup ElastiCache replikasi harus dienkripsi saat transit
- [\[ElastiCache.6\]](#) ElastiCache (Redis OSS) grup replikasi dari versi sebelumnya harus mengaktifkan Redis OSS AUTH
- [\[ElastiCache.7\]](#) ElastiCache cluster tidak boleh menggunakan grup subnet default
- [\[GlobalAccelerator.1\]](#) Akselerator Akselerator Global harus diberi tag
- [\[S3.24\]](#) Poin Akses Multi-Wilayah S3 harus mengaktifkan pengaturan akses publik blok

AS Timur (Ohio)

Kontrol berikut tidak didukung di Wilayah Timur AS (Ohio).

- [\[AppSync.1\]](#) Cache AWS AppSync API harus dienkripsi saat istirahat
- [\[AppSync.6\]](#) Cache AWS AppSync API harus dienkripsi saat transit
- [\[CloudFront.1\]](#) CloudFront distribusi harus memiliki objek root default yang dikonfigurasi
- [\[CloudFront.3\]](#) CloudFront distribusi harus memerlukan enkripsi dalam perjalanan
- [\[CloudFront.4\]](#) CloudFront distribusi harus memiliki failover asal yang dikonfigurasi
- [\[CloudFront.5\]](#) CloudFront distribusi seharusnya mengaktifkan logging
- [\[CloudFront.6\]](#) CloudFront distribusi harus mengaktifkan WAF
- [\[CloudFront.7\]](#) CloudFront distribusi harus menggunakan sertifikat SSL/TLS khusus
- [\[CloudFront.8\]](#) CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS

- [\[CloudFront.9\] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus](#)
- [\[CloudFront.10\] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal kustom](#)
- [\[CloudFront.12\] CloudFront distribusi seharusnya tidak menunjukkan asal S3 yang tidak ada](#)
- [\[CloudFront.13\] CloudFront distribusi harus menggunakan kontrol akses asal](#)
- [\[CloudFront.14\] CloudFront distribusi harus ditandai](#)
- [\[Connect.1\] Jenis objek Amazon Connect Customer Profiles harus diberi tag](#)
- [\[Connect.2\] Instans Amazon Connect seharusnya mengaktifkan logging CloudWatch](#)
- [\[EC2.24\] Jenis instance EC2 paravirtual Amazon tidak boleh digunakan](#)
- [\[EC2.173\] Permintaan Armada EC2 Spot harus mengaktifkan enkripsi untuk volume EBS terlampir](#)
- [\[ECR.4\] Repositori publik ECR harus ditandai](#)
- [\[GlobalAccelerator.1\] Akselerator Akselerator Global harus diberi tag](#)
- [\[IAM.26\] Sertifikat SSL/TLS kedaluwarsa yang dikelola di IAM harus dihapus](#)
- [\[IoT Twin Maker.1\] Pekerjaan sinkronisasi AWS IoT harus ditandai TwinMaker](#)
- [\[IoT Twin Maker.2\] Ruang kerja AWS IoT harus diberi tag TwinMaker](#)
- [\[IoT Twin Maker.3\] Adegan AWS IoT harus diberi tag TwinMaker](#)
- [\[IoT Twin Maker.4\] Entitas AWS IoT harus diberi tag TwinMaker](#)
- [\[IoT Wireless .1\] Grup multicast Nirkabel AWS IoT harus diberi tag](#)
- [\[IoT Wireless .2\] Profil layanan AWS IoT Wireless harus diberi tag](#)
- [\[IoT Wireless .3\] Tugas AWS IoT FUOTA harus ditandai](#)
- [\[IVS.1\] Pasangan kunci pemutaran IVS harus ditandai](#)
- [\[IVS.2\] Konfigurasi perekaman IVS harus ditandai](#)
- [\[IVS.3\] Saluran IVS harus ditandai](#)
- [\[RDS.31\] Grup keamanan RDS DB harus ditandai](#)
- [\[Route53.1\] Pemeriksaan kesehatan rute 53 harus ditandai](#)
- [\[Route53.2\] Route 53 zona yang dihosting publik harus mencatat kueri DNS](#)
- [\[S3.24\] Poin Akses Multi-Wilayah S3 harus mengaktifkan pengaturan akses publik blok](#)
- [\[WAF.1\] Pencatatan ACL Web Global AWS WAF Klasik harus diaktifkan](#)
- [\[WAF.6\] Aturan global AWS WAF klasik harus memiliki setidaknya satu syarat](#)
- [\[WAF.7\] Kelompok aturan global AWS WAF klasik harus memiliki setidaknya satu aturan](#)

- [\[WAF.8\] Web global AWS WAF klasik ACLs harus memiliki setidaknya satu aturan atau kelompok aturan](#)
- [\[WorkSpaces.1\] volume WorkSpaces pengguna harus dienkripsi saat istirahat](#)
- [\[WorkSpaces.2\] volume WorkSpaces root harus dienkripsi saat istirahat](#)

AS Barat (California Utara)

Kontrol berikut tidak didukung di Wilayah AS Barat (California Utara).

- [\[AppRunner.1\] Layanan App Runner harus diberi tag](#)
- [\[AppRunner.2\] Konektor VPC App Runner harus diberi tag](#)
- [\[AppSync.1\] Cache AWS AppSync API harus dienkripsi saat istirahat](#)
- [\[AppSync.6\] Cache AWS AppSync API harus dienkripsi saat transit](#)
- [\[CloudFront.1\] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi](#)
- [\[CloudFront.3\] CloudFront distribusi harus memerlukan enkripsi dalam perjalanan](#)
- [\[CloudFront.4\] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi](#)
- [\[CloudFront.5\] CloudFront distribusi seharusnya mengaktifkan logging](#)
- [\[CloudFront.6\] CloudFront distribusi harus mengaktifkan WAF](#)
- [\[CloudFront.7\] CloudFront distribusi harus menggunakan sertifikat SSL/TLS khusus](#)
- [\[CloudFront.8\] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS](#)
- [\[CloudFront.9\] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus](#)
- [\[CloudFront.10\] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal kustom](#)
- [\[CloudFront.12\] CloudFront distribusi seharusnya tidak menunjukkan asal S3 yang tidak ada](#)
- [\[CloudFront.13\] CloudFront distribusi harus menggunakan kontrol akses asal](#)
- [\[CloudFront.14\] CloudFront distribusi harus ditandai](#)
- [\[CodeArtifact.1\] CodeArtifact repositori harus ditandai](#)
- [\[CodeGuruProfiler.1\] Grup CodeGuru profil profiler harus diberi tag](#)
- [\[CodeGuruReviewer.1\] Asosiasi CodeGuru repositori peninjau harus diberi tag](#)
- [\[Connect.1\] Jenis objek Amazon Connect Customer Profiles harus diberi tag](#)
- [\[Connect.2\] Instans Amazon Connect seharusnya mengaktifkan logging CloudWatch](#)
- [\[DocumentDB.1\] Cluster Amazon DocumentDB harus dienkripsi saat istirahat](#)

- [\[DocumentDB.2\] Cluster Amazon DocumentDB harus memiliki periode retensi cadangan yang memadai](#)
- [\[DocumentDB.3\] Cuplikan cluster manual Amazon DocumentDB seharusnya tidak bersifat publik](#)
- [\[DocumentDB.4\] Cluster Amazon DocumentDB harus mempublikasikan log audit ke Log CloudWatch](#)
- [\[DocumentDB.5\] Cluster Amazon DocumentDB harus mengaktifkan perlindungan penghapusan](#)
- [\[DocumentDB.6\] Cluster Amazon DocumentDB harus dienkripsi saat transit](#)
- [\[EC2.173\] Permintaan Armada EC2 Spot harus mengaktifkan enkripsi untuk volume EBS terlampir](#)
- [\[ECR.4\] Repositori publik ECR harus ditandai](#)
- [\[FraudDetector.1\] Jenis entitas Amazon Fraud Detector harus diberi tag](#)
- [\[FraudDetector.2\] Label Amazon Fraud Detector harus diberi tag](#)
- [\[FraudDetector.3\] Hasil Amazon Fraud Detector harus ditandai](#)
- [\[FraudDetector.4\] Variabel Amazon Fraud Detector harus diberi tag](#)
- [\[GlobalAccelerator.1\] Akselerator Akselerator Global harus diberi tag](#)
- [\[IAM.26\] Sertifikat SSL/TLS kedaluwarsa yang dikelola di IAM harus dihapus](#)
- [\[Inspektor.3\] Pemindaian kode Amazon Inspector Lambda harus diaktifkan](#)
- [\[IoTEvents.1\] Input Peristiwa AWS IoT harus diberi tag](#)
- [\[IoTEvents.2\] Model detektor Acara AWS IoT harus diberi tag](#)
- [\[IoTEvents.3\] Model alarm AWS IoT Events harus diberi tag](#)
- [\[IoTSiteWise.1\] Model aset AWS IoT harus ditandai SiteWise](#)
- [\[IoTSiteWise.2\] Dasbor AWS IoT harus diberi tag SiteWise](#)
- [\[IoTSiteWise.3\] Gateway AWS IoT harus diberi tag SiteWise](#)
- [\[IoTSiteWise.4\] Portal AWS IoT harus diberi tag SiteWise](#)
- [\[IoTSiteWise.5\] Proyek AWS IoT harus diberi tag SiteWise](#)
- [\[IoTThingMaker.1\] Pekerjaan sinkronisasi AWS IoT harus ditandai ThingMaker](#)
- [\[IoTThingMaker.2\] Ruang kerja AWS IoT harus diberi tag ThingMaker](#)
- [\[IoTThingMaker.3\] Adegan AWS IoT harus diberi tag ThingMaker](#)
- [\[IoTThingMaker.4\] Entitas AWS IoT harus diberi tag ThingMaker](#)
- [\[IoTWireless.1\] Grup multicast Nirkabel AWS IoT harus diberi tag](#)
- [\[IoTWireless.2\] Profil layanan AWS IoT Wireless harus diberi tag](#)
- [\[IoTWireless.3\] Tugas AWS IoT FUOTA harus ditandai](#)

- [\[IVS.1\] Pasangan kunci pemutaran IVS harus ditandai](#)
- [\[IVS.2\] Konfigurasi perekaman IVS harus ditandai](#)
- [\[IVS.3\] Saluran IVS harus ditandai](#)
- [\[RDS.35\] Cluster RDS DB harus mengaktifkan peningkatan versi minor otomatis](#)
- [\[Route53.1\] Pemeriksaan kesehatan rute 53 harus ditandai](#)
- [\[Route53.2\] Route 53 zona yang dihosting publik harus mencatat kueri DNS](#)
- [\[S3.24\] Poin Akses Multi-Wilayah S3 harus mengaktifkan pengaturan akses publik blok](#)
- [\[WAF.1\] Pencatatan ACL Web Global AWS WAF Klasik harus diaktifkan](#)
- [\[WAF.6\] Aturan global AWS WAF klasik harus memiliki setidaknya satu syarat](#)
- [\[WAF.7\] Kelompok aturan global AWS WAF klasik harus memiliki setidaknya satu aturan](#)
- [\[WAF.8\] Web global AWS WAF klasik ACLs harus memiliki setidaknya satu aturan atau kelompok aturan](#)
- [\[WorkSpaces.1\] volume WorkSpaces pengguna harus dienkrpsi saat istirahat](#)
- [\[WorkSpaces.2\] volume WorkSpaces root harus dienkrpsi saat istirahat](#)

AS Barat (Oregon)

Kontrol berikut tidak didukung di Wilayah Barat AS (Oregon).

- [\[AppSync.1\] Cache AWS AppSync API harus dienkrpsi saat istirahat](#)
- [\[AppSync.6\] Cache AWS AppSync API harus dienkrpsi saat transit](#)
- [\[CloudFront.1\] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi](#)
- [\[CloudFront.3\] CloudFront distribusi harus memerlukan enkripsi dalam perjalanan](#)
- [\[CloudFront.4\] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi](#)
- [\[CloudFront.5\] CloudFront distribusi seharusnya mengaktifkan logging](#)
- [\[CloudFront.6\] CloudFront distribusi harus mengaktifkan WAF](#)
- [\[CloudFront.7\] CloudFront distribusi harus menggunakan sertifikat SSL/TLS khusus](#)
- [\[CloudFront.8\] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS](#)
- [\[CloudFront.9\] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus](#)
- [\[CloudFront.10\] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal kustom](#)
- [\[CloudFront.12\] CloudFront distribusi seharusnya tidak menunjukkan asal S3 yang tidak ada](#)

- [\[CloudFront.13\] CloudFront distribusi harus menggunakan kontrol akses asal](#)
- [\[CloudFront.14\] CloudFront distribusi harus ditandai](#)
- [\[EC2.173\] Permintaan Armada EC2 Spot harus mengaktifkan enkripsi untuk volume EBS terlampir](#)
- [\[ECR.4\] Repositori publik ECR harus ditandai](#)
- [\[IAM.26\] Sertifikat SSL/TLS kedaluwarsa yang dikelola di IAM harus dihapus](#)
- [\[Route53.1\] Pemeriksaan kesehatan rute 53 harus ditandai](#)
- [\[Route53.2\] Route 53 zona yang dihosting publik harus mencatat kueri DNS](#)
- [\[WAF.1\] Pencatatan ACL Web Global AWS WAF Klasik harus diaktifkan](#)
- [\[WAF.6\] Aturan global AWS WAF klasik harus memiliki setidaknya satu syarat](#)
- [\[WAF.7\] Kelompok aturan global AWS WAF klasik harus memiliki setidaknya satu aturan](#)
- [\[WAF.8\] Web global AWS WAF klasik ACLs harus memiliki setidaknya satu aturan atau kelompok aturan](#)

Afrika (Cape Town)

Kontrol berikut tidak didukung di Wilayah Afrika (Cape Town).

- [\[Amplify.1\] Aplikasi Amplify harus diberi tag](#)
- [\[Amplify.2\] Amplify branch harus diberi tag](#)
- [\[AppRunner.1\] Layanan App Runner harus diberi tag](#)
- [\[AppRunner.2\] Konektor VPC App Runner harus diberi tag](#)
- [\[AppSync.1\] Cache AWS AppSync API harus dienkrpsi saat istirahat](#)
- [\[AppSync.6\] Cache AWS AppSync API harus dienkrpsi saat transit](#)
- [\[CloudFront.1\] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi](#)
- [\[CloudFront.3\] CloudFront distribusi harus memerlukan enkripsi dalam perjalanan](#)
- [\[CloudFront.4\] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi](#)
- [\[CloudFront.5\] CloudFront distribusi seharusnya mengaktifkan logging](#)
- [\[CloudFront.6\] CloudFront distribusi harus mengaktifkan WAF](#)
- [\[CloudFront.7\] CloudFront distribusi harus menggunakan sertifikat SSL/TLS khusus](#)
- [\[CloudFront.8\] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS](#)
- [\[CloudFront.9\] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus](#)

- [\[CloudFront.10\] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal kustom](#)
- [\[CloudFront.12\] CloudFront distribusi seharusnya tidak menunjukkan asal S3 yang tidak ada](#)
- [\[CloudFront.13\] CloudFront distribusi harus menggunakan kontrol akses asal](#)
- [\[CloudFront.14\] CloudFront distribusi harus ditandai](#)
- [\[CodeArtifact.1\] CodeArtifact repositori harus ditandai](#)
- [\[CodeGuruProfiler.1\] Grup CodeGuru profil profiler harus diberi tag](#)
- [\[CodeGuruReviewer.1\] Asosiasi CodeGuru repositori peninjau harus diberi tag](#)
- [\[Cognito.1\] Kumpulan pengguna Cognito harus mengaktifkan perlindungan ancaman dengan mode penegakan fungsi penuh untuk otentikasi standar](#)
- [\[DMS.10\] Titik akhir DMS untuk database Neptunus harus mengaktifkan otorisasi IAM](#)
- [\[DocumentDB.1\] Cluster Amazon DocumentDB harus dienkripsi saat istirahat](#)
- [\[DocumentDB.2\] Cluster Amazon DocumentDB harus memiliki periode retensi cadangan yang memadai](#)
- [\[DocumentDB.3\] Cuplikan cluster manual Amazon DocumentDB seharusnya tidak bersifat publik](#)
- [\[DocumentDB.4\] Cluster Amazon DocumentDB harus mempublikasikan log audit ke Log CloudWatch](#)
- [\[DocumentDB.5\] Cluster Amazon DocumentDB harus mengaktifkan perlindungan penghapusan](#)
- [\[DocumentDB.6\] Cluster Amazon DocumentDB harus dienkripsi saat transit](#)
- [\[DynamoDB.3\] Cluster DynamoDB Accelerator \(DAX\) harus dienkripsi saat istirahat](#)
- [\[DynamoDB.7\] Cluster DynamoDB Accelerator harus dienkripsi saat transit](#)
- [\[EC2.4\] EC2 Instans yang dihentikan harus dihapus setelah periode waktu tertentu](#)
- [\[EC2.8\] EC2 instans harus menggunakan Instance Metadata Service Versi 2 \(\) IMDSv2](#)
- [\[EC2.14\] Grup keamanan seharusnya tidak mengizinkan masuknya dari 0.0.0.0/0 atau :/0 ke port 3389](#)
- [\[EC2.24\] Jenis instance EC2 paravirtual Amazon tidak boleh digunakan](#)
- [\[EC2.58\] VPCs harus dikonfigurasi dengan titik akhir antarmuka untuk Kontak Manajer Insiden Systems Manager](#)
- [\[EC2.60\] VPCs harus dikonfigurasi dengan titik akhir antarmuka untuk Systems Manager Incident Manager](#)
- [\[EC2.173\] Permintaan Armada EC2 Spot harus mengaktifkan enkripsi untuk volume EBS terlampir](#)
- [\[EC2.177\] Sesi cermin EC2 lalu lintas harus ditandai](#)

- [\[EC2.179\] Target cermin EC2 lalu lintas harus ditandai](#)
- [\[ECR.4\] Repositori publik ECR harus ditandai](#)
- [\[ELB.2\] Classic Load Balancer dengan pendengar SSL/HTTPS harus menggunakan sertifikat yang disediakan oleh AWS Certificate Manager](#)
- [\[ES.3\] Domain Elasticsearch harus mengenkripsi data yang dikirim antar node](#)
- [\[EventBridge.4\] titik akhir EventBridge global harus mengaktifkan replikasi acara](#)
- [\[FraudDetector.1\] Jenis entitas Amazon Fraud Detector harus diberi tag](#)
- [\[FraudDetector.2\] Label Amazon Fraud Detector harus diberi tag](#)
- [\[FraudDetector.3\] Hasil Amazon Fraud Detector harus ditandai](#)
- [\[FraudDetector.4\] Variabel Amazon Fraud Detector harus diberi tag](#)
- [\[GlobalAccelerator.1\] Akselerator Akselerator Global harus diberi tag](#)
- [\[IAM.18\] Memastikan peran dukungan telah dibuat untuk mengelola insiden dengan AWS Dukungan](#)
- [\[IAM.26\] Sertifikat SSL/TLS kedaluwarsa yang dikelola di IAM harus dihapus](#)
- [\[Inspektor.3\] Pemindaian kode Amazon Inspector Lambda harus diaktifkan](#)
- [\[IoT.1\] profil AWS IoT Device Defender keamanan harus ditandai](#)
- [\[IoT.2\] tindakan AWS IoT Core mitigasi harus ditandai](#)
- [AWS IoT Core Dimensi \[IoT.3\] harus ditandai](#)
- [\[IoT.4\] AWS IoT Core otorisasi harus diberi tag](#)
- [\[IoT.5\] alias AWS IoT Core peran harus ditandai](#)
- [AWS IoT Core Kebijakan \[IoT.6\] harus ditandai](#)
- [\[IoTEvents .1\] Input Peristiwa AWS IoT harus diberi tag](#)
- [\[IoTEvents .2\] Model detektor Acara AWS IoT harus diberi tag](#)
- [\[IoTEvents .3\] Model alarm AWS IoT Events harus diberi tag](#)
- [\[IoTSiteWise.1\] Model aset AWS IoT harus ditandai SiteWise](#)
- [\[IoTSiteWise.2\] Dasbor AWS IoT harus diberi tag SiteWise](#)
- [\[IoTSiteWise.3\] Gateway AWS IoT harus diberi tag SiteWise](#)
- [\[IoTSiteWise.4\] Portal AWS IoT harus diberi tag SiteWise](#)
- [\[IoTSiteWise.5\] Proyek AWS IoT harus diberi tag SiteWise](#)
- [\[IoT Twin Maker.1\] Pekerjaan sinkronisasi AWS IoT harus ditandai TwinMaker](#)
- [\[IoT Twin Maker.2\] Ruang kerja AWS IoT harus diberi tag TwinMaker](#)

- [\[Io TTwin Maker.3\] Adegan AWS IoT harus diberi tag TwinMaker](#)
- [\[Io TTwin Maker.4\] Entitas AWS IoT harus diberi tag TwinMaker](#)
- [\[Io TWireless .1\] Grup multicast Nirkabel AWS IoT harus diberi tag](#)
- [\[Io TWireless .2\] Profil layanan AWS IoT Wireless harus diberi tag](#)
- [\[Io TWireless .3\] Tugas AWS IoT FUOTA harus ditandai](#)
- [\[IVS.1\] Pasangan kunci pemutaran IVS harus ditandai](#)
- [\[IVS.2\] Konfigurasi perekaman IVS harus ditandai](#)
- [\[IVS.3\] Saluran IVS harus ditandai](#)
- [\[Keyspaces.1\] Ruang kunci Amazon Keyspaces harus diberi tag](#)
- [\[MSK.3\] Konektor MSK Connect harus dienkripsi saat transit](#)
- [\[RDS.1\] Snapshot RDS harus bersifat pribadi](#)
- [\[RDS.14\] Cluster Amazon Aurora seharusnya mengaktifkan backtracking](#)
- [\[RDS.31\] Grup keamanan RDS DB harus ditandai](#)
- [\[RedshiftServerless.1\] Grup kerja Amazon Redshift Tanpa Server harus menggunakan perutean VPC yang disempurnakan](#)
- [\[RedshiftServerless.2\] Koneksi ke grup kerja Redshift Serverless harus diperlukan untuk menggunakan SSL](#)
- [\[RedshiftServerless.3\] Kelompok kerja Redshift Tanpa Server harus melarang akses publik](#)
- [\[RedshiftServerless.4\] Ruang nama Redshift Tanpa Server harus dienkripsi dengan pengelolaan pelanggan AWS KMS keys](#)
- [\[RedshiftServerless.5\] Ruang nama Redshift Tanpa Server tidak boleh menggunakan nama pengguna admin default](#)
- [\[RedshiftServerless.6\] Ruang nama Redshift Tanpa Server harus mengeksport log ke Log CloudWatch](#)
- [\[RedshiftServerless.7\] Ruang nama Redshift Tanpa Server seharusnya tidak menggunakan nama database default](#)
- [\[Route53.1\] Pemeriksaan kesehatan rute 53 harus ditandai](#)
- [\[Route53.2\] Route 53 zona yang dihosting publik harus mencatat kueri DNS](#)
- [\[S3.24\] Poin Akses Multi-Wilayah S3 harus mengaktifkan pengaturan akses publik blok](#)
- [\[SSM.3\] EC2 Instans Amazon yang dikelola oleh Systems Manager harus memiliki status kepatuhan asosiasi COMPLIANT](#)
- [\[WAF.1\] Pencatatan ACL Web Global AWS WAF Klasik harus diaktifkan](#)

- [\[WAF.6\] Aturan global AWS WAF klasik harus memiliki setidaknya satu syarat](#)
- [\[WAF.7\] Kelompok aturan global AWS WAF klasik harus memiliki setidaknya satu aturan](#)
- [\[WAF.8\] Web global AWS WAF klasik ACLs harus memiliki setidaknya satu aturan atau kelompok aturan](#)

Asia Pasifik (Hong Kong)

Kontrol berikut tidak didukung di Wilayah Asia Pasifik (Hong Kong).

- [\[AppFlow.1\] AppFlow Aliran Amazon harus ditandai](#)
- [\[AppRunner.1\] Layanan App Runner harus diberi tag](#)
- [\[AppRunner.2\] Konektor VPC App Runner harus diberi tag](#)
- [\[AppSync.1\] Cache AWS AppSync API harus dienkripsi saat istirahat](#)
- [\[AppSync.6\] Cache AWS AppSync API harus dienkripsi saat transit](#)
- [\[CloudFront.1\] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi](#)
- [\[CloudFront.3\] CloudFront distribusi harus memerlukan enkripsi dalam perjalanan](#)
- [\[CloudFront.4\] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi](#)
- [\[CloudFront.5\] CloudFront distribusi seharusnya mengaktifkan logging](#)
- [\[CloudFront.6\] CloudFront distribusi harus mengaktifkan WAF](#)
- [\[CloudFront.7\] CloudFront distribusi harus menggunakan sertifikat SSL/TLS khusus](#)
- [\[CloudFront.8\] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS](#)
- [\[CloudFront.9\] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus](#)
- [\[CloudFront.10\] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal kustom](#)
- [\[CloudFront.12\] CloudFront distribusi seharusnya tidak menunjukkan asal S3 yang tidak ada](#)
- [\[CloudFront.13\] CloudFront distribusi harus menggunakan kontrol akses asal](#)
- [\[CloudFront.14\] CloudFront distribusi harus ditandai](#)
- [\[CodeArtifact.1\] CodeArtifact repositori harus ditandai](#)
- [\[CodeGuruProfiler.1\] Grup CodeGuru profil profiler harus diberi tag](#)
- [\[CodeGuruReviewer.1\] Asosiasi CodeGuru repositori peninjau harus diberi tag](#)
- [\[Cognito.1\] Kumpulan pengguna Cognito harus mengaktifkan perlindungan ancaman dengan mode penegakan fungsi penuh untuk otentikasi standar](#)

- [\[Connect.1\] Jenis objek Amazon Connect Customer Profiles harus diberi tag](#)
- [\[Connect.2\] Instans Amazon Connect seharusnya mengaktifkan logging CloudWatch](#)
- [\[DynamoDB.3\] Cluster DynamoDB Accelerator \(DAX\) harus dienkrpsi saat istirahat](#)
- [\[DynamoDB.7\] Cluster DynamoDB Accelerator harus dienkrpsi saat transit](#)
- [\[EC2.24\] Jenis instance EC2 paravirtual Amazon tidak boleh digunakan](#)
- [\[EC2.58\] VPCs harus dikonfigurasi dengan titik akhir antarmuka untuk Kontak Manajer Insiden Systems Manager](#)
- [\[EC2.60\] VPCs harus dikonfigurasi dengan titik akhir antarmuka untuk Systems Manager Incident Manager](#)
- [\[EC2.173\] Permintaan Armada EC2 Spot harus mengaktifkan enkripsi untuk volume EBS terlampir](#)
- [\[ECR.4\] Repositori publik ECR harus ditandai](#)
- [\[EventBridge.4\] titik akhir EventBridge global harus mengaktifkan replikasi acara](#)
- [\[FraudDetector.1\] Jenis entitas Amazon Fraud Detector harus diberi tag](#)
- [\[FraudDetector.2\] Label Amazon Fraud Detector harus diberi tag](#)
- [\[FraudDetector.3\] Hasil Amazon Fraud Detector harus ditandai](#)
- [\[FraudDetector.4\] Variabel Amazon Fraud Detector harus diberi tag](#)
- [\[GlobalAccelerator.1\] Akselerator Akselerator Global harus diberi tag](#)
- [\[IAM.26\] Sertifikat SSL/TLS kedaluwarsa yang dikelola di IAM harus dihapus](#)
- [\[Inspektor.3\] Pemindaian kode Amazon Inspector Lambda harus diaktifkan](#)
- [\[IoTEvents.1\] Input Peristiwa AWS IoT harus diberi tag](#)
- [\[IoTEvents.2\] Model detektor Acara AWS IoT harus diberi tag](#)
- [\[IoTEvents.3\] Model alarm AWS IoT Events harus diberi tag](#)
- [\[IoTSiteWise.1\] Model aset AWS IoT harus ditandai SiteWise](#)
- [\[IoTSiteWise.2\] Dasbor AWS IoT harus diberi tag SiteWise](#)
- [\[IoTSiteWise.3\] Gateway AWS IoT harus diberi tag SiteWise](#)
- [\[IoTSiteWise.4\] Portal AWS IoT harus diberi tag SiteWise](#)
- [\[IoTSiteWise.5\] Proyek AWS IoT harus diberi tag SiteWise](#)
- [\[IoTThingMaker.1\] Pekerjaan sinkronisasi AWS IoT harus ditandai ThingMaker](#)
- [\[IoTThingMaker.2\] Ruang kerja AWS IoT harus diberi tag ThingMaker](#)
- [\[IoTThingMaker.3\] Adegan AWS IoT harus diberi tag ThingMaker](#)
- [\[IoTThingMaker.4\] Entitas AWS IoT harus diberi tag ThingMaker](#)

- [\[Io TWireless .1\] Grup multicast Nirkabel AWS IoT harus diberi tag](#)
- [\[Io TWireless .2\] Profil layanan AWS IoT Wireless harus diberi tag](#)
- [\[Io TWireless .3\] Tugas AWS IoT FUOTA harus ditandai](#)
- [\[IVS.1\] Pasangan kunci pemutaran IVS harus ditandai](#)
- [\[IVS.2\] Konfigurasi perekaman IVS harus ditandai](#)
- [\[IVS.3\] Saluran IVS harus ditandai](#)
- [\[MSK.3\] Konektor MSK Connect harus dienkripsi saat transit](#)
- [\[RDS.14\] Cluster Amazon Aurora seharusnya mengaktifkan backtracking](#)
- [\[RDS.31\] Grup keamanan RDS DB harus ditandai](#)
- [\[RedshiftServerless.1\] Grup kerja Amazon Redshift Tanpa Server harus menggunakan perutean VPC yang disempurnakan](#)
- [\[RedshiftServerless.2\] Koneksi ke grup kerja Redshift Serverless harus diperlukan untuk menggunakan SSL](#)
- [\[Route53.1\] Pemeriksaan kesehatan rute 53 harus ditandai](#)
- [\[Route53.2\] Route 53 zona yang dihosting publik harus mencatat kueri DNS](#)
- [\[S3.24\] Poin Akses Multi-Wilayah S3 harus mengaktifkan pengaturan akses publik blok](#)
- [\[SES.1\] Daftar kontak SES harus ditandai](#)
- [\[SES.2\] Set konfigurasi SES harus ditandai](#)
- [\[WAF.1\] Pencatatan ACL Web Global AWS WAF Klasik harus diaktifkan](#)
- [\[WAF.6\] Aturan global AWS WAF klasik harus memiliki setidaknya satu syarat](#)
- [\[WAF.7\] Kelompok aturan global AWS WAF klasik harus memiliki setidaknya satu aturan](#)
- [\[WAF.8\] Web global AWS WAF klasik ACLs harus memiliki setidaknya satu aturan atau kelompok aturan](#)
- [\[WorkSpaces.1\] volume WorkSpaces pengguna harus dienkripsi saat istirahat](#)
- [\[WorkSpaces.2\] volume WorkSpaces root harus dienkripsi saat istirahat](#)

Asia Pasifik (Hyderabad)

Kontrol berikut tidak didukung di Wilayah Asia Pasifik (Hyderabad).

- [\[Akun.2\] Akun AWS harus menjadi bagian dari organisasi AWS Organizations](#)
- [\[APIGateway.8\] Rute API Gateway harus menentukan jenis otorisasi](#)

- [\[APIGateway.9\] Pencatatan akses harus dikonfigurasi untuk Tahap API Gateway V2](#)
- [\[Amplify.1\] Aplikasi Amplify harus diberi tag](#)
- [\[Amplify.2\] Amplify branch harus diberi tag](#)
- [\[AppConfig.1\] AWS AppConfig aplikasi harus diberi tag](#)
- [\[AppConfig.2\] profil AWS AppConfig konfigurasi harus ditandai](#)
- [\[AppConfig.3\] AWS AppConfig lingkungan harus ditandai](#)
- [\[AppFlow.1\] AppFlow Aliran Amazon harus ditandai](#)
- [\[AppRunner.1\] Layanan App Runner harus diberi tag](#)
- [\[AppRunner.2\] Konektor VPC App Runner harus diberi tag](#)
- [\[AppSync.1\] Cache AWS AppSync API harus dienkrpsi saat istirahat](#)
- [\[AppSync.6\] Cache AWS AppSync API harus dienkrpsi saat transit](#)
- [\[Backup.1\] titik AWS Backup pemulihan harus dienkrpsi saat istirahat](#)
- [\[Backup.4\] rencana AWS Backup laporan harus ditandai](#)
- [\[CloudFront.1\] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi](#)
- [\[CloudFront.3\] CloudFront distribusi harus memerlukan enkripsi dalam perjalanan](#)
- [\[CloudFront.4\] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi](#)
- [\[CloudFront.5\] CloudFront distribusi seharusnya mengaktifkan logging](#)
- [\[CloudFront.6\] CloudFront distribusi harus mengaktifkan WAF](#)
- [\[CloudFront.7\] CloudFront distribusi harus menggunakan sertifikat SSL/TLS khusus](#)
- [\[CloudFront.8\] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS](#)
- [\[CloudFront.9\] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus](#)
- [\[CloudFront.10\] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal kustom](#)
- [\[CloudFront.12\] CloudFront distribusi seharusnya tidak menunjukkan asal S3 yang tidak ada](#)
- [\[CloudFront.13\] CloudFront distribusi harus menggunakan kontrol akses asal](#)
- [\[CloudFront.14\] CloudFront distribusi harus ditandai](#)
- [\[CloudTrail.6\] Pastikan bucket S3 yang digunakan untuk menyimpan CloudTrail log tidak dapat diakses publik](#)
- [\[CloudTrail.7\] Pastikan pencatatan akses bucket S3 diaktifkan pada bucket CloudTrail S3](#)
- [\[CodeArtifact.1\] CodeArtifact repositori harus ditandai](#)
- [\[CodeGuruProfiler.1\] Grup CodeGuru profil profiler harus diberi tag](#)

- [\[CodeGuruReviewer.1\] Asosiasi CodeGuru repositori peninjau harus diberi tag](#)
- [\[Cognito.1\] Kumpulan pengguna Cognito harus mengaktifkan perlindungan ancaman dengan mode penegakan fungsi penuh untuk otentikasi standar](#)
- [\[Connect.1\] Jenis objek Amazon Connect Customer Profiles harus diberi tag](#)
- [\[Connect.2\] Instans Amazon Connect seharusnya mengaktifkan logging CloudWatch](#)
- [\[Detective.1\] Grafik perilaku detektif harus diberi tag](#)
- [\[DMS.2\] Sertifikat DMS harus ditandai](#)
- [\[DMS.3\] Langganan acara DMS harus ditandai](#)
- [\[DMS.4\] Contoh replikasi DMS harus ditandai](#)
- [\[DMS.5\] Grup subnet replikasi DMS harus ditandai](#)
- [\[DMS.6\] Instans replikasi DMS harus mengaktifkan peningkatan versi minor otomatis](#)
- [\[DMS.7\] Tugas replikasi DMS untuk database target seharusnya mengaktifkan logging](#)
- [\[DMS.8\] Tugas replikasi DMS untuk database sumber seharusnya mengaktifkan logging](#)
- [\[DMS.9\] Titik akhir DMS harus menggunakan SSL](#)
- [\[DMS.10\] Titik akhir DMS untuk database Neptune harus mengaktifkan otorisasi IAM](#)
- [\[DMS.11\] Titik akhir DMS untuk MongoDB harus mengaktifkan mekanisme otentikasi](#)
- [\[DMS.12\] Titik akhir DMS untuk Redis OSS seharusnya mengaktifkan TLS](#)
- [\[DynamoDB.3\] Cluster DynamoDB Accelerator \(DAX\) harus dienkripsi saat istirahat](#)
- [\[DynamoDB.4\] Tabel DynamoDB harus ada dalam rencana cadangan](#)
- [\[DynamoDB.7\] Cluster DynamoDB Accelerator harus dienkripsi saat transit](#)
- [\[EC2.14\] Grup keamanan seharusnya tidak mengizinkan masuknya dari 0.0.0.0/0 atau :/0 ke port 3389](#)
- [\[EC2.22\] Grup EC2 keamanan Amazon yang tidak digunakan harus dihapus](#)
- [\[EC2.24\] Jenis instance EC2 paravirtual Amazon tidak boleh digunakan](#)
- [\[EC2.25\] Templat EC2 peluncuran Amazon tidak boleh menetapkan publik IPs ke antarmuka jaringan](#)
- [\[EC2.28\] Volume EBS harus dicakup oleh rencana cadangan](#)
- [\[EC2.34\] tabel rute gateway EC2 transit harus ditandai](#)
- [\[EC2.40\] Gateway EC2 NAT harus ditandai](#)
- [\[EC2.48\] Log aliran VPC Amazon harus diberi tag](#)
- [\[EC2.51\] Titik akhir EC2 Client VPN harus mengaktifkan pencatatan koneksi klien](#)

- [\[EC2.58\] VPCs harus dikonfigurasi dengan titik akhir antarmuka untuk Kontak Manajer Insiden Systems Manager](#)
- [\[EC2.60\] VPCs harus dikonfigurasi dengan titik akhir antarmuka untuk Systems Manager Incident Manager](#)
- [\[EC2.170\] templat EC2 peluncuran harus menggunakan Layanan Metadata Instance Versi 2 \(\) IMDSv2](#)
- [\[EC2.173\] Permintaan Armada EC2 Spot harus mengaktifkan enkripsi untuk volume EBS terlampir](#)
- [\[EC2.175\] templat EC2 peluncuran harus diberi tag](#)
- [\[EC2.177\] Sesi cermin EC2 lalu lintas harus ditandai](#)
- [\[EC2.179\] Target cermin EC2 lalu lintas harus ditandai](#)
- [\[ECR.4\] Repositori publik ECR harus ditandai](#)
- [\[EFS.1\] Sistem File Elastis harus dikonfigurasi untuk mengenkripsi data file saat istirahat menggunakan AWS KMS](#)
- [\[EFS.2\] Volume Amazon EFS harus dalam rencana cadangan](#)
- [\[ELB.14\] Classic Load Balancer harus dikonfigurasi dengan mode mitigasi desync defensif atau paling ketat](#)
- [\[ELB.17\] Aplikasi dan Penyeimbang Beban Jaringan dengan pendengar harus menggunakan kebijakan keamanan yang direkomendasikan](#)
- [\[ElastiCache.1\] Cluster ElastiCache \(Redis OSS\) harus mengaktifkan pencadangan otomatis](#)
- [\[ElastiCache.6\] ElastiCache \(Redis OSS\) grup replikasi dari versi sebelumnya harus mengaktifkan Redis OSS AUTH](#)
- [\[ElastiCache.7\] ElastiCache cluster tidak boleh menggunakan grup subnet default](#)
- [\[ElasticBeanstalk.1\] Lingkungan Elastic Beanstalk seharusnya mengaktifkan pelaporan kesehatan yang ditingkatkan](#)
- [\[ElasticBeanstalk.2\] Pembaruan platform yang dikelola Elastic Beanstalk harus diaktifkan](#)
- [\[ElasticBeanstalk.3\] Elastic Beanstalk harus mengalirkan log ke CloudWatch](#)
- [\[EMR.1\] Node primer kluster EMR Amazon seharusnya tidak memiliki alamat IP publik](#)
- [\[ES.4\] Kesalahan domain Elasticsearch yang masuk ke CloudWatch Log harus diaktifkan](#)
- [\[EventBridge.4\] titik akhir EventBridge global harus mengaktifkan replikasi acara](#)
- [\[FraudDetector.1\] Jenis entitas Amazon Fraud Detector harus diberi tag](#)
- [\[FraudDetector.2\] Label Amazon Fraud Detector harus diberi tag](#)
- [\[FraudDetector.3\] Hasil Amazon Fraud Detector harus ditandai](#)

- [\[FraudDetector.4\] Variabel Amazon Fraud Detector harus diberi tag](#)
- [\[GlobalAccelerator.1\] Akselerator Akselerator Global harus diberi tag](#)
- [\[Glue.4\] Pekerjaan AWS Glue percikan harus berjalan pada versi yang didukung AWS Glue](#)
- [\[GuardDuty.2\] GuardDuty filter harus diberi tag](#)
- [\[IAM.1\] Kebijakan IAM seharusnya tidak mengizinkan hak administratif “*” penuh](#)
- [\[IAM.2\] Pengguna IAM seharusnya tidak memiliki kebijakan IAM yang dilampirkan](#)
- [\[IAM.3\] Kunci akses pengguna IAM harus diputar setiap 90 hari atau kurang](#)
- [\[IAM.5\] MFA harus diaktifkan untuk semua pengguna IAM yang memiliki kata sandi konsol](#)
- [\[IAM.8\] Kredensi pengguna IAM yang tidak digunakan harus dihapus](#)
- [\[IAM.18\] Memastikan peran dukungan telah dibuat untuk mengelola insiden dengan AWS Dukungan](#)
- [\[IAM.19\] MFA harus diaktifkan untuk semua pengguna IAM](#)
- [\[IAM.21\] Kebijakan terkelola pelanggan IAM yang Anda buat seharusnya tidak mengizinkan tindakan wildcard untuk layanan](#)
- [\[IAM.22\] Kredensi pengguna IAM yang tidak digunakan selama 45 hari harus dihapus](#)
- [\[IAM.24\] Peran IAM harus ditandai](#)
- [\[IAM.25\] Pengguna IAM harus diberi tag](#)
- [\[IAM.26\] Sertifikat SSL/TLS kedaluwarsa yang dikelola di IAM harus dihapus](#)
- [\[IAM.27\] Identitas IAM seharusnya tidak memiliki kebijakan yang dilampirkan AWSCloudShellFullAccess](#)
- [\[Inspektor.1\] Pemindaian Amazon Inspector harus diaktifkan EC2](#)
- [\[Inspektor.2\] Pemindaian ECR Amazon Inspector harus diaktifkan](#)
- [\[Inspektor.3\] Pemindaian kode Amazon Inspector Lambda harus diaktifkan](#)
- [\[Inspektor.4\] Pemindaian standar Amazon Inspector Lambda harus diaktifkan](#)
- [\[IoT.1\] profil AWS IoT Device Defender keamanan harus ditandai](#)
- [\[IoT.2\] tindakan AWS IoT Core mitigasi harus ditandai](#)
- [AWS IoT Core Dimensi \[IoT.3\] harus ditandai](#)
- [\[IoT.4\] AWS IoT Core otorisasi harus diberi tag](#)
- [\[IoT.5\] alias AWS IoT Core peran harus ditandai](#)
- [AWS IoT Core Kebijakan \[IoT.6\] harus ditandai](#)
- [\[IoTEvents.1\] Input Peristiwa AWS IoT harus diberi tag](#)

- [\[Io TEvents .2\] Model detektor Acara AWS IoT harus diberi tag](#)
- [\[Io TEvents .3\] Model alarm AWS IoT Events harus diberi tag](#)
- [\[Io TSite Wise.1\] Model aset AWS IoT harus ditandai SiteWise](#)
- [\[Io TSite Wise.2\] Dasbor AWS IoT harus diberi tag SiteWise](#)
- [\[Io TSite Wise.3\] Gateway AWS IoT harus diberi tag SiteWise](#)
- [\[Io TSite Wise.4\] Portal AWS IoT harus diberi tag SiteWise](#)
- [\[Io TSite Wise.5\] Proyek AWS IoT harus diberi tag SiteWise](#)
- [\[Io TTwin Maker.1\] Pekerjaan sinkronisasi AWS IoT harus ditandai TwinMaker](#)
- [\[Io TTwin Maker.2\] Ruang kerja AWS IoT harus diberi tag TwinMaker](#)
- [\[Io TTwin Maker.3\] Adegan AWS IoT harus diberi tag TwinMaker](#)
- [\[Io TTwin Maker.4\] Entitas AWS IoT harus diberi tag TwinMaker](#)
- [\[Io TWireless .1\] Grup multicast Nirkabel AWS IoT harus diberi tag](#)
- [\[Io TWireless .2\] Profil layanan AWS IoT Wireless harus diberi tag](#)
- [\[Io TWireless .3\] Tugas AWS IoT FUOTA harus ditandai](#)
- [\[IVS.1\] Pasangan kunci pemutaran IVS harus ditandai](#)
- [\[IVS.2\] Konfigurasi perekaman IVS harus ditandai](#)
- [\[IVS.3\] Saluran IVS harus ditandai](#)
- [\[Keyspaces.1\] Ruang kunci Amazon Keyspaces harus diberi tag](#)
- [\[KMS.1\] Kebijakan yang dikelola pelanggan IAM tidak boleh mengizinkan tindakan dekripsi pada semua kunci KMS](#)
- [\[KMS.2\] Prinsipal IAM tidak boleh memiliki kebijakan inline IAM yang memungkinkan tindakan dekripsi pada semua kunci KMS](#)
- [\[Macie.1\] Amazon Macie harus diaktifkan](#)
- [\[Macie.2\] Penemuan data sensitif otomatis Macie harus diaktifkan](#)
- [\[MQ.2\] Broker ActiveMQ harus mengalirkan log audit ke CloudWatch](#)
- [\[MQ.3\] Broker Amazon MQ harus mengaktifkan peningkatan versi minor otomatis](#)
- [\[MQ.4\] Broker Amazon MQ harus diberi tag](#)
- [\[MQ.5\] Broker ActiveMQ harus menggunakan mode penerapan aktif/siaga](#)
- [\[MQ.6\] Broker RabbitMQ harus menggunakan mode penerapan cluster](#)
- [\[MSK.3\] Konektor MSK Connect harus dienkrpsi saat transit](#)
- [\[Neptunus.1\] Cluster DB Neptunus harus dienkrpsi saat istirahat](#)

- [\[Neptune.2\] Cluster DB Neptune harus menerbitkan log audit ke Log CloudWatch](#)
- [\[Neptune.3\] Snapshot cluster Neptune DB seharusnya tidak publik](#)
- [\[Neptune.4\] Cluster DB Neptune harus mengaktifkan perlindungan penghapusan](#)
- [\[Neptune.5\] Cluster DB Neptune harus mengaktifkan cadangan otomatis](#)
- [\[Neptune.6\] Snapshot cluster Neptune DB harus dienkripsi saat istirahat](#)
- [\[Neptune.7\] Cluster DB Neptune harus mengaktifkan otentikasi basis data IAM](#)
- [\[Neptune.8\] Cluster DB Neptune harus dikonfigurasi untuk menyalin tag ke snapshot](#)
- [\[Neptune.9\] Cluster DB Neptune harus digunakan di beberapa Availability Zone](#)
- [\[OpenSearch.1\] OpenSearch domain harus mengaktifkan enkripsi saat istirahat](#)
- [\[OpenSearch.2\] OpenSearch domain tidak boleh diakses publik](#)
- [\[OpenSearch.3\] OpenSearch domain harus mengenkripsi data yang dikirim antar node](#)
- [\[OpenSearch.4\] login kesalahan OpenSearch domain ke Log harus diaktifkan CloudWatch](#)
- [\[OpenSearch.5\] OpenSearch domain harus mengaktifkan pencatatan audit](#)
- [\[OpenSearch.6\] OpenSearch domain harus memiliki setidaknya tiga node data](#)
- [\[OpenSearch.7\] OpenSearch domain harus mengaktifkan kontrol akses berbutir halus](#)
- [\[OpenSearch.8\] Koneksi ke OpenSearch domain harus dienkripsi menggunakan kebijakan keamanan TLS terbaru](#)
- [\[OpenSearch.9\] domain harus ditandai OpenSearch](#)
- [\[OpenSearch.10\] OpenSearch domain harus menginstal pembaruan perangkat lunak terbaru](#)
- [\[OpenSearch.11\] OpenSearch domain harus memiliki setidaknya tiga node primer khusus](#)
- [\[RDS.14\] Cluster Amazon Aurora seharusnya mengaktifkan backtracking](#)
- [\[RDS.15\] Cluster RDS DB harus dikonfigurasi untuk beberapa Availability Zone](#)
- [\[RDS.26\] Instans RDS DB harus dilindungi oleh rencana cadangan](#)
- [\[RDS.31\] Grup keamanan RDS DB harus ditandai](#)
- [\[RDS.35\] Cluster RDS DB harus mengaktifkan peningkatan versi minor otomatis](#)
- [\[RDS.37\] Cluster Aurora PostgreSQL DB harus menerbitkan log ke Log CloudWatch](#)
- [\[Redshift.10\] Cluster Redshift harus dienkripsi saat istirahat](#)
- [\[RedshiftServerless.1\] Grup kerja Amazon Redshift Tanpa Server harus menggunakan perutean VPC yang disempurnakan](#)
- [\[RedshiftServerless.2\] Koneksi ke grup kerja Redshift Serverless harus diperlukan untuk menggunakan SSL](#)

- [\[RedshiftServerless.3\] Kelompok kerja Redshift Tanpa Server harus melarang akses publik](#)
- [\[RedshiftServerless.4\] Ruang nama Redshift Tanpa Server harus dienkripsi dengan pengelolaan pelanggan AWS KMS keys](#)
- [\[RedshiftServerless.5\] Ruang nama Redshift Tanpa Server tidak boleh menggunakan nama pengguna admin default](#)
- [\[RedshiftServerless.6\] Ruang nama Redshift Tanpa Server harus mengeksport log ke Log CloudWatch](#)
- [\[RedshiftServerless.7\] Ruang nama Redshift Tanpa Server seharusnya tidak menggunakan nama database default](#)
- [\[Route53.1\] Pemeriksaan kesehatan rute 53 harus ditandai](#)
- [\[Route53.2\] Route 53 zona yang dihosting publik harus mencatat kueri DNS](#)
- [\[S3.6\] Kebijakan bucket tujuan umum S3 harus membatasi akses ke yang lain Akun AWS](#)
- [\[S3.24\] Poin Akses Multi-Wilayah S3 harus mengaktifkan pengaturan akses publik blok](#)
- [\[SageMaker.1\] Instans SageMaker notebook Amazon seharusnya tidak memiliki akses internet langsung](#)
- [\[SageMaker.2\] instance SageMaker notebook harus diluncurkan dalam VPC khusus](#)
- [\[SageMaker.3\] Pengguna seharusnya tidak memiliki akses root ke instance SageMaker notebook](#)
- [\[SageMaker.5\] SageMaker model harus memblokir lalu lintas masuk](#)
- [\[SageMaker.6\] konfigurasi gambar SageMaker aplikasi harus ditandai](#)
- [\[SageMaker.7\] SageMaker gambar harus diberi tag](#)
- [\[SES.1\] Daftar kontak SES harus ditandai](#)
- [\[SES.2\] Set konfigurasi SES harus ditandai](#)
- [\[SQS.1\] Antrian Amazon SQS harus dienkripsi saat istirahat](#)
- [\[SQS.2\] Antrian SQS harus ditandai](#)
- [\[SQS.3\] Kebijakan akses antrian SQS seharusnya tidak mengizinkan akses publik](#)
- [\[SSM.3\] EC2 Instans Amazon yang dikelola oleh Systems Manager harus memiliki status kepatuhan asosiasi COMPLIANT](#)
- [\[Transfer.3\] Konektor Transfer Family seharusnya mengaktifkan logging](#)
- [\[Transfer.4\] Perjanjian Transfer Family harus ditandai](#)
- [\[WAF.1\] Pencatatan ACL Web Global AWS WAF Klasik harus diaktifkan](#)
- [\[WAF.3\] Kelompok aturan Regional AWS WAF Klasik harus memiliki setidaknya satu aturan](#)

- [\[WAF.6\] Aturan global AWS WAF klasik harus memiliki setidaknya satu syarat](#)
- [\[WAF.7\] Kelompok aturan global AWS WAF klasik harus memiliki setidaknya satu aturan](#)
- [\[WAF.8\] Web global AWS WAF klasik ACLs harus memiliki setidaknya satu aturan atau kelompok aturan](#)
- [\[WAF.10\] AWS WAF web ACLs harus memiliki setidaknya satu aturan atau kelompok aturan](#)
- [\[WAF.11\] pencatatan ACL AWS WAF web harus diaktifkan](#)
- [\[WorkSpaces.1\] volume WorkSpaces pengguna harus dienkrpsi saat istirahat](#)
- [\[WorkSpaces.2\] volume WorkSpaces root harus dienkrpsi saat istirahat](#)

Asia Pasifik (Jakarta)

Kontrol berikut tidak didukung di Wilayah Asia Pasifik (Jakarta).

- [\[Akun.2\] Akun AWS harus menjadi bagian dari organisasi AWS Organizations](#)
- [\[APIGateway.8\] Rute API Gateway harus menentukan jenis otorisasi](#)
- [\[APIGateway.9\] Pencatatan akses harus dikonfigurasi untuk Tahap API Gateway V2](#)
- [\[Amplify.1\] Aplikasi Amplify harus diberi tag](#)
- [\[Amplify.2\] Amplify branch harus diberi tag](#)
- [\[AppFlow.1\] AppFlow Aliran Amazon harus ditandai](#)
- [\[AppRunner.1\] Layanan App Runner harus diberi tag](#)
- [\[AppRunner.2\] Konektor VPC App Runner harus diberi tag](#)
- [\[AppSync.1\] Cache AWS AppSync API harus dienkrpsi saat istirahat](#)
- [\[AppSync.6\] Cache AWS AppSync API harus dienkrpsi saat transit](#)
- [\[Backup.1\] titik AWS Backup pemulihan harus dienkrpsi saat istirahat](#)
- [\[Backup.4\] rencana AWS Backup laporan harus ditandai](#)
- [\[CloudFront.1\] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi](#)
- [\[CloudFront.3\] CloudFront distribusi harus memerlukan enkripsi dalam perjalanan](#)
- [\[CloudFront.4\] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi](#)
- [\[CloudFront.5\] CloudFront distribusi seharusnya mengaktifkan logging](#)
- [\[CloudFront.6\] CloudFront distribusi harus mengaktifkan WAF](#)
- [\[CloudFront.7\] CloudFront distribusi harus menggunakan sertifikat SSL/TLS khusus](#)

- [\[CloudFront.8\] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS](#)
- [\[CloudFront.9\] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus](#)
- [\[CloudFront.10\] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal kustom](#)
- [\[CloudFront.12\] CloudFront distribusi seharusnya tidak menunjukkan asal S3 yang tidak ada](#)
- [\[CloudFront.13\] CloudFront distribusi harus menggunakan kontrol akses asal](#)
- [\[CloudFront.14\] CloudFront distribusi harus ditandai](#)
- [\[CodeArtifact.1\] CodeArtifact repositori harus ditandai](#)
- [\[CodeBuild.1\] Repositori sumber CodeBuild Bitbucket tidak URLs boleh berisi kredensial sensitif](#)
- [\[CodeBuild.2\] variabel lingkungan CodeBuild proyek tidak boleh berisi kredensial teks yang jelas](#)
- [\[CodeBuild.3\] Log CodeBuild S3 harus dienkripsi](#)
- [\[CodeBuild.4\] lingkungan CodeBuild proyek harus memiliki urasi logging AWS Config](#)
- [\[CodeGuruProfiler.1\] Grup CodeGuru profil profiler harus diberi tag](#)
- [\[CodeGuruReviewer.1\] Asosiasi CodeGuru repositori peninjau harus diberi tag](#)
- [\[Cognito.1\] Kumpulan pengguna Cognito harus mengaktifkan perlindungan ancaman dengan mode penegakan fungsi penuh untuk otentikasi standar](#)
- [\[Connect.1\] Jenis objek Amazon Connect Customer Profiles harus diberi tag](#)
- [\[Connect.2\] Instans Amazon Connect seharusnya mengaktifkan logging CloudWatch](#)
- [\[Detective.1\] Grafik perilaku detektif harus diberi tag](#)
- [\[DMS.2\] Sertifikat DMS harus ditandai](#)
- [\[DMS.3\] Langganan acara DMS harus ditandai](#)
- [\[DMS.4\] Contoh replikasi DMS harus ditandai](#)
- [\[DMS.5\] Grup subnet replikasi DMS harus ditandai](#)
- [\[DMS.6\] Instans replikasi DMS harus mengaktifkan peningkatan versi minor otomatis](#)
- [\[DMS.7\] Tugas replikasi DMS untuk database target seharusnya mengaktifkan logging](#)
- [\[DMS.8\] Tugas replikasi DMS untuk database sumber seharusnya mengaktifkan logging](#)
- [\[DMS.9\] Titik akhir DMS harus menggunakan SSL](#)
- [\[DMS.10\] Titik akhir DMS untuk database Neptune harus mengaktifkan otorisasi IAM](#)
- [\[DMS.11\] Titik akhir DMS untuk MongoDB harus mengaktifkan mekanisme otentikasi](#)
- [\[DMS.12\] Titik akhir DMS untuk Redis OSS seharusnya mengaktifkan TLS](#)
- [\[DocumentDB.1\] Cluster Amazon DocumentDB harus dienkripsi saat istirahat](#)

- [\[DocumentDB.2\] Cluster Amazon DocumentDB harus memiliki periode retensi cadangan yang memadai](#)
- [\[DocumentDB.3\] Cuplikan cluster manual Amazon DocumentDB seharusnya tidak bersifat publik](#)
- [\[DocumentDB.4\] Cluster Amazon DocumentDB harus mempublikasikan log audit ke Log CloudWatch](#)
- [\[DocumentDB.5\] Cluster Amazon DocumentDB harus mengaktifkan perlindungan penghapusan](#)
- [\[DocumentDB.6\] Cluster Amazon DocumentDB harus dienkripsi saat transit](#)
- [\[DynamoDB.3\] Cluster DynamoDB Accelerator \(DAX\) harus dienkripsi saat istirahat](#)
- [\[DynamoDB.4\] Tabel DynamoDB harus ada dalam rencana cadangan](#)
- [\[DynamoDB.7\] Cluster DynamoDB Accelerator harus dienkripsi saat transit](#)
- [\[EC2.14\] Grup keamanan seharusnya tidak mengizinkan masuknya dari 0.0.0.0/0 atau :/0 ke port 3389](#)
- [\[EC2.22\] Grup EC2 keamanan Amazon yang tidak digunakan harus dihapus](#)
- [\[EC2.24\] Jenis instance EC2 paravirtual Amazon tidak boleh digunakan](#)
- [\[EC2.28\] Volume EBS harus dicakup oleh rencana cadangan](#)
- [\[EC2.51\] Titik akhir EC2 Client VPN harus mengaktifkan pencatatan koneksi klien](#)
- [\[EC2.58\] VPCs harus dikonfigurasi dengan titik akhir antarmuka untuk Kontak Manajer Insiden Systems Manager](#)
- [\[EC2.60\] VPCs harus dikonfigurasi dengan titik akhir antarmuka untuk Systems Manager Incident Manager](#)
- [\[EC2.173\] Permintaan Armada EC2 Spot harus mengaktifkan enkripsi untuk volume EBS terlampir](#)
- [\[EC2.177\] Sesi cermin EC2 lalu lintas harus ditandai](#)
- [\[EC2.179\] Target cermin EC2 lalu lintas harus ditandai](#)
- [\[ECR.4\] Repositori publik ECR harus ditandai](#)
- [\[EFS.1\] Sistem File Elastis harus dikonfigurasi untuk mengenkripsi data file saat istirahat menggunakan AWS KMS](#)
- [\[EFS.2\] Volume Amazon EFS harus dalam rencana cadangan](#)
- [\[ELB.17\] Aplikasi dan Penyeimbang Beban Jaringan dengan pendengar harus menggunakan kebijakan keamanan yang direkomendasikan](#)
- [\[ElastiCache.1\] Cluster ElastiCache \(Redis OSS\) harus mengaktifkan pencadangan otomatis](#)
- [\[ElastiCache.6\] ElastiCache \(Redis OSS\) grup replikasi dari versi sebelumnya harus mengaktifkan Redis OSS AUTH](#)

- [\[ElastiCache.7\]](#) ElastiCache cluster tidak boleh menggunakan grup subnet default
- [\[ElasticBeanstalk.1\]](#) Lingkungan Elastic Beanstalk seharusnya mengaktifkan pelaporan kesehatan yang ditingkatkan
- [\[ElasticBeanstalk.2\]](#) Pembaruan platform yang dikelola Elastic Beanstalk harus diaktifkan
- [\[EventBridge.4\]](#) titik akhir EventBridge global harus mengaktifkan replikasi acara
- [\[FraudDetector.1\]](#) Jenis entitas Amazon Fraud Detector harus diberi tag
- [\[FraudDetector.2\]](#) Label Amazon Fraud Detector harus diberi tag
- [\[FraudDetector.3\]](#) Hasil Amazon Fraud Detector harus ditandai
- [\[FraudDetector.4\]](#) Variabel Amazon Fraud Detector harus diberi tag
- [\[GlobalAccelerator.1\]](#) Akselerator Akselerator Global harus diberi tag
- [\[GuardDuty.2\]](#) GuardDuty filter harus diberi tag
- [\[IAM.18\]](#) Memastikan peran dukungan telah dibuat untuk mengelola insiden dengan AWS Dukungan
- [\[IAM.26\]](#) Sertifikat SSL/TLS kedaluwarsa yang dikelola di IAM harus dihapus
- [\[Inspektor.3\]](#) Pemindaian kode Amazon Inspector Lambda harus diaktifkan
- [\[IoT.1\]](#) profil AWS IoT Device Defender keamanan harus ditandai
- [\[IoT.2\]](#) tindakan AWS IoT Core mitigasi harus ditandai
- [AWS IoT Core Dimensi \[IoT.3\]](#) harus ditandai
- [\[IoT.4\]](#) AWS IoT Core otorisasi harus diberi tag
- [\[IoT.5\]](#) alias AWS IoT Core peran harus ditandai
- [AWS IoT Core Kebijakan \[IoT.6\]](#) harus ditandai
- [\[IoTEvents .1\]](#) Input Peristiwa AWS IoT harus diberi tag
- [\[IoTEvents .2\]](#) Model detektor Acara AWS IoT harus diberi tag
- [\[IoTEvents .3\]](#) Model alarm AWS IoT Events harus diberi tag
- [\[IoTSiteWise.1\]](#) Model aset AWS IoT harus ditandai SiteWise
- [\[IoTSiteWise.2\]](#) Dasbor AWS IoT harus diberi tag SiteWise
- [\[IoTSiteWise.3\]](#) Gateway AWS IoT harus diberi tag SiteWise
- [\[IoTSiteWise.4\]](#) Portal AWS IoT harus diberi tag SiteWise
- [\[IoTSiteWise.5\]](#) Proyek AWS IoT harus diberi tag SiteWise
- [\[IoTThingMaker.1\]](#) Pekerjaan sinkronisasi AWS IoT harus ditandai TwinMaker
- [\[IoTThingMaker.2\]](#) Ruang kerja AWS IoT harus diberi tag TwinMaker

- [\[Io TTwin Maker.3\] Adegan AWS IoT harus diberi tag TwinMaker](#)
- [\[Io TTwin Maker.4\] Entitas AWS IoT harus diberi tag TwinMaker](#)
- [\[Io TWireless .1\] Grup multicast Nirkabel AWS IoT harus diberi tag](#)
- [\[Io TWireless .2\] Profil layanan AWS IoT Wireless harus diberi tag](#)
- [\[Io TWireless .3\] Tugas AWS IoT FUOTA harus ditandai](#)
- [\[IVS.1\] Pasangan kunci pemutaran IVS harus ditandai](#)
- [\[IVS.2\] Konfigurasi perekaman IVS harus ditandai](#)
- [\[IVS.3\] Saluran IVS harus ditandai](#)
- [\[Keyspaces.1\] Ruang kunci Amazon Keyspaces harus diberi tag](#)
- [\[Macie.1\] Amazon Macie harus diaktifkan](#)
- [\[Macie.2\] Penemuan data sensitif otomatis Macie harus diaktifkan](#)
- [\[MSK.3\] Konektor MSK Connect harus dienkripsi saat transit](#)
- [\[Neptunus.1\] Cluster DB Neptunus harus dienkripsi saat istirahat](#)
- [\[Neptune.2\] Cluster DB Neptunus harus menerbitkan log audit ke Log CloudWatch](#)
- [\[Neptune.3\] Snapshot cluster Neptunus DB seharusnya tidak publik](#)
- [\[Neptunus.4\] Cluster DB Neptunus harus mengaktifkan perlindungan penghapusan](#)
- [\[Neptunus.5\] Cluster DB Neptunus harus mengaktifkan cadangan otomatis](#)
- [\[Neptune.6\] Snapshot cluster Neptunus DB harus dienkripsi saat istirahat](#)
- [\[Neptune.7\] Cluster DB Neptunus harus mengaktifkan otentikasi basis data IAM](#)
- [\[Neptunus.8\] Cluster DB Neptunus harus dikonfigurasi untuk menyalin tag ke snapshot](#)
- [\[Neptunus.9\] Cluster DB Neptunus harus digunakan di beberapa Availability Zone](#)
- [\[Opensearch.5\] OpenSearch domain harus mengaktifkan pencatatan audit](#)
- [\[Opensearch.6\] OpenSearch domain harus memiliki setidaknya tiga node data](#)
- [\[RDS.14\] Cluster Amazon Aurora seharusnya mengaktifkan backtracking](#)
- [\[RDS.26\] Instans RDS DB harus dilindungi oleh rencana cadangan](#)
- [\[RDS.31\] Grup keamanan RDS DB harus ditandai](#)
- [\[RedshiftServerless.1\] Grup kerja Amazon Redshift Tanpa Server harus menggunakan perutean VPC yang disempurnakan](#)
- [\[RedshiftServerless.2\] Koneksi ke grup kerja Redshift Serverless harus diperlukan untuk menggunakan SSL](#)
- [\[Route53.1\] Pemeriksaan kesehatan rute 53 harus ditandai](#)

- [\[Route53.2\] Route 53 zona yang dihosting publik harus mencatat kueri DNS](#)
- [\[S3.11\] Bucket tujuan umum S3 harus mengaktifkan pemberitahuan acara](#)
- [\[S3.24\] Poin Akses Multi-Wilayah S3 harus mengaktifkan pengaturan akses publik blok](#)
- [\[ServiceCatalog.1\] Portofolio Service Catalog harus dibagikan hanya dalam suatu organisasi AWS](#)
- [\[SQS.1\] Antrian Amazon SQS harus dienkripsi saat istirahat](#)
- [\[SQS.2\] Antrian SQS harus ditandai](#)
- [\[SQS.3\] Kebijakan akses antrian SQS seharusnya tidak mengizinkan akses publik](#)
- [\[SSM.3\] EC2 Instans Amazon yang dikelola oleh Systems Manager harus memiliki status kepatuhan asosiasi COMPLIANT](#)
- [\[WAF.1\] Pencatatan ACL Web Global AWS WAF Klasik harus diaktifkan](#)
- [\[WAF.3\] Kelompok aturan Regional AWS WAF Klasik harus memiliki setidaknya satu aturan](#)
- [\[WAF.6\] Aturan global AWS WAF klasik harus memiliki setidaknya satu syarat](#)
- [\[WAF.7\] Kelompok aturan global AWS WAF klasik harus memiliki setidaknya satu aturan](#)
- [\[WAF.8\] Web global AWS WAF klasik ACLs harus memiliki setidaknya satu aturan atau kelompok aturan](#)
- [\[WAF.10\] AWS WAF web ACLs harus memiliki setidaknya satu aturan atau kelompok aturan](#)
- [\[WorkSpaces.1\] volume WorkSpaces pengguna harus dienkripsi saat istirahat](#)
- [\[WorkSpaces.2\] volume WorkSpaces root harus dienkripsi saat istirahat](#)

Asia Pasifik (Malaysia)

Kontrol berikut tidak didukung di Wilayah Asia Pasifik (Malaysia).

- [\[ACM.1\] Sertifikat yang diimpor dan diterbitkan ACM harus diperbarui setelah jangka waktu tertentu](#)
- [\[ACM.2\] Sertifikat RSA yang dikelola oleh ACM harus menggunakan panjang kunci minimal 2.048 bit](#)
- [\[Akun.1\] Informasi kontak keamanan harus disediakan untuk Akun AWS](#)
- [\[Akun.2\] Akun AWS harus menjadi bagian dari organisasi AWS Organizations](#)
- [\[APIGateway.8\] Rute API Gateway harus menentukan jenis otorisasi](#)
- [\[APIGateway.9\] Pencatatan akses harus dikonfigurasi untuk Tahap API Gateway V2](#)
- [\[Amplify.1\] Aplikasi Amplify harus diberi tag](#)
- [\[Amplify.2\] Amplify branch harus diberi tag](#)

- [\[AppConfig.1\] AWS AppConfig aplikasi harus diberi tag](#)
- [\[AppConfig.2\] profil AWS AppConfig konfigurasi harus ditandai](#)
- [\[AppConfig.3\] AWS AppConfig lingkungan harus ditandai](#)
- [\[AppConfig.4\] asosiasi AWS AppConfig ekstensi harus ditandai](#)
- [\[AppFlow.1\] AppFlow Aliran Amazon harus ditandai](#)
- [\[AppRunner.1\] Layanan App Runner harus diberi tag](#)
- [\[AppRunner.2\] Konektor VPC App Runner harus diberi tag](#)
- [\[AppSync.1\] Cache AWS AppSync API harus dienkripsi saat istirahat](#)
- [\[AppSync.2\] AWS AppSync harus mengaktifkan logging tingkat lapangan](#)
- [\[AppSync.4\] AWS AppSync APIs GraphQL harus diberi tag](#)
- [\[AppSync.5\] AWS AppSync APIs GraphQL tidak boleh diautentikasi dengan kunci API](#)
- [\[AppSync.6\] Cache AWS AppSync API harus dienkripsi saat transit](#)
- [\[Athena.2\] Katalog data Athena harus ditandai](#)
- [\[Athena.3\] Kelompok kerja Athena harus ditandai](#)
- [\[Athena.4\] Kelompok kerja Athena seharusnya mengaktifkan logging](#)
- [\[AutoScaling.2\] Grup EC2 Auto Scaling Amazon harus mencakup beberapa Availability Zone](#)
- [\[AutoScaling.3\] Konfigurasi peluncuran grup Auto Scaling harus EC2 mengonfigurasi instance agar memerlukan Layanan Metadata Instance Versi 2 \(\) IMDSv2](#)
- [\[AutoScaling.6\] Grup Auto Scaling harus menggunakan beberapa jenis instance di beberapa Availability Zone](#)
- [\[AutoScaling.9\] Grup EC2 Auto Scaling Amazon harus menggunakan templat peluncuran Amazon EC2](#)
- [\[Backup.1\] titik AWS Backup pemulihan harus dienkripsi saat istirahat](#)
- [\[Backup.2\] poin AWS Backup pemulihan harus ditandai](#)
- [\[Backup.3\] AWS Backup brankas harus ditandai](#)
- [\[Backup.4\] rencana AWS Backup laporan harus ditandai](#)
- [\[Backup.5\] rencana AWS Backup cadangan harus ditandai](#)
- [\[Batch.1\] Antrian pekerjaan batch harus ditandai](#)
- [\[Batch.2\] Kebijakan penjadwalan batch harus ditandai](#)
- [\[Batch.3\] Lingkungan komputasi Batch harus ditandai](#)
- [\[Batch.4\] Properti sumber daya komputasi di lingkungan komputasi Batch terkelola harus ditandai](#)

- [\[CloudFormation.2\] CloudFormation tumpukan harus ditandai](#)
- [\[CloudFront.1\] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi](#)
- [\[CloudFront.3\] CloudFront distribusi harus memerlukan enkripsi dalam perjalanan](#)
- [\[CloudFront.4\] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi](#)
- [\[CloudFront.5\] CloudFront distribusi seharusnya mengaktifkan logging](#)
- [\[CloudFront.6\] CloudFront distribusi harus mengaktifkan WAF](#)
- [\[CloudFront.7\] CloudFront distribusi harus menggunakan sertifikat SSL/TLS khusus](#)
- [\[CloudFront.8\] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS](#)
- [\[CloudFront.9\] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus](#)
- [\[CloudFront.10\] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal kustom](#)
- [\[CloudFront.12\] CloudFront distribusi seharusnya tidak menunjukkan asal S3 yang tidak ada](#)
- [\[CloudFront.13\] CloudFront distribusi harus menggunakan kontrol akses asal](#)
- [\[CloudFront.14\] CloudFront distribusi harus ditandai](#)
- [\[CloudTrail.6\] Pastikan bucket S3 yang digunakan untuk menyimpan CloudTrail log tidak dapat diakses publik](#)
- [\[CloudTrail.7\] Pastikan pencatatan akses bucket S3 diaktifkan pada bucket CloudTrail S3](#)
- [\[CloudTrail.10\] Penyimpanan data acara CloudTrail harus dienkripsi dengan pelanggan yang dikelola AWS KMS keys](#)
- [\[CloudWatch.17\] tindakan CloudWatch alarm harus diaktifkan](#)
- [\[CodeArtifact.1\] CodeArtifact repositori harus ditandai](#)
- [\[CodeBuild.1\] Repositori sumber CodeBuild Bitbucket tidak URLs boleh berisi kredensial sensitif](#)
- [\[CodeBuild.2\] variabel lingkungan CodeBuild proyek tidak boleh berisi kredensial teks yang jelas](#)
- [\[CodeBuild.3\] Log CodeBuild S3 harus dienkripsi](#)
- [\[CodeBuild.4\] lingkungan CodeBuild proyek harus memiliki urasi logging AWS Config](#)
- [\[CodeBuild.7\] ekspor kelompok CodeBuild laporan harus dienkripsi saat istirahat](#)
- [\[CodeGuruProfiler.1\] Grup CodeGuru profil profiler harus diberi tag](#)
- [\[CodeGuruReviewer.1\] Asosiasi CodeGuru repositori peninjau harus diberi tag](#)
- [\[Cognito.1\] Kumpulan pengguna Cognito harus mengaktifkan perlindungan ancaman dengan mode penegakan fungsi penuh untuk otentikasi standar](#)
- [\[Connect.1\] Jenis objek Amazon Connect Customer Profiles harus diberi tag](#)

- [\[Connect.2\] Instans Amazon Connect seharusnya mengaktifkan logging CloudWatch](#)
- [\[DataFirehose.1\] Aliran pengiriman Firehose harus dienkripsi saat istirahat](#)
- [\[DataSync.1\] DataSync tugas harus mengaktifkan logging](#)
- [\[DataSync.2\] DataSync tugas harus ditandai](#)
- [\[Detective.1\] Grafik perilaku detektif harus diberi tag](#)
- [\[DMS.2\] Sertifikat DMS harus ditandai](#)
- [\[DMS.3\] Langganan acara DMS harus ditandai](#)
- [\[DMS.4\] Contoh replikasi DMS harus ditandai](#)
- [\[DMS.5\] Grup subnet replikasi DMS harus ditandai](#)
- [\[DMS.6\] Instans replikasi DMS harus mengaktifkan peningkatan versi minor otomatis](#)
- [\[DMS.7\] Tugas replikasi DMS untuk database target seharusnya mengaktifkan logging](#)
- [\[DMS.8\] Tugas replikasi DMS untuk database sumber seharusnya mengaktifkan logging](#)
- [\[DMS.9\] Titik akhir DMS harus menggunakan SSL](#)
- [\[DMS.10\] Titik akhir DMS untuk database Neptunus harus mengaktifkan otorisasi IAM](#)
- [\[DMS.11\] Titik akhir DMS untuk MongoDB harus mengaktifkan mekanisme otentikasi](#)
- [\[DMS.12\] Titik akhir DMS untuk Redis OSS seharusnya mengaktifkan TLS](#)
- [\[DocumentDB.1\] Cluster Amazon DocumentDB harus dienkripsi saat istirahat](#)
- [\[DocumentDB.2\] Cluster Amazon DocumentDB harus memiliki periode retensi cadangan yang memadai](#)
- [\[DocumentDB.3\] Cuplikan cluster manual Amazon DocumentDB seharusnya tidak bersifat publik](#)
- [\[DocumentDB.4\] Cluster Amazon DocumentDB harus mempublikasikan log audit ke Log CloudWatch](#)
- [\[DocumentDB.5\] Cluster Amazon DocumentDB harus mengaktifkan perlindungan penghapusan](#)
- [\[DocumentDB.6\] Cluster Amazon DocumentDB harus dienkripsi saat transit](#)
- [\[DynamoDB.3\] Cluster DynamoDB Accelerator \(DAX\) harus dienkripsi saat istirahat](#)
- [\[DynamoDB.4\] Tabel DynamoDB harus ada dalam rencana cadangan](#)
- [\[DynamoDB.6\] Tabel DynamoDB harus mengaktifkan perlindungan penghapusan](#)
- [\[DynamoDB.7\] Cluster DynamoDB Accelerator harus dienkripsi saat transit](#)
- [\[EC2.4\] EC2 Instans yang dihentikan harus dihapus setelah periode waktu tertentu](#)
- [\[EC2.21\] Jaringan ACLs seharusnya tidak mengizinkan masuknya dari 0.0.0.0/0 ke port 22 atau port 3389.](#)

- [\[EC2.22\] Grup EC2 keamanan Amazon yang tidak digunakan harus dihapus](#)
- [\[EC2.23\] Amazon EC2 Transit Gateways seharusnya tidak secara otomatis menerima permintaan lampiran VPC](#)
- [\[EC2.24\] Jenis instance EC2 paravirtual Amazon tidak boleh digunakan](#)
- [\[EC2.25\] Templat EC2 peluncuran Amazon tidak boleh menetapkan publik IPs ke antarmuka jaringan](#)
- [\[EC2.28\] Volume EBS harus dicakup oleh rencana cadangan](#)
- [\[EC2.33\] lampiran gateway EC2 transit harus ditandai](#)
- [\[EC2.34\] tabel rute gateway EC2 transit harus ditandai](#)
- [\[EC2.40\] Gateway EC2 NAT harus ditandai](#)
- [\[EC2.48\] Log aliran VPC Amazon harus diberi tag](#)
- [\[EC2.51\] Titik akhir EC2 Client VPN harus mengaktifkan pencatatan koneksi klien](#)
- [\[EC2.52\] gateway EC2 transit harus ditandai](#)
- [\[EC2.53\] grup EC2 keamanan seharusnya tidak mengizinkan masuknya dari 0.0.0.0/0 ke port administrasi server jarak jauh](#)
- [\[EC2.54\] grup EC2 keamanan tidak boleh mengizinkan masuknya dari :/0 ke port administrasi server jarak jauh](#)
- [\[EC2.55\] VPCs harus dikonfigurasi dengan titik akhir antarmuka untuk ECR API](#)
- [\[EC2.56\] VPCs harus dikonfigurasi dengan titik akhir antarmuka untuk Docker Registry](#)
- [\[EC2.57\] VPCs harus dikonfigurasi dengan titik akhir antarmuka untuk Systems Manager](#)
- [\[EC2.58\] VPCs harus dikonfigurasi dengan titik akhir antarmuka untuk Kontak Manajer Insiden Systems Manager](#)
- [\[EC2.60\] VPCs harus dikonfigurasi dengan titik akhir antarmuka untuk Systems Manager Incident Manager](#)
- [\[EC2.170\] templat EC2 peluncuran harus menggunakan Layanan Metadata Instance Versi 2 \(\) IMDSv2](#)
- [\[EC2.171\] Koneksi EC2 VPN seharusnya mengaktifkan logging](#)
- [\[EC2.173\] Permintaan Armada EC2 Spot harus mengaktifkan enkripsi untuk volume EBS terlampir](#)
- [\[EC2.174\] Set opsi EC2 DHCP harus ditandai](#)
- [\[EC2.175\] templat EC2 peluncuran harus diberi tag](#)
- [\[EC2.176\] daftar EC2 awalan harus ditandai](#)
- [\[EC2.177\] Sesi cermin EC2 lalu lintas harus ditandai](#)

- [\[EC2.178\] Filter cermin EC2 lalu lintas harus ditandai](#)
- [\[EC2.179\] Target cermin EC2 lalu lintas harus ditandai](#)
- [\[ECR.1\] Repositori pribadi ECR harus memiliki pemindaian gambar yang dikonfigurasi](#)
- [\[ECR.2\] Repositori pribadi ECR harus memiliki kekekalan tag yang dikonfigurasi](#)
- [\[ECR.3\] Repositori ECR harus memiliki setidaknya satu kebijakan siklus hidup yang dikonfigurasi](#)
- [\[ECR.4\] Repositori publik ECR harus ditandai](#)
- [\[ECR.5\] Repositori ECR harus dienkripsi dengan pelanggan yang dikelola AWS KMS keys](#)
- [\[ECS.3\] Definisi tugas ECS tidak boleh membagikan namespace proses host](#)
- [\[ECS.4\] Kontainer ECS harus berjalan sebagai non-hak istimewa](#)
- [\[ECS.5\] Wadah ECS harus dibatasi pada akses hanya-baca ke sistem file root](#)
- [\[ECS.8\] Rahasia tidak boleh diteruskan sebagai variabel lingkungan kontainer](#)
- [\[ECS.9\] Definisi tugas ECS harus memiliki konfigurasi logging](#)
- [\[ECS.10\] Layanan ECS Fargate harus berjalan pada versi platform Fargate terbaru](#)
- [\[ECS.12\] Cluster ECS harus menggunakan Wawasan Kontainer](#)
- [\[ECS.16\] Set tugas ECS seharusnya tidak secara otomatis menetapkan alamat IP publik](#)
- [\[ECS.17\] Definisi tugas ECS tidak boleh menggunakan mode jaringan host](#)
- [\[EFS.1\] Sistem File Elastis harus dikonfigurasi untuk mengenkripsi data file saat istirahat menggunakan AWS KMS](#)
- [\[EFS.2\] Volume Amazon EFS harus dalam rencana cadangan](#)
- [\[EFS.3\] Titik akses EFS harus menegakkan direktori root](#)
- [\[EFS.4\] Titik akses EFS harus menegakkan identitas pengguna](#)
- [\[EFS.5\] Titik akses EFS harus ditandai](#)
- [\[EFS.6\] Target pemasangan EFS tidak boleh dikaitkan dengan subnet publik](#)
- [\[EFS.7\] Sistem file EFS harus mengaktifkan pencadangan otomatis](#)
- [\[EFS.8\] Sistem file EFS harus dienkripsi saat istirahat](#)
- [\[EKS.2\] Kluster EKS harus berjalan pada versi Kubernetes yang didukung](#)
- [\[EKS.3\] Kluster EKS harus menggunakan rahasia Kubernetes terenkripsi](#)
- [\[EKS.6\] Kluster EKS harus ditandai](#)
- [\[EKS.7\] Konfigurasi penyedia identitas EKS harus ditandai](#)
- [\[EKS.8\] Kluster EKS harus mengaktifkan pencatatan audit](#)

- [\[ELB.10\] Classic Load Balancer harus menjangkau beberapa Availability Zone](#)
- [\[ELB.12\] Application Load Balancer harus dikonfigurasi dengan mode mitigasi desync defensif atau paling ketat](#)
- [\[ELB.13\] Penyeimbang Beban Aplikasi, Jaringan, dan Gateway harus mencakup beberapa Availability Zone](#)
- [\[ELB.14\] Classic Load Balancer harus dikonfigurasi dengan mode mitigasi desync defensif atau paling ketat](#)
- [\[ELB.17\] Aplikasi dan Penyeimbang Beban Jaringan dengan pendengar harus menggunakan kebijakan keamanan yang direkomendasikan](#)
- [\[ElastiCache.1\] Cluster ElastiCache \(Redis OSS\) harus mengaktifkan pencadangan otomatis](#)
- [\[ElastiCache.2\] ElastiCache cluster harus mengaktifkan peningkatan versi minor otomatis](#)
- [\[ElastiCache.3\] grup ElastiCache replikasi harus mengaktifkan failover otomatis](#)
- [\[ElastiCache.4\] grup ElastiCache replikasi harus dienkripsi saat istirahat](#)
- [\[ElastiCache.5\] grup ElastiCache replikasi harus dienkripsi saat transit](#)
- [\[ElastiCache.6\] ElastiCache \(Redis OSS\) grup replikasi dari versi sebelumnya harus mengaktifkan Redis OSS AUTH](#)
- [\[ElastiCache.7\] ElastiCache cluster tidak boleh menggunakan grup subnet default](#)
- [\[ElasticBeanstalk.1\] Lingkungan Elastic Beanstalk seharusnya mengaktifkan pelaporan kesehatan yang ditingkatkan](#)
- [\[ElasticBeanstalk.2\] Pembaruan platform yang dikelola Elastic Beanstalk harus diaktifkan](#)
- [\[ElasticBeanstalk.3\] Elastic Beanstalk harus mengalirkan log ke CloudWatch](#)
- [\[EMR.1\] Node primer kluster EMR Amazon seharusnya tidak memiliki alamat IP publik](#)
- [\[EMR.2\] Pengaturan akses publik blok EMR Amazon harus diaktifkan](#)
- [\[EMR.3\] Konfigurasi keamanan Amazon EMR harus dienkripsi saat istirahat](#)
- [\[EMR.4\] Konfigurasi keamanan Amazon EMR harus dienkripsi saat transit](#)
- [\[ES.4\] Kesalahan domain Elasticsearch yang masuk ke CloudWatch Log harus diaktifkan](#)
- [\[ES.9\] Domain Elasticsearch harus diberi tag](#)
- [\[EventBridge.2\] bus EventBridge acara harus diberi tag](#)
- [\[EventBridge.3\] bus acara EventBridge khusus harus memiliki kebijakan berbasis sumber daya terlampir](#)
- [\[EventBridge.4\] titik akhir EventBridge global harus mengaktifkan replikasi acara](#)
- [\[FraudDetector.1\] Jenis entitas Amazon Fraud Detector harus diberi tag](#)

- [\[FraudDetector.2\] Label Amazon Fraud Detector harus diberi tag](#)
- [\[FraudDetector.3\] Hasil Amazon Fraud Detector harus ditandai](#)
- [\[FraudDetector.4\] Variabel Amazon Fraud Detector harus diberi tag](#)
- [\[FSx.1\] FSx untuk sistem file OpenZFS harus dikonfigurasi untuk menyalin tag ke cadangan dan volume](#)
- [\[FSx.2\] FSx untuk sistem file Lustre harus dikonfigurasi untuk menyalin tag ke cadangan](#)
- [\[FSx.3\] FSx untuk sistem file OpenZFS harus dikonfigurasi untuk penyebaran Multi-AZ](#)
- [\[FSx.4\] FSx untuk sistem file NetApp ONTAP harus dikonfigurasi untuk penyebaran Multi-AZ](#)
- [\[FSx.5\] FSx untuk sistem file Windows File Server harus dikonfigurasi untuk penyebaran Multi-AZ](#)
- [\[GlobalAccelerator.1\] Akselerator Global harus diberi tag](#)
- [AWS Glue Pekerjaan \[Glue.1\] harus ditandai](#)
- [\[Glue.3\] transformasi pembelajaran AWS Glue mesin harus dienkripsi saat istirahat](#)
- [\[Glue.4\] Pekerjaan AWS Glue percikan harus berjalan pada versi yang didukung AWS Glue](#)
- [\[GuardDuty.2\] GuardDuty filter harus diberi tag](#)
- [\[GuardDuty.3\] GuardDuty IPSets harus ditandai](#)
- [\[GuardDuty.4\] GuardDuty detektor harus diberi tag](#)
- [\[GuardDuty.5\] Pemantauan Log Audit GuardDuty EKS harus diaktifkan](#)
- [\[GuardDuty.6\] Perlindungan GuardDuty Lambda harus diaktifkan](#)
- [\[GuardDuty.7\] GuardDuty EKS Runtime Monitoring harus diaktifkan](#)
- [\[GuardDuty.8\] Perlindungan GuardDuty Malware untuk EC2 harus diaktifkan](#)
- [\[GuardDuty.9\] Perlindungan GuardDuty RDS harus diaktifkan](#)
- [\[GuardDuty.10\] Perlindungan GuardDuty S3 harus diaktifkan](#)
- [\[GuardDuty.11\] GuardDuty Runtime Monitoring harus diaktifkan](#)
- [\[GuardDuty.12\] GuardDuty ECS Runtime Monitoring harus diaktifkan](#)
- [\[GuardDuty.13\] GuardDuty EC2 Runtime Monitoring harus diaktifkan](#)
- [\[IAM.1\] Kebijakan IAM seharusnya tidak mengizinkan hak administratif “*” penuh](#)
- [\[IAM.2\] Pengguna IAM seharusnya tidak memiliki kebijakan IAM yang dilampirkan](#)
- [\[IAM.3\] Kunci akses pengguna IAM harus diputar setiap 90 hari atau kurang](#)
- [\[IAM.4\] Kunci akses pengguna root IAM seharusnya tidak ada](#)
- [\[IAM.5\] MFA harus diaktifkan untuk semua pengguna IAM yang memiliki kata sandi konsol](#)
- [\[IAM.6\] MFA perangkat keras harus diaktifkan untuk pengguna root](#)

- [\[IAM.7\] Kebijakan kata sandi untuk pengguna IAM harus memiliki konfigurasi yang kuat](#)
- [\[IAM.8\] Kredensi pengguna IAM yang tidak digunakan harus dihapus](#)
- [\[IAM.9\] MFA harus diaktifkan untuk pengguna root](#)
- [\[IAM.10\] Kebijakan kata sandi untuk pengguna IAM harus memiliki konfigurasi yang kuat](#)
- [\[IAM.11\] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu huruf besar](#)
- [\[IAM.12\] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu huruf kecil](#)
- [\[IAM.13\] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu simbol](#)
- [\[IAM.14\] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu nomor](#)
- [\[IAM.15\] Pastikan kebijakan kata sandi IAM membutuhkan panjang kata sandi minimum 14 atau lebih](#)
- [\[IAM.16\] Pastikan kebijakan kata sandi IAM mencegah penggunaan kembali kata sandi](#)
- [\[IAM.17\] Pastikan kebijakan kata sandi IAM kedaluwarsa kata sandi dalam waktu 90 hari atau kurang](#)
- [\[IAM.18\] Memastikan peran dukungan telah dibuat untuk mengelola insiden dengan AWS Dukungan](#)
- [\[IAM.19\] MFA harus diaktifkan untuk semua pengguna IAM](#)
- [\[IAM.21\] Kebijakan terkelola pelanggan IAM yang Anda buat seharusnya tidak mengizinkan tindakan wildcard untuk layanan](#)
- [\[IAM.22\] Kredensi pengguna IAM yang tidak digunakan selama 45 hari harus dihapus](#)
- [\[IAM.23\] Penganalisis Akses IAM harus ditandai](#)
- [\[IAM.24\] Peran IAM harus ditandai](#)
- [\[IAM.25\] Pengguna IAM harus diberi tag](#)
- [\[IAM.26\] Sertifikat SSL/TLS kedaluwarsa yang dikelola di IAM harus dihapus](#)
- [\[IAM.27\] Identitas IAM seharusnya tidak memiliki kebijakan yang dilampirkan AWSCloudShellFullAccess](#)
- [\[IAM.28\] IAM Access Analyzer penganalisis akses eksternal harus diaktifkan](#)
- [\[Inspektor.1\] Pemindaian Amazon Inspector harus diaktifkan EC2](#)
- [\[Inspektor.2\] Pemindaian ECR Amazon Inspector harus diaktifkan](#)
- [\[Inspektor.3\] Pemindaian kode Amazon Inspector Lambda harus diaktifkan](#)
- [\[Inspektor.4\] Pemindaian standar Amazon Inspector Lambda harus diaktifkan](#)
- [\[IoT.1\] profil AWS IoT Device Defender keamanan harus ditandai](#)

- [\[IoT.2\] tindakan AWS IoT Core mitigasi harus ditandai](#)
- [AWS IoT Core Dimensi \[IoT.3\] harus ditandai](#)
- [\[IoT.4\] AWS IoT Core otorisasi harus diberi tag](#)
- [\[IoT.5\] alias AWS IoT Core peran harus ditandai](#)
- [AWS IoT Core Kebijakan \[IoT.6\] harus ditandai](#)
- [\[IoT TEEvents .1\] Input Peristiwa AWS IoT harus diberi tag](#)
- [\[IoT TEEvents .2\] Model detektor Acara AWS IoT harus diberi tag](#)
- [\[IoT TEEvents .3\] Model alarm AWS IoT Events harus diberi tag](#)
- [\[IoT TSite Wise.1\] Model aset AWS IoT harus ditandai SiteWise](#)
- [\[IoT TSite Wise.2\] Dasbor AWS IoT harus diberi tag SiteWise](#)
- [\[IoT TSite Wise.3\] Gateway AWS IoT harus diberi tag SiteWise](#)
- [\[IoT TSite Wise.4\] Portal AWS IoT harus diberi tag SiteWise](#)
- [\[IoT TSite Wise.5\] Proyek AWS IoT harus diberi tag SiteWise](#)
- [\[IoT TTwin Maker.1\] Pekerjaan sinkronisasi AWS IoT harus ditandai TwinMaker](#)
- [\[IoT TTwin Maker.2\] Ruang kerja AWS IoT harus diberi tag TwinMaker](#)
- [\[IoT TTwin Maker.3\] Adegan AWS IoT harus diberi tag TwinMaker](#)
- [\[IoT TTwin Maker.4\] Entitas AWS IoT harus diberi tag TwinMaker](#)
- [\[IoT TWireless .1\] Grup multicast Nirkabel AWS IoT harus diberi tag](#)
- [\[IoT TWireless .2\] Profil layanan AWS IoT Wireless harus diberi tag](#)
- [\[IoT TWireless .3\] Tugas AWS IoT FUOTA harus ditandai](#)
- [\[IVS.1\] Pasangan kunci pemutaran IVS harus ditandai](#)
- [\[IVS.2\] Konfigurasi perekaman IVS harus ditandai](#)
- [\[IVS.3\] Saluran IVS harus ditandai](#)
- [\[Keyspaces.1\] Ruang kunci Amazon Keyspaces harus diberi tag](#)
- [\[Kinesis.1\] Aliran kinesis harus dienkripsi saat istirahat](#)
- [\[Kinesis.2\] Aliran kinesis harus ditandai](#)
- [\[Kinesis.3\] Aliran kinesis harus memiliki periode retensi data yang memadai](#)
- [\[KMS.1\] Kebijakan yang dikelola pelanggan IAM tidak boleh mengizinkan tindakan dekripsi pada semua kunci KMS](#)
- [\[KMS.2\] Prinsipal IAM tidak boleh memiliki kebijakan inline IAM yang memungkinkan tindakan dekripsi pada semua kunci KMS](#)

- [\[KMS.5\] Kunci KMS tidak boleh diakses publik](#)
- [\[Lambda.5\] Fungsi VPC Lambda harus beroperasi di beberapa Availability Zone](#)
- [\[Macie.1\] Amazon Macie harus diaktifkan](#)
- [\[Macie.2\] Penemuan data sensitif otomatis Macie harus diaktifkan](#)
- [\[MQ.2\] Broker ActiveMQ harus mengalirkan log audit ke CloudWatch](#)
- [\[MQ.3\] Broker Amazon MQ harus mengaktifkan peningkatan versi minor otomatis](#)
- [\[MQ.4\] Broker Amazon MQ harus diberi tag](#)
- [\[MQ.5\] Broker ActiveMQ harus menggunakan mode penerapan aktif/siaga](#)
- [\[MQ.6\] Broker RabbitMQ harus menggunakan mode penerapan cluster](#)
- [\[MSK.1\] Kluster MSK harus dienkripsi saat transit di antara node broker](#)
- [\[MSK.2\] Kluster MSK seharusnya telah meningkatkan pemantauan yang dikonfigurasi](#)
- [\[MSK.3\] Konektor MSK Connect harus dienkripsi saat transit](#)
- [\[Neptunus.1\] Cluster DB Neptunus harus dienkripsi saat istirahat](#)
- [\[Neptune.2\] Cluster DB Neptune harus menerbitkan log audit ke Log CloudWatch](#)
- [\[Neptune.3\] Snapshot cluster Neptune DB seharusnya tidak publik](#)
- [\[Neptunus.4\] Cluster DB Neptunus harus mengaktifkan perlindungan penghapusan](#)
- [\[Neptunus.5\] Cluster DB Neptunus harus mengaktifkan cadangan otomatis](#)
- [\[Neptune.6\] Snapshot cluster Neptune DB harus dienkripsi saat istirahat](#)
- [\[Neptune.7\] Cluster DB Neptune harus mengaktifkan otentikasi basis data IAM](#)
- [\[Neptunus.8\] Cluster DB Neptunus harus dikonfigurasi untuk menyalin tag ke snapshot](#)
- [\[Neptunus.9\] Cluster DB Neptunus harus digunakan di beberapa Availability Zone](#)
- [\[NetworkFirewall.1\] Firewall Jaringan harus digunakan di beberapa Availability Zone](#)
- [\[NetworkFirewall.2\] Pencatatan Firewall Jaringan harus diaktifkan](#)
- [\[NetworkFirewall.3\] Kebijakan Network Firewall harus memiliki setidaknya satu kelompok aturan yang terkait](#)
- [\[NetworkFirewall.4\] Tindakan stateless default untuk kebijakan Network Firewall harus drop atau forward untuk paket penuh](#)
- [\[NetworkFirewall.5\] Tindakan stateless default untuk kebijakan Network Firewall harus drop atau forward untuk paket yang terfragmentasi](#)
- [\[NetworkFirewall.6\] Grup aturan Stateless Network Firewall tidak boleh kosong](#)
- [\[NetworkFirewall.9\] Firewall Jaringan harus mengaktifkan perlindungan penghapusan](#)

- [\[NetworkFirewall.10\] Firewall Jaringan harus mengaktifkan perlindungan perubahan subnet](#)
- [\[Opensearch.1\] OpenSearch domain harus mengaktifkan enkripsi saat istirahat](#)
- [\[Opensearch.2\] OpenSearch domain tidak boleh diakses publik](#)
- [\[Opensearch.3\] OpenSearch domain harus mengenkripsi data yang dikirim antar node](#)
- [\[Opensearch.4\] login kesalahan OpenSearch domain ke Log harus diaktifkan CloudWatch](#)
- [\[Opensearch.5\] OpenSearch domain harus mengaktifkan pencatatan audit](#)
- [\[Opensearch.6\] OpenSearch domain harus memiliki setidaknya tiga node data](#)
- [\[Opensearch.7\] OpenSearch domain harus mengaktifkan kontrol akses berbutir halus](#)
- [\[Opensearch.8\] Koneksi ke OpenSearch domain harus dienkripsi menggunakan kebijakan keamanan TLS terbaru](#)
- [\[Opensearch.9\] domain harus ditandai OpenSearch](#)
- [\[Opensearch.10\] OpenSearch domain harus menginstal pembaruan perangkat lunak terbaru](#)
- [\[Opensearch.11\] OpenSearch domain harus memiliki setidaknya tiga node primer khusus](#)
- [\[PCA.1\] otoritas sertifikat AWS Private CA root harus dinonaktifkan](#)
- [\[PCA.2\] Otoritas sertifikat CA AWS swasta harus ditandai](#)
- [\[RDS.14\] Cluster Amazon Aurora seharusnya mengaktifkan backtracking](#)
- [\[RDS.18\] Instans RDS harus digunakan di VPC](#)
- [\[RDS.24\] Kluster Database RDS harus menggunakan nama pengguna administrator khusus](#)
- [\[RDS.25\] Instans database RDS harus menggunakan nama pengguna administrator khusus](#)
- [\[RDS.26\] Instans RDS DB harus dilindungi oleh rencana cadangan](#)
- [\[RDS.27\] Cluster RDS DB harus dienkripsi saat istirahat](#)
- [\[RDS.31\] Grup keamanan RDS DB harus ditandai](#)
- [\[RDS.34\] Kluster Aurora MySQL DB harus menerbitkan log audit ke Log CloudWatch](#)
- [\[RDS.35\] Cluster RDS DB harus mengaktifkan peningkatan versi minor otomatis](#)
- [\[RDS.36\] RDS untuk instance PostgreSQL DB harus menerbitkan log ke Log CloudWatch](#)
- [\[RDS.37\] Cluster Aurora PostgreSQL DB harus menerbitkan log ke Log CloudWatch](#)
- [\[RDS.38\] RDS untuk instance PostgreSQL DB harus dienkripsi saat transit](#)
- [\[RDS.39\] RDS untuk instance MySQL DB harus dienkripsi saat transit](#)
- [\[RDS.40\] RDS untuk instance SQL Server DB harus menerbitkan log ke Log CloudWatch](#)
- [\[RDS.41\] RDS untuk instance SQL Server DB harus dienkripsi saat transit](#)

- [\[RDS.42\] RDS untuk instance MariaDB DB harus menerbitkan log ke Log CloudWatch](#)
- [\[RDS.44\] RDS untuk instance MariaDB DB harus dienkripsi saat transit](#)
- [\[Redshift.1\] Cluster Amazon Redshift harus melarang akses publik](#)
- [\[Redshift.2\] Koneksi ke cluster Amazon Redshift harus dienkripsi saat transit](#)
- [\[Redshift.3\] Cluster Amazon Redshift harus mengaktifkan snapshot otomatis](#)
- [\[Redshift.4\] Cluster Amazon Redshift harus mengaktifkan pencatatan audit](#)
- [\[Redshift.6\] Amazon Redshift harus mengaktifkan peningkatan otomatis ke versi utama](#)
- [\[Redshift.7\] Cluster Redshift harus menggunakan perutean VPC yang ditingkatkan](#)
- [\[Redshift.8\] Cluster Amazon Redshift tidak boleh menggunakan nama pengguna Admin default](#)
- [\[Redshift.9\] Cluster Redshift tidak boleh menggunakan nama database default](#)
- [\[Redshift.10\] Cluster Redshift harus dienkripsi saat istirahat](#)
- [\[Redshift.11\] Cluster Redshift harus ditandai](#)
- [\[Redshift.13\] Snapshot cluster Redshift harus ditandai](#)
- [\[Redshift.15\] Grup keamanan Redshift harus mengizinkan masuknya port cluster hanya dari asal yang dibatasi](#)
- [\[Redshift.16\] Grup subnet cluster Redshift harus memiliki subnet dari beberapa Availability Zone](#)
- [\[Redshift.17\] Grup parameter cluster Redshift harus ditandai](#)
- [\[RedshiftServerless.1\] Grup kerja Amazon Redshift Tanpa Server harus menggunakan perutean VPC yang disempurnakan](#)
- [\[RedshiftServerless.2\] Koneksi ke grup kerja Redshift Serverless harus diperlukan untuk menggunakan SSL](#)
- [\[RedshiftServerless.3\] Kelompok kerja Redshift Tanpa Server harus melarang akses publik](#)
- [\[RedshiftServerless.4\] Ruang nama Redshift Tanpa Server harus dienkripsi dengan pengelolaan pelanggan AWS KMS keys](#)
- [\[RedshiftServerless.5\] Ruang nama Redshift Tanpa Server tidak boleh menggunakan nama pengguna admin default](#)
- [\[RedshiftServerless.6\] Ruang nama Redshift Tanpa Server harus mengeksport log ke Log CloudWatch](#)
- [\[RedshiftServerless.7\] Ruang nama Redshift Tanpa Server seharusnya tidak menggunakan nama database default](#)
- [\[Route53.1\] Pemeriksaan kesehatan rute 53 harus ditandai](#)
- [\[Route53.2\] Route 53 zona yang dihosting publik harus mencatat kueri DNS](#)

- [\[S3.7\] Ember tujuan umum S3 harus menggunakan replikasi lintas wilayah](#)
- [\[S3.10\] Bucket tujuan umum S3 dengan versi diaktifkan harus memiliki konfigurasi Siklus Hidup](#)
- [\[S3.11\] Bucket tujuan umum S3 harus mengaktifkan pemberitahuan acara](#)
- [\[S3.12\] tidak ACLs boleh digunakan untuk mengelola akses pengguna ke bucket tujuan umum S3](#)
- [\[S3.13\] Bucket tujuan umum S3 harus memiliki konfigurasi Siklus Hidup](#)
- [\[S3.19\] Titik akses S3 harus mengaktifkan pengaturan akses publik blok](#)
- [\[S3.20\] Bucket tujuan umum S3 harus mengaktifkan penghapusan MFA](#)
- [\[S3.22\] Bucket tujuan umum S3 harus mencatat peristiwa penulisan tingkat objek](#)
- [\[S3.23\] Bucket tujuan umum S3 harus mencatat peristiwa pembacaan tingkat objek](#)
- [\[S3.24\] Poin Akses Multi-Wilayah S3 harus mengaktifkan pengaturan akses publik blok](#)
- [\[SageMaker.1\] Instans SageMaker notebook Amazon seharusnya tidak memiliki akses internet langsung](#)
- [\[SageMaker.2\] instance SageMaker notebook harus diluncurkan dalam VPC khusus](#)
- [\[SageMaker.3\] Pengguna seharusnya tidak memiliki akses root ke instance SageMaker notebook](#)
- [\[SageMaker.4\] varian produksi SageMaker titik akhir harus memiliki jumlah instance awal yang lebih besar dari 1](#)
- [\[SageMaker.5\] SageMaker model harus memblokir lalu lintas masuk](#)
- [\[SageMaker.6\] konfigurasi gambar SageMaker aplikasi harus ditandai](#)
- [\[SageMaker.7\] SageMaker gambar harus diberi tag](#)
- [\[SageMaker.8\] instance SageMaker notebook harus berjalan pada platform yang didukung](#)
- [\[SES.1\] Daftar kontak SES harus ditandai](#)
- [\[SES.2\] Set konfigurasi SES harus ditandai](#)
- [\[ServiceCatalog.1\] Portofolio Service Catalog harus dibagikan hanya dalam suatu organisasi AWS](#)
- [\[SNS.4\] Kebijakan akses topik SNS seharusnya tidak mengizinkan akses publik](#)
- [\[SQS.1\] Antrian Amazon SQS harus dienkripsi saat istirahat](#)
- [\[SQS.2\] Antrian SQS harus ditandai](#)
- [\[SQS.3\] Kebijakan akses antrian SQS seharusnya tidak mengizinkan akses publik](#)
- [\[SSM.3\] EC2 Instans Amazon yang dikelola oleh Systems Manager harus memiliki status kepatuhan asosiasi COMPLIANT](#)
- [\[SSM.4\] Dokumen SSM seharusnya tidak bersifat publik](#)
- [\[SSM.5\] Dokumen SSM harus ditandai](#)

- [\[StepFunctions.1\] Mesin status Step Functions seharusnya mengaktifkan logging](#)
- [\[StepFunctions.2\] Aktivitas Step Functions harus diberi tag](#)
- [\[Transfer.1\] AWS Transfer Family alur kerja harus ditandai](#)
- [\[Transfer.2\] Server Transfer Family tidak boleh menggunakan protokol FTP untuk koneksi titik akhir](#)
- [\[Transfer.3\] Konektor Transfer Family seharusnya mengaktifkan logging](#)
- [\[Transfer.4\] Perjanjian Transfer Family harus ditandai](#)
- [\[Transfer.5\] Sertifikat Transfer Family harus diberi tag](#)
- [\[Transfer.6\] Konektor Transfer Family harus diberi tag](#)
- [\[Transfer.7\] Profil Transfer Family harus diberi tag](#)
- [\[WAF.1\] Pencatatan ACL Web Global AWS WAF Klasik harus diaktifkan](#)
- [\[WAF.2\] Aturan Regional AWS WAF Klasik harus memiliki setidaknya satu syarat](#)
- [\[WAF.3\] Kelompok aturan Regional AWS WAF Klasik harus memiliki setidaknya satu aturan](#)
- [\[WAF.4\] Web Regional AWS WAF Klasik ACLs harus memiliki setidaknya satu aturan atau kelompok aturan](#)
- [\[WAF.6\] Aturan global AWS WAF klasik harus memiliki setidaknya satu syarat](#)
- [\[WAF.7\] Kelompok aturan global AWS WAF klasik harus memiliki setidaknya satu aturan](#)
- [\[WAF.8\] Web global AWS WAF klasik ACLs harus memiliki setidaknya satu aturan atau kelompok aturan](#)
- [\[WAF.10\] AWS WAF web ACLs harus memiliki setidaknya satu aturan atau kelompok aturan](#)
- [AWS WAF Aturan \[WAF.12\] harus mengaktifkan metrik CloudWatch](#)
- [\[WorkSpaces.1\] volume WorkSpaces pengguna harus dienkripsi saat istirahat](#)
- [\[WorkSpaces.2\] volume WorkSpaces root harus dienkripsi saat istirahat](#)

Asia Pasifik (Melbourne)

Kontrol berikut tidak didukung di Wilayah Asia Pasifik (Melbourne).

- [\[APIGateway.8\] Rute API Gateway harus menentukan jenis otorisasi](#)
- [\[APIGateway.9\] Pencatatan akses harus dikonfigurasi untuk Tahap API Gateway V2](#)
- [\[Amplify.1\] Aplikasi Amplify harus diberi tag](#)
- [\[Amplify.2\] Amplify branch harus diberi tag](#)
- [\[AppFlow.1\] AppFlow Aliran Amazon harus ditandai](#)

- [\[AppRunner.1\] Layanan App Runner harus diberi tag](#)
- [\[AppRunner.2\] Konektor VPC App Runner harus diberi tag](#)
- [\[AppSync.1\] Cache AWS AppSync API harus dienkripsi saat istirahat](#)
- [\[AppSync.2\] AWS AppSync harus mengaktifkan logging tingkat lapangan](#)
- [\[AppSync.5\] AWS AppSync APIs GraphQL tidak boleh diautentikasi dengan kunci API](#)
- [\[AppSync.6\] Cache AWS AppSync API harus dienkripsi saat transit](#)
- [\[Backup.1\] titik AWS Backup pemulihan harus dienkripsi saat istirahat](#)
- [\[Backup.4\] rencana AWS Backup laporan harus ditandai](#)
- [\[Batch.1\] Antrian pekerjaan batch harus ditandai](#)
- [\[Batch.3\] Lingkungan komputasi Batch harus ditandai](#)
- [\[Batch.4\] Properti sumber daya komputasi di lingkungan komputasi Batch terkelola harus ditandai](#)
- [\[CloudFront.1\] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi](#)
- [\[CloudFront.3\] CloudFront distribusi harus memerlukan enkripsi dalam perjalanan](#)
- [\[CloudFront.4\] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi](#)
- [\[CloudFront.5\] CloudFront distribusi seharusnya mengaktifkan logging](#)
- [\[CloudFront.6\] CloudFront distribusi harus mengaktifkan WAF](#)
- [\[CloudFront.7\] CloudFront distribusi harus menggunakan sertifikat SSL/TLS khusus](#)
- [\[CloudFront.8\] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS](#)
- [\[CloudFront.9\] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus](#)
- [\[CloudFront.10\] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal kustom](#)
- [\[CloudFront.12\] CloudFront distribusi seharusnya tidak menunjukkan asal S3 yang tidak ada](#)
- [\[CloudFront.13\] CloudFront distribusi harus menggunakan kontrol akses asal](#)
- [\[CloudFront.14\] CloudFront distribusi harus ditandai](#)
- [\[CodeArtifact.1\] CodeArtifact repositori harus ditandai](#)
- [\[CodeGuruProfiler.1\] Grup CodeGuru profil profiler harus diberi tag](#)
- [\[CodeGuruReviewer.1\] Asosiasi CodeGuru repositori peninjau harus diberi tag](#)
- [\[Cognito.1\] Kumpulan pengguna Cognito harus mengaktifkan perlindungan ancaman dengan mode penegakan fungsi penuh untuk otentikasi standar](#)
- [\[Connect.1\] Jenis objek Amazon Connect Customer Profiles harus diberi tag](#)
- [\[Connect.2\] Instans Amazon Connect seharusnya mengaktifkan logging CloudWatch](#)

- [\[Detective.1\] Grafik perilaku detektif harus diberi tag](#)
- [\[DMS.2\] Sertifikat DMS harus ditandai](#)
- [\[DMS.3\] Langganan acara DMS harus ditandai](#)
- [\[DMS.4\] Contoh replikasi DMS harus ditandai](#)
- [\[DMS.5\] Grup subnet replikasi DMS harus ditandai](#)
- [\[DMS.6\] Instans replikasi DMS harus mengaktifkan peningkatan versi minor otomatis](#)
- [\[DMS.7\] Tugas replikasi DMS untuk database target seharusnya mengaktifkan logging](#)
- [\[DMS.8\] Tugas replikasi DMS untuk database sumber seharusnya mengaktifkan logging](#)
- [\[DMS.9\] Titik akhir DMS harus menggunakan SSL](#)
- [\[DMS.10\] Titik akhir DMS untuk database Neptune harus mengaktifkan otorisasi IAM](#)
- [\[DMS.11\] Titik akhir DMS untuk MongoDB harus mengaktifkan mekanisme otentikasi](#)
- [\[DMS.12\] Titik akhir DMS untuk Redis OSS seharusnya mengaktifkan TLS](#)
- [\[DocumentDB.1\] Cluster Amazon DocumentDB harus dienkripsi saat istirahat](#)
- [\[DocumentDB.2\] Cluster Amazon DocumentDB harus memiliki periode retensi cadangan yang memadai](#)
- [\[DocumentDB.3\] Cuplikan cluster manual Amazon DocumentDB seharusnya tidak bersifat publik](#)
- [\[DocumentDB.4\] Cluster Amazon DocumentDB harus mempublikasikan log audit ke Log CloudWatch](#)
- [\[DocumentDB.5\] Cluster Amazon DocumentDB harus mengaktifkan perlindungan penghapusan](#)
- [\[DocumentDB.6\] Cluster Amazon DocumentDB harus dienkripsi saat transit](#)
- [\[DynamoDB.3\] Cluster DynamoDB Accelerator \(DAX\) harus dienkripsi saat istirahat](#)
- [\[DynamoDB.4\] Tabel DynamoDB harus ada dalam rencana cadangan](#)
- [\[DynamoDB.7\] Cluster DynamoDB Accelerator harus dienkripsi saat transit](#)
- [\[EC2.1\] Cuplikan Amazon EBS tidak boleh dipulihkan secara publik](#)
- [\[EC2.4\] EC2 Instans yang dihentikan harus dihapus setelah periode waktu tertentu](#)
- [\[EC2.8\] EC2 instans harus menggunakan Instance Metadata Service Versi 2 \(\) IMDSv2](#)
- [\[EC2.14\] Grup keamanan seharusnya tidak mengizinkan masuknya dari 0.0.0.0/0 atau :/0 ke port 3389](#)
- [\[EC2.18\] Grup keamanan seharusnya hanya mengizinkan lalu lintas masuk yang tidak terbatas untuk port resmi](#)
- [\[EC2.22\] Grup EC2 keamanan Amazon yang tidak digunakan harus dihapus](#)

- [\[EC2.23\] Amazon EC2 Transit Gateways seharusnya tidak secara otomatis menerima permintaan lampiran VPC](#)
- [\[EC2.24\] Jenis instance EC2 paravirtual Amazon tidak boleh digunakan](#)
- [\[EC2.25\] Templat EC2 peluncuran Amazon tidak boleh menetapkan publik IPs ke antarmuka jaringan](#)
- [\[EC2.28\] Volume EBS harus dicakup oleh rencana cadangan](#)
- [\[EC2.34\] tabel rute gateway EC2 transit harus ditandai](#)
- [\[EC2.40\] Gateway EC2 NAT harus ditandai](#)
- [\[EC2.48\] Log aliran VPC Amazon harus diberi tag](#)
- [\[EC2.58\] VPCs harus dikonfigurasi dengan titik akhir antarmuka untuk Kontak Manajer Insiden Systems Manager](#)
- [\[EC2.60\] VPCs harus dikonfigurasi dengan titik akhir antarmuka untuk Systems Manager Incident Manager](#)
- [\[EC2.170\] templat EC2 peluncuran harus menggunakan Layanan Metadata Instance Versi 2 \(\) IMDSv2](#)
- [\[EC2.173\] Permintaan Armada EC2 Spot harus mengaktifkan enkripsi untuk volume EBS terlampir](#)
- [\[EC2.175\] templat EC2 peluncuran harus diberi tag](#)
- [\[ECR.4\] Repositori publik ECR harus ditandai](#)
- [\[EFS.1\] Sistem File Elastis harus dikonfigurasi untuk mengenkripsi data file saat istirahat menggunakan AWS KMS](#)
- [\[EFS.2\] Volume Amazon EFS harus dalam rencana cadangan](#)
- [\[ELB.14\] Classic Load Balancer harus dikonfigurasi dengan mode mitigasi desync defensif atau paling ketat](#)
- [\[ELB.17\] Aplikasi dan Penyeimbang Beban Jaringan dengan pendengar harus menggunakan kebijakan keamanan yang direkomendasikan](#)
- [\[ElastiCache.1\] Cluster ElastiCache \(Redis OSS\) harus mengaktifkan pencadangan otomatis](#)
- [\[ElastiCache.2\] ElastiCache cluster harus mengaktifkan peningkatan versi minor otomatis](#)
- [\[ElastiCache.3\] grup ElastiCache replikasi harus mengaktifkan failover otomatis](#)
- [\[ElastiCache.4\] grup ElastiCache replikasi harus dienkripsi saat istirahat](#)
- [\[ElastiCache.5\] grup ElastiCache replikasi harus dienkripsi saat transit](#)
- [\[ElastiCache.6\] ElastiCache \(Redis OSS\) grup replikasi dari versi sebelumnya harus mengaktifkan Redis OSS AUTH](#)

- [\[ElastiCache.7\] ElastiCache cluster tidak boleh menggunakan grup subnet default](#)
- [\[ElasticBeanstalk.1\] Lingkungan Elastic Beanstalk seharusnya mengaktifkan pelaporan kesehatan yang ditingkatkan](#)
- [\[ElasticBeanstalk.2\] Pembaruan platform yang dikelola Elastic Beanstalk harus diaktifkan](#)
- [\[ElasticBeanstalk.3\] Elastic Beanstalk harus mengalirkan log ke CloudWatch](#)
- [\[EMR.1\] Node primer kluster EMR Amazon seharusnya tidak memiliki alamat IP publik](#)
- [\[ES.4\] Kesalahan domain Elasticsearch yang masuk ke CloudWatch Log harus diaktifkan](#)
- [\[EventBridge.4\] titik akhir EventBridge global harus mengaktifkan replikasi acara](#)
- [\[FraudDetector.1\] Jenis entitas Amazon Fraud Detector harus diberi tag](#)
- [\[FraudDetector.2\] Label Amazon Fraud Detector harus diberi tag](#)
- [\[FraudDetector.3\] Hasil Amazon Fraud Detector harus ditandai](#)
- [\[FraudDetector.4\] Variabel Amazon Fraud Detector harus diberi tag](#)
- [\[FSx.1\] FSx untuk sistem file OpenZFS harus dikonfigurasi untuk menyalin tag ke cadangan dan volume](#)
- [\[FSx.3\] FSx untuk sistem file OpenZFS harus dikonfigurasi untuk penyebaran Multi-AZ](#)
- [\[GlobalAccelerator.1\] Akselerator Akselerator Global harus diberi tag](#)
- [\[Glue.4\] Pekerjaan AWS Glue percikan harus berjalan pada versi yang didukung AWS Glue](#)
- [\[GuardDuty.2\] GuardDuty filter harus diberi tag](#)
- [\[IAM.1\] Kebijakan IAM seharusnya tidak mengizinkan hak administratif “*” penuh](#)
- [\[IAM.2\] Pengguna IAM seharusnya tidak memiliki kebijakan IAM yang dilampirkan](#)
- [\[IAM.3\] Kunci akses pengguna IAM harus diputar setiap 90 hari atau kurang](#)
- [\[IAM.5\] MFA harus diaktifkan untuk semua pengguna IAM yang memiliki kata sandi konsol](#)
- [\[IAM.6\] MFA perangkat keras harus diaktifkan untuk pengguna root](#)
- [\[IAM.8\] Kredensi pengguna IAM yang tidak digunakan harus dihapus](#)
- [\[IAM.10\] Kebijakan kata sandi untuk pengguna IAM harus memiliki konfigurasi yang kuat](#)
- [\[IAM.11\] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu huruf besar](#)
- [\[IAM.12\] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu huruf kecil](#)
- [\[IAM.13\] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu simbol](#)
- [\[IAM.14\] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu nomor](#)
- [\[IAM.15\] Pastikan kebijakan kata sandi IAM membutuhkan panjang kata sandi minimum 14 atau lebih](#)

- [\[IAM.16\] Pastikan kebijakan kata sandi IAM mencegah penggunaan kembali kata sandi](#)
- [\[IAM.17\] Pastikan kebijakan kata sandi IAM kedaluwarsa kata sandi dalam waktu 90 hari atau kurang](#)
- [\[IAM.18\] Memastikan peran dukungan telah dibuat untuk mengelola insiden dengan AWS Dukungan](#)
- [\[IAM.19\] MFA harus diaktifkan untuk semua pengguna IAM](#)
- [\[IAM.21\] Kebijakan terkelola pelanggan IAM yang Anda buat seharusnya tidak mengizinkan tindakan wildcard untuk layanan](#)
- [\[IAM.22\] Kredensi pengguna IAM yang tidak digunakan selama 45 hari harus dihapus](#)
- [\[IAM.24\] Peran IAM harus ditandai](#)
- [\[IAM.25\] Pengguna IAM harus diberi tag](#)
- [\[IAM.26\] Sertifikat SSL/TLS kedaluwarsa yang dikelola di IAM harus dihapus](#)
- [\[IAM.27\] Identitas IAM seharusnya tidak memiliki kebijakan yang dilampirkan AWSCloudShellFullAccess](#)
- [\[Inspektor.1\] Pemindaian Amazon Inspector harus diaktifkan EC2](#)
- [\[Inspektor.2\] Pemindaian ECR Amazon Inspector harus diaktifkan](#)
- [\[Inspektor.3\] Pemindaian kode Amazon Inspector Lambda harus diaktifkan](#)
- [\[Inspektor.4\] Pemindaian standar Amazon Inspector Lambda harus diaktifkan](#)
- [\[IoT.1\] profil AWS IoT Device Defender keamanan harus ditandai](#)
- [\[IoT.2\] tindakan AWS IoT Core mitigasi harus ditandai](#)
- [AWS IoT Core Dimensi \[IoT.3\] harus ditandai](#)
- [\[IoT.4\] AWS IoT Core otorisasi harus diberi tag](#)
- [\[IoT.5\] alias AWS IoT Core peran harus ditandai](#)
- [AWS IoT Core Kebijakan \[IoT.6\] harus ditandai](#)
- [\[IoTEvents .1\] Input Peristiwa AWS IoT harus diberi tag](#)
- [\[IoTEvents .2\] Model detektor Acara AWS IoT harus diberi tag](#)
- [\[IoTEvents .3\] Model alarm AWS IoT Events harus diberi tag](#)
- [\[IoT Site Wise.1\] Model aset AWS IoT harus ditandai SiteWise](#)
- [\[IoT Site Wise.2\] Dasbor AWS IoT harus diberi tag SiteWise](#)
- [\[IoT Site Wise.3\] Gateway AWS IoT harus diberi tag SiteWise](#)
- [\[IoT Site Wise.4\] Portal AWS IoT harus diberi tag SiteWise](#)

- [\[Io TSite Wise.5\] Proyek AWS IoT harus diberi tag SiteWise](#)
- [\[Io TTwin Maker.1\] Pekerjaan sinkronisasi AWS IoT harus ditandai TwinMaker](#)
- [\[Io TTwin Maker.2\] Ruang kerja AWS IoT harus diberi tag TwinMaker](#)
- [\[Io TTwin Maker.3\] Adegan AWS IoT harus diberi tag TwinMaker](#)
- [\[Io TTwin Maker.4\] Entitas AWS IoT harus diberi tag TwinMaker](#)
- [\[Io TWireless .1\] Grup multicast Nirkabel AWS IoT harus diberi tag](#)
- [\[Io TWireless .2\] Profil layanan AWS IoT Wireless harus diberi tag](#)
- [\[Io TWireless .3\] Tugas AWS IoT FUOTA harus ditandai](#)
- [\[IVS.1\] Pasangan kunci pemutaran IVS harus ditandai](#)
- [\[IVS.2\] Konfigurasi perekaman IVS harus ditandai](#)
- [\[IVS.3\] Saluran IVS harus ditandai](#)
- [\[Keyspaces.1\] Ruang kunci Amazon Keyspaces harus diberi tag](#)
- [\[Kinesis.1\] Aliran kinesis harus dienkripsi saat istirahat](#)
- [\[KMS.1\] Kebijakan yang dikelola pelanggan IAM tidak boleh mengizinkan tindakan dekripsi pada semua kunci KMS](#)
- [\[KMS.2\] Prinsipal IAM tidak boleh memiliki kebijakan inline IAM yang memungkinkan tindakan dekripsi pada semua kunci KMS](#)
- [\[Macie.1\] Amazon Macie harus diaktifkan](#)
- [\[Macie.2\] Penemuan data sensitif otomatis Macie harus diaktifkan](#)
- [\[MQ.6\] Broker RabbitMQ harus menggunakan mode penerapan cluster](#)
- [\[MSK.3\] Konektor MSK Connect harus dienkripsi saat transit](#)
- [\[Neptunus.1\] Cluster DB Neptunus harus dienkripsi saat istirahat](#)
- [\[Neptune.2\] Cluster DB Neptunus harus menerbitkan log audit ke Log CloudWatch](#)
- [\[Neptune.3\] Snapshot cluster Neptunus DB seharusnya tidak publik](#)
- [\[Neptunus.4\] Cluster DB Neptunus harus mengaktifkan perlindungan penghapusan](#)
- [\[Neptunus.5\] Cluster DB Neptunus harus mengaktifkan cadangan otomatis](#)
- [\[Neptune.6\] Snapshot cluster Neptunus DB harus dienkripsi saat istirahat](#)
- [\[Neptune.7\] Cluster DB Neptunus harus mengaktifkan otentikasi basis data IAM](#)
- [\[Neptunus.8\] Cluster DB Neptunus harus dikonfigurasi untuk menyalin tag ke snapshot](#)
- [\[Neptunus.9\] Cluster DB Neptunus harus digunakan di beberapa Availability Zone](#)

- [\[Opensearch.1\] OpenSearch domain harus mengaktifkan enkripsi saat istirahat](#)
- [\[Opensearch.2\] OpenSearch domain tidak boleh diakses publik](#)
- [\[Opensearch.3\] OpenSearch domain harus mengenkripsi data yang dikirim antar node](#)
- [\[Opensearch.4\] login kesalahan OpenSearch domain ke Log harus diaktifkan CloudWatch](#)
- [\[Opensearch.5\] OpenSearch domain harus mengaktifkan pencatatan audit](#)
- [\[Opensearch.6\] OpenSearch domain harus memiliki setidaknya tiga node data](#)
- [\[Opensearch.7\] OpenSearch domain harus mengaktifkan kontrol akses berbutir halus](#)
- [\[Opensearch.8\] Koneksi ke OpenSearch domain harus dienkripsi menggunakan kebijakan keamanan TLS terbaru](#)
- [\[Opensearch.9\] domain harus ditandai OpenSearch](#)
- [\[Opensearch.10\] OpenSearch domain harus menginstal pembaruan perangkat lunak terbaru](#)
- [\[Opensearch.11\] OpenSearch domain harus memiliki setidaknya tiga node primer khusus](#)
- [\[RDS.1\] Snapshot RDS harus bersifat pribadi](#)
- [\[RDS.14\] Cluster Amazon Aurora seharusnya mengaktifkan backtracking](#)
- [\[RDS.15\] Cluster RDS DB harus dikonfigurasi untuk beberapa Availability Zone](#)
- [\[RDS.26\] Instans RDS DB harus dilindungi oleh rencana cadangan](#)
- [\[RDS.31\] Grup keamanan RDS DB harus ditandai](#)
- [\[RDS.35\] Cluster RDS DB harus mengaktifkan peningkatan versi minor otomatis](#)
- [\[RDS.37\] Cluster Aurora PostgreSQL DB harus menerbitkan log ke Log CloudWatch](#)
- [\[RedshiftServerless.1\] Grup kerja Amazon Redshift Tanpa Server harus menggunakan perutean VPC yang disempurnakan](#)
- [\[RedshiftServerless.2\] Koneksi ke grup kerja Redshift Serverless harus diperlukan untuk menggunakan SSL](#)
- [\[RedshiftServerless.3\] Kelompok kerja Redshift Tanpa Server harus melarang akses publik](#)
- [\[RedshiftServerless.4\] Ruang nama Redshift Tanpa Server harus dienkripsi dengan pengelolaan pelanggan AWS KMS keys](#)
- [\[RedshiftServerless.5\] Ruang nama Redshift Tanpa Server tidak boleh menggunakan nama pengguna admin default](#)
- [\[RedshiftServerless.6\] Ruang nama Redshift Tanpa Server harus mengeksport log ke Log CloudWatch](#)
- [\[RedshiftServerless.7\] Ruang nama Redshift Tanpa Server seharusnya tidak menggunakan nama database default](#)

- [\[Route53.1\] Pemeriksaan kesehatan rute 53 harus ditandai](#)
- [\[Route53.2\] Route 53 zona yang dihosting publik harus mencatat kueri DNS](#)
- [\[S3.24\] Poin Akses Multi-Wilayah S3 harus mengaktifkan pengaturan akses publik blok](#)
- [\[SageMaker.1\] Instans SageMaker notebook Amazon seharusnya tidak memiliki akses internet langsung](#)
- [\[SageMaker.2\] instance SageMaker notebook harus diluncurkan dalam VPC khusus](#)
- [\[SageMaker.3\] Pengguna seharusnya tidak memiliki akses root ke instance SageMaker notebook](#)
- [\[SageMaker.5\] SageMaker model harus memblokir lalu lintas masuk](#)
- [\[SageMaker.6\] konfigurasi gambar SageMaker aplikasi harus ditandai](#)
- [\[SageMaker.7\] SageMaker gambar harus diberi tag](#)
- [\[SageMaker.8\] instance SageMaker notebook harus berjalan pada platform yang didukung](#)
- [\[SES.1\] Daftar kontak SES harus ditandai](#)
- [\[SES.2\] Set konfigurasi SES harus ditandai](#)
- [\[SQS.1\] Antrian Amazon SQS harus dienkripsi saat istirahat](#)
- [\[SQS.2\] Antrian SQS harus ditandai](#)
- [\[SQS.3\] Kebijakan akses antrian SQS seharusnya tidak mengizinkan akses publik](#)
- [\[SSM.3\] EC2 Instans Amazon yang dikelola oleh Systems Manager harus memiliki status kepatuhan asosiasi COMPLIANT](#)
- [\[SSM.4\] Dokumen SSM seharusnya tidak bersifat publik](#)
- [\[StepFunctions.1\] Mesin status Step Functions seharusnya mengaktifkan logging](#)
- [\[Transfer.3\] Konektor Transfer Family seharusnya mengaktifkan logging](#)
- [\[Transfer.4\] Perjanjian Transfer Family harus ditandai](#)
- [\[WAF.1\] Pencatatan ACL Web Global AWS WAF Klasik harus diaktifkan](#)
- [\[WAF.6\] Aturan global AWS WAF klasik harus memiliki setidaknya satu syarat](#)
- [\[WAF.7\] Kelompok aturan global AWS WAF klasik harus memiliki setidaknya satu aturan](#)
- [\[WAF.8\] Web global AWS WAF klasik ACLs harus memiliki setidaknya satu aturan atau kelompok aturan](#)
- [\[WAF.11\] pencatatan ACL AWS WAF web harus diaktifkan](#)
- [\[WorkSpaces.1\] volume WorkSpaces pengguna harus dienkripsi saat istirahat](#)
- [\[WorkSpaces.2\] volume WorkSpaces root harus dienkripsi saat istirahat](#)

Asia Pasifik (Mumbai)

Kontrol berikut tidak didukung di Wilayah Asia Pasifik (Mumbai).

- [\[AppSync.1\] Cache AWS AppSync API harus dienkrpsi saat istirahat](#)
- [\[AppSync.6\] Cache AWS AppSync API harus dienkrpsi saat transit](#)
- [\[CloudFront.1\] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi](#)
- [\[CloudFront.3\] CloudFront distribusi harus memerlukan enkripsi dalam perjalanan](#)
- [\[CloudFront.4\] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi](#)
- [\[CloudFront.5\] CloudFront distribusi seharusnya mengaktifkan logging](#)
- [\[CloudFront.6\] CloudFront distribusi harus mengaktifkan WAF](#)
- [\[CloudFront.7\] CloudFront distribusi harus menggunakan sertifikat SSL/TLS khusus](#)
- [\[CloudFront.8\] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS](#)
- [\[CloudFront.9\] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus](#)
- [\[CloudFront.10\] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal kustom](#)
- [\[CloudFront.12\] CloudFront distribusi seharusnya tidak menunjukkan asal S3 yang tidak ada](#)
- [\[CloudFront.13\] CloudFront distribusi harus menggunakan kontrol akses asal](#)
- [\[CloudFront.14\] CloudFront distribusi harus ditandai](#)
- [\[CodeGuruProfiler.1\] Grup CodeGuru profil profiler harus diberi tag](#)
- [\[CodeGuruReviewer.1\] Asosiasi CodeGuru repositori peninjau harus diberi tag](#)
- [\[Connect.1\] Jenis objek Amazon Connect Customer Profiles harus diberi tag](#)
- [\[Connect.2\] Instans Amazon Connect seharusnya mengaktifkan logging CloudWatch](#)
- [\[EC2.24\] Jenis instance EC2 paravirtual Amazon tidak boleh digunakan](#)
- [\[EC2.173\] Permintaan Armada EC2 Spot harus mengaktifkan enkripsi untuk volume EBS terlampir](#)
- [\[ECR.4\] Repositori publik ECR harus ditandai](#)
- [\[FraudDetector.1\] Jenis entitas Amazon Fraud Detector harus diberi tag](#)
- [\[FraudDetector.2\] Label Amazon Fraud Detector harus diberi tag](#)
- [\[FraudDetector.3\] Hasil Amazon Fraud Detector harus ditandai](#)
- [\[FraudDetector.4\] Variabel Amazon Fraud Detector harus diberi tag](#)
- [\[GlobalAccelerator.1\] Akselerator Akselerator Global harus diberi tag](#)
- [\[IAM.26\] Sertifikat SSL/TLS kedaluwarsa yang dikelola di IAM harus dihapus](#)

- [\[Inspector.3\] Pemindaian kode Amazon Inspector Lambda harus diaktifkan](#)
- [\[IoT Twin Maker.4\] Entitas AWS IoT harus diberi tag TwinMaker](#)
- [\[IoT Wireless .1\] Grup multicast Nirkabel AWS IoT harus diberi tag](#)
- [\[IoT Wireless .2\] Profil layanan AWS IoT Wireless harus diberi tag](#)
- [\[IoT Wireless .3\] Tugas AWS IoT FUOTA harus ditandai](#)
- [\[RDS.31\] Grup keamanan RDS DB harus ditandai](#)
- [\[Route53.1\] Pemeriksaan kesehatan rute 53 harus ditandai](#)
- [\[Route53.2\] Route 53 zona yang dihosting publik harus mencatat kueri DNS](#)
- [\[S3.24\] Poin Akses Multi-Wilayah S3 harus mengaktifkan pengaturan akses publik blok](#)
- [\[WAF.1\] Pencatatan ACL Web Global AWS WAF Klasik harus diaktifkan](#)
- [\[WAF.6\] Aturan global AWS WAF klasik harus memiliki setidaknya satu syarat](#)
- [\[WAF.7\] Kelompok aturan global AWS WAF klasik harus memiliki setidaknya satu aturan](#)
- [\[WAF.8\] Web global AWS WAF klasik ACLs harus memiliki setidaknya satu aturan atau kelompok aturan](#)

Asia Pasifik (Osaka)

Kontrol berikut tidak didukung di Wilayah Asia Pasifik (Osaka).

- [\[ACM.1\] Sertifikat yang diimpor dan diterbitkan ACM harus diperbarui setelah jangka waktu tertentu](#)
- [\[AppFlow.1\] AppFlow Aliran Amazon harus ditandai](#)
- [\[AppRunner.1\] Layanan App Runner harus diberi tag](#)
- [\[AppRunner.2\] Konektor VPC App Runner harus diberi tag](#)
- [\[AppSync.1\] Cache AWS AppSync API harus dienkripsi saat istirahat](#)
- [\[AppSync.6\] Cache AWS AppSync API harus dienkripsi saat transit](#)
- [\[Backup.1\] titik AWS Backup pemulihan harus dienkripsi saat istirahat](#)
- [\[Backup.4\] rencana AWS Backup laporan harus ditandai](#)
- [\[CloudFront.1\] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi](#)
- [\[CloudFront.3\] CloudFront distribusi harus memerlukan enkripsi dalam perjalanan](#)
- [\[CloudFront.4\] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi](#)
- [\[CloudFront.5\] CloudFront distribusi seharusnya mengaktifkan logging](#)
- [\[CloudFront.6\] CloudFront distribusi harus mengaktifkan WAF](#)

- [\[CloudFront.7\]](#) CloudFront distribusi harus menggunakan sertifikat SSL/TLS khusus
- [\[CloudFront.8\]](#) CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS
- [\[CloudFront.9\]](#) CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus
- [\[CloudFront.10\]](#) CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal kustom
- [\[CloudFront.12\]](#) CloudFront distribusi seharusnya tidak menunjukkan asal S3 yang tidak ada
- [\[CloudFront.13\]](#) CloudFront distribusi harus menggunakan kontrol akses asal
- [\[CloudFront.14\]](#) CloudFront distribusi harus ditandai
- [\[CodeArtifact.1\]](#) CodeArtifact repositori harus ditandai
- [\[CodeGuruProfiler.1\]](#) Grup CodeGuru profil profiler harus diberi tag
- [\[CodeGuruReviewer.1\]](#) Asosiasi CodeGuru repositori peninjau harus diberi tag
- [\[Connect.1\]](#) Jenis objek Amazon Connect Customer Profiles harus diberi tag
- [\[Connect.2\]](#) Instans Amazon Connect seharusnya mengaktifkan logging CloudWatch
- [\[Detective.1\]](#) Grafik perilaku detektif harus diberi tag
- [\[DMS.7\]](#) Tugas replikasi DMS untuk database target seharusnya mengaktifkan logging
- [\[DMS.8\]](#) Tugas replikasi DMS untuk database sumber seharusnya mengaktifkan logging
- [\[DMS.10\]](#) Titik akhir DMS untuk database Neptune harus mengaktifkan otorisasi IAM
- [\[DocumentDB.1\]](#) Cluster Amazon DocumentDB harus dienkripsi saat istirahat
- [\[DocumentDB.2\]](#) Cluster Amazon DocumentDB harus memiliki periode retensi cadangan yang memadai
- [\[DocumentDB.3\]](#) Cuplikan cluster manual Amazon DocumentDB seharusnya tidak bersifat publik
- [\[DocumentDB.4\]](#) Cluster Amazon DocumentDB harus mempublikasikan log audit ke Log CloudWatch
- [\[DocumentDB.5\]](#) Cluster Amazon DocumentDB harus mengaktifkan perlindungan penghapusan
- [\[DocumentDB.6\]](#) Cluster Amazon DocumentDB harus dienkripsi saat transit
- [\[DynamoDB.3\]](#) Cluster DynamoDB Accelerator (DAX) harus dienkripsi saat istirahat
- [\[DynamoDB.7\]](#) Cluster DynamoDB Accelerator harus dienkripsi saat transit
- [\[EC2.4\]](#) EC2 Instans yang dihentikan harus dihapus setelah periode waktu tertentu
- [\[EC2.8\]](#) EC2 instans harus menggunakan Instance Metadata Service Versi 2 () IMDSv2
- [\[EC2.14\]](#) Grup keamanan seharusnya tidak mengizinkan masuknya dari 0.0.0.0/0 atau ::/0 ke port [3389](#)

- [\[EC2.20\] Kedua terowongan VPN untuk koneksi AWS Site-to-Site VPN harus siap](#)
- [\[EC2.22\] Grup EC2 keamanan Amazon yang tidak digunakan harus dihapus](#)
- [\[EC2.23\] Amazon EC2 Transit Gateways seharusnya tidak secara otomatis menerima permintaan lampiran VPC](#)
- [\[EC2.24\] Jenis instance EC2 paravirtual Amazon tidak boleh digunakan](#)
- [\[EC2.55\] VPCs harus dikonfigurasi dengan titik akhir antarmuka untuk ECR API](#)
- [\[EC2.56\] VPCs harus dikonfigurasi dengan titik akhir antarmuka untuk Docker Registry](#)
- [\[EC2.57\] VPCs harus dikonfigurasi dengan titik akhir antarmuka untuk Systems Manager](#)
- [\[EC2.58\] VPCs harus dikonfigurasi dengan titik akhir antarmuka untuk Kontak Manajer Insiden Systems Manager](#)
- [\[EC2.60\] VPCs harus dikonfigurasi dengan titik akhir antarmuka untuk Systems Manager Incident Manager](#)
- [\[EC2.173\] Permintaan Armada EC2 Spot harus mengaktifkan enkripsi untuk volume EBS terlampir](#)
- [\[ECR.4\] Repositori publik ECR harus ditandai](#)
- [\[ELB.1\] Application Load Balancer harus dikonfigurasi untuk mengalihkan semua permintaan HTTP ke HTTPS](#)
- [\[ELB.2\] Classic Load Balancer dengan pendengar SSL/HTTPS harus menggunakan sertifikat yang disediakan oleh AWS Certificate Manager](#)
- [\[ELB.3\] Pendengar Classic Load Balancer harus dikonfigurasi dengan penghentian HTTPS atau TLS](#)
- [\[ELB.4\] Application Load Balancer harus dikonfigurasi untuk menjatuhkan header http yang tidak valid](#)
- [\[ELB.6\] Aplikasi, Gateway, dan Network Load Balancer harus mengaktifkan perlindungan penghapusan](#)
- [\[ELB.8\] Classic Load Balancer dengan pendengar SSL harus menggunakan kebijakan keamanan yang telah ditentukan sebelumnya yang memiliki urasi yang kuat AWS Config](#)
- [\[ELB.16\] Application Load Balancers harus dikaitkan dengan ACL web AWS WAF](#)
- [\[ElastiCache.1\] Cluster ElastiCache \(Redis OSS\) harus mengaktifkan pencadangan otomatis](#)
- [\[ElastiCache.7\] ElastiCache cluster tidak boleh menggunakan grup subnet default](#)
- [\[ElasticBeanstalk.1\] Lingkungan Elastic Beanstalk seharusnya mengaktifkan pelaporan kesehatan yang ditingkatkan](#)
- [\[ElasticBeanstalk.2\] Pembaruan platform yang dikelola Elastic Beanstalk harus diaktifkan](#)

- [\[EMR.1\] Node primer kluster EMR Amazon seharusnya tidak memiliki alamat IP publik](#)
- [\[FraudDetector.1\] Jenis entitas Amazon Fraud Detector harus diberi tag](#)
- [\[FraudDetector.2\] Label Amazon Fraud Detector harus diberi tag](#)
- [\[FraudDetector.3\] Hasil Amazon Fraud Detector harus ditandai](#)
- [\[FraudDetector.4\] Variabel Amazon Fraud Detector harus diberi tag](#)
- [\[GlobalAccelerator.1\] Akselerator Akselerator Global harus diberi tag](#)
- [\[IAM.4\] Kunci akses pengguna root IAM seharusnya tidak ada](#)
- [\[IAM.18\] Memastikan peran dukungan telah dibuat untuk mengelola insiden dengan AWS Dukungan](#)
- [\[IAM.26\] Sertifikat SSL/TLS kedaluwarsa yang dikelola di IAM harus dihapus](#)
- [\[Inspektor.3\] Pemindaian kode Amazon Inspector Lambda harus diaktifkan](#)
- [\[IoT.1\] profil AWS IoT Device Defender keamanan harus ditandai](#)
- [\[IoT.2\] tindakan AWS IoT Core mitigasi harus ditandai](#)
- [AWS IoT Core Dimensi \[IoT.3\] harus ditandai](#)
- [\[IoT.4\] AWS IoT Core otorisasi harus diberi tag](#)
- [\[IoT.5\] alias AWS IoT Core peran harus ditandai](#)
- [AWS IoT Core Kebijakan \[IoT.6\] harus ditandai](#)
- [\[IoT Events .1\] Input Peristiwa AWS IoT harus diberi tag](#)
- [\[IoT Events .2\] Model detektor Acara AWS IoT harus diberi tag](#)
- [\[IoT Events .3\] Model alarm AWS IoT Events harus diberi tag](#)
- [\[IoT Site Wise.1\] Model aset AWS IoT harus ditandai SiteWise](#)
- [\[IoT Site Wise.2\] Dasbor AWS IoT harus diberi tag SiteWise](#)
- [\[IoT Site Wise.3\] Gateway AWS IoT harus diberi tag SiteWise](#)
- [\[IoT Site Wise.4\] Portal AWS IoT harus diberi tag SiteWise](#)
- [\[IoT Site Wise.5\] Proyek AWS IoT harus diberi tag SiteWise](#)
- [\[IoT Twin Maker.1\] Pekerjaan sinkronisasi AWS IoT harus ditandai TwinMaker](#)
- [\[IoT Twin Maker.2\] Ruang kerja AWS IoT harus diberi tag TwinMaker](#)
- [\[IoT Twin Maker.3\] Adegan AWS IoT harus diberi tag TwinMaker](#)
- [\[IoT Twin Maker.4\] Entitas AWS IoT harus diberi tag TwinMaker](#)
- [\[IoT Wireless .1\] Grup multicast Nirkabel AWS IoT harus diberi tag](#)

- [\[IoTWireless .2\] Profil layanan AWS IoT Wireless harus diberi tag](#)
- [\[IoTWireless .3\] Tugas AWS IoT FUOTA harus ditandai](#)
- [\[IVS.1\] Pasangan kunci pemutaran IVS harus ditandai](#)
- [\[IVS.2\] Konfigurasi perekaman IVS harus ditandai](#)
- [\[IVS.3\] Saluran IVS harus ditandai](#)
- [\[Keyspaces.1\] Ruang kunci Amazon Keyspaces harus diberi tag](#)
- [\[MSK.3\] Konektor MSK Connect harus dienkripsi saat transit](#)
- [\[RDS.31\] Grup keamanan RDS DB harus ditandai](#)
- [\[RedshiftServerless.1\] Grup kerja Amazon Redshift Tanpa Server harus menggunakan perutean VPC yang disempurnakan](#)
- [\[RedshiftServerless.2\] Koneksi ke grup kerja Redshift Serverless harus diperlukan untuk menggunakan SSL](#)
- [\[RedshiftServerless.3\] Kelompok kerja Redshift Tanpa Server harus melarang akses publik](#)
- [\[RedshiftServerless.4\] Ruang nama Redshift Tanpa Server harus dienkripsi dengan pengelolaan pelanggan AWS KMS keys](#)
- [\[RedshiftServerless.5\] Ruang nama Redshift Tanpa Server tidak boleh menggunakan nama pengguna admin default](#)
- [\[RedshiftServerless.6\] Ruang nama Redshift Tanpa Server harus mengeksport log ke Log CloudWatch](#)
- [\[RedshiftServerless.7\] Ruang nama Redshift Tanpa Server seharusnya tidak menggunakan nama database default](#)
- [\[Route53.1\] Pemeriksaan kesehatan rute 53 harus ditandai](#)
- [\[Route53.2\] Route 53 zona yang dihosting publik harus mencatat kueri DNS](#)
- [\[S3.24\] Poin Akses Multi-Wilayah S3 harus mengaktifkan pengaturan akses publik blok](#)
- [\[SSM.2\] EC2 Instans Amazon yang dikelola oleh Systems Manager harus memiliki status kepatuhan patch COMPLIANT setelah instalasi patch](#)
- [\[SSM.3\] EC2 Instans Amazon yang dikelola oleh Systems Manager harus memiliki status kepatuhan asosiasi COMPLIANT](#)
- [\[WAF.1\] Pencatatan ACL Web Global AWS WAF Klasik harus diaktifkan](#)
- [\[WAF.3\] Kelompok aturan Regional AWS WAF Klasik harus memiliki setidaknya satu aturan](#)
- [\[WAF.6\] Aturan global AWS WAF klasik harus memiliki setidaknya satu syarat](#)
- [\[WAF.7\] Kelompok aturan global AWS WAF klasik harus memiliki setidaknya satu aturan](#)

- [\[WAF.8\] Web global AWS WAF klasik ACLs harus memiliki setidaknya satu aturan atau kelompok aturan](#)
- [\[WAF.10\] AWS WAF web ACLs harus memiliki setidaknya satu aturan atau kelompok aturan](#)
- [\[WAF.11\] pencatatan ACL AWS WAF web harus diaktifkan](#)
- [\[WorkSpaces.1\] volume WorkSpaces pengguna harus dienkripsi saat istirahat](#)
- [\[WorkSpaces.2\] volume WorkSpaces root harus dienkripsi saat istirahat](#)

Asia Pasifik (Seoul)

Kontrol berikut tidak didukung di Wilayah Asia Pasifik (Seoul).

- [\[AppRunner.1\] Layanan App Runner harus diberi tag](#)
- [\[AppRunner.2\] Konektor VPC App Runner harus diberi tag](#)
- [\[AppSync.1\] Cache AWS AppSync API harus dienkripsi saat istirahat](#)
- [\[AppSync.6\] Cache AWS AppSync API harus dienkripsi saat transit](#)
- [\[CloudFront.1\] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi](#)
- [\[CloudFront.3\] CloudFront distribusi harus memerlukan enkripsi dalam perjalanan](#)
- [\[CloudFront.4\] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi](#)
- [\[CloudFront.5\] CloudFront distribusi seharusnya mengaktifkan logging](#)
- [\[CloudFront.6\] CloudFront distribusi harus mengaktifkan WAF](#)
- [\[CloudFront.7\] CloudFront distribusi harus menggunakan sertifikat SSL/TLS khusus](#)
- [\[CloudFront.8\] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS](#)
- [\[CloudFront.9\] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus](#)
- [\[CloudFront.10\] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal kustom](#)
- [\[CloudFront.12\] CloudFront distribusi seharusnya tidak menunjukkan asal S3 yang tidak ada](#)
- [\[CloudFront.13\] CloudFront distribusi harus menggunakan kontrol akses asal](#)
- [\[CloudFront.14\] CloudFront distribusi harus ditandai](#)
- [\[CodeArtifact.1\] CodeArtifact repositori harus ditandai](#)
- [\[CodeGuruProfiler.1\] Grup CodeGuru profil profiler harus diberi tag](#)
- [\[CodeGuruReviewer.1\] Asosiasi CodeGuru repositori peninjau harus diberi tag](#)
- [\[DynamoDB.3\] Cluster DynamoDB Accelerator \(DAX\) harus dienkripsi saat istirahat](#)

- [\[DynamoDB.7\] Cluster DynamoDB Accelerator harus dienkripsi saat transit](#)
- [\[EC2.24\] Jenis instance EC2 paravirtual Amazon tidak boleh digunakan](#)
- [\[EC2.173\] Permintaan Armada EC2 Spot harus mengaktifkan enkripsi untuk volume EBS terlampir](#)
- [\[ECR.4\] Repositori publik ECR harus ditandai](#)
- [\[FraudDetector.1\] Jenis entitas Amazon Fraud Detector harus diberi tag](#)
- [\[FraudDetector.2\] Label Amazon Fraud Detector harus diberi tag](#)
- [\[FraudDetector.3\] Hasil Amazon Fraud Detector harus ditandai](#)
- [\[FraudDetector.4\] Variabel Amazon Fraud Detector harus diberi tag](#)
- [\[GlobalAccelerator.1\] Akselerator Akselerator Global harus diberi tag](#)
- [\[Glue.4\] Pekerjaan AWS Glue percikan harus berjalan pada versi yang didukung AWS Glue](#)
- [\[IAM.26\] Sertifikat SSL/TLS kedaluwarsa yang dikelola di IAM harus dihapus](#)
- [\[Inspektor.3\] Pemindaian kode Amazon Inspector Lambda harus diaktifkan](#)
- [\[IoT Twin Maker.4\] Entitas AWS IoT harus diberi tag TwinMaker](#)
- [\[IoT Wireless .1\] Grup multicast Nirkabel AWS IoT harus diberi tag](#)
- [\[IoT Wireless .2\] Profil layanan AWS IoT Wireless harus diberi tag](#)
- [\[IoT Wireless .3\] Tugas AWS IoT FUOTA harus ditandai](#)
- [\[RDS.31\] Grup keamanan RDS DB harus ditandai](#)
- [\[Route53.1\] Pemeriksaan kesehatan rute 53 harus ditandai](#)
- [\[Route53.2\] Route 53 zona yang dihosting publik harus mencatat kueri DNS](#)
- [\[S3.24\] Poin Akses Multi-Wilayah S3 harus mengaktifkan pengaturan akses publik blok](#)
- [\[WAF.1\] Pencatatan ACL Web Global AWS WAF Klasik harus diaktifkan](#)
- [\[WAF.6\] Aturan global AWS WAF klasik harus memiliki setidaknya satu syarat](#)
- [\[WAF.7\] Kelompok aturan global AWS WAF klasik harus memiliki setidaknya satu aturan](#)
- [\[WAF.8\] Web global AWS WAF klasik ACLs harus memiliki setidaknya satu aturan atau kelompok aturan](#)

Asia Pasifik (Singapura)

Kontrol berikut tidak didukung di Wilayah Asia Pasifik (Singapura).

- [\[AppSync.1\] Cache AWS AppSync API harus dienkripsi saat istirahat](#)
- [\[AppSync.6\] Cache AWS AppSync API harus dienkripsi saat transit](#)

- [\[CloudFront.1\]](#) CloudFront distribusi harus memiliki objek root default yang dikonfigurasi
- [\[CloudFront.3\]](#) CloudFront distribusi harus memerlukan enkripsi dalam perjalanan
- [\[CloudFront.4\]](#) CloudFront distribusi harus memiliki failover asal yang dikonfigurasi
- [\[CloudFront.5\]](#) CloudFront distribusi seharusnya mengaktifkan logging
- [\[CloudFront.6\]](#) CloudFront distribusi harus mengaktifkan WAF
- [\[CloudFront.7\]](#) CloudFront distribusi harus menggunakan sertifikat SSL/TLS khusus
- [\[CloudFront.8\]](#) CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS
- [\[CloudFront.9\]](#) CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus
- [\[CloudFront.10\]](#) CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal kustom
- [\[CloudFront.12\]](#) CloudFront distribusi seharusnya tidak menunjukkan asal S3 yang tidak ada
- [\[CloudFront.13\]](#) CloudFront distribusi harus menggunakan kontrol akses asal
- [\[CloudFront.14\]](#) CloudFront distribusi harus ditandai
- [\[EC2.173\]](#) Permintaan Armada EC2 Spot harus mengaktifkan enkripsi untuk volume EBS terlampir
- [\[ECR.4\]](#) Repositori publik ECR harus ditandai
- [\[GlobalAccelerator.1\]](#) Akselerator Akselerator Global harus diberi tag
- [\[IAM.26\]](#) Sertifikat SSL/TLS kedaluwarsa yang dikelola di IAM harus dihapus
- [\[IoTWireless.1\]](#) Grup multicast Nirkabel AWS IoT harus diberi tag
- [\[IoTWireless.2\]](#) Profil layanan AWS IoT Wireless harus diberi tag
- [\[IoTWireless.3\]](#) Tugas AWS IoT FUOTA harus ditandai
- [\[IVS.1\]](#) Pasangan kunci pemutaran IVS harus ditandai
- [\[IVS.2\]](#) Konfigurasi perekaman IVS harus ditandai
- [\[IVS.3\]](#) Saluran IVS harus ditandai
- [\[Route53.1\]](#) Pemeriksaan kesehatan rute 53 harus ditandai
- [\[Route53.2\]](#) Route 53 zona yang dihosting publik harus mencatat kueri DNS
- [\[S3.24\]](#) Poin Akses Multi-Wilayah S3 harus mengaktifkan pengaturan akses publik blok
- [\[WAF.1\]](#) Pencatatan ACL Web Global AWS WAF Klasik harus diaktifkan
- [\[WAF.6\]](#) Aturan global AWS WAF klasik harus memiliki setidaknya satu syarat
- [\[WAF.7\]](#) Kelompok aturan global AWS WAF klasik harus memiliki setidaknya satu aturan
- [\[WAF.8\]](#) Web global AWS WAF klasik ACLs harus memiliki setidaknya satu aturan atau kelompok aturan

Asia Pasifik (Sydney)

Kontrol berikut tidak didukung di Wilayah Asia Pasifik (Sydney).

- [\[AppSync.1\] Cache AWS AppSync API harus dienkripsi saat istirahat](#)
- [\[AppSync.6\] Cache AWS AppSync API harus dienkripsi saat transit](#)
- [\[CloudFront.1\] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi](#)
- [\[CloudFront.3\] CloudFront distribusi harus memerlukan enkripsi dalam perjalanan](#)
- [\[CloudFront.4\] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi](#)
- [\[CloudFront.5\] CloudFront distribusi seharusnya mengaktifkan logging](#)
- [\[CloudFront.6\] CloudFront distribusi harus mengaktifkan WAF](#)
- [\[CloudFront.7\] CloudFront distribusi harus menggunakan sertifikat SSL/TLS khusus](#)
- [\[CloudFront.8\] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS](#)
- [\[CloudFront.9\] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus](#)
- [\[CloudFront.10\] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal kustom](#)
- [\[CloudFront.12\] CloudFront distribusi seharusnya tidak menunjukkan asal S3 yang tidak ada](#)
- [\[CloudFront.13\] CloudFront distribusi harus menggunakan kontrol akses asal](#)
- [\[CloudFront.14\] CloudFront distribusi harus ditandai](#)
- [\[EC2.173\] Permintaan Armada EC2 Spot harus mengaktifkan enkripsi untuk volume EBS terlampir](#)
- [\[ECR.4\] Repositori publik ECR harus ditandai](#)
- [\[GlobalAccelerator.1\] Akselerator Akselerator Global harus diberi tag](#)
- [\[IAM.26\] Sertifikat SSL/TLS kedaluwarsa yang dikelola di IAM harus dihapus](#)
- [\[IVS.1\] Pasangan kunci pemutaran IVS harus ditandai](#)
- [\[IVS.2\] Konfigurasi perekaman IVS harus ditandai](#)
- [\[IVS.3\] Saluran IVS harus ditandai](#)
- [\[Route53.1\] Pemeriksaan kesehatan rute 53 harus ditandai](#)
- [\[Route53.2\] Route 53 zona yang dihosting publik harus mencatat kueri DNS](#)
- [\[S3.24\] Poin Akses Multi-Wilayah S3 harus mengaktifkan pengaturan akses publik blok](#)
- [\[WAF.1\] Pencatatan ACL Web Global AWS WAF Klasik harus diaktifkan](#)
- [\[WAF.6\] Aturan global AWS WAF klasik harus memiliki setidaknya satu syarat](#)
- [\[WAF.7\] Kelompok aturan global AWS WAF klasik harus memiliki setidaknya satu aturan](#)

- [\[WAF.8\] Web global AWS WAF klasik ACLs harus memiliki setidaknya satu aturan atau kelompok aturan](#)

Asia Pasifik (Thailand)

Kontrol berikut tidak didukung di Wilayah Asia Pasifik (Thailand).

- [\[ACM.1\] Sertifikat yang diimpor dan diterbitkan ACM harus diperbarui setelah jangka waktu tertentu](#)
- [\[ACM.2\] Sertifikat RSA yang dikelola oleh ACM harus menggunakan panjang kunci minimal 2.048 bit](#)
- [\[ACM.3\] Sertifikat ACM harus ditandai](#)
- [\[Akun.1\] Informasi kontak keamanan harus disediakan untuk Akun AWS](#)
- [\[Akun.2\] Akun AWS harus menjadi bagian dari organisasi AWS Organizations](#)
- [\[APIGateway.1\] API Gateway REST dan pencatatan eksekusi WebSocket API harus diaktifkan](#)
- [\[APIGateway.5\] Data cache API Gateway REST API harus dienkripsi saat istirahat](#)
- [\[APIGateway.8\] Rute API Gateway harus menentukan jenis otorisasi](#)
- [\[APIGateway.9\] Pencatatan akses harus dikonfigurasi untuk Tahap API Gateway V2](#)
- [\[Amplify.1\] Aplikasi Amplify harus diberi tag](#)
- [\[Amplify.2\] Amplify branch harus diberi tag](#)
- [\[AppConfig.1\] AWS AppConfig aplikasi harus diberi tag](#)
- [\[AppConfig.2\] profil AWS AppConfig konfigurasi harus ditandai](#)
- [\[AppConfig.3\] AWS AppConfig lingkungan harus ditandai](#)
- [\[AppConfig.4\] asosiasi AWS AppConfig ekstensi harus ditandai](#)
- [\[AppFlow.1\] AppFlow Aliran Amazon harus ditandai](#)
- [\[AppRunner.1\] Layanan App Runner harus diberi tag](#)
- [\[AppRunner.2\] Konektor VPC App Runner harus diberi tag](#)
- [\[AppSync.1\] Cache AWS AppSync API harus dienkripsi saat istirahat](#)
- [\[AppSync.2\] AWS AppSync harus mengaktifkan logging tingkat lapangan](#)
- [\[AppSync.4\] AWS AppSync APIs GraphQL harus diberi tag](#)
- [\[AppSync.5\] AWS AppSync APIs GraphQL tidak boleh diautentikasi dengan kunci API](#)
- [\[AppSync.6\] Cache AWS AppSync API harus dienkripsi saat transit](#)
- [\[Athena.2\] Katalog data Athena harus ditandai](#)

- [\[Athena.3\] Kelompok kerja Athena harus ditandai](#)
- [\[Athena.4\] Kelompok kerja Athena seharusnya mengaktifkan logging](#)
- [\[AutoScaling.2\] Grup EC2 Auto Scaling Amazon harus mencakup beberapa Availability Zone](#)
- [\[AutoScaling.3\] Konfigurasi peluncuran grup Auto Scaling harus EC2 mengonfigurasi instance agar memerlukan Layanan Metadata Instance Versi 2 \(\) IMDSv2](#)
- [\[AutoScaling.6\] Grup Auto Scaling harus menggunakan beberapa jenis instance di beberapa Availability Zone](#)
- [\[AutoScaling.9\] Grup EC2 Auto Scaling Amazon harus menggunakan templat peluncuran Amazon EC2](#)
- [\[AutoScaling.10\] Grup EC2 Auto Scaling harus diberi tag](#)
- [\[Backup.1\] titik AWS Backup pemulihan harus dienkripsi saat istirahat](#)
- [\[Backup.2\] poin AWS Backup pemulihan harus ditandai](#)
- [\[Backup.3\] AWS Backup brankas harus ditandai](#)
- [\[Backup.4\] rencana AWS Backup laporan harus ditandai](#)
- [\[Backup.5\] rencana AWS Backup cadangan harus ditandai](#)
- [\[Batch.1\] Antrian pekerjaan batch harus ditandai](#)
- [\[Batch.2\] Kebijakan penjadwalan batch harus ditandai](#)
- [\[Batch.3\] Lingkungan komputasi Batch harus ditandai](#)
- [\[Batch.4\] Properti sumber daya komputasi di lingkungan komputasi Batch terkelola harus ditandai](#)
- [\[CloudFormation.2\] CloudFormation tumpukan harus ditandai](#)
- [\[CloudFront.1\] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi](#)
- [\[CloudFront.3\] CloudFront distribusi harus memerlukan enkripsi dalam perjalanan](#)
- [\[CloudFront.4\] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi](#)
- [\[CloudFront.5\] CloudFront distribusi seharusnya mengaktifkan logging](#)
- [\[CloudFront.6\] CloudFront distribusi harus mengaktifkan WAF](#)
- [\[CloudFront.7\] CloudFront distribusi harus menggunakan sertifikat SSL/TLS khusus](#)
- [\[CloudFront.8\] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS](#)
- [\[CloudFront.9\] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus](#)
- [\[CloudFront.10\] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal kustom](#)
- [\[CloudFront.12\] CloudFront distribusi seharusnya tidak menunjukkan asal S3 yang tidak ada](#)

- [\[CloudFront.13\] CloudFront distribusi harus menggunakan kontrol akses asal](#)
- [\[CloudFront.14\] CloudFront distribusi harus ditandai](#)
- [\[CloudTrail.6\] Pastikan bucket S3 yang digunakan untuk menyimpan CloudTrail log tidak dapat diakses publik](#)
- [\[CloudTrail.7\] Pastikan pencatatan akses bucket S3 diaktifkan pada bucket CloudTrail S3](#)
- [\[CloudTrail.9\] CloudTrail jejak harus ditandai](#)
- [\[CloudTrail.10\] Penyimpanan data acara CloudTrail danau harus dienkripsi dengan pelanggan yang dikelola AWS KMS keys](#)
- [\[CloudWatch.17\] tindakan CloudWatch alarm harus diaktifkan](#)
- [\[CodeArtifact.1\] CodeArtifact repositori harus ditandai](#)
- [\[CodeBuild.1\] Repositori sumber CodeBuild Bitbucket tidak URLs boleh berisi kredensial sensitif](#)
- [\[CodeBuild.2\] variabel lingkungan CodeBuild proyek tidak boleh berisi kredensial teks yang jelas](#)
- [\[CodeBuild.3\] Log CodeBuild S3 harus dienkripsi](#)
- [\[CodeBuild.4\] lingkungan CodeBuild proyek harus memiliki urasi logging AWS Config](#)
- [\[CodeBuild.7\] ekspor kelompok CodeBuild laporan harus dienkripsi saat istirahat](#)
- [\[CodeGuruProfiler.1\] Grup CodeGuru profil profiler harus diberi tag](#)
- [\[CodeGuruReviewer.1\] Asosiasi CodeGuru repositori peninjau harus diberi tag](#)
- [\[Cognito.1\] Kumpulan pengguna Cognito harus mengaktifkan perlindungan ancaman dengan mode penegakan fungsi penuh untuk otentikasi standar](#)
- [\[Connect.1\] Jenis objek Amazon Connect Customer Profiles harus diberi tag](#)
- [\[Connect.2\] Instans Amazon Connect seharusnya mengaktifkan logging CloudWatch](#)
- [\[DataFirehose.1\] Aliran pengiriman Firehose harus dienkripsi saat istirahat](#)
- [\[DataSync.1\] DataSync tugas harus mengaktifkan logging](#)
- [\[DataSync.2\] DataSync tugas harus ditandai](#)
- [\[Detective.1\] Grafik perilaku detektif harus diberi tag](#)
- [\[DMS.1\] Instans replikasi Layanan Migrasi Database tidak boleh bersifat publik](#)
- [\[DMS.2\] Sertifikat DMS harus ditandai](#)
- [\[DMS.3\] Langganan acara DMS harus ditandai](#)
- [\[DMS.4\] Contoh replikasi DMS harus ditandai](#)
- [\[DMS.5\] Grup subnet replikasi DMS harus ditandai](#)
- [\[DMS.6\] Instans replikasi DMS harus mengaktifkan peningkatan versi minor otomatis](#)

- [\[DMS.7\] Tugas replikasi DMS untuk database target seharusnya mengaktifkan logging](#)
- [\[DMS.8\] Tugas replikasi DMS untuk database sumber seharusnya mengaktifkan logging](#)
- [\[DMS.9\] Titik akhir DMS harus menggunakan SSL](#)
- [\[DMS.10\] Titik akhir DMS untuk database Neptune harus mengaktifkan otorisasi IAM](#)
- [\[DMS.11\] Titik akhir DMS untuk MongoDB harus mengaktifkan mekanisme otentikasi](#)
- [\[DMS.12\] Titik akhir DMS untuk Redis OSS seharusnya mengaktifkan TLS](#)
- [\[DocumentDB.1\] Cluster Amazon DocumentDB harus dienkripsi saat istirahat](#)
- [\[DocumentDB.2\] Cluster Amazon DocumentDB harus memiliki periode retensi cadangan yang memadai](#)
- [\[DocumentDB.3\] Cuplikan cluster manual Amazon DocumentDB seharusnya tidak bersifat publik](#)
- [\[DocumentDB.4\] Cluster Amazon DocumentDB harus mempublikasikan log audit ke Log CloudWatch](#)
- [\[DocumentDB.5\] Cluster Amazon DocumentDB harus mengaktifkan perlindungan penghapusan](#)
- [\[DocumentDB.6\] Cluster Amazon DocumentDB harus dienkripsi saat transit](#)
- [\[DynamoDB.3\] Cluster DynamoDB Accelerator \(DAX\) harus dienkripsi saat istirahat](#)
- [\[DynamoDB.4\] Tabel DynamoDB harus ada dalam rencana cadangan](#)
- [\[DynamoDB.5\] Tabel DynamoDB harus diberi tag](#)
- [\[DynamoDB.6\] Tabel DynamoDB harus mengaktifkan perlindungan penghapusan](#)
- [\[DynamoDB.7\] Cluster DynamoDB Accelerator harus dienkripsi saat transit](#)
- [\[EC2.4\] EC2 Instans yang dihentikan harus dihapus setelah periode waktu tertentu](#)
- [\[EC2.21\] Jaringan ACLs seharusnya tidak mengizinkan masuknya dari 0.0.0.0/0 ke port 22 atau port 3389.](#)
- [\[EC2.22\] Grup EC2 keamanan Amazon yang tidak digunakan harus dihapus](#)
- [\[EC2.23\] Amazon EC2 Transit Gateways seharusnya tidak secara otomatis menerima permintaan lampiran VPC](#)
- [\[EC2.24\] Jenis instance EC2 paravirtual Amazon tidak boleh digunakan](#)
- [\[EC2.25\] Templat EC2 peluncuran Amazon tidak boleh menetapkan publik IPs ke antarmuka jaringan](#)
- [\[EC2.28\] Volume EBS harus dicakup oleh rencana cadangan](#)
- [\[EC2.33\] lampiran gateway EC2 transit harus ditandai](#)
- [\[EC2.34\] tabel rute gateway EC2 transit harus ditandai](#)

- [\[EC2.35\] antarmuka EC2 jaringan harus ditandai](#)
- [\[EC2.36\] gateway EC2 pelanggan harus ditandai](#)
- [\[EC2.37\] Alamat IP EC2 elastis harus ditandai](#)
- [\[EC2.38\] EC2 instance harus ditandai](#)
- [\[EC2.39\] gateway EC2 internet harus ditandai](#)
- [\[EC2.40\] Gateway EC2 NAT harus ditandai](#)
- [\[EC2.41\] EC2 jaringan ACLs harus ditandai](#)
- [\[EC2.42\] tabel EC2 rute harus ditandai](#)
- [\[EC2.43\] grup EC2 keamanan harus ditandai](#)
- [\[EC2.44\] EC2 subnet harus ditandai](#)
- [\[EC2.45\] EC2 volume harus ditandai](#)
- [\[EC2.46\] Amazon VPCs harus diberi tag](#)
- [\[EC2.47\] Layanan titik akhir Amazon VPC harus diberi tag](#)
- [\[EC2.48\] Log aliran VPC Amazon harus diberi tag](#)
- [\[EC2.49\] Koneksi peering VPC Amazon harus ditandai](#)
- [\[EC2.50\] Gateway EC2 VPN harus diberi tag](#)
- [\[EC2.51\] Titik akhir EC2 Client VPN harus mengaktifkan pencatatan koneksi klien](#)
- [\[EC2.52\] gateway EC2 transit harus ditandai](#)
- [\[EC2.53\] grup EC2 keamanan seharusnya tidak mengizinkan masuknya dari 0.0.0.0/0 ke port administrasi server jarak jauh](#)
- [\[EC2.54\] grup EC2 keamanan tidak boleh mengizinkan masuknya dari :/0 ke port administrasi server jarak jauh](#)
- [\[EC2.55\] VPCs harus dikonfigurasi dengan titik akhir antarmuka untuk ECR API](#)
- [\[EC2.56\] VPCs harus dikonfigurasi dengan titik akhir antarmuka untuk Docker Registry](#)
- [\[EC2.57\] VPCs harus dikonfigurasi dengan titik akhir antarmuka untuk Systems Manager](#)
- [\[EC2.58\] VPCs harus dikonfigurasi dengan titik akhir antarmuka untuk Kontak Manajer Insiden Systems Manager](#)
- [\[EC2.60\] VPCs harus dikonfigurasi dengan titik akhir antarmuka untuk Systems Manager Incident Manager](#)
- [\[EC2.170\] templat EC2 peluncuran harus menggunakan Layanan Metadata Instance Versi 2 \(\[IMDSv2\]\(#\)\)](#)

- [\[EC2.171\] Koneksi EC2 VPN seharusnya mengaktifkan logging](#)
- [\[EC2.172\] Pengaturan Akses Publik Blok EC2 VPC harus memblokir lalu lintas gateway internet](#)
- [\[EC2.173\] Permintaan Armada EC2 Spot harus mengaktifkan enkripsi untuk volume EBS terlampir](#)
- [\[EC2.174\] Set opsi EC2 DHCP harus ditandai](#)
- [\[EC2.175\] templat EC2 peluncuran harus diberi tag](#)
- [\[EC2.176\] daftar EC2 awalan harus ditandai](#)
- [\[EC2.177\] Sesi cermin EC2 lalu lintas harus ditandai](#)
- [\[EC2.178\] Filter cermin EC2 lalu lintas harus ditandai](#)
- [\[EC2.179\] Target cermin EC2 lalu lintas harus ditandai](#)
- [\[ECR.1\] Repositori pribadi ECR harus memiliki pemindaian gambar yang dikonfigurasi](#)
- [\[ECR.2\] Repositori pribadi ECR harus memiliki kekekalan tag yang dikonfigurasi](#)
- [\[ECR.3\] Repositori ECR harus memiliki setidaknya satu kebijakan siklus hidup yang dikonfigurasi](#)
- [\[ECR.4\] Repositori publik ECR harus ditandai](#)
- [\[ECR.5\] Repositori ECR harus dienkrpsi dengan pelanggan yang dikelola AWS KMS keys](#)
- [\[ECS.2\] Layanan ECS seharusnya tidak memiliki alamat IP publik yang ditetapkan kepadanya secara otomatis](#)
- [\[ECS.3\] Definisi tugas ECS tidak boleh membagikan namespace proses host](#)
- [\[ECS.4\] Kontainer ECS harus berjalan sebagai non-hak istimewa](#)
- [\[ECS.5\] Wadah ECS harus dibatasi pada akses hanya-baca ke sistem file root](#)
- [\[ECS.8\] Rahasia tidak boleh diteruskan sebagai variabel lingkungan kontainer](#)
- [\[ECS.9\] Definisi tugas ECS harus memiliki konfigurasi logging](#)
- [\[ECS.10\] Layanan ECS Fargate harus berjalan pada versi platform Fargate terbaru](#)
- [\[ECS.12\] Cluster ECS harus menggunakan Wawasan Kontainer](#)
- [\[ECS.13\] Layanan ECS harus ditandai](#)
- [\[ECS.14\] Cluster ECS harus ditandai](#)
- [\[ECS.15\] Definisi tugas ECS harus ditandai](#)
- [\[ECS.16\] Set tugas ECS seharusnya tidak secara otomatis menetapkan alamat IP publik](#)
- [\[ECS.17\] Definisi tugas ECS tidak boleh menggunakan mode jaringan host](#)
- [\[EFS.1\] Sistem File Elastis harus dikonfigurasi untuk mengenkripsi data file saat istirahat menggunakan AWS KMS](#)
- [\[EFS.2\] Volume Amazon EFS harus dalam rencana cadangan](#)

- [\[EFS.3\] Titik akses EFS harus menegakkan direktori root](#)
- [\[EFS.4\] Titik akses EFS harus menegakkan identitas pengguna](#)
- [\[EFS.5\] Titik akses EFS harus ditandai](#)
- [\[EFS.6\] Target pemasangan EFS tidak boleh dikaitkan dengan subnet publik](#)
- [\[EFS.7\] Sistem file EFS harus mengaktifkan pencadangan otomatis](#)
- [\[EFS.8\] Sistem file EFS harus dienkrpsi saat istirahat](#)
- [\[EKS.2\] Kluster EKS harus berjalan pada versi Kubernetes yang didukung](#)
- [\[EKS.3\] Kluster EKS harus menggunakan rahasia Kubernetes terenkripsi](#)
- [\[EKS.6\] Kluster EKS harus ditandai](#)
- [\[EKS.7\] Konfigurasi penyedia identitas EKS harus ditandai](#)
- [\[EKS.8\] Kluster EKS harus mengaktifkan pencatatan audit](#)
- [\[ELB.7\] Classic Load Balancers harus mengaktifkan pengaturan koneksi](#)
- [\[ELB.10\] Classic Load Balancer harus menjangkau beberapa Availability Zone](#)
- [\[ELB.12\] Application Load Balancer harus dikonfigurasi dengan mode mitigasi desync defensif atau paling ketat](#)
- [\[ELB.13\] Penyeimbang Beban Aplikasi, Jaringan, dan Gateway harus mencakup beberapa Availability Zone](#)
- [\[ELB.14\] Classic Load Balancer harus dikonfigurasi dengan mode mitigasi desync defensif atau paling ketat](#)
- [\[ELB.17\] Aplikasi dan Penyeimbang Beban Jaringan dengan pendengar harus menggunakan kebijakan keamanan yang direkomendasikan](#)
- [\[ElastiCache.1\] Cluster ElastiCache \(Redis OSS\) harus mengaktifkan pencadangan otomatis](#)
- [\[ElastiCache.2\] ElastiCache cluster harus mengaktifkan peningkatan versi minor otomatis](#)
- [\[ElastiCache.3\] grup ElastiCache replikasi harus mengaktifkan failover otomatis](#)
- [\[ElastiCache.4\] grup ElastiCache replikasi harus dienkrpsi saat istirahat](#)
- [\[ElastiCache.5\] grup ElastiCache replikasi harus dienkrpsi saat transit](#)
- [\[ElastiCache.6\] ElastiCache \(Redis OSS\) grup replikasi dari versi sebelumnya harus mengaktifkan Redis OSS AUTH](#)
- [\[ElastiCache.7\] ElastiCache cluster tidak boleh menggunakan grup subnet default](#)
- [\[ElasticBeanstalk.1\] Lingkungan Elastic Beanstalk seharusnya mengaktifkan pelaporan kesehatan yang ditingkatkan](#)

- [\[ElasticBeanstalk.2\] Pembaruan platform yang dikelola Elastic Beanstalk harus diaktifkan](#)
- [\[ElasticBeanstalk.3\] Elastic Beanstalk harus mengalirkan log ke CloudWatch](#)
- [\[EMR.1\] Node primer kluster EMR Amazon seharusnya tidak memiliki alamat IP publik](#)
- [\[EMR.2\] Pengaturan akses publik blok EMR Amazon harus diaktifkan](#)
- [\[EMR.3\] Konfigurasi keamanan Amazon EMR harus dienkripsi saat istirahat](#)
- [\[EMR.4\] Konfigurasi keamanan Amazon EMR harus dienkripsi saat transit](#)
- [\[ES.3\] Domain Elasticsearch harus mengenkripsi data yang dikirim antar node](#)
- [\[ES.4\] Kesalahan domain Elasticsearch yang masuk ke CloudWatch Log harus diaktifkan](#)
- [\[ES.5\] Domain Elasticsearch harus mengaktifkan pencatatan audit](#)
- [\[ES.6\] Domain Elasticsearch harus memiliki setidaknya tiga node data](#)
- [\[ES.7\] Domain Elasticsearch harus dikonfigurasi dengan setidaknya tiga node master khusus](#)
- [\[ES.8\] Koneksi ke domain Elasticsearch harus dienkripsi menggunakan kebijakan keamanan TLS terbaru](#)
- [\[ES.9\] Domain Elasticsearch harus diberi tag](#)
- [\[EventBridge.2\] bus EventBridge acara harus diberi tag](#)
- [\[EventBridge.3\] bus acara EventBridge khusus harus memiliki kebijakan berbasis sumber daya terlampir](#)
- [\[EventBridge.4\] titik akhir EventBridge global harus mengaktifkan replikasi acara](#)
- [\[FraudDetector.1\] Jenis entitas Amazon Fraud Detector harus diberi tag](#)
- [\[FraudDetector.2\] Label Amazon Fraud Detector harus diberi tag](#)
- [\[FraudDetector.3\] Hasil Amazon Fraud Detector harus ditandai](#)
- [\[FraudDetector.4\] Variabel Amazon Fraud Detector harus diberi tag](#)
- [\[FSx.1\] FSx untuk sistem file OpenZFS harus dikonfigurasi untuk menyalin tag ke cadangan dan volume](#)
- [\[FSx.2\] FSx untuk sistem file Lustre harus dikonfigurasi untuk menyalin tag ke cadangan](#)
- [\[FSx.3\] FSx untuk sistem file OpenZFS harus dikonfigurasi untuk penyebaran Multi-AZ](#)
- [\[FSx.4\] FSx untuk sistem file NetApp ONTAP harus dikonfigurasi untuk penyebaran Multi-AZ](#)
- [\[FSx.5\] FSx untuk sistem file Windows File Server harus dikonfigurasi untuk penyebaran Multi-AZ](#)
- [\[GlobalAccelerator.1\] Akselerator Akselerator Global harus diberi tag](#)
- [AWS Glue Pekerjaan \[Glue.1\] harus ditandai](#)
- [\[Glue.3\] transformasi pembelajaran AWS Glue mesin harus dienkripsi saat istirahat](#)

- [\[Glue.4\] Pekerjaan AWS Glue percikan harus berjalan pada versi yang didukung AWS Glue](#)
- [\[GuardDuty.1\] GuardDuty harus diaktifkan](#)
- [\[GuardDuty.2\] GuardDuty filter harus diberi tag](#)
- [\[GuardDuty.3\] GuardDuty IPSets harus ditandai](#)
- [\[GuardDuty.4\] GuardDuty detektor harus diberi tag](#)
- [\[GuardDuty.5\] Pemantauan Log Audit GuardDuty EKS harus diaktifkan](#)
- [\[GuardDuty.6\] Perlindungan GuardDuty Lambda harus diaktifkan](#)
- [\[GuardDuty.7\] GuardDuty EKS Runtime Monitoring harus diaktifkan](#)
- [\[GuardDuty.8\] Perlindungan GuardDuty Malware untuk EC2 harus diaktifkan](#)
- [\[GuardDuty.9\] Perlindungan GuardDuty RDS harus diaktifkan](#)
- [\[GuardDuty.10\] Perlindungan GuardDuty S3 harus diaktifkan](#)
- [\[GuardDuty.11\] GuardDuty Runtime Monitoring harus diaktifkan](#)
- [\[GuardDuty.12\] GuardDuty ECS Runtime Monitoring harus diaktifkan](#)
- [\[GuardDuty.13\] GuardDuty EC2 Runtime Monitoring harus diaktifkan](#)
- [\[IAM.1\] Kebijakan IAM seharusnya tidak mengizinkan hak administratif “*” penuh](#)
- [\[IAM.2\] Pengguna IAM seharusnya tidak memiliki kebijakan IAM yang dilampirkan](#)
- [\[IAM.3\] Kunci akses pengguna IAM harus diputar setiap 90 hari atau kurang](#)
- [\[IAM.4\] Kunci akses pengguna root IAM seharusnya tidak ada](#)
- [\[IAM.5\] MFA harus diaktifkan untuk semua pengguna IAM yang memiliki kata sandi konsol](#)
- [\[IAM.6\] MFA perangkat keras harus diaktifkan untuk pengguna root](#)
- [\[IAM.7\] Kebijakan kata sandi untuk pengguna IAM harus memiliki konfigurasi yang kuat](#)
- [\[IAM.8\] Kredensi pengguna IAM yang tidak digunakan harus dihapus](#)
- [\[IAM.9\] MFA harus diaktifkan untuk pengguna root](#)
- [\[IAM.10\] Kebijakan kata sandi untuk pengguna IAM harus memiliki konfigurasi yang kuat](#)
- [\[IAM.11\] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu huruf besar](#)
- [\[IAM.12\] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu huruf kecil](#)
- [\[IAM.13\] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu simbol](#)
- [\[IAM.14\] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu nomor](#)
- [\[IAM.15\] Pastikan kebijakan kata sandi IAM membutuhkan panjang kata sandi minimum 14 atau lebih](#)
- [\[IAM.16\] Pastikan kebijakan kata sandi IAM mencegah penggunaan kembali kata sandi](#)

- [\[IAM.17\] Pastikan kebijakan kata sandi IAM kedaluwarsa kata sandi dalam waktu 90 hari atau kurang](#)
- [\[IAM.18\] Memastikan peran dukungan telah dibuat untuk mengelola insiden dengan AWS Dukungan](#)
- [\[IAM.19\] MFA harus diaktifkan untuk semua pengguna IAM](#)
- [\[IAM.21\] Kebijakan terkelola pelanggan IAM yang Anda buat seharusnya tidak mengizinkan tindakan wildcard untuk layanan](#)
- [\[IAM.22\] Kredensi pengguna IAM yang tidak digunakan selama 45 hari harus dihapus](#)
- [\[IAM.23\] Penganalisis Akses IAM harus ditandai](#)
- [\[IAM.24\] Peran IAM harus ditandai](#)
- [\[IAM.25\] Pengguna IAM harus diberi tag](#)
- [\[IAM.26\] Sertifikat SSL/TLS kedaluwarsa yang dikelola di IAM harus dihapus](#)
- [\[IAM.27\] Identitas IAM seharusnya tidak memiliki kebijakan yang dilampirkan AWSCloudShellFullAccess](#)
- [\[IAM.28\] IAM Access Analyzer penganalisis akses eksternal harus diaktifkan](#)
- [\[Inspektor.1\] Pemindaian Amazon Inspector harus diaktifkan EC2](#)
- [\[Inspektor.2\] Pemindaian ECR Amazon Inspector harus diaktifkan](#)
- [\[Inspektor.3\] Pemindaian kode Amazon Inspector Lambda harus diaktifkan](#)
- [\[Inspektor.4\] Pemindaian standar Amazon Inspector Lambda harus diaktifkan](#)
- [\[IoT.1\] profil AWS IoT Device Defender keamanan harus ditandai](#)
- [\[IoT.2\] tindakan AWS IoT Core mitigasi harus ditandai](#)
- [AWS IoT Core Dimensi \[IoT.3\] harus ditandai](#)
- [\[IoT.4\] AWS IoT Core otorisasi harus diberi tag](#)
- [\[IoT.5\] alias AWS IoT Core peran harus ditandai](#)
- [AWS IoT Core Kebijakan \[IoT.6\] harus ditandai](#)
- [\[IoT Events .1\] Input Peristiwa AWS IoT harus diberi tag](#)
- [\[IoT Events .2\] Model detektor Acara AWS IoT harus diberi tag](#)
- [\[IoT Events .3\] Model alarm AWS IoT Events harus diberi tag](#)
- [\[IoT Site Wise.1\] Model aset AWS IoT harus ditandai SiteWise](#)
- [\[IoT Site Wise.2\] Dasbor AWS IoT harus diberi tag SiteWise](#)
- [\[IoT Site Wise.3\] Gateway AWS IoT harus diberi tag SiteWise](#)

- [\[Io TSite Wise.4\] Portal AWS IoT harus diberi tag SiteWise](#)
- [\[Io TSite Wise.5\] Proyek AWS IoT harus diberi tag SiteWise](#)
- [\[Io TTwin Maker.1\] Pekerjaan sinkronisasi AWS IoT harus ditandai TwinMaker](#)
- [\[Io TTwin Maker.2\] Ruang kerja AWS IoT harus diberi tag TwinMaker](#)
- [\[Io TTwin Maker.3\] Adegan AWS IoT harus diberi tag TwinMaker](#)
- [\[Io TTwin Maker.4\] Entitas AWS IoT harus diberi tag TwinMaker](#)
- [\[Io TWireless .1\] Grup multicast Nirkabel AWS IoT harus diberi tag](#)
- [\[Io TWireless .2\] Profil layanan AWS IoT Wireless harus diberi tag](#)
- [\[Io TWireless .3\] Tugas AWS IoT FUOTA harus ditandai](#)
- [\[IVS.1\] Pasangan kunci pemutaran IVS harus ditandai](#)
- [\[IVS.2\] Konfigurasi perekaman IVS harus ditandai](#)
- [\[IVS.3\] Saluran IVS harus ditandai](#)
- [\[Keyspaces.1\] Ruang kunci Amazon Keyspaces harus diberi tag](#)
- [\[Kinesis.1\] Aliran kinesis harus dienkripsi saat istirahat](#)
- [\[Kinesis.2\] Aliran kinesis harus ditandai](#)
- [\[Kinesis.3\] Aliran kinesis harus memiliki periode retensi data yang memadai](#)
- [\[KMS.1\] Kebijakan yang dikelola pelanggan IAM tidak boleh mengizinkan tindakan dekripsi pada semua kunci KMS](#)
- [\[KMS.2\] Prinsipal IAM tidak boleh memiliki kebijakan inline IAM yang memungkinkan tindakan dekripsi pada semua kunci KMS](#)
- [\[KMS.3\] tidak AWS KMS keys boleh dihapus secara tidak sengaja](#)
- [\[KMS.5\] Kunci KMS tidak boleh diakses publik](#)
- [\[Lambda.5\] Fungsi VPC Lambda harus beroperasi di beberapa Availability Zone](#)
- [\[Lambda.6\] Fungsi Lambda harus ditandai](#)
- [\[Macie.1\] Amazon Macie harus diaktifkan](#)
- [\[Macie.2\] Penemuan data sensitif otomatis Macie harus diaktifkan](#)
- [\[MQ.2\] Broker ActiveMQ harus mengalirkan log audit ke CloudWatch](#)
- [\[MQ.3\] Broker Amazon MQ harus mengaktifkan peningkatan versi minor otomatis](#)
- [\[MQ.4\] Broker Amazon MQ harus diberi tag](#)
- [\[MQ.5\] Broker ActiveMQ harus menggunakan mode penerapan aktif/siaga](#)
- [\[MQ.6\] Broker RabbitMQ harus menggunakan mode penerapan cluster](#)

- [\[MSK.1\] Kluster MSK harus dienkripsi saat transit di antara node broker](#)
- [\[MSK.2\] Kluster MSK seharusnya telah meningkatkan pemantauan yang dikonfigurasi](#)
- [\[MSK.3\] Konektor MSK Connect harus dienkripsi saat transit](#)
- [\[Neptunus.1\] Cluster DB Neptunus harus dienkripsi saat istirahat](#)
- [\[Neptune.2\] Cluster DB Neptunus harus menerbitkan log audit ke Log CloudWatch](#)
- [\[Neptune.3\] Snapshot cluster Neptunus DB seharusnya tidak publik](#)
- [\[Neptunus.4\] Cluster DB Neptunus harus mengaktifkan perlindungan penghapusan](#)
- [\[Neptunus.5\] Cluster DB Neptunus harus mengaktifkan cadangan otomatis](#)
- [\[Neptune.6\] Snapshot cluster Neptunus DB harus dienkripsi saat istirahat](#)
- [\[Neptune.7\] Cluster DB Neptunus harus mengaktifkan otentikasi basis data IAM](#)
- [\[Neptunus.8\] Cluster DB Neptunus harus dikonfigurasi untuk menyalin tag ke snapshot](#)
- [\[Neptunus.9\] Cluster DB Neptunus harus digunakan di beberapa Availability Zone](#)
- [\[NetworkFirewall.1\] Firewall Jaringan harus digunakan di beberapa Availability Zone](#)
- [\[NetworkFirewall.2\] Pencatatan Firewall Jaringan harus diaktifkan](#)
- [\[NetworkFirewall.3\] Kebijakan Network Firewall harus memiliki setidaknya satu kelompok aturan yang terkait](#)
- [\[NetworkFirewall.4\] Tindakan stateless default untuk kebijakan Network Firewall harus drop atau forward untuk paket penuh](#)
- [\[NetworkFirewall.5\] Tindakan stateless default untuk kebijakan Network Firewall harus drop atau forward untuk paket yang terfragmentasi](#)
- [\[NetworkFirewall.6\] Grup aturan Stateless Network Firewall tidak boleh kosong](#)
- [\[NetworkFirewall.7\] Firewall Jaringan harus diberi tag](#)
- [\[NetworkFirewall.8\] Kebijakan firewall Network Firewall harus ditandai](#)
- [\[NetworkFirewall.9\] Firewall Jaringan harus mengaktifkan perlindungan penghapusan](#)
- [\[NetworkFirewall.10\] Firewall Jaringan harus mengaktifkan perlindungan perubahan subnet](#)
- [\[Opensearch.1\] OpenSearch domain harus mengaktifkan enkripsi saat istirahat](#)
- [\[Opensearch.2\] OpenSearch domain tidak boleh diakses publik](#)
- [\[Opensearch.3\] OpenSearch domain harus mengenkripsi data yang dikirim antar node](#)
- [\[Opensearch.4\] login kesalahan OpenSearch domain ke Log harus diaktifkan CloudWatch](#)
- [\[Opensearch.5\] OpenSearch domain harus mengaktifkan pencatatan audit](#)
- [\[Opensearch.6\] OpenSearch domain harus memiliki setidaknya tiga node data](#)

- [\[Opensearch.7\] OpenSearch domain harus mengaktifkan kontrol akses berbutir halus](#)
- [\[Opensearch.8\] Koneksi ke OpenSearch domain harus dienkripsi menggunakan kebijakan keamanan TLS terbaru](#)
- [\[Opensearch.9\] domain harus ditandai OpenSearch](#)
- [\[Opensearch.10\] OpenSearch domain harus menginstal pembaruan perangkat lunak terbaru](#)
- [\[Opensearch.11\] OpenSearch domain harus memiliki setidaknya tiga node primer khusus](#)
- [\[PCA.1\] otoritas sertifikat AWS Private CA root harus dinonaktifkan](#)
- [\[PCA.2\] Otoritas sertifikat CA AWS swasta harus ditandai](#)
- [\[RDS.14\] Cluster Amazon Aurora seharusnya mengaktifkan backtracking](#)
- [\[RDS.16\] Cluster RDS DB harus dikonfigurasi untuk menyalin tag ke snapshot](#)
- [\[RDS.17\] Instans RDS DB harus dikonfigurasi untuk menyalin tag ke snapshot](#)
- [\[RDS.18\] Instans RDS harus digunakan di VPC](#)
- [\[RDS.19\] Langganan pemberitahuan acara RDS yang ada harus dikonfigurasi untuk peristiwa kluster penting](#)
- [\[RDS.20\] Langganan pemberitahuan acara RDS yang ada harus dikonfigurasi untuk peristiwa instance basis data penting](#)
- [\[RDS.21\] Langganan pemberitahuan acara RDS harus dikonfigurasi untuk peristiwa grup parameter basis data penting](#)
- [\[RDS.22\] Langganan pemberitahuan acara RDS harus dikonfigurasi untuk acara grup keamanan basis data penting](#)
- [\[RDS.23\] Instans RDS tidak boleh menggunakan port default mesin database](#)
- [\[RDS.24\] Kluster Database RDS harus menggunakan nama pengguna administrator khusus](#)
- [\[RDS.25\] Instans database RDS harus menggunakan nama pengguna administrator khusus](#)
- [\[RDS.26\] Instans RDS DB harus dilindungi oleh rencana cadangan](#)
- [\[RDS.27\] Cluster RDS DB harus dienkripsi saat istirahat](#)
- [\[RDS.28\] Cluster RDS DB harus ditandai](#)
- [\[RDS.29\] Snapshot cluster RDS DB harus ditandai](#)
- [\[RDS.30\] Instans RDS DB harus ditandai](#)
- [\[RDS.31\] Grup keamanan RDS DB harus ditandai](#)
- [\[RDS.32\] Snapshot RDS DB harus ditandai](#)
- [\[RDS.33\] Grup subnet RDS DB harus ditandai](#)

- [\[RDS.34\] Kluster Aurora MySQL DB harus menerbitkan log audit ke Log CloudWatch](#)
- [\[RDS.35\] Cluster RDS DB harus mengaktifkan peningkatan versi minor otomatis](#)
- [\[RDS.36\] RDS untuk instance PostgreSQL DB harus menerbitkan log ke Log CloudWatch](#)
- [\[RDS.37\] Cluster Aurora PostgreSQL DB harus menerbitkan log ke Log CloudWatch](#)
- [\[RDS.38\] RDS untuk instance PostgreSQL DB harus dienkripsi saat transit](#)
- [\[RDS.39\] RDS untuk instance MySQL DB harus dienkripsi saat transit](#)
- [\[RDS.40\] RDS untuk instance SQL Server DB harus menerbitkan log ke Log CloudWatch](#)
- [\[RDS.41\] RDS untuk instance SQL Server DB harus dienkripsi saat transit](#)
- [\[RDS.42\] RDS untuk instance MariaDB DB harus menerbitkan log ke Log CloudWatch](#)
- [\[RDS.44\] RDS untuk instance MariaDB DB harus dienkripsi saat transit](#)
- [\[Redshift.1\] Cluster Amazon Redshift harus melarang akses publik](#)
- [\[Redshift.2\] Koneksi ke cluster Amazon Redshift harus dienkripsi saat transit](#)
- [\[Redshift.3\] Cluster Amazon Redshift harus mengaktifkan snapshot otomatis](#)
- [\[Redshift.4\] Cluster Amazon Redshift harus mengaktifkan pencatatan audit](#)
- [\[Redshift.6\] Amazon Redshift harus mengaktifkan peningkatan otomatis ke versi utama](#)
- [\[Redshift.7\] Cluster Redshift harus menggunakan perutean VPC yang ditingkatkan](#)
- [\[Redshift.8\] Cluster Amazon Redshift tidak boleh menggunakan nama pengguna Admin default](#)
- [\[Redshift.9\] Cluster Redshift tidak boleh menggunakan nama database default](#)
- [\[Redshift.10\] Cluster Redshift harus dienkripsi saat istirahat](#)
- [\[Redshift.11\] Cluster Redshift harus ditandai](#)
- [\[Redshift.12\] Langganan pemberitahuan acara Redshift harus ditandai](#)
- [\[Redshift.13\] Snapshot cluster Redshift harus ditandai](#)
- [\[Redshift.14\] Grup subnet cluster Redshift harus ditandai](#)
- [\[Redshift.15\] Grup keamanan Redshift harus mengizinkan masuknya port cluster hanya dari asal yang dibatasi](#)
- [\[Redshift.16\] Grup subnet cluster Redshift harus memiliki subnet dari beberapa Availability Zone](#)
- [\[Redshift.17\] Grup parameter cluster Redshift harus ditandai](#)
- [\[RedshiftServerless.1\] Grup kerja Amazon Redshift Tanpa Server harus menggunakan perutean VPC yang disempurnakan](#)
- [\[RedshiftServerless.2\] Koneksi ke grup kerja Redshift Serverless harus diperlukan untuk menggunakan SSL](#)

- [\[RedshiftServerless.3\] Kelompok kerja Redshift Tanpa Server harus melarang akses publik](#)
- [\[RedshiftServerless.4\] Ruang nama Redshift Tanpa Server harus dienkripsi dengan pengelolaan pelanggan AWS KMS keys](#)
- [\[RedshiftServerless.5\] Ruang nama Redshift Tanpa Server tidak boleh menggunakan nama pengguna admin default](#)
- [\[RedshiftServerless.6\] Ruang nama Redshift Tanpa Server harus mengeksport log ke Log CloudWatch](#)
- [\[RedshiftServerless.7\] Ruang nama Redshift Tanpa Server seharusnya tidak menggunakan nama database default](#)
- [\[Route53.1\] Pemeriksaan kesehatan rute 53 harus ditandai](#)
- [\[Route53.2\] Route 53 zona yang dihosting publik harus mencatat kueri DNS](#)
- [\[S3.7\] Ember tujuan umum S3 harus menggunakan replikasi lintas wilayah](#)
- [\[S3.10\] Bucket tujuan umum S3 dengan versi diaktifkan harus memiliki konfigurasi Siklus Hidup](#)
- [\[S3.11\] Bucket tujuan umum S3 harus mengaktifkan pemberitahuan acara](#)
- [\[S3.12\] tidak ACLs boleh digunakan untuk mengelola akses pengguna ke bucket tujuan umum S3](#)
- [\[S3.13\] Bucket tujuan umum S3 harus memiliki konfigurasi Siklus Hidup](#)
- [\[S3.19\] Titik akses S3 harus mengaktifkan pengaturan akses publik blok](#)
- [\[S3.20\] Bucket tujuan umum S3 harus mengaktifkan penghapusan MFA](#)
- [\[S3.22\] Bucket tujuan umum S3 harus mencatat peristiwa penulisan tingkat objek](#)
- [\[S3.23\] Bucket tujuan umum S3 harus mencatat peristiwa pembacaan tingkat objek](#)
- [\[S3.24\] Poin Akses Multi-Wilayah S3 harus mengaktifkan pengaturan akses publik blok](#)
- [\[SageMaker.1\] Instans SageMaker notebook Amazon seharusnya tidak memiliki akses internet langsung](#)
- [\[SageMaker.2\] instance SageMaker notebook harus diluncurkan dalam VPC khusus](#)
- [\[SageMaker.3\] Pengguna seharusnya tidak memiliki akses root ke instance SageMaker notebook](#)
- [\[SageMaker.4\] varian produksi SageMaker titik akhir harus memiliki jumlah instance awal yang lebih besar dari 1](#)
- [\[SageMaker.5\] SageMaker model harus memblokir lalu lintas masuk](#)
- [\[SageMaker.6\] konfigurasi gambar SageMaker aplikasi harus ditandai](#)
- [\[SageMaker.7\] SageMaker gambar harus diberi tag](#)
- [\[SageMaker.8\] instance SageMaker notebook harus berjalan pada platform yang didukung](#)

- [\[SES.1\] Daftar kontak SES harus ditandai](#)
- [\[SES.2\] Set konfigurasi SES harus ditandai](#)
- [\[SecretsManager.5\] Rahasia Secrets Manager harus ditandai](#)
- [\[ServiceCatalog.1\] Portofolio Service Catalog harus dibagikan hanya dalam suatu organisasi AWS](#)
- [\[SNS.3\] Topik SNS harus ditandai](#)
- [\[SNS.4\] Kebijakan akses topik SNS seharusnya tidak mengizinkan akses publik](#)
- [\[SQS.1\] Antrian Amazon SQS harus dienkripsi saat istirahat](#)
- [\[SQS.2\] Antrian SQS harus ditandai](#)
- [\[SQS.3\] Kebijakan akses antrian SQS seharusnya tidak mengizinkan akses publik](#)
- [\[SSM.3\] EC2 Instans Amazon yang dikelola oleh Systems Manager harus memiliki status kepatuhan asosiasi COMPLIANT](#)
- [\[SSM.4\] Dokumen SSM seharusnya tidak bersifat publik](#)
- [\[SSM.5\] Dokumen SSM harus ditandai](#)
- [\[StepFunctions.1\] Mesin status Step Functions seharusnya mengaktifkan logging](#)
- [\[StepFunctions.2\] Aktivitas Step Functions harus diberi tag](#)
- [\[Transfer.1\] AWS Transfer Family alur kerja harus ditandai](#)
- [\[Transfer.2\] Server Transfer Family tidak boleh menggunakan protokol FTP untuk koneksi titik akhir](#)
- [\[Transfer.3\] Konektor Transfer Family seharusnya mengaktifkan logging](#)
- [\[Transfer.4\] Perjanjian Transfer Family harus ditandai](#)
- [\[Transfer.5\] Sertifikat Transfer Family harus diberi tag](#)
- [\[Transfer.6\] Konektor Transfer Family harus diberi tag](#)
- [\[Transfer.7\] Profil Transfer Family harus diberi tag](#)
- [\[WAF.1\] Pencatatan ACL Web Global AWS WAF Klasik harus diaktifkan](#)
- [\[WAF.2\] Aturan Regional AWS WAF Klasik harus memiliki setidaknya satu syarat](#)
- [\[WAF.3\] Kelompok aturan Regional AWS WAF Klasik harus memiliki setidaknya satu aturan](#)
- [\[WAF.4\] Web Regional AWS WAF Klasik ACLs harus memiliki setidaknya satu aturan atau kelompok aturan](#)
- [\[WAF.6\] Aturan global AWS WAF klasik harus memiliki setidaknya satu syarat](#)
- [\[WAF.7\] Kelompok aturan global AWS WAF klasik harus memiliki setidaknya satu aturan](#)
- [\[WAF.8\] Web global AWS WAF klasik ACLs harus memiliki setidaknya satu aturan atau kelompok aturan](#)

- [\[WAF.10\] AWS WAF web ACLs harus memiliki setidaknya satu aturan atau kelompok aturan](#)
- [\[WAF.11\] pencatatan ACL AWS WAF web harus diaktifkan](#)
- [AWS WAF Aturan \[WAF.12\] harus mengaktifkan metrik CloudWatch](#)
- [\[WorkSpaces.1\] volume WorkSpaces pengguna harus dienkripsi saat istirahat](#)
- [\[WorkSpaces.2\] volume WorkSpaces root harus dienkripsi saat istirahat](#)

Asia Pasifik (Tokyo)

Kontrol berikut tidak didukung di Wilayah Asia Pasifik (Tokyo).

- [\[AppSync.1\] Cache AWS AppSync API harus dienkripsi saat istirahat](#)
- [\[AppSync.6\] Cache AWS AppSync API harus dienkripsi saat transit](#)
- [\[CloudFront.1\] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi](#)
- [\[CloudFront.3\] CloudFront distribusi harus memerlukan enkripsi dalam perjalanan](#)
- [\[CloudFront.4\] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi](#)
- [\[CloudFront.5\] CloudFront distribusi seharusnya mengaktifkan logging](#)
- [\[CloudFront.6\] CloudFront distribusi harus mengaktifkan WAF](#)
- [\[CloudFront.7\] CloudFront distribusi harus menggunakan sertifikat SSL/TLS khusus](#)
- [\[CloudFront.8\] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS](#)
- [\[CloudFront.9\] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus](#)
- [\[CloudFront.10\] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal kustom](#)
- [\[CloudFront.12\] CloudFront distribusi seharusnya tidak menunjukkan asal S3 yang tidak ada](#)
- [\[CloudFront.13\] CloudFront distribusi harus menggunakan kontrol akses asal](#)
- [\[CloudFront.14\] CloudFront distribusi harus ditandai](#)
- [\[EC2.173\] Permintaan Armada EC2 Spot harus mengaktifkan enkripsi untuk volume EBS terlampir](#)
- [\[ECR.4\] Repositori publik ECR harus ditandai](#)
- [\[FraudDetector.1\] Jenis entitas Amazon Fraud Detector harus diberi tag](#)
- [\[FraudDetector.2\] Label Amazon Fraud Detector harus diberi tag](#)
- [\[FraudDetector.3\] Hasil Amazon Fraud Detector harus ditandai](#)
- [\[FraudDetector.4\] Variabel Amazon Fraud Detector harus diberi tag](#)

- [\[GlobalAccelerator.1\]](#) Akselerator Akselerator Global harus diberi tag
- [\[IAM.26\]](#) Sertifikat SSL/TLS kedaluwarsa yang dikelola di IAM harus dihapus
- [\[IoT Twin Maker.4\]](#) Entitas AWS IoT harus diberi tag TwinMaker
- [\[Route53.1\]](#) Pemeriksaan kesehatan rute 53 harus ditandai
- [\[Route53.2\]](#) Route 53 zona yang dihosting publik harus mencatat kueri DNS
- [\[S3.24\]](#) Poin Akses Multi-Wilayah S3 harus mengaktifkan pengaturan akses publik blok
- [\[WAF.1\]](#) Pencatatan ACL Web Global AWS WAF Klasik harus diaktifkan
- [\[WAF.6\]](#) Aturan global AWS WAF klasik harus memiliki setidaknya satu syarat
- [\[WAF.7\]](#) Kelompok aturan global AWS WAF klasik harus memiliki setidaknya satu aturan
- [\[WAF.8\]](#) Web global AWS WAF klasik ACLs harus memiliki setidaknya satu aturan atau kelompok aturan

Kanada (Pusat)

Kontrol berikut tidak didukung di Wilayah Kanada (Tengah).

- [\[AppRunner.1\]](#) Layanan App Runner harus diberi tag
- [\[AppRunner.2\]](#) Konektor VPC App Runner harus diberi tag
- [\[AppSync.1\]](#) Cache AWS AppSync API harus dienkrpsi saat istirahat
- [\[AppSync.6\]](#) Cache AWS AppSync API harus dienkrpsi saat transit
- [\[CloudFront.1\]](#) CloudFront distribusi harus memiliki objek root default yang dikonfigurasi
- [\[CloudFront.3\]](#) CloudFront distribusi harus memerlukan enkripsi dalam perjalanan
- [\[CloudFront.4\]](#) CloudFront distribusi harus memiliki failover asal yang dikonfigurasi
- [\[CloudFront.5\]](#) CloudFront distribusi seharusnya mengaktifkan logging
- [\[CloudFront.6\]](#) CloudFront distribusi harus mengaktifkan WAF
- [\[CloudFront.7\]](#) CloudFront distribusi harus menggunakan sertifikat SSL/TLS khusus
- [\[CloudFront.8\]](#) CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS
- [\[CloudFront.9\]](#) CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus
- [\[CloudFront.10\]](#) CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal kustom
- [\[CloudFront.12\]](#) CloudFront distribusi seharusnya tidak menunjukkan asal S3 yang tidak ada
- [\[CloudFront.13\]](#) CloudFront distribusi harus menggunakan kontrol akses asal

- [\[CloudFront.14\] CloudFront distribusi harus ditandai](#)
- [\[CodeArtifact.1\] CodeArtifact repositori harus ditandai](#)
- [\[CodeGuruProfiler.1\] Grup CodeGuru profil profiler harus diberi tag](#)
- [\[CodeGuruReviewer.1\] Asosiasi CodeGuru repositori peninjau harus diberi tag](#)
- [\[DynamoDB.3\] Cluster DynamoDB Accelerator \(DAX\) harus dienkripsi saat istirahat](#)
- [\[DynamoDB.7\] Cluster DynamoDB Accelerator harus dienkripsi saat transit](#)
- [\[EC2.24\] Jenis instance EC2 paravirtual Amazon tidak boleh digunakan](#)
- [\[EC2.173\] Permintaan Armada EC2 Spot harus mengaktifkan enkripsi untuk volume EBS terlampir](#)
- [\[ECR.4\] Repositori publik ECR harus ditandai](#)
- [\[FraudDetector.1\] Jenis entitas Amazon Fraud Detector harus diberi tag](#)
- [\[FraudDetector.2\] Label Amazon Fraud Detector harus diberi tag](#)
- [\[FraudDetector.3\] Hasil Amazon Fraud Detector harus ditandai](#)
- [\[FraudDetector.4\] Variabel Amazon Fraud Detector harus diberi tag](#)
- [\[GlobalAccelerator.1\] Akselerator Akselerator Global harus diberi tag](#)
- [\[IAM.26\] Sertifikat SSL/TLS kedaluwarsa yang dikelola di IAM harus dihapus](#)
- [\[Inspektor.3\] Pemindaian kode Amazon Inspector Lambda harus diaktifkan](#)
- [\[IoT Twin Maker.1\] Pekerjaan sinkronisasi AWS IoT harus ditandai TwinMaker](#)
- [\[IoT Twin Maker.2\] Ruang kerja AWS IoT harus diberi tag TwinMaker](#)
- [\[IoT Twin Maker.3\] Adegan AWS IoT harus diberi tag TwinMaker](#)
- [\[IoT Twin Maker.4\] Entitas AWS IoT harus diberi tag TwinMaker](#)
- [\[IoT Wireless .1\] Grup multicast Nirkabel AWS IoT harus diberi tag](#)
- [\[IoT Wireless .2\] Profil layanan AWS IoT Wireless harus diberi tag](#)
- [\[IoT Wireless .3\] Tugas AWS IoT FUOTA harus ditandai](#)
- [\[IVS.1\] Pasangan kunci pemutaran IVS harus ditandai](#)
- [\[IVS.2\] Konfigurasi perekaman IVS harus ditandai](#)
- [\[IVS.3\] Saluran IVS harus ditandai](#)
- [\[Kinesis.3\] Aliran kinesis harus memiliki periode retensi data yang memadai](#)
- [\[RDS.31\] Grup keamanan RDS DB harus ditandai](#)
- [\[Route53.1\] Pemeriksaan kesehatan rute 53 harus ditandai](#)
- [\[Route53.2\] Route 53 zona yang dihosting publik harus mencatat kueri DNS](#)

- [\[S3.24\] Poin Akses Multi-Wilayah S3 harus mengaktifkan pengaturan akses publik blok](#)
- [\[WAF.1\] Pencatatan ACL Web Global AWS WAF Klasik harus diaktifkan](#)
- [\[WAF.6\] Aturan global AWS WAF klasik harus memiliki setidaknya satu syarat](#)
- [\[WAF.7\] Kelompok aturan global AWS WAF klasik harus memiliki setidaknya satu aturan](#)
- [\[WAF.8\] Web global AWS WAF klasik ACLs harus memiliki setidaknya satu aturan atau kelompok aturan](#)

Kanada Barat (Calgary)

Kontrol berikut tidak didukung di Wilayah Kanada Barat (Calgary).

- [\[ACM.1\] Sertifikat yang diimpor dan diterbitkan ACM harus diperbarui setelah jangka waktu tertentu](#)
- [\[ACM.2\] Sertifikat RSA yang dikelola oleh ACM harus menggunakan panjang kunci minimal 2.048 bit](#)
- [\[Akun.1\] Informasi kontak keamanan harus disediakan untuk Akun AWS](#)
- [\[Akun.2\] Akun AWS harus menjadi bagian dari organisasi AWS Organizations](#)
- [\[APIGateway.8\] Rute API Gateway harus menentukan jenis otorisasi](#)
- [\[APIGateway.9\] Pencatatan akses harus dikonfigurasi untuk Tahap API Gateway V2](#)
- [\[Amplify.1\] Aplikasi Amplify harus diberi tag](#)
- [\[Amplify.2\] Amplify branch harus diberi tag](#)
- [\[AppConfig.1\] AWS AppConfig aplikasi harus diberi tag](#)
- [\[AppConfig.2\] profil AWS AppConfig konfigurasi harus ditandai](#)
- [\[AppConfig.3\] AWS AppConfig lingkungan harus ditandai](#)
- [\[AppConfig.4\] asosiasi AWS AppConfig ekstensi harus ditandai](#)
- [\[AppFlow.1\] AppFlow Aliran Amazon harus ditandai](#)
- [\[AppRunner.1\] Layanan App Runner harus diberi tag](#)
- [\[AppRunner.2\] Konektor VPC App Runner harus diberi tag](#)
- [\[AppSync.1\] Cache AWS AppSync API harus dienkrpsi saat istirahat](#)
- [\[AppSync.2\] AWS AppSync harus mengaktifkan logging tingkat lapangan](#)
- [\[AppSync.4\] AWS AppSync APIs GraphQL harus diberi tag](#)
- [\[AppSync.5\] AWS AppSync APIs GraphQL tidak boleh diautentikasi dengan kunci API](#)
- [\[AppSync.6\] Cache AWS AppSync API harus dienkrpsi saat transit](#)

- [\[Athena.4\] Kelompok kerja Athena seharusnya mengaktifkan logging](#)
- [\[AutoScaling.2\] Grup EC2 Auto Scaling Amazon harus mencakup beberapa Availability Zone](#)
- [\[AutoScaling.3\] Konfigurasi peluncuran grup Auto Scaling harus EC2 mengonfigurasi instance agar memerlukan Layanan Metadata Instance Versi 2 \(\) IMDSv2](#)
- [\[AutoScaling.6\] Grup Auto Scaling harus menggunakan beberapa jenis instance di beberapa Availability Zone](#)
- [\[AutoScaling.9\] Grup EC2 Auto Scaling Amazon harus menggunakan templat peluncuran Amazon EC2](#)
- [\[Backup.1\] titik AWS Backup pemulihan harus dienkripsi saat istirahat](#)
- [\[Backup.4\] rencana AWS Backup laporan harus ditandai](#)
- [\[Batch.1\] Antrian pekerjaan batch harus ditandai](#)
- [\[Batch.3\] Lingkungan komputasi Batch harus ditandai](#)
- [\[Batch.4\] Properti sumber daya komputasi di lingkungan komputasi Batch terkelola harus ditandai](#)
- [\[CloudFront.1\] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi](#)
- [\[CloudFront.3\] CloudFront distribusi harus memerlukan enkripsi dalam perjalanan](#)
- [\[CloudFront.4\] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi](#)
- [\[CloudFront.5\] CloudFront distribusi seharusnya mengaktifkan logging](#)
- [\[CloudFront.6\] CloudFront distribusi harus mengaktifkan WAF](#)
- [\[CloudFront.7\] CloudFront distribusi harus menggunakan sertifikat SSL/TLS khusus](#)
- [\[CloudFront.8\] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS](#)
- [\[CloudFront.9\] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus](#)
- [\[CloudFront.10\] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal kustom](#)
- [\[CloudFront.12\] CloudFront distribusi seharusnya tidak menunjukkan asal S3 yang tidak ada](#)
- [\[CloudFront.13\] CloudFront distribusi harus menggunakan kontrol akses asal](#)
- [\[CloudFront.14\] CloudFront distribusi harus ditandai](#)
- [\[CloudTrail.6\] Pastikan bucket S3 yang digunakan untuk menyimpan CloudTrail log tidak dapat diakses publik](#)
- [\[CloudTrail.7\] Pastikan pencatatan akses bucket S3 diaktifkan pada bucket CloudTrail S3](#)
- [\[CloudTrail.10\] Penyimpanan data acara CloudTrail danau harus dienkripsi dengan pelanggan yang dikelola AWS KMS keys](#)

- [\[CloudWatch.17\] tindakan CloudWatch alarm harus diaktifkan](#)
- [\[CodeArtifact.1\] CodeArtifact repositori harus ditandai](#)
- [\[CodeBuild.1\] Repositori sumber CodeBuild Bitbucket tidak URLs boleh berisi kredensial sensitif](#)
- [\[CodeBuild.2\] variabel lingkungan CodeBuild proyek tidak boleh berisi kredensial teks yang jelas](#)
- [\[CodeBuild.3\] Log CodeBuild S3 harus dienkripsi](#)
- [\[CodeBuild.4\] lingkungan CodeBuild proyek harus memiliki urasi logging AWS Config](#)
- [\[CodeBuild.7\] ekspor kelompok CodeBuild laporan harus dienkripsi saat istirahat](#)
- [\[CodeGuruProfiler.1\] Grup CodeGuru profil profiler harus diberi tag](#)
- [\[CodeGuruReviewer.1\] Asosiasi CodeGuru repositori peninjau harus diberi tag](#)
- [\[Cognito.1\] Kumpulan pengguna Cognito harus mengaktifkan perlindungan ancaman dengan mode penegakan fungsi penuh untuk otentikasi standar](#)
- [\[Connect.1\] Jenis objek Amazon Connect Customer Profiles harus diberi tag](#)
- [\[Connect.2\] Instans Amazon Connect seharusnya mengaktifkan logging CloudWatch](#)
- [\[DataFirehose.1\] Aliran pengiriman Firehose harus dienkripsi saat istirahat](#)
- [\[DataSync.1\] DataSync tugas harus mengaktifkan logging](#)
- [\[Detective.1\] Grafik perilaku detektif harus diberi tag](#)
- [\[DMS.2\] Sertifikat DMS harus ditandai](#)
- [\[DMS.3\] Langganan acara DMS harus ditandai](#)
- [\[DMS.4\] Contoh replikasi DMS harus ditandai](#)
- [\[DMS.5\] Grup subnet replikasi DMS harus ditandai](#)
- [\[DMS.6\] Instans replikasi DMS harus mengaktifkan peningkatan versi minor otomatis](#)
- [\[DMS.7\] Tugas replikasi DMS untuk database target seharusnya mengaktifkan logging](#)
- [\[DMS.8\] Tugas replikasi DMS untuk database sumber seharusnya mengaktifkan logging](#)
- [\[DMS.9\] Titik akhir DMS harus menggunakan SSL](#)
- [\[DMS.10\] Titik akhir DMS untuk database Neptune harus mengaktifkan otorisasi IAM](#)
- [\[DMS.11\] Titik akhir DMS untuk MongoDB harus mengaktifkan mekanisme otentikasi](#)
- [\[DMS.12\] Titik akhir DMS untuk Redis OSS seharusnya mengaktifkan TLS](#)
- [\[DocumentDB.1\] Cluster Amazon DocumentDB harus dienkripsi saat istirahat](#)
- [\[DocumentDB.2\] Cluster Amazon DocumentDB harus memiliki periode retensi cadangan yang memadai](#)
- [\[DocumentDB.3\] Cuplikan cluster manual Amazon DocumentDB seharusnya tidak bersifat publik](#)

- [\[DocumentDB.4\] Cluster Amazon DocumentDB harus mempublikasikan log audit ke Log CloudWatch](#)
- [\[DocumentDB.5\] Cluster Amazon DocumentDB harus mengaktifkan perlindungan penghapusan](#)
- [\[DocumentDB.6\] Cluster Amazon DocumentDB harus dienkripsi saat transit](#)
- [\[DynamoDB.3\] Cluster DynamoDB Accelerator \(DAX\) harus dienkripsi saat istirahat](#)
- [\[DynamoDB.4\] Tabel DynamoDB harus ada dalam rencana cadangan](#)
- [\[DynamoDB.6\] Tabel DynamoDB harus mengaktifkan perlindungan penghapusan](#)
- [\[DynamoDB.7\] Cluster DynamoDB Accelerator harus dienkripsi saat transit](#)
- [\[EC2.4\] EC2 Instans yang dihentikan harus dihapus setelah periode waktu tertentu](#)
- [\[EC2.21\] Jaringan ACLs seharusnya tidak mengizinkan masuknya dari 0.0.0.0/0 ke port 22 atau port 3389.](#)
- [\[EC2.22\] Grup EC2 keamanan Amazon yang tidak digunakan harus dihapus](#)
- [\[EC2.23\] Amazon EC2 Transit Gateways seharusnya tidak secara otomatis menerima permintaan lampiran VPC](#)
- [\[EC2.24\] Jenis instance EC2 paravirtual Amazon tidak boleh digunakan](#)
- [\[EC2.25\] Templat EC2 peluncuran Amazon tidak boleh menetapkan publik IPs ke antarmuka jaringan](#)
- [\[EC2.28\] Volume EBS harus dicakup oleh rencana cadangan](#)
- [\[EC2.33\] lampiran gateway EC2 transit harus ditandai](#)
- [\[EC2.34\] tabel rute gateway EC2 transit harus ditandai](#)
- [\[EC2.40\] Gateway EC2 NAT harus ditandai](#)
- [\[EC2.48\] Log aliran VPC Amazon harus diberi tag](#)
- [\[EC2.51\] Titik akhir EC2 Client VPN harus mengaktifkan pencatatan koneksi klien](#)
- [\[EC2.53\] grup EC2 keamanan seharusnya tidak mengizinkan masuknya dari 0.0.0.0/0 ke port administrasi server jarak jauh](#)
- [\[EC2.54\] grup EC2 keamanan tidak boleh mengizinkan masuknya dari: :/0 ke port administrasi server jarak jauh](#)
- [\[EC2.55\] VPCs harus dikonfigurasi dengan titik akhir antarmuka untuk ECR API](#)
- [\[EC2.56\] VPCs harus dikonfigurasi dengan titik akhir antarmuka untuk Docker Registry](#)
- [\[EC2.57\] VPCs harus dikonfigurasi dengan titik akhir antarmuka untuk Systems Manager](#)
- [\[EC2.58\] VPCs harus dikonfigurasi dengan titik akhir antarmuka untuk Kontak Manajer Insiden Systems Manager](#)

- [\[EC2.60\] VPCs harus dikonfigurasi dengan titik akhir antarmuka untuk Systems Manager Incident Manager](#)
- [\[EC2.170\] templat EC2 peluncuran harus menggunakan Layanan Metadata Instance Versi 2 \(\) IMDSv2](#)
- [\[EC2.171\] Koneksi EC2 VPN seharusnya mengaktifkan logging](#)
- [\[EC2.173\] Permintaan Armada EC2 Spot harus mengaktifkan enkripsi untuk volume EBS terlampir](#)
- [\[EC2.175\] templat EC2 peluncuran harus diberi tag](#)
- [\[EC2.177\] Sesi cermin EC2 lalu lintas harus ditandai](#)
- [\[EC2.179\] Target cermin EC2 lalu lintas harus ditandai](#)
- [\[ECR.1\] Repositori pribadi ECR harus memiliki pemindaian gambar yang dikonfigurasi](#)
- [\[ECR.2\] Repositori pribadi ECR harus memiliki kekekalan tag yang dikonfigurasi](#)
- [\[ECR.3\] Repositori ECR harus memiliki setidaknya satu kebijakan siklus hidup yang dikonfigurasi](#)
- [\[ECR.4\] Repositori publik ECR harus ditandai](#)
- [\[ECR.5\] Repositori ECR harus dienkripsi dengan pelanggan yang dikelola AWS KMS keys](#)
- [\[ECS.3\] Definisi tugas ECS tidak boleh membagikan namespace proses host](#)
- [\[ECS.4\] Kontainer ECS harus berjalan sebagai non-hak istimewa](#)
- [\[ECS.5\] Wadah ECS harus dibatasi pada akses hanya-baca ke sistem file root](#)
- [\[ECS.8\] Rahasia tidak boleh diteruskan sebagai variabel lingkungan kontainer](#)
- [\[ECS.9\] Definisi tugas ECS harus memiliki konfigurasi logging](#)
- [\[ECS.10\] Layanan ECS Fargate harus berjalan pada versi platform Fargate terbaru](#)
- [\[ECS.12\] Cluster ECS harus menggunakan Wawasan Kontainer](#)
- [\[ECS.16\] Set tugas ECS seharusnya tidak secara otomatis menetapkan alamat IP publik](#)
- [\[ECS.17\] Definisi tugas ECS tidak boleh menggunakan mode jaringan host](#)
- [\[EFS.1\] Sistem File Elastis harus dikonfigurasi untuk mengenkripsi data file saat istirahat menggunakan AWS KMS](#)
- [\[EFS.2\] Volume Amazon EFS harus dalam rencana cadangan](#)
- [\[EFS.3\] Titik akses EFS harus menegakkan direktori root](#)
- [\[EFS.4\] Titik akses EFS harus menegakkan identitas pengguna](#)
- [\[EFS.6\] Target pemasangan EFS tidak boleh dikaitkan dengan subnet publik](#)
- [\[EFS.7\] Sistem file EFS harus mengaktifkan pencadangan otomatis](#)
- [\[EFS.8\] Sistem file EFS harus dienkripsi saat istirahat](#)

- [\[EKS.2\] Kluster EKS harus berjalan pada versi Kubernetes yang didukung](#)
- [\[EKS.3\] Kluster EKS harus menggunakan rahasia Kubernetes terenkripsi](#)
- [\[EKS.6\] Kluster EKS harus ditandai](#)
- [\[EKS.7\] Konfigurasi penyedia identitas EKS harus ditandai](#)
- [\[EKS.8\] Kluster EKS harus mengaktifkan pencatatan audit](#)
- [\[ELB.2\] Classic Load Balancer dengan pendengar SSL/HTTPS harus menggunakan sertifikat yang disediakan oleh AWS Certificate Manager](#)
- [\[ELB.10\] Classic Load Balancer harus menjangkau beberapa Availability Zone](#)
- [\[ELB.12\] Application Load Balancer harus dikonfigurasi dengan mode mitigasi desync defensif atau paling ketat](#)
- [\[ELB.13\] Penyeimbang Beban Aplikasi, Jaringan, dan Gateway harus mencakup beberapa Availability Zone](#)
- [\[ELB.14\] Classic Load Balancer harus dikonfigurasi dengan mode mitigasi desync defensif atau paling ketat](#)
- [\[ELB.17\] Aplikasi dan Penyeimbang Beban Jaringan dengan pendengar harus menggunakan kebijakan keamanan yang direkomendasikan](#)
- [\[ElastiCache.1\] Cluster ElastiCache \(Redis OSS\) harus mengaktifkan pencadangan otomatis](#)
- [\[ElastiCache.2\] ElastiCache cluster harus mengaktifkan peningkatan versi minor otomatis](#)
- [\[ElastiCache.3\] grup ElastiCache replikasi harus mengaktifkan failover otomatis](#)
- [\[ElastiCache.4\] grup ElastiCache replikasi harus dienkripsi saat istirahat](#)
- [\[ElastiCache.5\] grup ElastiCache replikasi harus dienkripsi saat transit](#)
- [\[ElastiCache.6\] ElastiCache \(Redis OSS\) grup replikasi dari versi sebelumnya harus mengaktifkan Redis OSS AUTH](#)
- [\[ElastiCache.7\] ElastiCache cluster tidak boleh menggunakan grup subnet default](#)
- [\[ElasticBeanstalk.1\] Lingkungan Elastic Beanstalk seharusnya mengaktifkan pelaporan kesehatan yang ditingkatkan](#)
- [\[ElasticBeanstalk.2\] Pembaruan platform yang dikelola Elastic Beanstalk harus diaktifkan](#)
- [\[ElasticBeanstalk.3\] Elastic Beanstalk harus mengalirkan log ke CloudWatch](#)
- [\[EMR.1\] Node primer kluster EMR Amazon seharusnya tidak memiliki alamat IP publik](#)
- [\[EMR.2\] Pengaturan akses publik blok EMR Amazon harus diaktifkan](#)
- [\[EMR.3\] Konfigurasi keamanan Amazon EMR harus dienkripsi saat istirahat](#)
- [\[ES.3\] Domain Elasticsearch harus mengenkripsi data yang dikirim antar node](#)

- [\[ES.4\] Kesalahan domain Elasticsearch yang masuk ke CloudWatch Log harus diaktifkan](#)
- [\[EventBridge.3\] bus acara EventBridge khusus harus memiliki kebijakan berbasis sumber daya terlampir](#)
- [\[EventBridge.4\] titik akhir EventBridge global harus mengaktifkan replikasi acara](#)
- [\[FraudDetector.1\] Jenis entitas Amazon Fraud Detector harus diberi tag](#)
- [\[FraudDetector.2\] Label Amazon Fraud Detector harus diberi tag](#)
- [\[FraudDetector.3\] Hasil Amazon Fraud Detector harus ditandai](#)
- [\[FraudDetector.4\] Variabel Amazon Fraud Detector harus diberi tag](#)
- [\[FSx.1\] FSx untuk sistem file OpenZFS harus dikonfigurasi untuk menyalin tag ke cadangan dan volume](#)
- [\[FSx.2\] FSx untuk sistem file Lustre harus dikonfigurasi untuk menyalin tag ke cadangan](#)
- [\[FSx.3\] FSx untuk sistem file OpenZFS harus dikonfigurasi untuk penyebaran Multi-AZ](#)
- [\[FSx.4\] FSx untuk sistem file NetApp ONTAP harus dikonfigurasi untuk penyebaran Multi-AZ](#)
- [\[FSx.5\] FSx untuk sistem file Windows File Server harus dikonfigurasi untuk penyebaran Multi-AZ](#)
- [\[GlobalAccelerator.1\] Akselerator Akselerator Global harus diberi tag](#)
- [\[Glue.3\] transformasi pembelajaran AWS Glue mesin harus dienkripsi saat istirahat](#)
- [\[Glue.4\] Pekerjaan AWS Glue percikan harus berjalan pada versi yang didukung AWS Glue](#)
- [\[GuardDuty.2\] GuardDuty filter harus diberi tag](#)
- [\[GuardDuty.3\] GuardDuty IPSets harus ditandai](#)
- [\[GuardDuty.5\] Pemantauan Log Audit GuardDuty EKS harus diaktifkan](#)
- [\[GuardDuty.6\] Perlindungan GuardDuty Lambda harus diaktifkan](#)
- [\[GuardDuty.7\] GuardDuty EKS Runtime Monitoring harus diaktifkan](#)
- [\[GuardDuty.8\] Perlindungan GuardDuty Malware untuk EC2 harus diaktifkan](#)
- [\[GuardDuty.9\] Perlindungan GuardDuty RDS harus diaktifkan](#)
- [\[GuardDuty.10\] Perlindungan GuardDuty S3 harus diaktifkan](#)
- [\[GuardDuty.11\] GuardDuty Runtime Monitoring harus diaktifkan](#)
- [\[GuardDuty.12\] GuardDuty ECS Runtime Monitoring harus diaktifkan](#)
- [\[GuardDuty.13\] GuardDuty EC2 Runtime Monitoring harus diaktifkan](#)
- [\[IAM.1\] Kebijakan IAM seharusnya tidak mengizinkan hak administratif “*” penuh](#)
- [\[IAM.2\] Pengguna IAM seharusnya tidak memiliki kebijakan IAM yang dilampirkan](#)
- [\[IAM.3\] Kunci akses pengguna IAM harus diputar setiap 90 hari atau kurang](#)

- [\[IAM.4\] Kunci akses pengguna root IAM seharusnya tidak ada](#)
- [\[IAM.5\] MFA harus diaktifkan untuk semua pengguna IAM yang memiliki kata sandi konsol](#)
- [\[IAM.6\] MFA perangkat keras harus diaktifkan untuk pengguna root](#)
- [\[IAM.7\] Kebijakan kata sandi untuk pengguna IAM harus memiliki konfigurasi yang kuat](#)
- [\[IAM.8\] Kredensi pengguna IAM yang tidak digunakan harus dihapus](#)
- [\[IAM.9\] MFA harus diaktifkan untuk pengguna root](#)
- [\[IAM.10\] Kebijakan kata sandi untuk pengguna IAM harus memiliki konfigurasi yang kuat](#)
- [\[IAM.11\] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu huruf besar](#)
- [\[IAM.12\] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu huruf kecil](#)
- [\[IAM.13\] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu simbol](#)
- [\[IAM.14\] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu nomor](#)
- [\[IAM.15\] Pastikan kebijakan kata sandi IAM membutuhkan panjang kata sandi minimum 14 atau lebih](#)
- [\[IAM.16\] Pastikan kebijakan kata sandi IAM mencegah penggunaan kembali kata sandi](#)
- [\[IAM.17\] Pastikan kebijakan kata sandi IAM kedaluwarsa kata sandi dalam waktu 90 hari atau kurang](#)
- [\[IAM.18\] Memastikan peran dukungan telah dibuat untuk mengelola insiden dengan AWS Dukungan](#)
- [\[IAM.19\] MFA harus diaktifkan untuk semua pengguna IAM](#)
- [\[IAM.21\] Kebijakan terkelola pelanggan IAM yang Anda buat seharusnya tidak mengizinkan tindakan wildcard untuk layanan](#)
- [\[IAM.22\] Kredensi pengguna IAM yang tidak digunakan selama 45 hari harus dihapus](#)
- [\[IAM.24\] Peran IAM harus ditandai](#)
- [\[IAM.25\] Pengguna IAM harus diberi tag](#)
- [\[IAM.26\] Sertifikat SSL/TLS kedaluwarsa yang dikelola di IAM harus dihapus](#)
- [\[IAM.27\] Identitas IAM seharusnya tidak memiliki kebijakan yang dilampirkan AWS Cloud Shell Full Access](#)
- [\[IAM.28\] IAM Access Analyzer penganalisis akses eksternal harus diaktifkan](#)
- [\[Inspektor.1\] Pemindaian Amazon Inspector harus diaktifkan EC2](#)
- [\[Inspektor.2\] Pemindaian ECR Amazon Inspector harus diaktifkan](#)
- [\[Inspektor.3\] Pemindaian kode Amazon Inspector Lambda harus diaktifkan](#)

- [\[Inspektor.4\] Pemindaian standar Amazon Inspector Lambda harus diaktifkan](#)
- [\[IoT.1\] profil AWS IoT Device Defender keamanan harus ditandai](#)
- [\[IoT.2\] tindakan AWS IoT Core mitigasi harus ditandai](#)
- [AWS IoT Core Dimensi \[IoT.3\] harus ditandai](#)
- [\[IoT.4\] AWS IoT Core otorisasi harus diberi tag](#)
- [\[IoT.5\] alias AWS IoT Core peran harus ditandai](#)
- [AWS IoT Core Kebijakan \[IoT.6\] harus ditandai](#)
- [\[IoT Events .1\] Input Peristiwa AWS IoT harus diberi tag](#)
- [\[IoT Events .2\] Model detektor Acara AWS IoT harus diberi tag](#)
- [\[IoT Events .3\] Model alarm AWS IoT Events harus diberi tag](#)
- [\[IoT Site Wise.1\] Model aset AWS IoT harus ditandai SiteWise](#)
- [\[IoT Site Wise.2\] Dasbor AWS IoT harus diberi tag SiteWise](#)
- [\[IoT Site Wise.3\] Gateway AWS IoT harus diberi tag SiteWise](#)
- [\[IoT Site Wise.4\] Portal AWS IoT harus diberi tag SiteWise](#)
- [\[IoT Site Wise.5\] Proyek AWS IoT harus diberi tag SiteWise](#)
- [\[IoT Twin Maker.1\] Pekerjaan sinkronisasi AWS IoT harus ditandai TwinMaker](#)
- [\[IoT Twin Maker.2\] Ruang kerja AWS IoT harus diberi tag TwinMaker](#)
- [\[IoT Twin Maker.3\] Adegan AWS IoT harus diberi tag TwinMaker](#)
- [\[IoT Twin Maker.4\] Entitas AWS IoT harus diberi tag TwinMaker](#)
- [\[IoT Wireless .1\] Grup multicast Nirkabel AWS IoT harus diberi tag](#)
- [\[IoT Wireless .2\] Profil layanan AWS IoT Wireless harus diberi tag](#)
- [\[IoT Wireless .3\] Tugas AWS IoT FUOTA harus ditandai](#)
- [\[IVS.1\] Pasangan kunci pemutaran IVS harus ditandai](#)
- [\[IVS.2\] Konfigurasi perekaman IVS harus ditandai](#)
- [\[IVS.3\] Saluran IVS harus ditandai](#)
- [\[Keyspaces.1\] Ruang kunci Amazon Keyspaces harus diberi tag](#)
- [\[Kinesis.1\] Aliran kinesis harus dienkripsi saat istirahat](#)
- [\[Kinesis.2\] Aliran kinesis harus ditandai](#)
- [\[Kinesis.3\] Aliran kinesis harus memiliki periode retensi data yang memadai](#)
- [\[KMS.1\] Kebijakan yang dikelola pelanggan IAM tidak boleh mengizinkan tindakan dekripsi pada semua kunci KMS](#)

- [\[KMS.2\] Prinsipal IAM tidak boleh memiliki kebijakan inline IAM yang memungkinkan tindakan dekripsi pada semua kunci KMS](#)
- [\[KMS.5\] Kunci KMS tidak boleh diakses publik](#)
- [\[Lambda.5\] Fungsi VPC Lambda harus beroperasi di beberapa Availability Zone](#)
- [\[Macie.1\] Amazon Macie harus diaktifkan](#)
- [\[Macie.2\] Penemuan data sensitif otomatis Macie harus diaktifkan](#)
- [\[MQ.2\] Broker ActiveMQ harus mengalirkan log audit ke CloudWatch](#)
- [\[MQ.3\] Broker Amazon MQ harus mengaktifkan peningkatan versi minor otomatis](#)
- [\[MQ.4\] Broker Amazon MQ harus diberi tag](#)
- [\[MQ.5\] Broker ActiveMQ harus menggunakan mode penerapan aktif/siaga](#)
- [\[MQ.6\] Broker RabbitMQ harus menggunakan mode penerapan cluster](#)
- [\[MSK.1\] Kluster MSK harus dienkripsi saat transit di antara node broker](#)
- [\[MSK.2\] Kluster MSK seharusnya telah meningkatkan pemantauan yang dikonfigurasi](#)
- [\[MSK.3\] Konektor MSK Connect harus dienkripsi saat transit](#)
- [\[Neptunus.1\] Cluster DB Neptunus harus dienkripsi saat istirahat](#)
- [\[Neptune.2\] Cluster DB Neptunus harus menerbitkan log audit ke Log CloudWatch](#)
- [\[Neptune.3\] Snapshot cluster Neptunus DB seharusnya tidak publik](#)
- [\[Neptunus.4\] Cluster DB Neptunus harus mengaktifkan perlindungan penghapusan](#)
- [\[Neptunus.5\] Cluster DB Neptunus harus mengaktifkan cadangan otomatis](#)
- [\[Neptune.6\] Snapshot cluster Neptunus DB harus dienkripsi saat istirahat](#)
- [\[Neptune.7\] Cluster DB Neptunus harus mengaktifkan otentikasi basis data IAM](#)
- [\[Neptunus.8\] Cluster DB Neptunus harus dikonfigurasi untuk menyalin tag ke snapshot](#)
- [\[Neptunus.9\] Cluster DB Neptunus harus digunakan di beberapa Availability Zone](#)
- [\[NetworkFirewall.1\] Firewall Jaringan harus digunakan di beberapa Availability Zone](#)
- [\[NetworkFirewall.2\] Pencatatan Firewall Jaringan harus diaktifkan](#)
- [\[NetworkFirewall.3\] Kebijakan Network Firewall harus memiliki setidaknya satu kelompok aturan yang terkait](#)
- [\[NetworkFirewall.4\] Tindakan stateless default untuk kebijakan Network Firewall harus drop atau forward untuk paket penuh](#)
- [\[NetworkFirewall.5\] Tindakan stateless default untuk kebijakan Network Firewall harus drop atau forward untuk paket yang terfragmentasi](#)

- [\[NetworkFirewall.6\] Grup aturan Stateless Network Firewall tidak boleh kosong](#)
- [\[NetworkFirewall.9\] Firewall Jaringan harus mengaktifkan perlindungan penghapusan](#)
- [\[NetworkFirewall.10\] Firewall Jaringan harus mengaktifkan perlindungan perubahan subnet](#)
- [\[Opensearch.1\] OpenSearch domain harus mengaktifkan enkripsi saat istirahat](#)
- [\[Opensearch.2\] OpenSearch domain tidak boleh diakses publik](#)
- [\[Opensearch.3\] OpenSearch domain harus mengenkripsi data yang dikirim antar node](#)
- [\[Opensearch.4\] login kesalahan OpenSearch domain ke Log harus diaktifkan CloudWatch](#)
- [\[Opensearch.5\] OpenSearch domain harus mengaktifkan pencatatan audit](#)
- [\[Opensearch.6\] OpenSearch domain harus memiliki setidaknya tiga node data](#)
- [\[Opensearch.7\] OpenSearch domain harus mengaktifkan kontrol akses berbutir halus](#)
- [\[Opensearch.8\] Koneksi ke OpenSearch domain harus dienkrpsi menggunakan kebijakan keamanan TLS terbaru](#)
- [\[Opensearch.9\] domain harus ditandai OpenSearch](#)
- [\[Opensearch.10\] OpenSearch domain harus menginstal pembaruan perangkat lunak terbaru](#)
- [\[Opensearch.11\] OpenSearch domain harus memiliki setidaknya tiga node primer khusus](#)
- [\[PCA.1\] otoritas sertifikat AWS Private CA root harus dinonaktifkan](#)
- [\[RDS.14\] Cluster Amazon Aurora seharusnya mengaktifkan backtracking](#)
- [\[RDS.18\] Instans RDS harus digunakan di VPC](#)
- [\[RDS.24\] Kluster Database RDS harus menggunakan nama pengguna administrator khusus](#)
- [\[RDS.25\] Instans database RDS harus menggunakan nama pengguna administrator khusus](#)
- [\[RDS.26\] Instans RDS DB harus dilindungi oleh rencana cadangan](#)
- [\[RDS.27\] Cluster RDS DB harus dienkrpsi saat istirahat](#)
- [\[RDS.31\] Grup keamanan RDS DB harus ditandai](#)
- [\[RDS.34\] Kluster Aurora MySQL DB harus menerbitkan log audit ke Log CloudWatch](#)
- [\[RDS.35\] Cluster RDS DB harus mengaktifkan peningkatan versi minor otomatis](#)
- [\[RDS.36\] RDS untuk instance PostgreSQL DB harus menerbitkan log ke Log CloudWatch](#)
- [\[RDS.37\] Cluster Aurora PostgreSQL DB harus menerbitkan log ke Log CloudWatch](#)
- [\[RDS.38\] RDS untuk instance PostgreSQL DB harus dienkrpsi saat transit](#)
- [\[RDS.39\] RDS untuk instance MySQL DB harus dienkrpsi saat transit](#)
- [\[RDS.40\] RDS untuk instance SQL Server DB harus menerbitkan log ke Log CloudWatch](#)
- [\[RDS.41\] RDS untuk instance SQL Server DB harus dienkrpsi saat transit](#)

- [\[RDS.42\] RDS untuk instance MariaDB DB harus menerbitkan log ke Log CloudWatch](#)
- [\[RDS.44\] RDS untuk instance MariaDB DB harus dienkripsi saat transit](#)
- [\[Redshift.3\] Cluster Amazon Redshift harus mengaktifkan snapshot otomatis](#)
- [\[Redshift.6\] Amazon Redshift harus mengaktifkan peningkatan otomatis ke versi utama](#)
- [\[Redshift.7\] Cluster Redshift harus menggunakan perutean VPC yang ditingkatkan](#)
- [\[Redshift.8\] Cluster Amazon Redshift tidak boleh menggunakan nama pengguna Admin default](#)
- [\[Redshift.9\] Cluster Redshift tidak boleh menggunakan nama database default](#)
- [\[Redshift.10\] Cluster Redshift harus dienkripsi saat istirahat](#)
- [\[Redshift.15\] Grup keamanan Redshift harus mengizinkan masuknya port cluster hanya dari asal yang dibatasi](#)
- [\[Redshift.16\] Grup subnet cluster Redshift harus memiliki subnet dari beberapa Availability Zone](#)
- [\[RedshiftServerless.1\] Grup kerja Amazon Redshift Tanpa Server harus menggunakan perutean VPC yang disempurnakan](#)
- [\[RedshiftServerless.2\] Koneksi ke grup kerja Redshift Serverless harus diperlukan untuk menggunakan SSL](#)
- [\[RedshiftServerless.3\] Kelompok kerja Redshift Tanpa Server harus melarang akses publik](#)
- [\[RedshiftServerless.4\] Ruang nama Redshift Tanpa Server harus dienkripsi dengan pengelolaan pelanggan AWS KMS keys](#)
- [\[RedshiftServerless.5\] Ruang nama Redshift Tanpa Server tidak boleh menggunakan nama pengguna admin default](#)
- [\[RedshiftServerless.6\] Ruang nama Redshift Tanpa Server harus mengeksport log ke Log CloudWatch](#)
- [\[RedshiftServerless.7\] Ruang nama Redshift Tanpa Server seharusnya tidak menggunakan nama database default](#)
- [\[Route53.1\] Pemeriksaan kesehatan rute 53 harus ditandai](#)
- [\[Route53.2\] Route 53 zona yang dihosting publik harus mencatat kueri DNS](#)
- [\[S3.7\] Ember tujuan umum S3 harus menggunakan replikasi lintas wilayah](#)
- [\[S3.10\] Bucket tujuan umum S3 dengan versi diaktifkan harus memiliki konfigurasi Siklus Hidup](#)
- [\[S3.11\] Bucket tujuan umum S3 harus mengaktifkan pemberitahuan acara](#)
- [\[S3.12\] tidak ACLs boleh digunakan untuk mengelola akses pengguna ke bucket tujuan umum S3](#)
- [\[S3.13\] Bucket tujuan umum S3 harus memiliki konfigurasi Siklus Hidup](#)
- [\[S3.19\] Titik akses S3 harus mengaktifkan pengaturan akses publik blok](#)

- [\[S3.20\] Bucket tujuan umum S3 harus mengaktifkan penghapusan MFA](#)
- [\[S3.22\] Bucket tujuan umum S3 harus mencatat peristiwa penulisan tingkat objek](#)
- [\[S3.23\] Bucket tujuan umum S3 harus mencatat peristiwa pembacaan tingkat objek](#)
- [\[S3.24\] Poin Akses Multi-Wilayah S3 harus mengaktifkan pengaturan akses publik blok](#)
- [\[SageMaker.1\] Instans SageMaker notebook Amazon seharusnya tidak memiliki akses internet langsung](#)
- [\[SageMaker.2\] instance SageMaker notebook harus diluncurkan dalam VPC khusus](#)
- [\[SageMaker.3\] Pengguna seharusnya tidak memiliki akses root ke instance SageMaker notebook](#)
- [\[SageMaker.4\] varian produksi SageMaker titik akhir harus memiliki jumlah instance awal yang lebih besar dari 1](#)
- [\[SageMaker.5\] SageMaker model harus memblokir lalu lintas masuk](#)
- [\[SageMaker.6\] konfigurasi gambar SageMaker aplikasi harus ditandai](#)
- [\[SageMaker.7\] SageMaker gambar harus diberi tag](#)
- [\[SageMaker.8\] instance SageMaker notebook harus berjalan pada platform yang didukung](#)
- [\[SES.1\] Daftar kontak SES harus ditandai](#)
- [\[SES.2\] Set konfigurasi SES harus ditandai](#)
- [\[ServiceCatalog.1\] Portofolio Service Catalog harus dibagikan hanya dalam suatu organisasi AWS](#)
- [\[SNS.4\] Kebijakan akses topik SNS seharusnya tidak mengizinkan akses publik](#)
- [\[SQS.1\] Antrian Amazon SQS harus dienkripsi saat istirahat](#)
- [\[SQS.2\] Antrian SQS harus ditandai](#)
- [\[SQS.3\] Kebijakan akses antrian SQS seharusnya tidak mengizinkan akses publik](#)
- [\[SSM.2\] EC2 Instans Amazon yang dikelola oleh Systems Manager harus memiliki status kepatuhan patch COMPLIANT setelah instalasi patch](#)
- [\[SSM.3\] EC2 Instans Amazon yang dikelola oleh Systems Manager harus memiliki status kepatuhan asosiasi COMPLIANT](#)
- [\[SSM.4\] Dokumen SSM seharusnya tidak bersifat publik](#)
- [\[StepFunctions.1\] Mesin status Step Functions seharusnya mengaktifkan logging](#)
- [\[Transfer.2\] Server Transfer Family tidak boleh menggunakan protokol FTP untuk koneksi titik akhir](#)
- [\[Transfer.3\] Konektor Transfer Family seharusnya mengaktifkan logging](#)
- [\[Transfer.4\] Perjanjian Transfer Family harus ditandai](#)
- [\[WAF.1\] Pencatatan ACL Web Global AWS WAF Klasik harus diaktifkan](#)

- [\[WAF.2\] Aturan Regional AWS WAF Klasik harus memiliki setidaknya satu syarat](#)
- [\[WAF.3\] Kelompok aturan Regional AWS WAF Klasik harus memiliki setidaknya satu aturan](#)
- [\[WAF.4\] Web Regional AWS WAF Klasik ACLs harus memiliki setidaknya satu aturan atau kelompok aturan](#)
- [\[WAF.6\] Aturan global AWS WAF klasik harus memiliki setidaknya satu syarat](#)
- [\[WAF.7\] Kelompok aturan global AWS WAF klasik harus memiliki setidaknya satu aturan](#)
- [\[WAF.8\] Web global AWS WAF klasik ACLs harus memiliki setidaknya satu aturan atau kelompok aturan](#)
- [\[WAF.10\] AWS WAF web ACLs harus memiliki setidaknya satu aturan atau kelompok aturan](#)
- [\[WAF.11\] pencatatan ACL AWS WAF web harus diaktifkan](#)
- [AWS WAF Aturan \[WAF.12\] harus mengaktifkan metrik CloudWatch](#)
- [\[WorkSpaces.1\] volume WorkSpaces pengguna harus dienkrpsi saat istirahat](#)
- [\[WorkSpaces.2\] volume WorkSpaces root harus dienkrpsi saat istirahat](#)

Tiongkok (Beijing)

Kontrol berikut tidak didukung di Wilayah Tiongkok (Beijing).

- [\[ACM.1\] Sertifikat yang diimpor dan diterbitkan ACM harus diperbarui setelah jangka waktu tertentu](#)
- [\[ACM.2\] Sertifikat RSA yang dikelola oleh ACM harus menggunakan panjang kunci minimal 2.048 bit](#)
- [\[Akun.2\] Akun AWS harus menjadi bagian dari organisasi AWS Organizations](#)
- [\[APIGateway.2\] Tahapan API Gateway REST API harus dikonfigurasi untuk menggunakan sertifikat SSL untuk otentikasi backend](#)
- [\[Amplify.1\] Aplikasi Amplify harus diberi tag](#)
- [\[Amplify.2\] Amplify branch harus diberi tag](#)
- [\[AppConfig.1\] AWS AppConfig aplikasi harus diberi tag](#)
- [\[AppConfig.2\] profil AWS AppConfig konfigurasi harus ditandai](#)
- [\[AppConfig.3\] AWS AppConfig lingkungan harus ditandai](#)
- [\[AppConfig.4\] asosiasi AWS AppConfig ekstensi harus ditandai](#)
- [\[AppFlow.1\] AppFlow Aliran Amazon harus ditandai](#)
- [\[AppRunner.1\] Layanan App Runner harus diberi tag](#)

- [\[AppRunner.2\] Konektor VPC App Runner harus diberi tag](#)
- [\[AppSync.1\] Cache AWS AppSync API harus dienkripsi saat istirahat](#)
- [\[AppSync.6\] Cache AWS AppSync API harus dienkripsi saat transit](#)
- [\[AutoScaling.10\] Grup EC2 Auto Scaling harus diberi tag](#)
- [\[Backup.1\] titik AWS Backup pemulihan harus dienkripsi saat istirahat](#)
- [\[Backup.4\] rencana AWS Backup laporan harus ditandai](#)
- [\[Batch.1\] Antrian pekerjaan batch harus ditandai](#)
- [\[Batch.2\] Kebijakan penjadwalan batch harus ditandai](#)
- [\[Batch.3\] Lingkungan komputasi Batch harus ditandai](#)
- [\[Batch.4\] Properti sumber daya komputasi di lingkungan komputasi Batch terkelola harus ditandai](#)
- [\[CloudFront.1\] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi](#)
- [\[CloudFront.3\] CloudFront distribusi harus memerlukan enkripsi dalam perjalanan](#)
- [\[CloudFront.4\] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi](#)
- [\[CloudFront.5\] CloudFront distribusi seharusnya mengaktifkan logging](#)
- [\[CloudFront.6\] CloudFront distribusi harus mengaktifkan WAF](#)
- [\[CloudFront.7\] CloudFront distribusi harus menggunakan sertifikat SSL/TLS khusus](#)
- [\[CloudFront.8\] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS](#)
- [\[CloudFront.9\] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus](#)
- [\[CloudFront.10\] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal kustom](#)
- [\[CloudFront.13\] CloudFront distribusi harus menggunakan kontrol akses asal](#)
- [\[CloudFront.14\] CloudFront distribusi harus ditandai](#)
- [\[CloudTrail.10\] Penyimpanan data acara CloudTrail harus dienkripsi dengan pelanggan yang dikelola AWS KMS keys](#)
- [\[CodeArtifact.1\] CodeArtifact repositori harus ditandai](#)
- [\[CodeGuruProfiler.1\] Grup CodeGuru profil profiler harus diberi tag](#)
- [\[CodeGuruReviewer.1\] Asosiasi CodeGuru repositori peninjau harus diberi tag](#)
- [\[Cognito.1\] Kumpulan pengguna Cognito harus mengaktifkan perlindungan ancaman dengan mode penegakan fungsi penuh untuk otentikasi standar](#)
- [\[Connect.1\] Jenis objek Amazon Connect Customer Profiles harus diberi tag](#)
- [\[Connect.2\] Instans Amazon Connect seharusnya mengaktifkan logging CloudWatch](#)

- [\[DataFirehose.1\]](#) Aliran pengiriman Firehose harus dienkripsi saat istirahat
- [\[DataSync.2\]](#) DataSync tugas harus ditandai
- [\[Detective.1\]](#) Grafik perilaku detektif harus diberi tag
- [\[DMS.4\]](#) Contoh replikasi DMS harus ditandai
- [\[DMS.5\]](#) Grup subnet replikasi DMS harus ditandai
- [\[DMS.10\]](#) Titik akhir DMS untuk database Neptune harus mengaktifkan otorisasi IAM
- [\[DMS.11\]](#) Titik akhir DMS untuk MongoDB harus mengaktifkan mekanisme otentikasi
- [\[DMS.12\]](#) Titik akhir DMS untuk Redis OSS seharusnya mengaktifkan TLS
- [\[DocumentDB.1\]](#) Cluster Amazon DocumentDB harus dienkripsi saat istirahat
- [\[DocumentDB.2\]](#) Cluster Amazon DocumentDB harus memiliki periode retensi cadangan yang memadai
- [\[DocumentDB.3\]](#) Cuplikan cluster manual Amazon DocumentDB seharusnya tidak bersifat publik
- [\[DocumentDB.4\]](#) Cluster Amazon DocumentDB harus mempublikasikan log audit ke Log CloudWatch
- [\[DocumentDB.5\]](#) Cluster Amazon DocumentDB harus mengaktifkan perlindungan penghapusan
- [\[DynamoDB.3\]](#) Cluster DynamoDB Accelerator (DAX) harus dienkripsi saat istirahat
- [\[DynamoDB.4\]](#) Tabel DynamoDB harus ada dalam rencana cadangan
- [\[DynamoDB.7\]](#) Cluster DynamoDB Accelerator harus dienkripsi saat transit
- [\[EC2.15\]](#) EC2 Subnet Amazon seharusnya tidak secara otomatis menetapkan alamat IP publik
- [\[EC2.16\]](#) Daftar Kontrol Akses Jaringan yang Tidak Digunakan harus dihapus
- [\[EC2.20\]](#) Kedua terowongan VPN untuk koneksi AWS Site-to-Site VPN harus siap
- [\[EC2.22\]](#) Grup EC2 keamanan Amazon yang tidak digunakan harus dihapus
- [\[EC2.23\]](#) Amazon EC2 Transit Gateways seharusnya tidak secara otomatis menerima permintaan lampiran VPC
- [\[EC2.28\]](#) Volume EBS harus dicakup oleh rencana cadangan
- [\[EC2.33\]](#) Lampiran gateway EC2 transit harus ditandai
- [\[EC2.34\]](#) tabel rute gateway EC2 transit harus ditandai
- [\[EC2.35\]](#) antarmuka EC2 jaringan harus ditandai
- [\[EC2.36\]](#) gateway EC2 pelanggan harus ditandai
- [\[EC2.40\]](#) Gateway EC2 NAT harus ditandai
- [\[EC2.41\]](#) EC2 jaringan ACLs harus ditandai

- [\[EC2.42\] tabel EC2 rute harus ditandai](#)
- [\[EC2.43\] grup EC2 keamanan harus ditandai](#)
- [\[EC2.44\] EC2 subnet harus ditandai](#)
- [\[EC2.46\] Amazon VPCs harus diberi tag](#)
- [\[EC2.47\] Layanan titik akhir Amazon VPC harus diberi tag](#)
- [\[EC2.48\] Log aliran VPC Amazon harus diberi tag](#)
- [\[EC2.49\] Koneksi peering VPC Amazon harus ditandai](#)
- [\[EC2.51\] Titik akhir EC2 Client VPN harus mengaktifkan pencatatan koneksi klien](#)
- [\[EC2.53\] grup EC2 keamanan seharusnya tidak mengizinkan masuknya dari 0.0.0.0/0 ke port administrasi server jarak jauh](#)
- [\[EC2.54\] grup EC2 keamanan tidak boleh mengizinkan masuknya dari :/0 ke port administrasi server jarak jauh](#)
- [\[EC2.58\] VPCs harus dikonfigurasi dengan titik akhir antarmuka untuk Kontak Manajer Insiden Systems Manager](#)
- [\[EC2.60\] VPCs harus dikonfigurasi dengan titik akhir antarmuka untuk Systems Manager Incident Manager](#)
- [\[EC2.171\] Koneksi EC2 VPN seharusnya mengaktifkan logging](#)
- [\[EC2.173\] Permintaan Armada EC2 Spot harus mengaktifkan enkripsi untuk volume EBS terlampir](#)
- [\[EC2.174\] Set opsi EC2 DHCP harus ditandai](#)
- [\[EC2.175\] templat EC2 peluncuran harus diberi tag](#)
- [\[EC2.176\] daftar EC2 awalan harus ditandai](#)
- [\[EC2.177\] Sesi cermin EC2 lalu lintas harus ditandai](#)
- [\[EC2.178\] Filter cermin EC2 lalu lintas harus ditandai](#)
- [\[EC2.179\] Target cermin EC2 lalu lintas harus ditandai](#)
- [\[ECR.1\] Repositori pribadi ECR harus memiliki pemindaian gambar yang dikonfigurasi](#)
- [\[ECR.4\] Repositori publik ECR harus ditandai](#)
- [\[ECS.13\] Layanan ECS harus ditandai](#)
- [\[ECS.15\] Definisi tugas ECS harus ditandai](#)
- [\[EFS.6\] Target pemasangan EFS tidak boleh dikaitkan dengan subnet publik](#)
- [\[EKS.3\] Kluster EKS harus menggunakan rahasia Kubernetes terenkripsi](#)
- [\[EKS.6\] Kluster EKS harus ditandai](#)

- [\[EKS.7\] Konfigurasi penyedia identitas EKS harus ditandai](#)
- [\[ELB.2\] Classic Load Balancer dengan pendengar SSL/HTTPS harus menggunakan sertifikat yang disediakan oleh AWS Certificate Manager](#)
- [\[ELB.16\] Application Load Balancers harus dikaitkan dengan ACL web AWS WAF](#)
- [\[ELB.17\] Aplikasi dan Penyeimbang Beban Jaringan dengan pendengar harus menggunakan kebijakan keamanan yang direkomendasikan](#)
- [\[ElastiCache.1\] Cluster ElastiCache \(Redis OSS\) harus mengaktifkan pencadangan otomatis](#)
- [\[ElasticBeanstalk.3\] Elastic Beanstalk harus mengalirkan log ke CloudWatch](#)
- [\[EMR.2\] Pengaturan akses publik blok EMR Amazon harus diaktifkan](#)
- [\[EMR.3\] Konfigurasi keamanan Amazon EMR harus dienkripsi saat istirahat](#)
- [\[EMR.4\] Konfigurasi keamanan Amazon EMR harus dienkripsi saat transit](#)
- [\[ES.4\] Kesalahan domain Elasticsearch yang masuk ke CloudWatch Log harus diaktifkan](#)
- [\[EventBridge.4\] titik akhir EventBridge global harus mengaktifkan replikasi acara](#)
- [\[FraudDetector.1\] Jenis entitas Amazon Fraud Detector harus diberi tag](#)
- [\[FraudDetector.2\] Label Amazon Fraud Detector harus diberi tag](#)
- [\[FraudDetector.3\] Hasil Amazon Fraud Detector harus ditandai](#)
- [\[FraudDetector.4\] Variabel Amazon Fraud Detector harus diberi tag](#)
- [\[FSx.1\] FSx untuk sistem file OpenZFS harus dikonfigurasi untuk menyalin tag ke cadangan dan volume](#)
- [\[FSx.2\] FSx untuk sistem file Lustre harus dikonfigurasi untuk menyalin tag ke cadangan](#)
- [\[FSx.5\] FSx untuk sistem file Windows File Server harus dikonfigurasi untuk penyebaran Multi-AZ](#)
- [\[GlobalAccelerator.1\] Akselerator Akselerator Global harus diberi tag](#)
- [\[GuardDuty.3\] GuardDuty IPSets harus ditandai](#)
- [\[GuardDuty.4\] GuardDuty detektor harus diberi tag](#)
- [\[GuardDuty.5\] Pemantauan Log Audit GuardDuty EKS harus diaktifkan](#)
- [\[GuardDuty.6\] Perlindungan GuardDuty Lambda harus diaktifkan](#)
- [\[GuardDuty.7\] GuardDuty EKS Runtime Monitoring harus diaktifkan](#)
- [\[GuardDuty.8\] Perlindungan GuardDuty Malware untuk EC2 harus diaktifkan](#)
- [\[GuardDuty.9\] Perlindungan GuardDuty RDS harus diaktifkan](#)
- [\[GuardDuty.10\] Perlindungan GuardDuty S3 harus diaktifkan](#)
- [\[GuardDuty.11\] GuardDuty Runtime Monitoring harus diaktifkan](#)

- [\[GuardDuty.12\] GuardDuty ECS Runtime Monitoring harus diaktifkan](#)
- [\[GuardDuty.13\] GuardDuty EC2 Runtime Monitoring harus diaktifkan](#)
- [\[IAM.6\] MFA perangkat keras harus diaktifkan untuk pengguna root](#)
- [\[IAM.9\] MFA harus diaktifkan untuk pengguna root](#)
- [\[IAM.21\] Kebijakan terkelola pelanggan IAM yang Anda buat seharusnya tidak mengizinkan tindakan wildcard untuk layanan](#)
- [\[IAM.23\] Penganalisis Akses IAM harus ditandai](#)
- [\[IAM.24\] Peran IAM harus ditandai](#)
- [\[IAM.25\] Pengguna IAM harus diberi tag](#)
- [\[IAM.26\] Sertifikat SSL/TLS kedaluwarsa yang dikelola di IAM harus dihapus](#)
- [\[IAM.27\] Identitas IAM seharusnya tidak memiliki kebijakan yang dilampirkan `AWSCloudShellFullAccess`](#)
- [\[IAM.28\] IAM Access Analyzer penganalisis akses eksternal harus diaktifkan](#)
- [\[Inspektor.1\] Pemindaian Amazon Inspector harus diaktifkan EC2](#)
- [\[Inspektor.2\] Pemindaian ECR Amazon Inspector harus diaktifkan](#)
- [\[Inspektor.3\] Pemindaian kode Amazon Inspector Lambda harus diaktifkan](#)
- [\[Inspektor.4\] Pemindaian standar Amazon Inspector Lambda harus diaktifkan](#)
- [\[IoT Events .1\] Input Peristiwa AWS IoT harus diberi tag](#)
- [\[IoT Events .2\] Model detektor Acara AWS IoT harus diberi tag](#)
- [\[IoT Events .3\] Model alarm AWS IoT Events harus diberi tag](#)
- [\[IoT Site Wise.1\] Model aset AWS IoT harus ditandai SiteWise](#)
- [\[IoT Site Wise.2\] Dasbor AWS IoT harus diberi tag SiteWise](#)
- [\[IoT Site Wise.3\] Gateway AWS IoT harus diberi tag SiteWise](#)
- [\[IoT Site Wise.4\] Portal AWS IoT harus diberi tag SiteWise](#)
- [\[IoT Site Wise.5\] Proyek AWS IoT harus diberi tag SiteWise](#)
- [\[IoT Twin Maker.1\] Pekerjaan sinkronisasi AWS IoT harus ditandai TwinMaker](#)
- [\[IoT Twin Maker.2\] Ruang kerja AWS IoT harus diberi tag TwinMaker](#)
- [\[IoT Twin Maker.3\] Adegan AWS IoT harus diberi tag TwinMaker](#)
- [\[IoT Twin Maker.4\] Entitas AWS IoT harus diberi tag TwinMaker](#)
- [\[IoT Wireless .1\] Grup multicast Nirkabel AWS IoT harus diberi tag](#)
- [\[IoT Wireless .2\] Profil layanan AWS IoT Wireless harus diberi tag](#)

- [\[IoTWireless .3\] Tugas AWS IoT FUOTA harus ditandai](#)
- [\[IVS.1\] Pasangan kunci pemutaran IVS harus ditandai](#)
- [\[IVS.2\] Konfigurasi perekaman IVS harus ditandai](#)
- [\[IVS.3\] Saluran IVS harus ditandai](#)
- [\[Keyspaces.1\] Ruang kunci Amazon Keyspaces harus diberi tag](#)
- [\[Macie.1\] Amazon Macie harus diaktifkan](#)
- [\[Macie.2\] Penemuan data sensitif otomatis Macie harus diaktifkan](#)
- [\[MQ.2\] Broker ActiveMQ harus mengalirkan log audit ke CloudWatch](#)
- [\[MQ.4\] Broker Amazon MQ harus diberi tag](#)
- [\[MSK.3\] Konektor MSK Connect harus dienkripsi saat transit](#)
- [\[Neptunus.1\] Cluster DB Neptunus harus dienkripsi saat istirahat](#)
- [\[Neptune.2\] Cluster DB Neptune harus menerbitkan log audit ke Log CloudWatch](#)
- [\[Neptune.3\] Snapshot cluster Neptune DB seharusnya tidak publik](#)
- [\[Neptunus.4\] Cluster DB Neptunus harus mengaktifkan perlindungan penghapusan](#)
- [\[Neptunus.5\] Cluster DB Neptunus harus mengaktifkan cadangan otomatis](#)
- [\[Neptune.6\] Snapshot cluster Neptune DB harus dienkripsi saat istirahat](#)
- [\[Neptune.7\] Cluster DB Neptune harus mengaktifkan otentikasi basis data IAM](#)
- [\[Neptunus.8\] Cluster DB Neptunus harus dikonfigurasi untuk menyalin tag ke snapshot](#)
- [\[Neptunus.9\] Cluster DB Neptunus harus digunakan di beberapa Availability Zone](#)
- [\[NetworkFirewall.1\] Firewall Jaringan harus digunakan di beberapa Availability Zone](#)
- [\[NetworkFirewall.2\] Pencatatan Firewall Jaringan harus diaktifkan](#)
- [\[NetworkFirewall.3\] Kebijakan Network Firewall harus memiliki setidaknya satu kelompok aturan yang terkait](#)
- [\[NetworkFirewall.4\] Tindakan stateless default untuk kebijakan Network Firewall harus drop atau forward untuk paket penuh](#)
- [\[NetworkFirewall.5\] Tindakan stateless default untuk kebijakan Network Firewall harus drop atau forward untuk paket yang terfragmentasi](#)
- [\[NetworkFirewall.6\] Grup aturan Stateless Network Firewall tidak boleh kosong](#)
- [\[NetworkFirewall.7\] Firewall Jaringan harus diberi tag](#)
- [\[NetworkFirewall.9\] Firewall Jaringan harus mengaktifkan perlindungan penghapusan](#)
- [\[NetworkFirewall.10\] Firewall Jaringan harus mengaktifkan perlindungan perubahan subnet](#)

- [\[Opensearch.1\] OpenSearch domain harus mengaktifkan enkripsi saat istirahat](#)
- [\[Opensearch.2\] OpenSearch domain tidak boleh diakses publik](#)
- [\[Opensearch.3\] OpenSearch domain harus mengenkripsi data yang dikirim antar node](#)
- [\[Opensearch.4\] login kesalahan OpenSearch domain ke Log harus diaktifkan CloudWatch](#)
- [\[Opensearch.5\] OpenSearch domain harus mengaktifkan pencatatan audit](#)
- [\[Opensearch.6\] OpenSearch domain harus memiliki setidaknya tiga node data](#)
- [\[Opensearch.7\] OpenSearch domain harus mengaktifkan kontrol akses berbutir halus](#)
- [\[Opensearch.8\] Koneksi ke OpenSearch domain harus dienkripsi menggunakan kebijakan keamanan TLS terbaru](#)
- [\[Opensearch.11\] OpenSearch domain harus memiliki setidaknya tiga node primer khusus](#)
- [\[PCA.1\] otoritas sertifikat AWS Private CA root harus dinonaktifkan](#)
- [\[PCA.2\] Otoritas sertifikat CA AWS swasta harus ditandai](#)
- [\[RDS.7\] Cluster RDS harus mengaktifkan perlindungan penghapusan](#)
- [\[RDS.10\] Otentikasi IAM harus dikonfigurasi untuk instance RDS](#)
- [\[RDS.12\] Otentikasi IAM harus dikonfigurasi untuk cluster RDS](#)
- [\[RDS.13\] Peningkatan versi minor otomatis RDS harus diaktifkan](#)
- [\[RDS.14\] Cluster Amazon Aurora seharusnya mengaktifkan backtracking](#)
- [\[RDS.15\] Cluster RDS DB harus dikonfigurasi untuk beberapa Availability Zone](#)
- [\[RDS.16\] Cluster RDS DB harus dikonfigurasi untuk menyalin tag ke snapshot](#)
- [\[RDS.24\] Kluster Database RDS harus menggunakan nama pengguna administrator khusus](#)
- [\[RDS.25\] Instans database RDS harus menggunakan nama pengguna administrator khusus](#)
- [\[RDS.26\] Instans RDS DB harus dilindungi oleh rencana cadangan](#)
- [\[RDS.27\] Cluster RDS DB harus dienkripsi saat istirahat](#)
- [\[RDS.28\] Cluster RDS DB harus ditandai](#)
- [\[RDS.29\] Snapshot cluster RDS DB harus ditandai](#)
- [\[RDS.30\] Instans RDS DB harus ditandai](#)
- [\[RDS.31\] Grup keamanan RDS DB harus ditandai](#)
- [\[RDS.32\] Snapshot RDS DB harus ditandai](#)
- [\[RDS.33\] Grup subnet RDS DB harus ditandai](#)
- [\[RDS.34\] Kluster Aurora MySQL DB harus menerbitkan log audit ke Log CloudWatch](#)
- [\[RDS.35\] Cluster RDS DB harus mengaktifkan peningkatan versi minor otomatis](#)

- [\[RDS.37\] Cluster Aurora PostgreSQL DB harus menerbitkan log ke Log CloudWatch](#)
- [\[RDS.42\] RDS untuk instance MariaDB DB harus menerbitkan log ke Log CloudWatch](#)
- [\[RDS.44\] RDS untuk instance MariaDB DB harus dienkripsi saat transit](#)
- [\[Redshift.10\] Cluster Redshift harus dienkripsi saat istirahat](#)
- [\[Redshift.14\] Grup subnet cluster Redshift harus ditandai](#)
- [\[Redshift.15\] Grup keamanan Redshift harus mengizinkan masuknya port cluster hanya dari asal yang dibatasi](#)
- [\[Redshift.17\] Grup parameter cluster Redshift harus ditandai](#)
- [\[RedshiftServerless.1\] Grup kerja Amazon Redshift Tanpa Server harus menggunakan perutean VPC yang disempurnakan](#)
- [\[RedshiftServerless.2\] Koneksi ke grup kerja Redshift Serverless harus diperlukan untuk menggunakan SSL](#)
- [\[RedshiftServerless.3\] Kelompok kerja Redshift Tanpa Server harus melarang akses publik](#)
- [\[Route53.1\] Pemeriksaan kesehatan rute 53 harus ditandai](#)
- [\[Route53.2\] Route 53 zona yang dihosting publik harus mencatat kueri DNS](#)
- [\[S3.22\] Bucket tujuan umum S3 harus mencatat peristiwa penulisan tingkat objek](#)
- [\[S3.23\] Bucket tujuan umum S3 harus mencatat peristiwa pembacaan tingkat objek](#)
- [\[S3.24\] Poin Akses Multi-Wilayah S3 harus mengaktifkan pengaturan akses publik blok](#)
- [\[SageMaker.1\] Instans SageMaker notebook Amazon seharusnya tidak memiliki akses internet langsung](#)
- [\[SageMaker.4\] varian produksi SageMaker titik akhir harus memiliki jumlah instance awal yang lebih besar dari 1](#)
- [\[SageMaker.5\] SageMaker model harus memblokir lalu lintas masuk](#)
- [\[SageMaker.6\] konfigurasi gambar SageMaker aplikasi harus ditandai](#)
- [\[SageMaker.7\] SageMaker gambar harus diberi tag](#)
- [\[SES.1\] Daftar kontak SES harus ditandai](#)
- [\[SES.2\] Set konfigurasi SES harus ditandai](#)
- [\[ServiceCatalog.1\] Portofolio Service Catalog harus dibagikan hanya dalam suatu organisasi AWS](#)
- [\[SSM.5\] Dokumen SSM harus ditandai](#)
- [\[Transfer.2\] Server Transfer Family tidak boleh menggunakan protokol FTP untuk koneksi titik akhir](#)
- [\[Transfer.4\] Perjanjian Transfer Family harus ditandai](#)

- [\[Transfer.5\] Sertifikat Transfer Family harus diberi tag](#)
- [\[Transfer.6\] Konektor Transfer Family harus diberi tag](#)
- [\[Transfer.7\] Profil Transfer Family harus diberi tag](#)
- [\[WAF.1\] Pencatatan ACL Web Global AWS WAF Klasik harus diaktifkan](#)
- [\[WAF.3\] Kelompok aturan Regional AWS WAF Klasik harus memiliki setidaknya satu aturan](#)
- [\[WAF.6\] Aturan global AWS WAF klasik harus memiliki setidaknya satu syarat](#)
- [\[WAF.7\] Kelompok aturan global AWS WAF klasik harus memiliki setidaknya satu aturan](#)
- [\[WAF.8\] Web global AWS WAF klasik ACLs harus memiliki setidaknya satu aturan atau kelompok aturan](#)
- [\[WorkSpaces.1\] volume WorkSpaces pengguna harus dienkripsi saat istirahat](#)
- [\[WorkSpaces.2\] volume WorkSpaces root harus dienkripsi saat istirahat](#)

Tiongkok (Ningxia)

Kontrol berikut tidak didukung di Wilayah Tiongkok (Ningxia).

- [\[ACM.1\] Sertifikat yang diimpor dan diterbitkan ACM harus diperbarui setelah jangka waktu tertentu](#)
- [\[ACM.2\] Sertifikat RSA yang dikelola oleh ACM harus menggunakan panjang kunci minimal 2.048 bit](#)
- [\[Akun.2\] Akun AWS harus menjadi bagian dari organisasi AWS Organizations](#)
- [\[APIGateway.2\] Tahapan API Gateway REST API harus dikonfigurasi untuk menggunakan sertifikat SSL untuk otentikasi backend](#)
- [\[Amplify.1\] Aplikasi Amplify harus diberi tag](#)
- [\[Amplify.2\] Amplify branch harus diberi tag](#)
- [\[AppConfig.1\] AWS AppConfig aplikasi harus diberi tag](#)
- [\[AppConfig.2\] profil AWS AppConfig konfigurasi harus ditandai](#)
- [\[AppConfig.3\] AWS AppConfig lingkungan harus ditandai](#)
- [\[AppConfig.4\] asosiasi AWS AppConfig ekstensi harus ditandai](#)
- [\[AppFlow.1\] AppFlow Aliran Amazon harus ditandai](#)
- [\[AppRunner.1\] Layanan App Runner harus diberi tag](#)
- [\[AppRunner.2\] Konektor VPC App Runner harus diberi tag](#)
- [\[AppSync.1\] Cache AWS AppSync API harus dienkripsi saat istirahat](#)

- [\[AppSync.6\] Cache AWS AppSync API harus dienkripsi saat transit](#)
- [\[AutoScaling.10\] Grup EC2 Auto Scaling harus diberi tag](#)
- [\[Backup.1\] titik AWS Backup pemulihan harus dienkripsi saat istirahat](#)
- [\[Backup.4\] rencana AWS Backup laporan harus ditandai](#)
- [\[Batch.1\] Antrian pekerjaan batch harus ditandai](#)
- [\[Batch.2\] Kebijakan penjadwalan batch harus ditandai](#)
- [\[Batch.3\] Lingkungan komputasi Batch harus ditandai](#)
- [\[Batch.4\] Properti sumber daya komputasi di lingkungan komputasi Batch terkelola harus ditandai](#)
- [\[CloudFront.1\] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi](#)
- [\[CloudFront.3\] CloudFront distribusi harus memerlukan enkripsi dalam perjalanan](#)
- [\[CloudFront.4\] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi](#)
- [\[CloudFront.5\] CloudFront distribusi seharusnya mengaktifkan logging](#)
- [\[CloudFront.6\] CloudFront distribusi harus mengaktifkan WAF](#)
- [\[CloudFront.7\] CloudFront distribusi harus menggunakan sertifikat SSL/TLS khusus](#)
- [\[CloudFront.8\] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS](#)
- [\[CloudFront.9\] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus](#)
- [\[CloudFront.10\] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal kustom](#)
- [\[CloudFront.12\] CloudFront distribusi seharusnya tidak menunjukkan asal S3 yang tidak ada](#)
- [\[CloudFront.13\] CloudFront distribusi harus menggunakan kontrol akses asal](#)
- [\[CloudFront.14\] CloudFront distribusi harus ditandai](#)
- [\[CloudTrail.10\] Penyimpanan data acara CloudTrail danau harus dienkripsi dengan pelanggan yang dikelola AWS KMS keys](#)
- [\[CodeArtifact.1\] CodeArtifact repositori harus ditandai](#)
- [\[CodeGuruProfiler.1\] Grup CodeGuru profil profiler harus diberi tag](#)
- [\[CodeGuruReviewer.1\] Asosiasi CodeGuru repositori peninjau harus diberi tag](#)
- [\[Cognito.1\] Kumpulan pengguna Cognito harus mengaktifkan perlindungan ancaman dengan mode penegakan fungsi penuh untuk otentikasi standar](#)
- [\[Connect.1\] Jenis objek Amazon Connect Customer Profiles harus diberi tag](#)
- [\[Connect.2\] Instans Amazon Connect seharusnya mengaktifkan logging CloudWatch](#)
- [\[DataFirehose.1\] Aliran pengiriman Firehose harus dienkripsi saat istirahat](#)

- [\[DataSync.2\] DataSync tugas harus ditandai](#)
- [\[Detective.1\] Grafik perilaku detektif harus diberi tag](#)
- [\[DMS.4\] Contoh replikasi DMS harus ditandai](#)
- [\[DMS.5\] Grup subnet replikasi DMS harus ditandai](#)
- [\[DMS.10\] Titik akhir DMS untuk database Neptune harus mengaktifkan otorisasi IAM](#)
- [\[DMS.11\] Titik akhir DMS untuk MongoDB harus mengaktifkan mekanisme otentikasi](#)
- [\[DMS.12\] Titik akhir DMS untuk Redis OSS seharusnya mengaktifkan TLS](#)
- [\[DocumentDB.3\] Cuplikan cluster manual Amazon DocumentDB seharusnya tidak bersifat publik](#)
- [\[DynamoDB.3\] Cluster DynamoDB Accelerator \(DAX\) harus dienkripsi saat istirahat](#)
- [\[DynamoDB.4\] Tabel DynamoDB harus ada dalam rencana cadangan](#)
- [\[DynamoDB.7\] Cluster DynamoDB Accelerator harus dienkripsi saat transit](#)
- [\[EC2.15\] EC2 Subnet Amazon seharusnya tidak secara otomatis menetapkan alamat IP publik](#)
- [\[EC2.16\] Daftar Kontrol Akses Jaringan yang Tidak Digunakan harus dihapus](#)
- [\[EC2.20\] Kedua terowongan VPN untuk koneksi AWS Site-to-Site VPN harus siap](#)
- [\[EC2.22\] Grup EC2 keamanan Amazon yang tidak digunakan harus dihapus](#)
- [\[EC2.23\] Amazon EC2 Transit Gateways seharusnya tidak secara otomatis menerima permintaan lampiran VPC](#)
- [\[EC2.24\] Jenis instance EC2 paravirtual Amazon tidak boleh digunakan](#)
- [\[EC2.28\] Volume EBS harus dicakup oleh rencana cadangan](#)
- [\[EC2.33\] lampiran gateway EC2 transit harus ditandai](#)
- [\[EC2.34\] tabel rute gateway EC2 transit harus ditandai](#)
- [\[EC2.35\] antarmuka EC2 jaringan harus ditandai](#)
- [\[EC2.36\] gateway EC2 pelanggan harus ditandai](#)
- [\[EC2.40\] Gateway EC2 NAT harus ditandai](#)
- [\[EC2.41\] EC2 jaringan ACLs harus ditandai](#)
- [\[EC2.42\] tabel EC2 rute harus ditandai](#)
- [\[EC2.43\] grup EC2 keamanan harus ditandai](#)
- [\[EC2.44\] EC2 subnet harus ditandai](#)
- [\[EC2.46\] Amazon VPCs harus diberi tag](#)
- [\[EC2.47\] Layanan titik akhir Amazon VPC harus diberi tag](#)
- [\[EC2.48\] Log aliran VPC Amazon harus diberi tag](#)

- [\[EC2.49\] Koneksi peering VPC Amazon harus ditandai](#)
- [\[EC2.50\] Gateway EC2 VPN harus diberi tag](#)
- [\[EC2.51\] Titik akhir EC2 Client VPN harus mengaktifkan pencatatan koneksi klien](#)
- [\[EC2.58\] VPCs harus dikonfigurasi dengan titik akhir antarmuka untuk Kontak Manajer Insiden Systems Manager](#)
- [\[EC2.60\] VPCs harus dikonfigurasi dengan titik akhir antarmuka untuk Systems Manager Incident Manager](#)
- [\[EC2.171\] Koneksi EC2 VPN seharusnya mengaktifkan logging](#)
- [\[EC2.173\] Permintaan Armada EC2 Spot harus mengaktifkan enkripsi untuk volume EBS terlampir](#)
- [\[EC2.174\] Set opsi EC2 DHCP harus ditandai](#)
- [\[EC2.175\] templat EC2 peluncuran harus diberi tag](#)
- [\[EC2.176\] daftar EC2 awalan harus ditandai](#)
- [\[EC2.177\] Sesi cermin EC2 lalu lintas harus ditandai](#)
- [\[EC2.178\] Filter cermin EC2 lalu lintas harus ditandai](#)
- [\[EC2.179\] Target cermin EC2 lalu lintas harus ditandai](#)
- [\[ECR.1\] Repositori pribadi ECR harus memiliki pemindaian gambar yang dikonfigurasi](#)
- [\[ECR.4\] Repositori publik ECR harus ditandai](#)
- [\[ECS.13\] Layanan ECS harus ditandai](#)
- [\[ECS.15\] Definisi tugas ECS harus ditandai](#)
- [\[EFS.3\] Titik akses EFS harus menegakkan direktori root](#)
- [\[EFS.4\] Titik akses EFS harus menegakkan identitas pengguna](#)
- [\[EFS.6\] Target pemasangan EFS tidak boleh dikaitkan dengan subnet publik](#)
- [\[EKS.3\] Kluster EKS harus menggunakan rahasia Kubernetes terenkripsi](#)
- [\[EKS.6\] Kluster EKS harus ditandai](#)
- [\[EKS.7\] Konfigurasi penyedia identitas EKS harus ditandai](#)
- [\[ELB.2\] Classic Load Balancer dengan pendengar SSL/HTTPS harus menggunakan sertifikat yang disediakan oleh AWS Certificate Manager](#)
- [\[ELB.16\] Application Load Balancers harus dikaitkan dengan ACL web AWS WAF](#)
- [\[ELB.17\] Aplikasi dan Penyeimbang Beban Jaringan dengan pendengar harus menggunakan kebijakan keamanan yang direkomendasikan](#)
- [\[ElastiCache.1\] Cluster ElastiCache \(Redis OSS\) harus mengaktifkan pencadangan otomatis](#)

- [\[ElasticBeanstalk.3\] Elastic Beanstalk harus mengalirkan log ke CloudWatch](#)
- [\[EMR.2\] Pengaturan akses publik blok EMR Amazon harus diaktifkan](#)
- [\[EMR.3\] Konfigurasi keamanan Amazon EMR harus dienkripsi saat istirahat](#)
- [\[EMR.4\] Konfigurasi keamanan Amazon EMR harus dienkripsi saat transit](#)
- [\[ES.4\] Kesalahan domain Elasticsearch yang masuk ke CloudWatch Log harus diaktifkan](#)
- [\[EventBridge.4\] titik akhir EventBridge global harus mengaktifkan replikasi acara](#)
- [\[FraudDetector.1\] Jenis entitas Amazon Fraud Detector harus diberi tag](#)
- [\[FraudDetector.2\] Label Amazon Fraud Detector harus diberi tag](#)
- [\[FraudDetector.3\] Hasil Amazon Fraud Detector harus ditandai](#)
- [\[FraudDetector.4\] Variabel Amazon Fraud Detector harus diberi tag](#)
- [\[FSx.1\] FSx untuk sistem file OpenZFS harus dikonfigurasi untuk menyalin tag ke cadangan dan volume](#)
- [\[FSx.2\] FSx untuk sistem file Lustre harus dikonfigurasi untuk menyalin tag ke cadangan](#)
- [\[FSx.5\] FSx untuk sistem file Windows File Server harus dikonfigurasi untuk penyebaran Multi-AZ](#)
- [\[GlobalAccelerator.1\] Akselerator Akselerator Global harus diberi tag](#)
- [\[Glue.3\] transformasi pembelajaran AWS Glue mesin harus dienkripsi saat istirahat](#)
- [\[GuardDuty.3\] GuardDuty IPSets harus ditandai](#)
- [\[GuardDuty.4\] GuardDuty detektor harus diberi tag](#)
- [\[GuardDuty.5\] Pemantauan Log Audit GuardDuty EKS harus diaktifkan](#)
- [\[GuardDuty.6\] Perlindungan GuardDuty Lambda harus diaktifkan](#)
- [\[GuardDuty.7\] GuardDuty EKS Runtime Monitoring harus diaktifkan](#)
- [\[GuardDuty.8\] Perlindungan GuardDuty Malware untuk EC2 harus diaktifkan](#)
- [\[GuardDuty.9\] Perlindungan GuardDuty RDS harus diaktifkan](#)
- [\[GuardDuty.10\] Perlindungan GuardDuty S3 harus diaktifkan](#)
- [\[GuardDuty.11\] GuardDuty Runtime Monitoring harus diaktifkan](#)
- [\[GuardDuty.12\] GuardDuty ECS Runtime Monitoring harus diaktifkan](#)
- [\[GuardDuty.13\] GuardDuty EC2 Runtime Monitoring harus diaktifkan](#)
- [\[IAM.6\] MFA perangkat keras harus diaktifkan untuk pengguna root](#)
- [\[IAM.9\] MFA harus diaktifkan untuk pengguna root](#)
- [\[IAM.21\] Kebijakan terkelola pelanggan IAM yang Anda buat seharusnya tidak mengizinkan tindakan wildcard untuk layanan](#)

- [\[IAM.23\] Penganalisis Akses IAM harus ditandai](#)
- [\[IAM.24\] Peran IAM harus ditandai](#)
- [\[IAM.25\] Pengguna IAM harus diberi tag](#)
- [\[IAM.26\] Sertifikat SSL/TLS kedaluwarsa yang dikelola di IAM harus dihapus](#)
- [\[IAM.27\] Identitas IAM seharusnya tidak memiliki kebijakan yang dilampirkan AWSCloudShellFullAccess](#)
- [\[IAM.28\] IAM Access Analyzer penganalisis akses eksternal harus diaktifkan](#)
- [\[Inspektor.1\] Pemindaian Amazon Inspector harus diaktifkan EC2](#)
- [\[Inspektor.2\] Pemindaian ECR Amazon Inspector harus diaktifkan](#)
- [\[Inspektor.3\] Pemindaian kode Amazon Inspector Lambda harus diaktifkan](#)
- [\[Inspektor.4\] Pemindaian standar Amazon Inspector Lambda harus diaktifkan](#)
- [\[IoT Events .1\] Input Peristiwa AWS IoT harus diberi tag](#)
- [\[IoT Events .2\] Model detektor Acara AWS IoT harus diberi tag](#)
- [\[IoT Events .3\] Model alarm AWS IoT Events harus diberi tag](#)
- [\[IoT Site Wise.1\] Model aset AWS IoT harus ditandai SiteWise](#)
- [\[IoT Site Wise.2\] Dasbor AWS IoT harus diberi tag SiteWise](#)
- [\[IoT Site Wise.3\] Gateway AWS IoT harus diberi tag SiteWise](#)
- [\[IoT Site Wise.4\] Portal AWS IoT harus diberi tag SiteWise](#)
- [\[IoT Site Wise.5\] Proyek AWS IoT harus diberi tag SiteWise](#)
- [\[IoT Twin Maker.1\] Pekerjaan sinkronisasi AWS IoT harus ditandai TwinMaker](#)
- [\[IoT Twin Maker.2\] Ruang kerja AWS IoT harus diberi tag TwinMaker](#)
- [\[IoT Twin Maker.3\] Adegan AWS IoT harus diberi tag TwinMaker](#)
- [\[IoT Twin Maker.4\] Entitas AWS IoT harus diberi tag TwinMaker](#)
- [\[IoT Wireless .1\] Grup multicast Nirkabel AWS IoT harus diberi tag](#)
- [\[IoT Wireless .2\] Profil layanan AWS IoT Wireless harus diberi tag](#)
- [\[IoT Wireless .3\] Tugas AWS IoT FUOTA harus ditandai](#)
- [\[IVS.1\] Pasangan kunci pemutaran IVS harus ditandai](#)
- [\[IVS.2\] Konfigurasi perekaman IVS harus ditandai](#)
- [\[IVS.3\] Saluran IVS harus ditandai](#)
- [\[Keyspaces.1\] Ruang kunci Amazon Keyspaces harus diberi tag](#)
- [\[Lambda.1\] Kebijakan fungsi Lambda harus melarang akses publik](#)

- [\[Lambda.2\] Fungsi Lambda harus menggunakan runtime yang didukung](#)
- [\[Lambda.3\] Fungsi Lambda harus dalam VPC](#)
- [\[Lambda.5\] Fungsi VPC Lambda harus beroperasi di beberapa Availability Zone](#)
- [\[Lambda.6\] Fungsi Lambda harus ditandai](#)
- [\[Macie.1\] Amazon Macie harus diaktifkan](#)
- [\[Macie.2\] Penemuan data sensitif otomatis Macie harus diaktifkan](#)
- [\[MQ.2\] Broker ActiveMQ harus mengalirkan log audit ke CloudWatch](#)
- [\[MQ.4\] Broker Amazon MQ harus diberi tag](#)
- [\[MSK.3\] Konektor MSK Connect harus dienkripsi saat transit](#)
- [\[Neptune.3\] Snapshot cluster Neptunus DB seharusnya tidak publik](#)
- [\[NetworkFirewall.1\] Firewall Jaringan harus digunakan di beberapa Availability Zone](#)
- [\[NetworkFirewall.2\] Pencatatan Firewall Jaringan harus diaktifkan](#)
- [\[NetworkFirewall.3\] Kebijakan Network Firewall harus memiliki setidaknya satu kelompok aturan yang terkait](#)
- [\[NetworkFirewall.4\] Tindakan stateless default untuk kebijakan Network Firewall harus drop atau forward untuk paket penuh](#)
- [\[NetworkFirewall.5\] Tindakan stateless default untuk kebijakan Network Firewall harus drop atau forward untuk paket yang terfragmentasi](#)
- [\[NetworkFirewall.6\] Grup aturan Stateless Network Firewall tidak boleh kosong](#)
- [\[NetworkFirewall.7\] Firewall Jaringan harus diberi tag](#)
- [\[NetworkFirewall.9\] Firewall Jaringan harus mengaktifkan perlindungan penghapusan](#)
- [\[NetworkFirewall.10\] Firewall Jaringan harus mengaktifkan perlindungan perubahan subnet](#)
- [\[Opensearch.1\] OpenSearch domain harus mengaktifkan enkripsi saat istirahat](#)
- [\[Opensearch.2\] OpenSearch domain tidak boleh diakses publik](#)
- [\[Opensearch.3\] OpenSearch domain harus mengenkripsi data yang dikirim antar node](#)
- [\[Opensearch.4\] login kesalahan OpenSearch domain ke Log harus diaktifkan CloudWatch](#)
- [\[Opensearch.5\] OpenSearch domain harus mengaktifkan pencatatan audit](#)
- [\[Opensearch.6\] OpenSearch domain harus memiliki setidaknya tiga node data](#)
- [\[Opensearch.7\] OpenSearch domain harus mengaktifkan kontrol akses berbutir halus](#)
- [\[Opensearch.8\] Koneksi ke OpenSearch domain harus dienkripsi menggunakan kebijakan keamanan TLS terbaru](#)

- [\[Opensearch.11\] OpenSearch domain harus memiliki setidaknya tiga node primer khusus](#)
- [\[PCA.1\] otoritas sertifikat AWS Private CA root harus dinonaktifkan](#)
- [\[PCA.2\] Otoritas sertifikat CA AWS swasta harus ditandai](#)
- [\[RDS.7\] Cluster RDS harus mengaktifkan perlindungan penghapusan](#)
- [\[RDS.9\] Instans RDS DB harus menerbitkan log ke Log CloudWatch](#)
- [\[RDS.10\] Otentikasi IAM harus dikonfigurasi untuk instance RDS](#)
- [\[RDS.12\] Otentikasi IAM harus dikonfigurasi untuk cluster RDS](#)
- [\[RDS.13\] Peningkatan versi minor otomatis RDS harus diaktifkan](#)
- [\[RDS.14\] Cluster Amazon Aurora seharusnya mengaktifkan backtracking](#)
- [\[RDS.15\] Cluster RDS DB harus dikonfigurasi untuk beberapa Availability Zone](#)
- [\[RDS.24\] Kluster Database RDS harus menggunakan nama pengguna administrator khusus](#)
- [\[RDS.25\] Instans database RDS harus menggunakan nama pengguna administrator khusus](#)
- [\[RDS.26\] Instans RDS DB harus dilindungi oleh rencana cadangan](#)
- [\[RDS.28\] Cluster RDS DB harus ditandai](#)
- [\[RDS.29\] Snapshot cluster RDS DB harus ditandai](#)
- [\[RDS.30\] Instans RDS DB harus ditandai](#)
- [\[RDS.31\] Grup keamanan RDS DB harus ditandai](#)
- [\[RDS.32\] Snapshot RDS DB harus ditandai](#)
- [\[RDS.33\] Grup subnet RDS DB harus ditandai](#)
- [\[RDS.34\] Kluster Aurora MySQL DB harus menerbitkan log audit ke Log CloudWatch](#)
- [\[RDS.35\] Cluster RDS DB harus mengaktifkan peningkatan versi minor otomatis](#)
- [\[RDS.42\] RDS untuk instance MariaDB DB harus menerbitkan log ke Log CloudWatch](#)
- [\[RDS.44\] RDS untuk instance MariaDB DB harus dienkripsi saat transit](#)
- [\[Redshift.10\] Cluster Redshift harus dienkripsi saat istirahat](#)
- [\[Redshift.14\] Grup subnet cluster Redshift harus ditandai](#)
- [\[Redshift.15\] Grup keamanan Redshift harus mengizinkan masuknya port cluster hanya dari asal yang dibatasi](#)
- [\[Redshift.17\] Grup parameter cluster Redshift harus ditandai](#)
- [\[RedshiftServerless.1\] Grup kerja Amazon Redshift Tanpa Server harus menggunakan perutean VPC yang disempurnakan](#)

- [\[RedshiftServerless.2\] Koneksi ke grup kerja Redshift Serverless harus diperlukan untuk menggunakan SSL](#)
- [\[RedshiftServerless.3\] Kelompok kerja Redshift Tanpa Server harus melarang akses publik](#)
- [\[Route53.1\] Pemeriksaan kesehatan rute 53 harus ditandai](#)
- [\[Route53.2\] Route 53 zona yang dihosting publik harus mencatat kueri DNS](#)
- [\[S3.24\] Poin Akses Multi-Wilayah S3 harus mengaktifkan pengaturan akses publik blok](#)
- [\[SageMaker.1\] Instans SageMaker notebook Amazon seharusnya tidak memiliki akses internet langsung](#)
- [\[SageMaker.4\] varian produksi SageMaker titik akhir harus memiliki jumlah instance awal yang lebih besar dari 1](#)
- [\[SageMaker.5\] SageMaker model harus memblokir lalu lintas masuk](#)
- [\[SageMaker.6\] konfigurasi gambar SageMaker aplikasi harus ditandai](#)
- [\[SageMaker.7\] SageMaker gambar harus diberi tag](#)
- [\[ServiceCatalog.1\] Portofolio Service Catalog harus dibagikan hanya dalam suatu organisasi AWS](#)
- [\[SSM.5\] Dokumen SSM harus ditandai](#)
- [\[StepFunctions.2\] Aktivitas Step Functions harus diberi tag](#)
- [\[Transfer.2\] Server Transfer Family tidak boleh menggunakan protokol FTP untuk koneksi titik akhir](#)
- [\[Transfer.4\] Perjanjian Transfer Family harus ditandai](#)
- [\[Transfer.5\] Sertifikat Transfer Family harus diberi tag](#)
- [\[Transfer.6\] Konektor Transfer Family harus diberi tag](#)
- [\[Transfer.7\] Profil Transfer Family harus diberi tag](#)
- [\[WAF.1\] Pencatatan ACL Web Global AWS WAF Klasik harus diaktifkan](#)
- [\[WAF.3\] Kelompok aturan Regional AWS WAF Klasik harus memiliki setidaknya satu aturan](#)
- [\[WAF.6\] Aturan global AWS WAF klasik harus memiliki setidaknya satu syarat](#)
- [\[WAF.7\] Kelompok aturan global AWS WAF klasik harus memiliki setidaknya satu aturan](#)
- [\[WAF.8\] Web global AWS WAF klasik ACLs harus memiliki setidaknya satu aturan atau kelompok aturan](#)

Eropa (Frankfurt)

Kontrol berikut tidak didukung di Wilayah Eropa (Frankfurt).

- [\[CloudFront.1\]](#) CloudFront distribusi harus memiliki objek root default yang dikonfigurasi
- [\[CloudFront.3\]](#) CloudFront distribusi harus memerlukan enkripsi dalam perjalanan
- [\[CloudFront.4\]](#) CloudFront distribusi harus memiliki failover asal yang dikonfigurasi
- [\[CloudFront.5\]](#) CloudFront distribusi seharusnya mengaktifkan logging
- [\[CloudFront.6\]](#) CloudFront distribusi harus mengaktifkan WAF
- [\[CloudFront.7\]](#) CloudFront distribusi harus menggunakan sertifikat SSL/TLS khusus
- [\[CloudFront.8\]](#) CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS
- [\[CloudFront.9\]](#) CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus
- [\[CloudFront.10\]](#) CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal kustom
- [\[CloudFront.12\]](#) CloudFront distribusi seharusnya tidak menunjukkan asal S3 yang tidak ada
- [\[CloudFront.13\]](#) CloudFront distribusi harus menggunakan kontrol akses asal
- [\[CloudFront.14\]](#) CloudFront distribusi harus ditandai
- [\[EC2.173\]](#) Permintaan Armada EC2 Spot harus mengaktifkan enkripsi untuk volume EBS terlampir
- [\[ECR.4\]](#) Repositori publik ECR harus ditandai
- [\[FraudDetector.1\]](#) Jenis entitas Amazon Fraud Detector harus diberi tag
- [\[FraudDetector.2\]](#) Label Amazon Fraud Detector harus diberi tag
- [\[FraudDetector.3\]](#) Hasil Amazon Fraud Detector harus ditandai
- [\[FraudDetector.4\]](#) Variabel Amazon Fraud Detector harus diberi tag
- [\[GlobalAccelerator.1\]](#) Akselerator Akselerator Global harus diberi tag
- [\[IAM.26\]](#) Sertifikat SSL/TLS kedaluwarsa yang dikelola di IAM harus dihapus
- [\[RDS.31\]](#) Grup keamanan RDS DB harus ditandai
- [\[Route53.1\]](#) Pemeriksaan kesehatan rute 53 harus ditandai
- [\[Route53.2\]](#) Route 53 zona yang dihosting publik harus mencatat kueri DNS
- [\[S3.24\]](#) Poin Akses Multi-Wilayah S3 harus mengaktifkan pengaturan akses publik blok
- [\[WAF.1\]](#) Pencatatan ACL Web Global AWS WAF Klasik harus diaktifkan
- [\[WAF.6\]](#) Aturan global AWS WAF klasik harus memiliki setidaknya satu syarat
- [\[WAF.7\]](#) Kelompok aturan global AWS WAF klasik harus memiliki setidaknya satu aturan
- [\[WAF.8\]](#) Web global AWS WAF klasik ACLs harus memiliki setidaknya satu aturan atau kelompok aturan

Eropa (Irlandia)

Kontrol berikut tidak didukung di Wilayah Eropa (Irlandia).

- [\[AppSync.1\] Cache AWS AppSync API harus dienkrpsi saat istirahat](#)
- [\[AppSync.6\] Cache AWS AppSync API harus dienkrpsi saat transit](#)
- [\[CloudFront.1\] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi](#)
- [\[CloudFront.3\] CloudFront distribusi harus memerlukan enkripsi dalam perjalanan](#)
- [\[CloudFront.4\] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi](#)
- [\[CloudFront.5\] CloudFront distribusi seharusnya mengaktifkan logging](#)
- [\[CloudFront.6\] CloudFront distribusi harus mengaktifkan WAF](#)
- [\[CloudFront.7\] CloudFront distribusi harus menggunakan sertifikat SSL/TLS khusus](#)
- [\[CloudFront.8\] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS](#)
- [\[CloudFront.9\] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus](#)
- [\[CloudFront.10\] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal kustom](#)
- [\[CloudFront.12\] CloudFront distribusi seharusnya tidak menunjukkan asal S3 yang tidak ada](#)
- [\[CloudFront.13\] CloudFront distribusi harus menggunakan kontrol akses asal](#)
- [\[CloudFront.14\] CloudFront distribusi harus ditandai](#)
- [\[Connect.1\] Jenis objek Amazon Connect Customer Profiles harus diberi tag](#)
- [\[Connect.2\] Instans Amazon Connect seharusnya mengaktifkan logging CloudWatch](#)
- [\[ECR.4\] Repositori publik ECR harus ditandai](#)
- [\[GlobalAccelerator.1\] Akselerator Akselerator Global harus diberi tag](#)
- [\[IAM.26\] Sertifikat SSL/TLS kedaluwarsa yang dikelola di IAM harus dihapus](#)
- [\[Route53.1\] Pemeriksaan kesehatan rute 53 harus ditandai](#)
- [\[Route53.2\] Route 53 zona yang dihosting publik harus mencatat kueri DNS](#)
- [\[S3.24\] Poin Akses Multi-Wilayah S3 harus mengaktifkan pengaturan akses publik blok](#)
- [\[WAF.1\] Pencatatan ACL Web Global AWS WAF Klasik harus diaktifkan](#)
- [\[WAF.6\] Aturan global AWS WAF klasik harus memiliki setidaknya satu syarat](#)
- [\[WAF.7\] Kelompok aturan global AWS WAF klasik harus memiliki setidaknya satu aturan](#)
- [\[WAF.8\] Web global AWS WAF klasik ACLs harus memiliki setidaknya satu aturan atau kelompok aturan](#)

Eropa (London)

Kontrol berikut tidak didukung di Wilayah Eropa (London).

- [\[AppRunner.2\] Konektor VPC App Runner harus diberi tag](#)
- [\[AppSync.1\] Cache AWS AppSync API harus dienkripsi saat istirahat](#)
- [\[AppSync.6\] Cache AWS AppSync API harus dienkripsi saat transit](#)
- [\[CloudFront.1\] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi](#)
- [\[CloudFront.3\] CloudFront distribusi harus memerlukan enkripsi dalam perjalanan](#)
- [\[CloudFront.4\] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi](#)
- [\[CloudFront.5\] CloudFront distribusi seharusnya mengaktifkan logging](#)
- [\[CloudFront.6\] CloudFront distribusi harus mengaktifkan WAF](#)
- [\[CloudFront.7\] CloudFront distribusi harus menggunakan sertifikat SSL/TLS khusus](#)
- [\[CloudFront.8\] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS](#)
- [\[CloudFront.9\] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus](#)
- [\[CloudFront.10\] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal kustom](#)
- [\[CloudFront.12\] CloudFront distribusi seharusnya tidak menunjukkan asal S3 yang tidak ada](#)
- [\[CloudFront.13\] CloudFront distribusi harus menggunakan kontrol akses asal](#)
- [\[CloudFront.14\] CloudFront distribusi harus ditandai](#)
- [\[EC2.24\] Jenis instance EC2 paravirtual Amazon tidak boleh digunakan](#)
- [\[EC2.173\] Permintaan Armada EC2 Spot harus mengaktifkan enkripsi untuk volume EBS terlampir](#)
- [\[ECR.4\] Repositori publik ECR harus ditandai](#)
- [\[FraudDetector.1\] Jenis entitas Amazon Fraud Detector harus diberi tag](#)
- [\[FraudDetector.2\] Label Amazon Fraud Detector harus diberi tag](#)
- [\[FraudDetector.3\] Hasil Amazon Fraud Detector harus ditandai](#)
- [\[FraudDetector.4\] Variabel Amazon Fraud Detector harus diberi tag](#)
- [\[GlobalAccelerator.1\] Akselerator Akselerator Global harus diberi tag](#)
- [\[IAM.26\] Sertifikat SSL/TLS kedaluwarsa yang dikelola di IAM harus dihapus](#)
- [\[IoT Site Wise.1\] Model aset AWS IoT harus ditandai SiteWise](#)
- [\[IoT Site Wise.2\] Dasbor AWS IoT harus diberi tag SiteWise](#)

- [\[Io TSite Wise.3\] Gateway AWS IoT harus diberi tag SiteWise](#)
- [\[Io TSite Wise.4\] Portal AWS IoT harus diberi tag SiteWise](#)
- [\[Io TSite Wise.5\] Proyek AWS IoT harus diberi tag SiteWise](#)
- [\[Io TTwin Maker.1\] Pekerjaan sinkronisasi AWS IoT harus ditandai TwinMaker](#)
- [\[Io TTwin Maker.2\] Ruang kerja AWS IoT harus diberi tag TwinMaker](#)
- [\[Io TTwin Maker.3\] Adegan AWS IoT harus diberi tag TwinMaker](#)
- [\[Io TTwin Maker.4\] Entitas AWS IoT harus diberi tag TwinMaker](#)
- [\[Io TWireless .1\] Grup multicast Nirkabel AWS IoT harus diberi tag](#)
- [\[Io TWireless .2\] Profil layanan AWS IoT Wireless harus diberi tag](#)
- [\[Io TWireless .3\] Tugas AWS IoT FUOTA harus ditandai](#)
- [\[IVS.1\] Pasangan kunci pemutaran IVS harus ditandai](#)
- [\[IVS.2\] Konfigurasi perekaman IVS harus ditandai](#)
- [\[IVS.3\] Saluran IVS harus ditandai](#)
- [\[RDS.31\] Grup keamanan RDS DB harus ditandai](#)
- [\[Route53.1\] Pemeriksaan kesehatan rute 53 harus ditandai](#)
- [\[Route53.2\] Route 53 zona yang dihosting publik harus mencatat kueri DNS](#)
- [\[S3.24\] Poin Akses Multi-Wilayah S3 harus mengaktifkan pengaturan akses publik blok](#)
- [\[WAF.1\] Pencatatan ACL Web Global AWS WAF Klasik harus diaktifkan](#)
- [\[WAF.6\] Aturan global AWS WAF klasik harus memiliki setidaknya satu syarat](#)
- [\[WAF.7\] Kelompok aturan global AWS WAF klasik harus memiliki setidaknya satu aturan](#)
- [\[WAF.8\] Web global AWS WAF klasik ACLs harus memiliki setidaknya satu aturan atau kelompok aturan](#)

Eropa (Milan)

Kontrol berikut tidak didukung di Wilayah Eropa (Milan).

- [\[AppFlow.1\] AppFlow Aliran Amazon harus ditandai](#)
- [\[AppRunner.1\] Layanan App Runner harus diberi tag](#)
- [\[AppRunner.2\] Konektor VPC App Runner harus diberi tag](#)
- [\[AppSync.1\] Cache AWS AppSync API harus dienkripsi saat istirahat](#)

- [\[AppSync.6\] Cache AWS AppSync API harus dienkripsi saat transit](#)
- [\[CloudFront.1\] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi](#)
- [\[CloudFront.3\] CloudFront distribusi harus memerlukan enkripsi dalam perjalanan](#)
- [\[CloudFront.4\] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi](#)
- [\[CloudFront.5\] CloudFront distribusi seharusnya mengaktifkan logging](#)
- [\[CloudFront.6\] CloudFront distribusi harus mengaktifkan WAF](#)
- [\[CloudFront.7\] CloudFront distribusi harus menggunakan sertifikat SSL/TLS khusus](#)
- [\[CloudFront.8\] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS](#)
- [\[CloudFront.9\] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus](#)
- [\[CloudFront.10\] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal kustom](#)
- [\[CloudFront.12\] CloudFront distribusi seharusnya tidak menunjukkan asal S3 yang tidak ada](#)
- [\[CloudFront.13\] CloudFront distribusi harus menggunakan kontrol akses asal](#)
- [\[CloudFront.14\] CloudFront distribusi harus ditandai](#)
- [\[CodeGuruProfiler.1\] Grup CodeGuru profil profiler harus diberi tag](#)
- [\[CodeGuruReviewer.1\] Asosiasi CodeGuru repositori peninjau harus diberi tag](#)
- [\[Connect.1\] Jenis objek Amazon Connect Customer Profiles harus diberi tag](#)
- [\[Connect.2\] Instans Amazon Connect seharusnya mengaktifkan logging CloudWatch](#)
- [\[DMS.10\] Titik akhir DMS untuk database Neptune harus mengaktifkan otorisasi IAM](#)
- [\[DynamoDB.3\] Cluster DynamoDB Accelerator \(DAX\) harus dienkripsi saat istirahat](#)
- [\[DynamoDB.7\] Cluster DynamoDB Accelerator harus dienkripsi saat transit](#)
- [\[EC2.4\] EC2 Instans yang dihentikan harus dihapus setelah periode waktu tertentu](#)
- [\[EC2.8\] EC2 instans harus menggunakan Instance Metadata Service Versi 2 \(\) IMDSv2](#)
- [\[EC2.14\] Grup keamanan seharusnya tidak mengizinkan masuknya dari 0.0.0.0/0 atau :/0 ke port 3389](#)
- [\[EC2.24\] Jenis instance EC2 paravirtual Amazon tidak boleh digunakan](#)
- [\[EC2.58\] VPCs harus dikonfigurasi dengan titik akhir antarmuka untuk Kontak Manajer Insiden Systems Manager](#)
- [\[EC2.60\] VPCs harus dikonfigurasi dengan titik akhir antarmuka untuk Systems Manager Incident Manager](#)
- [\[EC2.173\] Permintaan Armada EC2 Spot harus mengaktifkan enkripsi untuk volume EBS terlampir](#)

- [\[EC2.177\] Sesi cermin EC2 lalu lintas harus ditandai](#)
- [\[ECR.4\] Repositori publik ECR harus ditandai](#)
- [\[ELB.2\] Classic Load Balancer dengan pendengar SSL/HTTPS harus menggunakan sertifikat yang disediakan oleh AWS Certificate Manager](#)
- [\[EventBridge.4\] titik akhir EventBridge global harus mengaktifkan replikasi acara](#)
- [\[FraudDetector.1\] Jenis entitas Amazon Fraud Detector harus diberi tag](#)
- [\[FraudDetector.2\] Label Amazon Fraud Detector harus diberi tag](#)
- [\[FraudDetector.3\] Hasil Amazon Fraud Detector harus ditandai](#)
- [\[FraudDetector.4\] Variabel Amazon Fraud Detector harus diberi tag](#)
- [\[GlobalAccelerator.1\] Akselerator Akselerator Global harus diberi tag](#)
- [\[IAM.18\] Memastikan peran dukungan telah dibuat untuk mengelola insiden dengan AWS Dukungan](#)
- [\[IAM.26\] Sertifikat SSL/TLS kedaluwarsa yang dikelola di IAM harus dihapus](#)
- [\[Inspektor.3\] Pemindaian kode Amazon Inspector Lambda harus diaktifkan](#)
- [\[IoT.1\] profil AWS IoT Device Defender keamanan harus ditandai](#)
- [\[IoT.2\] tindakan AWS IoT Core mitigasi harus ditandai](#)
- [AWS IoT Core Dimensi \[IoT.3\] harus ditandai](#)
- [\[IoT.4\] AWS IoT Core otorisasi harus diberi tag](#)
- [\[IoT.5\] alias AWS IoT Core peran harus ditandai](#)
- [AWS IoT Core Kebijakan \[IoT.6\] harus ditandai](#)
- [\[IoTEvents.1\] Input Peristiwa AWS IoT harus diberi tag](#)
- [\[IoTEvents.2\] Model detektor Acara AWS IoT harus diberi tag](#)
- [\[IoTEvents.3\] Model alarm AWS IoT Events harus diberi tag](#)
- [\[IoTSiteWise.1\] Model aset AWS IoT harus ditandai SiteWise](#)
- [\[IoTSiteWise.2\] Dasbor AWS IoT harus diberi tag SiteWise](#)
- [\[IoTSiteWise.3\] Gateway AWS IoT harus diberi tag SiteWise](#)
- [\[IoTSiteWise.4\] Portal AWS IoT harus diberi tag SiteWise](#)
- [\[IoTSiteWise.5\] Proyek AWS IoT harus diberi tag SiteWise](#)
- [\[IoT Twin Maker.1\] Pekerjaan sinkronisasi AWS IoT harus ditandai TwinMaker](#)
- [\[IoT Twin Maker.2\] Ruang kerja AWS IoT harus diberi tag TwinMaker](#)

- [\[Io TTwin Maker.3\] Adegan AWS IoT harus diberi tag TwinMaker](#)
- [\[Io TTwin Maker.4\] Entitas AWS IoT harus diberi tag TwinMaker](#)
- [\[Io TWireless .1\] Grup multicast Nirkabel AWS IoT harus diberi tag](#)
- [\[Io TWireless .2\] Profil layanan AWS IoT Wireless harus diberi tag](#)
- [\[Io TWireless .3\] Tugas AWS IoT FUOTA harus ditandai](#)
- [\[IVS.1\] Pasangan kunci pemutaran IVS harus ditandai](#)
- [\[IVS.2\] Konfigurasi perekaman IVS harus ditandai](#)
- [\[IVS.3\] Saluran IVS harus ditandai](#)
- [\[Keyspaces.1\] Ruang kunci Amazon Keyspaces harus diberi tag](#)
- [\[MSK.3\] Konektor MSK Connect harus dienkripsi saat transit](#)
- [\[Neptunus.1\] Cluster DB Neptunus harus dienkripsi saat istirahat](#)
- [\[Neptune.2\] Cluster DB Neptunus harus menerbitkan log audit ke Log CloudWatch](#)
- [\[Neptune.3\] Snapshot cluster Neptunus DB seharusnya tidak publik](#)
- [\[Neptunus.4\] Cluster DB Neptunus harus mengaktifkan perlindungan penghapusan](#)
- [\[Neptunus.5\] Cluster DB Neptunus harus mengaktifkan cadangan otomatis](#)
- [\[Neptune.6\] Snapshot cluster Neptunus DB harus dienkripsi saat istirahat](#)
- [\[Neptune.7\] Cluster DB Neptunus harus mengaktifkan otentikasi basis data IAM](#)
- [\[Neptunus.8\] Cluster DB Neptunus harus dikonfigurasi untuk menyalin tag ke snapshot](#)
- [\[Neptunus.9\] Cluster DB Neptunus harus digunakan di beberapa Availability Zone](#)
- [\[RDS.1\] Snapshot RDS harus bersifat pribadi](#)
- [\[RDS.14\] Cluster Amazon Aurora seharusnya mengaktifkan backtracking](#)
- [\[RDS.31\] Grup keamanan RDS DB harus ditandai](#)
- [\[RedshiftServerless.1\] Grup kerja Amazon Redshift Tanpa Server harus menggunakan perutean VPC yang disempurnakan](#)
- [\[RedshiftServerless.2\] Koneksi ke grup kerja Redshift Serverless harus diperlukan untuk menggunakan SSL](#)
- [\[RedshiftServerless.3\] Kelompok kerja Redshift Tanpa Server harus melarang akses publik](#)
- [\[RedshiftServerless.4\] Ruang nama Redshift Tanpa Server harus dienkripsi dengan pengelolaan pelanggan AWS KMS keys](#)
- [\[RedshiftServerless.5\] Ruang nama Redshift Tanpa Server tidak boleh menggunakan nama pengguna admin default](#)

- [\[RedshiftServerless.6\] Ruang nama Redshift Tanpa Server harus mengeksport log ke Log CloudWatch](#)
- [\[RedshiftServerless.7\] Ruang nama Redshift Tanpa Server seharusnya tidak menggunakan nama database default](#)
- [\[Route53.1\] Pemeriksaan kesehatan rute 53 harus ditandai](#)
- [\[Route53.2\] Route 53 zona yang dihosting publik harus mencatat kueri DNS](#)
- [\[S3.24\] Poin Akses Multi-Wilayah S3 harus mengaktifkan pengaturan akses publik blok](#)
- [\[SSM.2\] EC2 Instans Amazon yang dikelola oleh Systems Manager harus memiliki status kepatuhan patch COMPLIANT setelah instalasi patch](#)
- [\[SSM.3\] EC2 Instans Amazon yang dikelola oleh Systems Manager harus memiliki status kepatuhan asosiasi COMPLIANT](#)
- [\[WAF.1\] Pencatatan ACL Web Global AWS WAF Klasik harus diaktifkan](#)
- [\[WAF.6\] Aturan global AWS WAF klasik harus memiliki setidaknya satu syarat](#)
- [\[WAF.7\] Kelompok aturan global AWS WAF klasik harus memiliki setidaknya satu aturan](#)
- [\[WAF.8\] Web global AWS WAF klasik ACLs harus memiliki setidaknya satu aturan atau kelompok aturan](#)
- [\[WorkSpaces.1\] volume WorkSpaces pengguna harus dienkrpsi saat istirahat](#)
- [\[WorkSpaces.2\] volume WorkSpaces root harus dienkrpsi saat istirahat](#)

Eropa (Paris)

Kontrol berikut tidak didukung di Wilayah Eropa (Paris).

- [\[AppSync.1\] Cache AWS AppSync API harus dienkrpsi saat istirahat](#)
- [\[AppSync.6\] Cache AWS AppSync API harus dienkrpsi saat transit](#)
- [\[CloudFront.1\] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi](#)
- [\[CloudFront.3\] CloudFront distribusi harus memerlukan enkripsi dalam perjalanan](#)
- [\[CloudFront.4\] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi](#)
- [\[CloudFront.5\] CloudFront distribusi seharusnya mengaktifkan logging](#)
- [\[CloudFront.6\] CloudFront distribusi harus mengaktifkan WAF](#)
- [\[CloudFront.7\] CloudFront distribusi harus menggunakan sertifikat SSL/TLS khusus](#)
- [\[CloudFront.8\] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS](#)

- [\[CloudFront.9\] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus](#)
- [\[CloudFront.10\] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal kustom](#)
- [\[CloudFront.12\] CloudFront distribusi seharusnya tidak menunjukkan asal S3 yang tidak ada](#)
- [\[CloudFront.13\] CloudFront distribusi harus menggunakan kontrol akses asal](#)
- [\[CloudFront.14\] CloudFront distribusi harus ditandai](#)
- [\[CodeGuruProfiler.1\] Grup CodeGuru profil profiler harus diberi tag](#)
- [\[CodeGuruReviewer.1\] Asosiasi CodeGuru repositori peninjau harus diberi tag](#)
- [\[Connect.1\] Jenis objek Amazon Connect Customer Profiles harus diberi tag](#)
- [\[Connect.2\] Instans Amazon Connect seharusnya mengaktifkan logging CloudWatch](#)
- [\[EC2.24\] Jenis instance EC2 paravirtual Amazon tidak boleh digunakan](#)
- [\[EC2.173\] Permintaan Armada EC2 Spot harus mengaktifkan enkripsi untuk volume EBS terlampir](#)
- [\[ECR.4\] Repositori publik ECR harus ditandai](#)
- [\[FraudDetector.1\] Jenis entitas Amazon Fraud Detector harus diberi tag](#)
- [\[FraudDetector.2\] Label Amazon Fraud Detector harus diberi tag](#)
- [\[FraudDetector.3\] Hasil Amazon Fraud Detector harus ditandai](#)
- [\[FraudDetector.4\] Variabel Amazon Fraud Detector harus diberi tag](#)
- [\[FSx.5\] FSx untuk sistem file Windows File Server harus dikonfigurasi untuk penyebaran Multi-AZ](#)
- [\[GlobalAccelerator.1\] Akselerator Akselerator Global harus diberi tag](#)
- [\[IAM.26\] Sertifikat SSL/TLS kedaluwarsa yang dikelola di IAM harus dihapus](#)
- [\[Inspektor.3\] Pemindaian kode Amazon Inspector Lambda harus diaktifkan](#)
- [\[IoTEvents.1\] Input Peristiwa AWS IoT harus diberi tag](#)
- [\[IoTEvents.2\] Model detektor Acara AWS IoT harus diberi tag](#)
- [\[IoTEvents.3\] Model alarm AWS IoT Events harus diberi tag](#)
- [\[IoTSiteWise.1\] Model aset AWS IoT harus ditandai SiteWise](#)
- [\[IoTSiteWise.2\] Dasbor AWS IoT harus diberi tag SiteWise](#)
- [\[IoTSiteWise.3\] Gateway AWS IoT harus diberi tag SiteWise](#)
- [\[IoTSiteWise.4\] Portal AWS IoT harus diberi tag SiteWise](#)
- [\[IoTSiteWise.5\] Proyek AWS IoT harus diberi tag SiteWise](#)
- [\[IoTThingMaker.1\] Pekerjaan sinkronisasi AWS IoT harus ditandai TwinMaker](#)
- [\[IoTThingMaker.2\] Ruang kerja AWS IoT harus diberi tag TwinMaker](#)

- [\[Io TTwin Maker.3\] Adegan AWS IoT harus diberi tag TwinMaker](#)
- [\[Io TTwin Maker.4\] Entitas AWS IoT harus diberi tag TwinMaker](#)
- [\[Io TWireless .1\] Grup multicast Nirkabel AWS IoT harus diberi tag](#)
- [\[Io TWireless .2\] Profil layanan AWS IoT Wireless harus diberi tag](#)
- [\[Io TWireless .3\] Tugas AWS IoT FUOTA harus ditandai](#)
- [\[IVS.1\] Pasangan kunci pemutaran IVS harus ditandai](#)
- [\[IVS.2\] Konfigurasi perekaman IVS harus ditandai](#)
- [\[IVS.3\] Saluran IVS harus ditandai](#)
- [\[RDS.31\] Grup keamanan RDS DB harus ditandai](#)
- [\[Route53.1\] Pemeriksaan kesehatan rute 53 harus ditandai](#)
- [\[Route53.2\] Route 53 zona yang dihosting publik harus mencatat kueri DNS](#)
- [\[S3.24\] Poin Akses Multi-Wilayah S3 harus mengaktifkan pengaturan akses publik blok](#)
- [\[WAF.1\] Pencatatan ACL Web Global AWS WAF Klasik harus diaktifkan](#)
- [\[WAF.6\] Aturan global AWS WAF klasik harus memiliki setidaknya satu syarat](#)
- [\[WAF.7\] Kelompok aturan global AWS WAF klasik harus memiliki setidaknya satu aturan](#)
- [\[WAF.8\] Web global AWS WAF klasik ACLs harus memiliki setidaknya satu aturan atau kelompok aturan](#)
- [\[WorkSpaces.1\] volume WorkSpaces pengguna harus dienkrpsi saat istirahat](#)
- [\[WorkSpaces.2\] volume WorkSpaces root harus dienkrpsi saat istirahat](#)

Eropa (Spanyol)

Kontrol berikut tidak didukung di Wilayah Eropa (Spanyol).

- [\[Akun.2\] Akun AWS harus menjadi bagian dari organisasi AWS Organizations](#)
- [\[APIGateway.8\] Rute API Gateway harus menentukan jenis otorisasi](#)
- [\[APIGateway.9\] Pencatatan akses harus dikonfigurasi untuk Tahap API Gateway V2](#)
- [\[Amplify.1\] Aplikasi Amplify harus diberi tag](#)
- [\[Amplify.2\] Amplify branch harus diberi tag](#)
- [\[AppConfig.1\] AWS AppConfig aplikasi harus diberi tag](#)
- [\[AppConfig.2\] profil AWS AppConfig konfigurasi harus ditandai](#)
- [\[AppConfig.3\] AWS AppConfig lingkungan harus ditandai](#)

- [\[AppFlow.1\] AppFlow Aliran Amazon harus ditandai](#)
- [\[AppRunner.1\] Layanan App Runner harus diberi tag](#)
- [\[AppRunner.2\] Konektor VPC App Runner harus diberi tag](#)
- [\[AppSync.1\] Cache AWS AppSync API harus dienkripsi saat istirahat](#)
- [\[AppSync.6\] Cache AWS AppSync API harus dienkripsi saat transit](#)
- [\[Backup.1\] titik AWS Backup pemulihan harus dienkripsi saat istirahat](#)
- [\[Backup.4\] rencana AWS Backup laporan harus ditandai](#)
- [\[CloudFront.1\] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi](#)
- [\[CloudFront.3\] CloudFront distribusi harus memerlukan enkripsi dalam perjalanan](#)
- [\[CloudFront.4\] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi](#)
- [\[CloudFront.5\] CloudFront distribusi seharusnya mengaktifkan logging](#)
- [\[CloudFront.6\] CloudFront distribusi harus mengaktifkan WAF](#)
- [\[CloudFront.7\] CloudFront distribusi harus menggunakan sertifikat SSL/TLS khusus](#)
- [\[CloudFront.8\] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS](#)
- [\[CloudFront.9\] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus](#)
- [\[CloudFront.10\] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal kustom](#)
- [\[CloudFront.12\] CloudFront distribusi seharusnya tidak menunjukkan asal S3 yang tidak ada](#)
- [\[CloudFront.13\] CloudFront distribusi harus menggunakan kontrol akses asal](#)
- [\[CloudFront.14\] CloudFront distribusi harus ditandai](#)
- [\[CodeArtifact.1\] CodeArtifact repositori harus ditandai](#)
- [\[CodeGuruProfiler.1\] Grup CodeGuru profil profiler harus diberi tag](#)
- [\[CodeGuruReviewer.1\] Asosiasi CodeGuru repositori peninjau harus diberi tag](#)
- [\[Cognito.1\] Kumpulan pengguna Cognito harus mengaktifkan perlindungan ancaman dengan mode penegakan fungsi penuh untuk otentikasi standar](#)
- [\[Connect.1\] Jenis objek Amazon Connect Customer Profiles harus diberi tag](#)
- [\[Connect.2\] Instans Amazon Connect seharusnya mengaktifkan logging CloudWatch](#)
- [\[Detective.1\] Grafik perilaku detektif harus diberi tag](#)
- [\[DMS.2\] Sertifikat DMS harus ditandai](#)
- [\[DMS.3\] Langganan acara DMS harus ditandai](#)
- [\[DMS.4\] Contoh replikasi DMS harus ditandai](#)

- [\[DMS.5\] Grup subnet replikasi DMS harus ditandai](#)
- [\[DMS.6\] Instans replikasi DMS harus mengaktifkan peningkatan versi minor otomatis](#)
- [\[DMS.7\] Tugas replikasi DMS untuk database target seharusnya mengaktifkan logging](#)
- [\[DMS.8\] Tugas replikasi DMS untuk database sumber seharusnya mengaktifkan logging](#)
- [\[DMS.9\] Titik akhir DMS harus menggunakan SSL](#)
- [\[DMS.10\] Titik akhir DMS untuk database Neptune harus mengaktifkan otorisasi IAM](#)
- [\[DMS.11\] Titik akhir DMS untuk MongoDB harus mengaktifkan mekanisme otentikasi](#)
- [\[DMS.12\] Titik akhir DMS untuk Redis OSS seharusnya mengaktifkan TLS](#)
- [\[DocumentDB.1\] Cluster Amazon DocumentDB harus dienkripsi saat istirahat](#)
- [\[DocumentDB.2\] Cluster Amazon DocumentDB harus memiliki periode retensi cadangan yang memadai](#)
- [\[DocumentDB.3\] Cuplikan cluster manual Amazon DocumentDB seharusnya tidak bersifat publik](#)
- [\[DocumentDB.4\] Cluster Amazon DocumentDB harus mempublikasikan log audit ke Log CloudWatch](#)
- [\[DocumentDB.5\] Cluster Amazon DocumentDB harus mengaktifkan perlindungan penghapusan](#)
- [\[DocumentDB.6\] Cluster Amazon DocumentDB harus dienkripsi saat transit](#)
- [\[DynamoDB.3\] Cluster DynamoDB Accelerator \(DAX\) harus dienkripsi saat istirahat](#)
- [\[DynamoDB.4\] Tabel DynamoDB harus ada dalam rencana cadangan](#)
- [\[DynamoDB.7\] Cluster DynamoDB Accelerator harus dienkripsi saat transit](#)
- [\[EC2.1\] Cuplikan Amazon EBS tidak boleh dipulihkan secara publik](#)
- [\[EC2.4\] EC2 Instans yang dihentikan harus dihapus setelah periode waktu tertentu](#)
- [\[EC2.8\] EC2 instans harus menggunakan Instance Metadata Service Versi 2 \(\) IMDSv2](#)
- [\[EC2.14\] Grup keamanan seharusnya tidak mengizinkan masuknya dari 0.0.0.0/0 atau :/0 ke port 3389](#)
- [\[EC2.22\] Grup EC2 keamanan Amazon yang tidak digunakan harus dihapus](#)
- [\[EC2.24\] Jenis instance EC2 paravirtual Amazon tidak boleh digunakan](#)
- [\[EC2.25\] Templat EC2 peluncuran Amazon tidak boleh menetapkan publik IPs ke antarmuka jaringan](#)
- [\[EC2.28\] Volume EBS harus dicakup oleh rencana cadangan](#)
- [\[EC2.34\] tabel rute gateway EC2 transit harus ditandai](#)
- [\[EC2.40\] Gateway EC2 NAT harus ditandai](#)

- [\[EC2.48\] Log aliran VPC Amazon harus diberi tag](#)
- [\[EC2.51\] Titik akhir EC2 Client VPN harus mengaktifkan pencatatan koneksi klien](#)
- [\[EC2.58\] VPCs harus dikonfigurasi dengan titik akhir antarmuka untuk Kontak Manajer Insiden Systems Manager](#)
- [\[EC2.60\] VPCs harus dikonfigurasi dengan titik akhir antarmuka untuk Systems Manager Incident Manager](#)
- [\[EC2.170\] templat EC2 peluncuran harus menggunakan Layanan Metadata Instance Versi 2 \(\) IMDSv2](#)
- [\[EC2.173\] Permintaan Armada EC2 Spot harus mengaktifkan enkripsi untuk volume EBS terlampir](#)
- [\[EC2.175\] templat EC2 peluncuran harus diberi tag](#)
- [\[EC2.177\] Sesi cermin EC2 lalu lintas harus ditandai](#)
- [\[EC2.179\] Target cermin EC2 lalu lintas harus ditandai](#)
- [\[ECR.4\] Repositori publik ECR harus ditandai](#)
- [\[EFS.1\] Sistem File Elastis harus dikonfigurasi untuk mengenkripsi data file saat istirahat menggunakan AWS KMS](#)
- [\[EFS.2\] Volume Amazon EFS harus dalam rencana cadangan](#)
- [\[ELB.2\] Classic Load Balancer dengan pendengar SSL/HTTPS harus menggunakan sertifikat yang disediakan oleh AWS Certificate Manager](#)
- [\[ELB.14\] Classic Load Balancer harus dikonfigurasi dengan mode mitigasi desync defensif atau paling ketat](#)
- [\[ELB.17\] Aplikasi dan Penyeimbang Beban Jaringan dengan pendengar harus menggunakan kebijakan keamanan yang direkomendasikan](#)
- [\[ElastiCache.1\] Cluster ElastiCache \(Redis OSS\) harus mengaktifkan pencadangan otomatis](#)
- [\[ElastiCache.6\] ElastiCache \(Redis OSS\) grup replikasi dari versi sebelumnya harus mengaktifkan Redis OSS AUTH](#)
- [\[ElastiCache.7\] ElastiCache cluster tidak boleh menggunakan grup subnet default](#)
- [\[ElasticBeanstalk.1\] Lingkungan Elastic Beanstalk seharusnya mengaktifkan pelaporan kesehatan yang ditingkatkan](#)
- [\[ElasticBeanstalk.2\] Pembaruan platform yang dikelola Elastic Beanstalk harus diaktifkan](#)
- [\[ElasticBeanstalk.3\] Elastic Beanstalk harus mengalirkan log ke CloudWatch](#)
- [\[EMR.1\] Node primer kluster EMR Amazon seharusnya tidak memiliki alamat IP publik](#)
- [\[ES.4\] Kesalahan domain Elasticsearch yang masuk ke CloudWatch Log harus diaktifkan](#)

- [\[EventBridge.4\] titik akhir EventBridge global harus mengaktifkan replikasi acara](#)
- [\[FraudDetector.1\] Jenis entitas Amazon Fraud Detector harus diberi tag](#)
- [\[FraudDetector.2\] Label Amazon Fraud Detector harus diberi tag](#)
- [\[FraudDetector.3\] Hasil Amazon Fraud Detector harus ditandai](#)
- [\[FraudDetector.4\] Variabel Amazon Fraud Detector harus diberi tag](#)
- [\[GlobalAccelerator.1\] Akselerator Akselerator Global harus diberi tag](#)
- [\[Glue.4\] Pekerjaan AWS Glue percikan harus berjalan pada versi yang didukung AWS Glue](#)
- [\[GuardDuty.2\] GuardDuty filter harus diberi tag](#)
- [\[GuardDuty.3\] GuardDuty IPSets harus ditandai](#)
- [\[IAM.1\] Kebijakan IAM seharusnya tidak mengizinkan hak administratif “*” penuh](#)
- [\[IAM.2\] Pengguna IAM seharusnya tidak memiliki kebijakan IAM yang dilampirkan](#)
- [\[IAM.3\] Kunci akses pengguna IAM harus diputar setiap 90 hari atau kurang](#)
- [\[IAM.4\] Kunci akses pengguna root IAM seharusnya tidak ada](#)
- [\[IAM.5\] MFA harus diaktifkan untuk semua pengguna IAM yang memiliki kata sandi konsol](#)
- [\[IAM.8\] Kredensi pengguna IAM yang tidak digunakan harus dihapus](#)
- [\[IAM.18\] Memastikan peran dukungan telah dibuat untuk mengelola insiden dengan AWS Dukungan](#)
- [\[IAM.19\] MFA harus diaktifkan untuk semua pengguna IAM](#)
- [\[IAM.21\] Kebijakan terkelola pelanggan IAM yang Anda buat seharusnya tidak mengizinkan tindakan wildcard untuk layanan](#)
- [\[IAM.22\] Kredensi pengguna IAM yang tidak digunakan selama 45 hari harus dihapus](#)
- [\[IAM.24\] Peran IAM harus ditandai](#)
- [\[IAM.25\] Pengguna IAM harus diberi tag](#)
- [\[IAM.26\] Sertifikat SSL/TLS kedaluwarsa yang dikelola di IAM harus dihapus](#)
- [\[IAM.27\] Identitas IAM seharusnya tidak memiliki kebijakan yang dilampirkan AWSCloudShellFullAccess](#)
- [\[Inspektor.1\] Pemindaian Amazon Inspector harus diaktifkan EC2](#)
- [\[Inspektor.2\] Pemindaian ECR Amazon Inspector harus diaktifkan](#)
- [\[Inspektor.3\] Pemindaian kode Amazon Inspector Lambda harus diaktifkan](#)
- [\[Inspektor.4\] Pemindaian standar Amazon Inspector Lambda harus diaktifkan](#)
- [\[IoT.1\] profil AWS IoT Device Defender keamanan harus ditandai](#)

- [\[IoT.2\] tindakan AWS IoT Core mitigasi harus ditandai](#)
- [AWS IoT Core Dimensi \[IoT.3\] harus ditandai](#)
- [\[IoT.4\] AWS IoT Core otorisasi harus diberi tag](#)
- [\[IoT.5\] alias AWS IoT Core peran harus ditandai](#)
- [AWS IoT Core Kebijakan \[IoT.6\] harus ditandai](#)
- [\[IoT TEEvents .1\] Input Peristiwa AWS IoT harus diberi tag](#)
- [\[IoT TEEvents .2\] Model detektor Acara AWS IoT harus diberi tag](#)
- [\[IoT TEEvents .3\] Model alarm AWS IoT Events harus diberi tag](#)
- [\[IoT TSite Wise.1\] Model aset AWS IoT harus ditandai SiteWise](#)
- [\[IoT TSite Wise.2\] Dasbor AWS IoT harus diberi tag SiteWise](#)
- [\[IoT TSite Wise.3\] Gateway AWS IoT harus diberi tag SiteWise](#)
- [\[IoT TSite Wise.4\] Portal AWS IoT harus diberi tag SiteWise](#)
- [\[IoT TSite Wise.5\] Proyek AWS IoT harus diberi tag SiteWise](#)
- [\[IoT TTwin Maker.1\] Pekerjaan sinkronisasi AWS IoT harus ditandai TwinMaker](#)
- [\[IoT TTwin Maker.2\] Ruang kerja AWS IoT harus diberi tag TwinMaker](#)
- [\[IoT TTwin Maker.3\] Adegan AWS IoT harus diberi tag TwinMaker](#)
- [\[IoT TTwin Maker.4\] Entitas AWS IoT harus diberi tag TwinMaker](#)
- [\[IoT TWireless .1\] Grup multicast Nirkabel AWS IoT harus diberi tag](#)
- [\[IoT TWireless .2\] Profil layanan AWS IoT Wireless harus diberi tag](#)
- [\[IoT TWireless .3\] Tugas AWS IoT FUOTA harus ditandai](#)
- [\[IVS.1\] Pasangan kunci pemutaran IVS harus ditandai](#)
- [\[IVS.2\] Konfigurasi perekaman IVS harus ditandai](#)
- [\[IVS.3\] Saluran IVS harus ditandai](#)
- [\[Keyspaces.1\] Ruang kunci Amazon Keyspaces harus diberi tag](#)
- [\[KMS.1\] Kebijakan yang dikelola pelanggan IAM tidak boleh mengizinkan tindakan dekripsi pada semua kunci KMS](#)
- [\[KMS.2\] Prinsipal IAM tidak boleh memiliki kebijakan inline IAM yang memungkinkan tindakan dekripsi pada semua kunci KMS](#)
- [\[Lambda.1\] Kebijakan fungsi Lambda harus melarang akses publik](#)
- [\[Macie.1\] Amazon Macie harus diaktifkan](#)
- [\[Macie.2\] Penemuan data sensitif otomatis Macie harus diaktifkan](#)

- [\[MQ.2\] Broker ActiveMQ harus mengalirkan log audit ke CloudWatch](#)
- [\[MQ.3\] Broker Amazon MQ harus mengaktifkan peningkatan versi minor otomatis](#)
- [\[MQ.4\] Broker Amazon MQ harus diberi tag](#)
- [\[MQ.5\] Broker ActiveMQ harus menggunakan mode penerapan aktif/siaga](#)
- [\[MQ.6\] Broker RabbitMQ harus menggunakan mode penerapan cluster](#)
- [\[MSK.3\] Konektor MSK Connect harus dienkripsi saat transit](#)
- [\[Neptunus.1\] Cluster DB Neptunus harus dienkripsi saat istirahat](#)
- [\[Neptune.2\] Cluster DB Neptunus harus menerbitkan log audit ke Log CloudWatch](#)
- [\[Neptune.3\] Snapshot cluster Neptunus DB seharusnya tidak publik](#)
- [\[Neptunus.4\] Cluster DB Neptunus harus mengaktifkan perlindungan penghapusan](#)
- [\[Neptunus.5\] Cluster DB Neptunus harus mengaktifkan cadangan otomatis](#)
- [\[Neptune.6\] Snapshot cluster Neptunus DB harus dienkripsi saat istirahat](#)
- [\[Neptune.7\] Cluster DB Neptunus harus mengaktifkan otentikasi basis data IAM](#)
- [\[Neptunus.8\] Cluster DB Neptunus harus dikonfigurasi untuk menyalin tag ke snapshot](#)
- [\[Neptunus.9\] Cluster DB Neptunus harus digunakan di beberapa Availability Zone](#)
- [\[Opensearch.1\] OpenSearch domain harus mengaktifkan enkripsi saat istirahat](#)
- [\[Opensearch.2\] OpenSearch domain tidak boleh diakses publik](#)
- [\[Opensearch.3\] OpenSearch domain harus mengenkripsi data yang dikirim antar node](#)
- [\[Opensearch.4\] login kesalahan OpenSearch domain ke Log harus diaktifkan CloudWatch](#)
- [\[Opensearch.5\] OpenSearch domain harus mengaktifkan pencatatan audit](#)
- [\[Opensearch.6\] OpenSearch domain harus memiliki setidaknya tiga node data](#)
- [\[Opensearch.7\] OpenSearch domain harus mengaktifkan kontrol akses berbutir halus](#)
- [\[Opensearch.8\] Koneksi ke OpenSearch domain harus dienkripsi menggunakan kebijakan keamanan TLS terbaru](#)
- [\[Opensearch.9\] domain harus ditandai OpenSearch](#)
- [\[Opensearch.10\] OpenSearch domain harus menginstal pembaruan perangkat lunak terbaru](#)
- [\[Opensearch.11\] OpenSearch domain harus memiliki setidaknya tiga node primer khusus](#)
- [\[RDS.1\] Snapshot RDS harus bersifat pribadi](#)
- [\[RDS.14\] Cluster Amazon Aurora seharusnya mengaktifkan backtracking](#)
- [\[RDS.15\] Cluster RDS DB harus dikonfigurasi untuk beberapa Availability Zone](#)
- [\[RDS.26\] Instans RDS DB harus dilindungi oleh rencana cadangan](#)

- [\[RDS.31\] Grup keamanan RDS DB harus ditandai](#)
- [\[RDS.35\] Cluster RDS DB harus mengaktifkan peningkatan versi minor otomatis](#)
- [\[RDS.37\] Cluster Aurora PostgreSQL DB harus menerbitkan log ke Log CloudWatch](#)
- [\[Redshift.10\] Cluster Redshift harus dienkripsi saat istirahat](#)
- [\[Route53.1\] Pemeriksaan kesehatan rute 53 harus ditandai](#)
- [\[Route53.2\] Route 53 zona yang dihosting publik harus mencatat kueri DNS](#)
- [\[S3.6\] Kebijakan bucket tujuan umum S3 harus membatasi akses ke yang lain Akun AWS](#)
- [\[S3.24\] Poin Akses Multi-Wilayah S3 harus mengaktifkan pengaturan akses publik blok](#)
- [\[SageMaker.1\] Instans SageMaker notebook Amazon seharusnya tidak memiliki akses internet langsung](#)
- [\[SageMaker.2\] instance SageMaker notebook harus diluncurkan dalam VPC khusus](#)
- [\[SageMaker.3\] Pengguna seharusnya tidak memiliki akses root ke instance SageMaker notebook](#)
- [\[SageMaker.5\] SageMaker model harus memblokir lalu lintas masuk](#)
- [\[SES.1\] Daftar kontak SES harus ditandai](#)
- [\[SES.2\] Set konfigurasi SES harus ditandai](#)
- [\[SQS.1\] Antrian Amazon SQS harus dienkripsi saat istirahat](#)
- [\[SQS.2\] Antrian SQS harus ditandai](#)
- [\[SQS.3\] Kebijakan akses antrian SQS seharusnya tidak mengizinkan akses publik](#)
- [\[SSM.3\] EC2 Instans Amazon yang dikelola oleh Systems Manager harus memiliki status kepatuhan asosiasi COMPLIANT](#)
- [\[Transfer.3\] Konektor Transfer Family seharusnya mengaktifkan logging](#)
- [\[Transfer.4\] Perjanjian Transfer Family harus ditandai](#)
- [\[WAF.1\] Pencatatan ACL Web Global AWS WAF Klasik harus diaktifkan](#)
- [\[WAF.3\] Kelompok aturan Regional AWS WAF Klasik harus memiliki setidaknya satu aturan](#)
- [\[WAF.6\] Aturan global AWS WAF klasik harus memiliki setidaknya satu syarat](#)
- [\[WAF.7\] Kelompok aturan global AWS WAF klasik harus memiliki setidaknya satu aturan](#)
- [\[WAF.8\] Web global AWS WAF klasik ACLs harus memiliki setidaknya satu aturan atau kelompok aturan](#)
- [\[WAF.10\] AWS WAF web ACLs harus memiliki setidaknya satu aturan atau kelompok aturan](#)
- [\[WorkSpaces.1\] volume WorkSpaces pengguna harus dienkripsi saat istirahat](#)
- [\[WorkSpaces.2\] volume WorkSpaces root harus dienkripsi saat istirahat](#)

Eropa (Stockholm)

Kontrol berikut tidak didukung di Wilayah Eropa (Stockholm).

- [\[AppFlow.1\] AppFlow Aliran Amazon harus ditandai](#)
- [\[AppRunner.1\] Layanan App Runner harus diberi tag](#)
- [\[AppRunner.2\] Konektor VPC App Runner harus diberi tag](#)
- [\[AppSync.1\] Cache AWS AppSync API harus dienkripsi saat istirahat](#)
- [\[AppSync.6\] Cache AWS AppSync API harus dienkripsi saat transit](#)
- [\[CloudFront.1\] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi](#)
- [\[CloudFront.3\] CloudFront distribusi harus memerlukan enkripsi dalam perjalanan](#)
- [\[CloudFront.4\] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi](#)
- [\[CloudFront.5\] CloudFront distribusi seharusnya mengaktifkan logging](#)
- [\[CloudFront.6\] CloudFront distribusi harus mengaktifkan WAF](#)
- [\[CloudFront.7\] CloudFront distribusi harus menggunakan sertifikat SSL/TLS khusus](#)
- [\[CloudFront.8\] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS](#)
- [\[CloudFront.9\] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus](#)
- [\[CloudFront.10\] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal kustom](#)
- [\[CloudFront.12\] CloudFront distribusi seharusnya tidak menunjukkan asal S3 yang tidak ada](#)
- [\[CloudFront.13\] CloudFront distribusi harus menggunakan kontrol akses asal](#)
- [\[CloudFront.14\] CloudFront distribusi harus ditandai](#)
- [\[Connect.1\] Jenis objek Amazon Connect Customer Profiles harus diberi tag](#)
- [\[Connect.2\] Instans Amazon Connect seharusnya mengaktifkan logging CloudWatch](#)
- [\[DocumentDB.1\] Cluster Amazon DocumentDB harus dienkripsi saat istirahat](#)
- [\[DocumentDB.2\] Cluster Amazon DocumentDB harus memiliki periode retensi cadangan yang memadai](#)
- [\[DocumentDB.3\] Cuplikan cluster manual Amazon DocumentDB seharusnya tidak bersifat publik](#)
- [\[DocumentDB.4\] Cluster Amazon DocumentDB harus mempublikasikan log audit ke Log CloudWatch](#)
- [\[DocumentDB.5\] Cluster Amazon DocumentDB harus mengaktifkan perlindungan penghapusan](#)
- [\[DocumentDB.6\] Cluster Amazon DocumentDB harus dienkripsi saat transit](#)

- [\[DynamoDB.3\] Cluster DynamoDB Accelerator \(DAX\) harus dienkrpsi saat istirahat](#)
- [\[DynamoDB.7\] Cluster DynamoDB Accelerator harus dienkrpsi saat transit](#)
- [\[EC2.24\] Jenis instance EC2 paravirtual Amazon tidak boleh digunakan](#)
- [\[EC2.173\] Permintaan Armada EC2 Spot harus mengaktifkan enkripsi untuk volume EBS terlampir](#)
- [\[ECR.4\] Repositori publik ECR harus ditandai](#)
- [\[FraudDetector.1\] Jenis entitas Amazon Fraud Detector harus diberi tag](#)
- [\[FraudDetector.2\] Label Amazon Fraud Detector harus diberi tag](#)
- [\[FraudDetector.3\] Hasil Amazon Fraud Detector harus ditandai](#)
- [\[FraudDetector.4\] Variabel Amazon Fraud Detector harus diberi tag](#)
- [\[GlobalAccelerator.1\] Akselerator Akselerator Global harus diberi tag](#)
- [\[IAM.26\] Sertifikat SSL/TLS kedaluwarsa yang dikelola di IAM harus dihapus](#)
- [\[IoTEvents .1\] Input Peristiwa AWS IoT harus diberi tag](#)
- [\[IoTEvents .2\] Model detektor Acara AWS IoT harus diberi tag](#)
- [\[IoTEvents .3\] Model alarm AWS IoT Events harus diberi tag](#)
- [\[IoTSiteWise.1\] Model aset AWS IoT harus ditandai SiteWise](#)
- [\[IoTSiteWise.2\] Dasbor AWS IoT harus diberi tag SiteWise](#)
- [\[IoTSiteWise.3\] Gateway AWS IoT harus diberi tag SiteWise](#)
- [\[IoTSiteWise.4\] Portal AWS IoT harus diberi tag SiteWise](#)
- [\[IoTSiteWise.5\] Proyek AWS IoT harus diberi tag SiteWise](#)
- [\[IoTThingMaker.1\] Pekerjaan sinkronisasi AWS IoT harus ditandai ThingMaker](#)
- [\[IoTThingMaker.2\] Ruang kerja AWS IoT harus diberi tag ThingMaker](#)
- [\[IoTThingMaker.3\] Adegan AWS IoT harus diberi tag ThingMaker](#)
- [\[IoTThingMaker.4\] Entitas AWS IoT harus diberi tag ThingMaker](#)
- [\[IoTWireless .1\] Grup multicast Nirkabel AWS IoT harus diberi tag](#)
- [\[IoTWireless .2\] Profil layanan AWS IoT Wireless harus diberi tag](#)
- [\[IoTWireless .3\] Tugas AWS IoT FUOTA harus ditandai](#)
- [\[IVS.1\] Pasangan kunci pemutaran IVS harus ditandai](#)
- [\[IVS.2\] Konfigurasi perekaman IVS harus ditandai](#)
- [\[IVS.3\] Saluran IVS harus ditandai](#)
- [\[RDS.14\] Cluster Amazon Aurora seharusnya mengaktifkan backtracking](#)

- [\[RDS.31\] Grup keamanan RDS DB harus ditandai](#)
- [\[Route53.1\] Pemeriksaan kesehatan rute 53 harus ditandai](#)
- [\[Route53.2\] Route 53 zona yang dihosting publik harus mencatat kueri DNS](#)
- [\[S3.24\] Poin Akses Multi-Wilayah S3 harus mengaktifkan pengaturan akses publik blok](#)
- [\[WAF.1\] Pencatatan ACL Web Global AWS WAF Klasik harus diaktifkan](#)
- [\[WAF.6\] Aturan global AWS WAF klasik harus memiliki setidaknya satu syarat](#)
- [\[WAF.7\] Kelompok aturan global AWS WAF klasik harus memiliki setidaknya satu aturan](#)
- [\[WAF.8\] Web global AWS WAF klasik ACLs harus memiliki setidaknya satu aturan atau kelompok aturan](#)
- [\[WorkSpaces.1\] volume WorkSpaces pengguna harus dienkripsi saat istirahat](#)
- [\[WorkSpaces.2\] volume WorkSpaces root harus dienkripsi saat istirahat](#)

Eropa (Zürich)

Kontrol berikut tidak didukung di Wilayah Eropa (Zurich).

- [\[APIGateway.8\] Rute API Gateway harus menentukan jenis otorisasi](#)
- [\[APIGateway.9\] Pencatatan akses harus dikonfigurasi untuk Tahap API Gateway V2](#)
- [\[Amplify.1\] Aplikasi Amplify harus diberi tag](#)
- [\[Amplify.2\] Amplify branch harus diberi tag](#)
- [\[AppConfig.1\] AWS AppConfig aplikasi harus diberi tag](#)
- [\[AppConfig.2\] profil AWS AppConfig konfigurasi harus ditandai](#)
- [\[AppConfig.3\] AWS AppConfig lingkungan harus ditandai](#)
- [\[AppFlow.1\] AppFlow Aliran Amazon harus ditandai](#)
- [\[AppRunner.1\] Layanan App Runner harus diberi tag](#)
- [\[AppRunner.2\] Konektor VPC App Runner harus diberi tag](#)
- [\[AppSync.1\] Cache AWS AppSync API harus dienkripsi saat istirahat](#)
- [\[AppSync.6\] Cache AWS AppSync API harus dienkripsi saat transit](#)
- [\[Backup.1\] titik AWS Backup pemulihan harus dienkripsi saat istirahat](#)
- [\[Backup.4\] rencana AWS Backup laporan harus ditandai](#)
- [\[CloudFront.1\] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi](#)

- [\[CloudFront.3\] CloudFront distribusi harus memerlukan enkripsi dalam perjalanan](#)
- [\[CloudFront.4\] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi](#)
- [\[CloudFront.5\] CloudFront distribusi seharusnya mengaktifkan logging](#)
- [\[CloudFront.6\] CloudFront distribusi harus mengaktifkan WAF](#)
- [\[CloudFront.7\] CloudFront distribusi harus menggunakan sertifikat SSL/TLS khusus](#)
- [\[CloudFront.8\] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS](#)
- [\[CloudFront.9\] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus](#)
- [\[CloudFront.10\] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal kustom](#)
- [\[CloudFront.12\] CloudFront distribusi seharusnya tidak menunjukkan asal S3 yang tidak ada](#)
- [\[CloudFront.13\] CloudFront distribusi harus menggunakan kontrol akses asal](#)
- [\[CloudFront.14\] CloudFront distribusi harus ditandai](#)
- [\[CloudTrail.6\] Pastikan bucket S3 yang digunakan untuk menyimpan CloudTrail log tidak dapat diakses publik](#)
- [\[CloudTrail.7\] Pastikan pencatatan akses bucket S3 diaktifkan pada bucket CloudTrail S3](#)
- [\[CodeArtifact.1\] CodeArtifact repositori harus ditandai](#)
- [\[CodeGuruProfiler.1\] Grup CodeGuru profil profiler harus diberi tag](#)
- [\[CodeGuruReviewer.1\] Asosiasi CodeGuru repositori peninjau harus diberi tag](#)
- [\[Cognito.1\] Kumpulan pengguna Cognito harus mengaktifkan perlindungan ancaman dengan mode penegakan fungsi penuh untuk otentikasi standar](#)
- [\[Connect.1\] Jenis objek Amazon Connect Customer Profiles harus diberi tag](#)
- [\[Connect.2\] Instans Amazon Connect seharusnya mengaktifkan logging CloudWatch](#)
- [\[Detective.1\] Grafik perilaku detektif harus diberi tag](#)
- [\[DMS.2\] Sertifikat DMS harus ditandai](#)
- [\[DMS.3\] Langganan acara DMS harus ditandai](#)
- [\[DMS.4\] Contoh replikasi DMS harus ditandai](#)
- [\[DMS.5\] Grup subnet replikasi DMS harus ditandai](#)
- [\[DMS.6\] Instans replikasi DMS harus mengaktifkan peningkatan versi minor otomatis](#)
- [\[DMS.7\] Tugas replikasi DMS untuk database target seharusnya mengaktifkan logging](#)
- [\[DMS.8\] Tugas replikasi DMS untuk database sumber seharusnya mengaktifkan logging](#)
- [\[DMS.9\] Titik akhir DMS harus menggunakan SSL](#)

- [\[DMS.10\] Titik akhir DMS untuk database Neptune harus mengaktifkan otorisasi IAM](#)
- [\[DMS.11\] Titik akhir DMS untuk MongoDB harus mengaktifkan mekanisme otentikasi](#)
- [\[DMS.12\] Titik akhir DMS untuk Redis OSS seharusnya mengaktifkan TLS](#)
- [\[DocumentDB.1\] Cluster Amazon DocumentDB harus dienkripsi saat istirahat](#)
- [\[DocumentDB.2\] Cluster Amazon DocumentDB harus memiliki periode retensi cadangan yang memadai](#)
- [\[DocumentDB.3\] Cuplikan cluster manual Amazon DocumentDB seharusnya tidak bersifat publik](#)
- [\[DocumentDB.4\] Cluster Amazon DocumentDB harus mempublikasikan log audit ke Log CloudWatch](#)
- [\[DocumentDB.5\] Cluster Amazon DocumentDB harus mengaktifkan perlindungan penghapusan](#)
- [\[DocumentDB.6\] Cluster Amazon DocumentDB harus dienkripsi saat transit](#)
- [\[DynamoDB.3\] Cluster DynamoDB Accelerator \(DAX\) harus dienkripsi saat istirahat](#)
- [\[DynamoDB.4\] Tabel DynamoDB harus ada dalam rencana cadangan](#)
- [\[DynamoDB.7\] Cluster DynamoDB Accelerator harus dienkripsi saat transit](#)
- [\[EC2.4\] EC2 Instans yang dihentikan harus dihapus setelah periode waktu tertentu](#)
- [\[EC2.8\] EC2 instans harus menggunakan Instance Metadata Service Versi 2 \(\) IMDSv2](#)
- [\[EC2.14\] Grup keamanan seharusnya tidak mengizinkan masuknya dari 0.0.0.0/0 atau :/0 ke port 3389](#)
- [\[EC2.22\] Grup EC2 keamanan Amazon yang tidak digunakan harus dihapus](#)
- [\[EC2.24\] Jenis instance EC2 paravirtual Amazon tidak boleh digunakan](#)
- [\[EC2.25\] Templat EC2 peluncuran Amazon tidak boleh menetapkan publik IPs ke antarmuka jaringan](#)
- [\[EC2.28\] Volume EBS harus dicakup oleh rencana cadangan](#)
- [\[EC2.58\] VPCs harus dikonfigurasi dengan titik akhir antarmuka untuk Kontak Manajer Insiden Systems Manager](#)
- [\[EC2.60\] VPCs harus dikonfigurasi dengan titik akhir antarmuka untuk Systems Manager Incident Manager](#)
- [\[EC2.170\] templat EC2 peluncuran harus menggunakan Layanan Metadata Instance Versi 2 \(\) IMDSv2](#)
- [\[EC2.173\] Permintaan Armada EC2 Spot harus mengaktifkan enkripsi untuk volume EBS terlampir](#)
- [\[EC2.175\] templat EC2 peluncuran harus diberi tag](#)
- [\[ECR.4\] Repositori publik ECR harus ditandai](#)

- [\[EFS.1\] Sistem File Elastis harus dikonfigurasi untuk mengenkripsi data file saat istirahat menggunakan AWS KMS](#)
- [\[EFS.2\] Volume Amazon EFS harus dalam rencana cadangan](#)
- [\[ELB.2\] Classic Load Balancer dengan pendengar SSL/HTTPS harus menggunakan sertifikat yang disediakan oleh AWS Certificate Manager](#)
- [\[ELB.14\] Classic Load Balancer harus dikonfigurasi dengan mode mitigasi desync defensif atau paling ketat](#)
- [\[ELB.17\] Aplikasi dan Penyeimbang Beban Jaringan dengan pendengar harus menggunakan kebijakan keamanan yang direkomendasikan](#)
- [\[ElastiCache.1\] Cluster ElastiCache \(Redis OSS\) harus mengaktifkan pencadangan otomatis](#)
- [\[ElastiCache.6\] ElastiCache \(Redis OSS\) grup replikasi dari versi sebelumnya harus mengaktifkan Redis OSS AUTH](#)
- [\[ElastiCache.7\] ElastiCache cluster tidak boleh menggunakan grup subnet default](#)
- [\[ElasticBeanstalk.1\] Lingkungan Elastic Beanstalk seharusnya mengaktifkan pelaporan kesehatan yang ditingkatkan](#)
- [\[ElasticBeanstalk.2\] Pembaruan platform yang dikelola Elastic Beanstalk harus diaktifkan](#)
- [\[ElasticBeanstalk.3\] Elastic Beanstalk harus mengalirkan log ke CloudWatch](#)
- [\[EMR.1\] Node primer kluster EMR Amazon seharusnya tidak memiliki alamat IP publik](#)
- [\[ES.4\] Kesalahan domain Elasticsearch yang masuk ke CloudWatch Log harus diaktifkan](#)
- [\[EventBridge.4\] titik akhir EventBridge global harus mengaktifkan replikasi acara](#)
- [\[FraudDetector.1\] Jenis entitas Amazon Fraud Detector harus diberi tag](#)
- [\[FraudDetector.2\] Label Amazon Fraud Detector harus diberi tag](#)
- [\[FraudDetector.3\] Hasil Amazon Fraud Detector harus ditandai](#)
- [\[FraudDetector.4\] Variabel Amazon Fraud Detector harus diberi tag](#)
- [\[GlobalAccelerator.1\] Akselerator Akselerator Global harus diberi tag](#)
- [\[Glue.4\] Pekerjaan AWS Glue percikan harus berjalan pada versi yang didukung AWS Glue](#)
- [\[GuardDuty.2\] GuardDuty filter harus diberi tag](#)
- [\[GuardDuty.3\] GuardDuty IPSets harus ditandai](#)
- [\[IAM.1\] Kebijakan IAM seharusnya tidak mengizinkan hak administratif “*” penuh](#)
- [\[IAM.2\] Pengguna IAM seharusnya tidak memiliki kebijakan IAM yang dilampirkan](#)
- [\[IAM.3\] Kunci akses pengguna IAM harus diputar setiap 90 hari atau kurang](#)

- [\[IAM.4\] Kunci akses pengguna root IAM seharusnya tidak ada](#)
- [\[IAM.5\] MFA harus diaktifkan untuk semua pengguna IAM yang memiliki kata sandi konsol](#)
- [\[IAM.8\] Kredensi pengguna IAM yang tidak digunakan harus dihapus](#)
- [\[IAM.18\] Memastikan peran dukungan telah dibuat untuk mengelola insiden dengan AWS Dukungan](#)
- [\[IAM.19\] MFA harus diaktifkan untuk semua pengguna IAM](#)
- [\[IAM.21\] Kebijakan terkelola pelanggan IAM yang Anda buat seharusnya tidak mengizinkan tindakan wildcard untuk layanan](#)
- [\[IAM.22\] Kredensi pengguna IAM yang tidak digunakan selama 45 hari harus dihapus](#)
- [\[IAM.24\] Peran IAM harus ditandai](#)
- [\[IAM.25\] Pengguna IAM harus diberi tag](#)
- [\[IAM.26\] Sertifikat SSL/TLS kedaluwarsa yang dikelola di IAM harus dihapus](#)
- [\[IAM.27\] Identitas IAM seharusnya tidak memiliki kebijakan yang dilampirkan AWSCloudShellFullAccess](#)
- [\[Inspektor.3\] Pemindaian kode Amazon Inspector Lambda harus diaktifkan](#)
- [\[IoT.1\] profil AWS IoT Device Defender keamanan harus ditandai](#)
- [\[IoT.2\] tindakan AWS IoT Core mitigasi harus ditandai](#)
- [AWS IoT Core Dimensi \[IoT.3\] harus ditandai](#)
- [\[IoT.4\] AWS IoT Core otorisasi harus diberi tag](#)
- [\[IoT.5\] alias AWS IoT Core peran harus ditandai](#)
- [AWS IoT Core Kebijakan \[IoT.6\] harus ditandai](#)
- [\[IoT Events .1\] Input Peristiwa AWS IoT harus diberi tag](#)
- [\[IoT Events .2\] Model detektor Acara AWS IoT harus diberi tag](#)
- [\[IoT Events .3\] Model alarm AWS IoT Events harus diberi tag](#)
- [\[IoT Site Wise.1\] Model aset AWS IoT harus ditandai SiteWise](#)
- [\[IoT Site Wise.2\] Dasbor AWS IoT harus diberi tag SiteWise](#)
- [\[IoT Site Wise.3\] Gateway AWS IoT harus diberi tag SiteWise](#)
- [\[IoT Site Wise.4\] Portal AWS IoT harus diberi tag SiteWise](#)
- [\[IoT Site Wise.5\] Proyek AWS IoT harus diberi tag SiteWise](#)
- [\[IoT Twin Maker.1\] Pekerjaan sinkronisasi AWS IoT harus ditandai TwinMaker](#)
- [\[IoT Twin Maker.2\] Ruang kerja AWS IoT harus diberi tag TwinMaker](#)

- [\[Io TTwin Maker.3\] Adegan AWS IoT harus diberi tag TwinMaker](#)
- [\[Io TTwin Maker.4\] Entitas AWS IoT harus diberi tag TwinMaker](#)
- [\[Io TWireless .1\] Grup multicast Nirkabel AWS IoT harus diberi tag](#)
- [\[Io TWireless .2\] Profil layanan AWS IoT Wireless harus diberi tag](#)
- [\[Io TWireless .3\] Tugas AWS IoT FUOTA harus ditandai](#)
- [\[IVS.1\] Pasangan kunci pemutaran IVS harus ditandai](#)
- [\[IVS.2\] Konfigurasi perekaman IVS harus ditandai](#)
- [\[IVS.3\] Saluran IVS harus ditandai](#)
- [\[Keyspaces.1\] Ruang kunci Amazon Keyspaces harus diberi tag](#)
- [\[KMS.1\] Kebijakan yang dikelola pelanggan IAM tidak boleh mengizinkan tindakan dekripsi pada semua kunci KMS](#)
- [\[KMS.2\] Prinsipal IAM tidak boleh memiliki kebijakan inline IAM yang memungkinkan tindakan dekripsi pada semua kunci KMS](#)
- [\[Macie.1\] Amazon Macie harus diaktifkan](#)
- [\[Macie.2\] Penemuan data sensitif otomatis Macie harus diaktifkan](#)
- [\[MQ.2\] Broker ActiveMQ harus mengalirkan log audit ke CloudWatch](#)
- [\[MQ.3\] Broker Amazon MQ harus mengaktifkan peningkatan versi minor otomatis](#)
- [\[MQ.4\] Broker Amazon MQ harus diberi tag](#)
- [\[MQ.5\] Broker ActiveMQ harus menggunakan mode penerapan aktif/siaga](#)
- [\[MQ.6\] Broker RabbitMQ harus menggunakan mode penerapan cluster](#)
- [\[MSK.3\] Konektor MSK Connect harus dienkripsi saat transit](#)
- [\[Neptunus.1\] Cluster DB Neptunus harus dienkripsi saat istirahat](#)
- [\[Neptune.2\] Cluster DB Neptunus harus menerbitkan log audit ke Log CloudWatch](#)
- [\[Neptune.3\] Snapshot cluster Neptunus DB seharusnya tidak publik](#)
- [\[Neptunus.4\] Cluster DB Neptunus harus mengaktifkan perlindungan penghapusan](#)
- [\[Neptunus.5\] Cluster DB Neptunus harus mengaktifkan cadangan otomatis](#)
- [\[Neptune.6\] Snapshot cluster Neptunus DB harus dienkripsi saat istirahat](#)
- [\[Neptune.7\] Cluster DB Neptunus harus mengaktifkan otentikasi basis data IAM](#)
- [\[Neptunus.8\] Cluster DB Neptunus harus dikonfigurasi untuk menyalin tag ke snapshot](#)
- [\[Neptunus.9\] Cluster DB Neptunus harus digunakan di beberapa Availability Zone](#)
- [\[Opensearch.1\] OpenSearch domain harus mengaktifkan enkripsi saat istirahat](#)

- [\[Opensearch.2\] OpenSearch domain tidak boleh diakses publik](#)
- [\[Opensearch.3\] OpenSearch domain harus mengenkripsi data yang dikirim antar node](#)
- [\[Opensearch.4\] login kesalahan OpenSearch domain ke Log harus diaktifkan CloudWatch](#)
- [\[Opensearch.5\] OpenSearch domain harus mengaktifkan pencatatan audit](#)
- [\[Opensearch.6\] OpenSearch domain harus memiliki setidaknya tiga node data](#)
- [\[Opensearch.7\] OpenSearch domain harus mengaktifkan kontrol akses berbutir halus](#)
- [\[Opensearch.8\] Koneksi ke OpenSearch domain harus dienkripsi menggunakan kebijakan keamanan TLS terbaru](#)
- [\[Opensearch.9\] domain harus ditandai OpenSearch](#)
- [\[Opensearch.10\] OpenSearch domain harus menginstal pembaruan perangkat lunak terbaru](#)
- [\[Opensearch.11\] OpenSearch domain harus memiliki setidaknya tiga node primer khusus](#)
- [\[RDS.1\] Snapshot RDS harus bersifat pribadi](#)
- [\[RDS.14\] Cluster Amazon Aurora seharusnya mengaktifkan backtracking](#)
- [\[RDS.26\] Instans RDS DB harus dilindungi oleh rencana cadangan](#)
- [\[RDS.31\] Grup keamanan RDS DB harus ditandai](#)
- [\[RDS.35\] Cluster RDS DB harus mengaktifkan peningkatan versi minor otomatis](#)
- [\[Route53.1\] Pemeriksaan kesehatan rute 53 harus ditandai](#)
- [\[Route53.2\] Route 53 zona yang dihosting publik harus mencatat kueri DNS](#)
- [\[S3.24\] Poin Akses Multi-Wilayah S3 harus mengaktifkan pengaturan akses publik blok](#)
- [\[SageMaker.1\] Instans SageMaker notebook Amazon seharusnya tidak memiliki akses internet langsung](#)
- [\[SageMaker.2\] instance SageMaker notebook harus diluncurkan dalam VPC khusus](#)
- [\[SageMaker.3\] Pengguna seharusnya tidak memiliki akses root ke instance SageMaker notebook](#)
- [\[SageMaker.5\] SageMaker model harus memblokir lalu lintas masuk](#)
- [\[SageMaker.6\] konfigurasi gambar SageMaker aplikasi harus ditandai](#)
- [\[SageMaker.7\] SageMaker gambar harus diberi tag](#)
- [\[SES.1\] Daftar kontak SES harus ditandai](#)
- [\[SES.2\] Set konfigurasi SES harus ditandai](#)
- [\[SQS.1\] Antrian Amazon SQS harus dienkripsi saat istirahat](#)
- [\[SQS.2\] Antrian SQS harus ditandai](#)
- [\[SQS.3\] Kebijakan akses antrian SQS seharusnya tidak mengizinkan akses publik](#)

- [\[SSM.3\] EC2 Instans Amazon yang dikelola oleh Systems Manager harus memiliki status kepatuhan asosiasi COMPLIANT](#)
- [\[Transfer.3\] Konektor Transfer Family seharusnya mengaktifkan logging](#)
- [\[Transfer.4\] Perjanjian Transfer Family harus ditandai](#)
- [\[WAF.1\] Pencatatan ACL Web Global AWS WAF Klasik harus diaktifkan](#)
- [\[WAF.3\] Kelompok aturan Regional AWS WAF Klasik harus memiliki setidaknya satu aturan](#)
- [\[WAF.6\] Aturan global AWS WAF klasik harus memiliki setidaknya satu syarat](#)
- [\[WAF.7\] Kelompok aturan global AWS WAF klasik harus memiliki setidaknya satu aturan](#)
- [\[WAF.8\] Web global AWS WAF klasik ACLs harus memiliki setidaknya satu aturan atau kelompok aturan](#)
- [\[WAF.10\] AWS WAF web ACLs harus memiliki setidaknya satu aturan atau kelompok aturan](#)
- [\[WAF.11\] pencatatan ACL AWS WAF web harus diaktifkan](#)
- [\[WorkSpaces.1\] volume WorkSpaces pengguna harus dienkrpsi saat istirahat](#)
- [\[WorkSpaces.2\] volume WorkSpaces root harus dienkrpsi saat istirahat](#)

Israel (Tel Aviv)

Kontrol berikut tidak didukung di Wilayah Israel (Tel Aviv).

- [\[APIGateway.8\] Rute API Gateway harus menentukan jenis otorisasi](#)
- [\[APIGateway.9\] Pencatatan akses harus dikonfigurasi untuk Tahap API Gateway V2](#)
- [\[Amplify.1\] Aplikasi Amplify harus diberi tag](#)
- [\[Amplify.2\] Amplify branch harus diberi tag](#)
- [\[AppFlow.1\] AppFlow Aliran Amazon harus ditandai](#)
- [\[AppRunner.1\] Layanan App Runner harus diberi tag](#)
- [\[AppRunner.2\] Konektor VPC App Runner harus diberi tag](#)
- [\[AppSync.1\] Cache AWS AppSync API harus dienkrpsi saat istirahat](#)
- [\[AppSync.2\] AWS AppSync harus mengaktifkan logging tingkat lapangan](#)
- [\[AppSync.5\] AWS AppSync APIs GraphQL tidak boleh diautentikasi dengan kunci API](#)
- [\[AppSync.6\] Cache AWS AppSync API harus dienkrpsi saat transit](#)
- [\[Backup.1\] titik AWS Backup pemulihan harus dienkrpsi saat istirahat](#)
- [\[Backup.4\] rencana AWS Backup laporan harus ditandai](#)

- [\[Batch.1\] Antrian pekerjaan batch harus ditandai](#)
- [\[Batch.3\] Lingkungan komputasi Batch harus ditandai](#)
- [\[Batch.4\] Properti sumber daya komputasi di lingkungan komputasi Batch terkelola harus ditandai](#)
- [\[CloudFront.1\] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi](#)
- [\[CloudFront.3\] CloudFront distribusi harus memerlukan enkripsi dalam perjalanan](#)
- [\[CloudFront.4\] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi](#)
- [\[CloudFront.5\] CloudFront distribusi seharusnya mengaktifkan logging](#)
- [\[CloudFront.6\] CloudFront distribusi harus mengaktifkan WAF](#)
- [\[CloudFront.7\] CloudFront distribusi harus menggunakan sertifikat SSL/TLS khusus](#)
- [\[CloudFront.8\] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS](#)
- [\[CloudFront.9\] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus](#)
- [\[CloudFront.10\] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal kustom](#)
- [\[CloudFront.12\] CloudFront distribusi seharusnya tidak menunjukkan asal S3 yang tidak ada](#)
- [\[CloudFront.13\] CloudFront distribusi harus menggunakan kontrol akses asal](#)
- [\[CloudFront.14\] CloudFront distribusi harus ditandai](#)
- [\[CodeArtifact.1\] CodeArtifact repositori harus ditandai](#)
- [\[CodeGuruProfiler.1\] Grup CodeGuru profil profiler harus diberi tag](#)
- [\[CodeGuruReviewer.1\] Asosiasi CodeGuru repositori peninjau harus diberi tag](#)
- [\[Connect.1\] Jenis objek Amazon Connect Customer Profiles harus diberi tag](#)
- [\[Connect.2\] Instans Amazon Connect seharusnya mengaktifkan logging CloudWatch](#)
- [\[DMS.2\] Sertifikat DMS harus ditandai](#)
- [\[DMS.3\] Langganan acara DMS harus ditandai](#)
- [\[DMS.4\] Contoh replikasi DMS harus ditandai](#)
- [\[DMS.5\] Grup subnet replikasi DMS harus ditandai](#)
- [\[DMS.6\] Instans replikasi DMS harus mengaktifkan peningkatan versi minor otomatis](#)
- [\[DMS.7\] Tugas replikasi DMS untuk database target seharusnya mengaktifkan logging](#)
- [\[DMS.8\] Tugas replikasi DMS untuk database sumber seharusnya mengaktifkan logging](#)
- [\[DMS.9\] Titik akhir DMS harus menggunakan SSL](#)
- [\[DMS.10\] Titik akhir DMS untuk database Neptune harus mengaktifkan otorisasi IAM](#)
- [\[DMS.11\] Titik akhir DMS untuk MongoDB harus mengaktifkan mekanisme otentikasi](#)

- [\[DMS.12\] Titik akhir DMS untuk Redis OSS seharusnya mengaktifkan TLS](#)
- [\[DocumentDB.1\] Cluster Amazon DocumentDB harus dienkripsi saat istirahat](#)
- [\[DocumentDB.2\] Cluster Amazon DocumentDB harus memiliki periode retensi cadangan yang memadai](#)
- [\[DocumentDB.3\] Cuplikan cluster manual Amazon DocumentDB seharusnya tidak bersifat publik](#)
- [\[DocumentDB.4\] Cluster Amazon DocumentDB harus mempublikasikan log audit ke Log CloudWatch](#)
- [\[DocumentDB.5\] Cluster Amazon DocumentDB harus mengaktifkan perlindungan penghapusan](#)
- [\[DocumentDB.6\] Cluster Amazon DocumentDB harus dienkripsi saat transit](#)
- [\[DynamoDB.3\] Cluster DynamoDB Accelerator \(DAX\) harus dienkripsi saat istirahat](#)
- [\[DynamoDB.4\] Tabel DynamoDB harus ada dalam rencana cadangan](#)
- [\[DynamoDB.7\] Cluster DynamoDB Accelerator harus dienkripsi saat transit](#)
- [\[EC2.4\] EC2 Instans yang dihentikan harus dihapus setelah periode waktu tertentu](#)
- [\[EC2.14\] Grup keamanan seharusnya tidak mengizinkan masuknya dari 0.0.0.0/0 atau :/0 ke port 3389](#)
- [\[EC2.20\] Kedua terowongan VPN untuk koneksi AWS Site-to-Site VPN harus siap](#)
- [\[EC2.22\] Grup EC2 keamanan Amazon yang tidak digunakan harus dihapus](#)
- [\[EC2.23\] Amazon EC2 Transit Gateways seharusnya tidak secara otomatis menerima permintaan lampiran VPC](#)
- [\[EC2.24\] Jenis instance EC2 paravirtual Amazon tidak boleh digunakan](#)
- [\[EC2.25\] Templat EC2 peluncuran Amazon tidak boleh menetapkan publik IPs ke antarmuka jaringan](#)
- [\[EC2.28\] Volume EBS harus dicakup oleh rencana cadangan](#)
- [\[EC2.33\] lampiran gateway EC2 transit harus ditandai](#)
- [\[EC2.34\] tabel rute gateway EC2 transit harus ditandai](#)
- [\[EC2.40\] Gateway EC2 NAT harus ditandai](#)
- [\[EC2.48\] Log aliran VPC Amazon harus diberi tag](#)
- [\[EC2.51\] Titik akhir EC2 Client VPN harus mengaktifkan pencatatan koneksi klien](#)
- [\[EC2.55\] VPCs harus dikonfigurasi dengan titik akhir antarmuka untuk ECR API](#)
- [\[EC2.56\] VPCs harus dikonfigurasi dengan titik akhir antarmuka untuk Docker Registry](#)
- [\[EC2.57\] VPCs harus dikonfigurasi dengan titik akhir antarmuka untuk Systems Manager](#)

- [\[EC2.58\] VPCs harus dikonfigurasi dengan titik akhir antarmuka untuk Kontak Manajer Insiden Systems Manager](#)
- [\[EC2.60\] VPCs harus dikonfigurasi dengan titik akhir antarmuka untuk Systems Manager Incident Manager](#)
- [\[EC2.170\] templat EC2 peluncuran harus menggunakan Layanan Metadata Instance Versi 2 \(\) IMDSv2](#)
- [\[EC2.173\] Permintaan Armada EC2 Spot harus mengaktifkan enkripsi untuk volume EBS terlampir](#)
- [\[EC2.175\] templat EC2 peluncuran harus diberi tag](#)
- [\[EC2.177\] Sesi cermin EC2 lalu lintas harus ditandai](#)
- [\[EC2.179\] Target cermin EC2 lalu lintas harus ditandai](#)
- [\[ECR.2\] Repositori pribadi ECR harus memiliki kekekalan tag yang dikonfigurasi](#)
- [\[ECR.3\] Repositori ECR harus memiliki setidaknya satu kebijakan siklus hidup yang dikonfigurasi](#)
- [\[ECR.4\] Repositori publik ECR harus ditandai](#)
- [\[ECR.5\] Repositori ECR harus dienkrpsi dengan pelanggan yang dikelola AWS KMS keys](#)
- [\[ECS.16\] Set tugas ECS seharusnya tidak secara otomatis menetapkan alamat IP publik](#)
- [\[EFS.1\] Sistem File Elastis harus dikonfigurasi untuk mengenkripsi data file saat istirahat menggunakan AWS KMS](#)
- [\[EFS.2\] Volume Amazon EFS harus dalam rencana cadangan](#)
- [\[EFS.3\] Titik akses EFS harus menegakkan direktori root](#)
- [\[EFS.4\] Titik akses EFS harus menegakkan identitas pengguna](#)
- [\[EFS.8\] Sistem file EFS harus dienkrpsi saat istirahat](#)
- [\[EKS.2\] Kluster EKS harus berjalan pada versi Kubernetes yang didukung](#)
- [\[EKS.6\] Kluster EKS harus ditandai](#)
- [\[EKS.7\] Konfigurasi penyedia identitas EKS harus ditandai](#)
- [\[EKS.8\] Kluster EKS harus mengaktifkan pencatatan audit](#)
- [\[ELB.2\] Classic Load Balancer dengan pendengar SSL/HTTPS harus menggunakan sertifikat yang disediakan oleh AWS Certificate Manager](#)
- [\[ELB.14\] Classic Load Balancer harus dikonfigurasi dengan mode mitigasi desync defensif atau paling ketat](#)
- [\[ELB.17\] Aplikasi dan Penyeimbang Beban Jaringan dengan pendengar harus menggunakan kebijakan keamanan yang direkomendasikan](#)
- [\[ElastiCache.1\] Cluster ElastiCache \(Redis OSS\) harus mengaktifkan pencadangan otomatis](#)

- [\[ElastiCache.2\] ElastiCache cluster harus mengaktifkan peningkatan versi minor otomatis](#)
- [\[ElastiCache.3\] grup ElastiCache replikasi harus mengaktifkan failover otomatis](#)
- [\[ElastiCache.4\] grup ElastiCache replikasi harus dienkripsi saat istirahat](#)
- [\[ElastiCache.5\] grup ElastiCache replikasi harus dienkripsi saat transit](#)
- [\[ElastiCache.6\] ElastiCache \(Redis OSS\) grup replikasi dari versi sebelumnya harus mengaktifkan Redis OSS AUTH](#)
- [\[ElastiCache.7\] ElastiCache cluster tidak boleh menggunakan grup subnet default](#)
- [\[ElasticBeanstalk.1\] Lingkungan Elastic Beanstalk seharusnya mengaktifkan pelaporan kesehatan yang ditingkatkan](#)
- [\[ElasticBeanstalk.2\] Pembaruan platform yang dikelola Elastic Beanstalk harus diaktifkan](#)
- [\[ElasticBeanstalk.3\] Elastic Beanstalk harus mengalirkan log ke CloudWatch](#)
- [\[EMR.1\] Node primer kluster EMR Amazon seharusnya tidak memiliki alamat IP publik](#)
- [\[EMR.3\] Konfigurasi keamanan Amazon EMR harus dienkripsi saat istirahat](#)
- [\[ES.4\] Kesalahan domain Elasticsearch yang masuk ke CloudWatch Log harus diaktifkan](#)
- [\[EventBridge.4\] titik akhir EventBridge global harus mengaktifkan replikasi acara](#)
- [\[FraudDetector.1\] Jenis entitas Amazon Fraud Detector harus diberi tag](#)
- [\[FraudDetector.2\] Label Amazon Fraud Detector harus diberi tag](#)
- [\[FraudDetector.3\] Hasil Amazon Fraud Detector harus ditandai](#)
- [\[FraudDetector.4\] Variabel Amazon Fraud Detector harus diberi tag](#)
- [\[GlobalAccelerator.1\] Akselerator Akselerator Global harus diberi tag](#)
- [\[Glue.4\] Pekerjaan AWS Glue percikan harus berjalan pada versi yang didukung AWS Glue](#)
- [\[GuardDuty.2\] GuardDuty filter harus diberi tag](#)
- [\[GuardDuty.3\] GuardDuty IPSets harus ditandai](#)
- [\[IAM.1\] Kebijakan IAM seharusnya tidak mengizinkan hak administratif “*” penuh](#)
- [\[IAM.2\] Pengguna IAM seharusnya tidak memiliki kebijakan IAM yang dilampirkan](#)
- [\[IAM.3\] Kunci akses pengguna IAM harus diputar setiap 90 hari atau kurang](#)
- [\[IAM.4\] Kunci akses pengguna root IAM seharusnya tidak ada](#)
- [\[IAM.5\] MFA harus diaktifkan untuk semua pengguna IAM yang memiliki kata sandi konsol](#)
- [\[IAM.6\] MFA perangkat keras harus diaktifkan untuk pengguna root](#)
- [\[IAM.7\] Kebijakan kata sandi untuk pengguna IAM harus memiliki konfigurasi yang kuat](#)
- [\[IAM.8\] Kredensi pengguna IAM yang tidak digunakan harus dihapus](#)

- [\[IAM.9\] MFA harus diaktifkan untuk pengguna root](#)
- [\[IAM.10\] Kebijakan kata sandi untuk pengguna IAM harus memiliki konfigurasi yang kuat](#)
- [\[IAM.11\] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu huruf besar](#)
- [\[IAM.12\] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu huruf kecil](#)
- [\[IAM.13\] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu simbol](#)
- [\[IAM.14\] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu nomor](#)
- [\[IAM.15\] Pastikan kebijakan kata sandi IAM membutuhkan panjang kata sandi minimum 14 atau lebih](#)
- [\[IAM.16\] Pastikan kebijakan kata sandi IAM mencegah penggunaan kembali kata sandi](#)
- [\[IAM.17\] Pastikan kebijakan kata sandi IAM kedaluwarsa kata sandi dalam waktu 90 hari atau kurang](#)
- [\[IAM.18\] Memastikan peran dukungan telah dibuat untuk mengelola insiden dengan AWS Dukungan](#)
- [\[IAM.19\] MFA harus diaktifkan untuk semua pengguna IAM](#)
- [\[IAM.21\] Kebijakan terkelola pelanggan IAM yang Anda buat seharusnya tidak mengizinkan tindakan wildcard untuk layanan](#)
- [\[IAM.22\] Kredensi pengguna IAM yang tidak digunakan selama 45 hari harus dihapus](#)
- [\[IAM.24\] Peran IAM harus ditandai](#)
- [\[IAM.25\] Pengguna IAM harus diberi tag](#)
- [\[IAM.26\] Sertifikat SSL/TLS kedaluwarsa yang dikelola di IAM harus dihapus](#)
- [\[IAM.27\] Identitas IAM seharusnya tidak memiliki kebijakan yang dilampirkan AWSCloudShellFullAccess](#)
- [\[IAM.28\] IAM Access Analyzer penganalisis akses eksternal harus diaktifkan](#)
- [\[Inspektor.1\] Pemindaian Amazon Inspector harus diaktifkan EC2](#)
- [\[Inspektor.2\] Pemindaian ECR Amazon Inspector harus diaktifkan](#)
- [\[Inspektor.3\] Pemindaian kode Amazon Inspector Lambda harus diaktifkan](#)
- [\[Inspektor.4\] Pemindaian standar Amazon Inspector Lambda harus diaktifkan](#)
- [\[IoT.1\] profil AWS IoT Device Defender keamanan harus ditandai](#)
- [\[IoT.2\] tindakan AWS IoT Core mitigasi harus ditandai](#)
- [AWS IoT Core Dimensi \[IoT.3\] harus ditandai](#)
- [\[IoT.4\] AWS IoT Core otorisasi harus diberi tag](#)

- [\[IoT.5\] alias AWS IoT Core peran harus ditandai](#)
- [AWS IoT Core Kebijakan \[IoT.6\] harus ditandai](#)
- [\[IoTEvents .1\] Input Peristiwa AWS IoT harus diberi tag](#)
- [\[IoTEvents .2\] Model detektor Acara AWS IoT harus diberi tag](#)
- [\[IoTEvents .3\] Model alarm AWS IoT Events harus diberi tag](#)
- [\[IoTSiteWise.1\] Model aset AWS IoT harus ditandai SiteWise](#)
- [\[IoTSiteWise.2\] Dasbor AWS IoT harus diberi tag SiteWise](#)
- [\[IoTSiteWise.3\] Gateway AWS IoT harus diberi tag SiteWise](#)
- [\[IoTSiteWise.4\] Portal AWS IoT harus diberi tag SiteWise](#)
- [\[IoTSiteWise.5\] Proyek AWS IoT harus diberi tag SiteWise](#)
- [\[IoTThingMaker.1\] Pekerjaan sinkronisasi AWS IoT harus ditandai ThingMaker](#)
- [\[IoTThingMaker.2\] Ruang kerja AWS IoT harus diberi tag ThingMaker](#)
- [\[IoTThingMaker.3\] Adegan AWS IoT harus diberi tag ThingMaker](#)
- [\[IoTThingMaker.4\] Entitas AWS IoT harus diberi tag ThingMaker](#)
- [\[IoTWireless .1\] Grup multicast Nirkabel AWS IoT harus diberi tag](#)
- [\[IoTWireless .2\] Profil layanan AWS IoT Wireless harus diberi tag](#)
- [\[IoTWireless .3\] Tugas AWS IoT FUOTA harus ditandai](#)
- [\[IVS.1\] Pasangan kunci pemutaran IVS harus ditandai](#)
- [\[IVS.2\] Konfigurasi perekaman IVS harus ditandai](#)
- [\[IVS.3\] Saluran IVS harus ditandai](#)
- [\[Keyspaces.1\] Ruang kunci Amazon Keyspaces harus diberi tag](#)
- [\[Kinesis.1\] Aliran kinesis harus dienkripsi saat istirahat](#)
- [\[Kinesis.2\] Aliran kinesis harus ditandai](#)
- [\[Kinesis.3\] Aliran kinesis harus memiliki periode retensi data yang memadai](#)
- [\[KMS.1\] Kebijakan yang dikelola pelanggan IAM tidak boleh mengizinkan tindakan dekripsi pada semua kunci KMS](#)
- [\[KMS.2\] Prinsipal IAM tidak boleh memiliki kebijakan inline IAM yang memungkinkan tindakan dekripsi pada semua kunci KMS](#)
- [\[Lambda.5\] Fungsi VPC Lambda harus beroperasi di beberapa Availability Zone](#)
- [\[Macie.1\] Amazon Macie harus diaktifkan](#)
- [\[MQ.2\] Broker ActiveMQ harus mengalirkan log audit ke CloudWatch](#)

- [\[MQ.3\] Broker Amazon MQ harus mengaktifkan peningkatan versi minor otomatis](#)
- [\[MQ.4\] Broker Amazon MQ harus diberi tag](#)
- [\[MQ.5\] Broker ActiveMQ harus menggunakan mode penerapan aktif/siaga](#)
- [\[MQ.6\] Broker RabbitMQ harus menggunakan mode penerapan cluster](#)
- [\[MSK.1\] Kluster MSK harus dienkripsi saat transit di antara node broker](#)
- [\[MSK.2\] Kluster MSK seharusnya telah meningkatkan pemantauan yang dikonfigurasi](#)
- [\[MSK.3\] Konektor MSK Connect harus dienkripsi saat transit](#)
- [\[Neptune.3\] Snapshot cluster Neptunus DB seharusnya tidak publik](#)
- [\[Neptune.6\] Snapshot cluster Neptunus DB harus dienkripsi saat istirahat](#)
- [\[NetworkFirewall.10\] Firewall Jaringan harus mengaktifkan perlindungan perubahan subnet](#)
- [\[Opensearch.1\] OpenSearch domain harus mengaktifkan enkripsi saat istirahat](#)
- [\[Opensearch.2\] OpenSearch domain tidak boleh diakses publik](#)
- [\[Opensearch.3\] OpenSearch domain harus mengenkripsi data yang dikirim antar node](#)
- [\[Opensearch.4\] login kesalahan OpenSearch domain ke Log harus diaktifkan CloudWatch](#)
- [\[Opensearch.5\] OpenSearch domain harus mengaktifkan pencatatan audit](#)
- [\[Opensearch.6\] OpenSearch domain harus memiliki setidaknya tiga node data](#)
- [\[Opensearch.7\] OpenSearch domain harus mengaktifkan kontrol akses berbutir halus](#)
- [\[Opensearch.8\] Koneksi ke OpenSearch domain harus dienkripsi menggunakan kebijakan keamanan TLS terbaru](#)
- [\[Opensearch.9\] domain harus ditandai OpenSearch](#)
- [\[Opensearch.10\] OpenSearch domain harus menginstal pembaruan perangkat lunak terbaru](#)
- [\[Opensearch.11\] OpenSearch domain harus memiliki setidaknya tiga node primer khusus](#)
- [\[RDS.1\] Snapshot RDS harus bersifat pribadi](#)
- [\[RDS.4\] Snapshot cluster RDS dan snapshot database harus dienkripsi saat istirahat](#)
- [\[RDS.14\] Cluster Amazon Aurora seharusnya mengaktifkan backtracking](#)
- [\[RDS.15\] Cluster RDS DB harus dikonfigurasi untuk beberapa Availability Zone](#)
- [\[RDS.26\] Instans RDS DB harus dilindungi oleh rencana cadangan](#)
- [\[RDS.29\] Snapshot cluster RDS DB harus ditandai](#)
- [\[RDS.31\] Grup keamanan RDS DB harus ditandai](#)
- [\[RDS.35\] Cluster RDS DB harus mengaktifkan peningkatan versi minor otomatis](#)
- [\[RDS.37\] Cluster Aurora PostgreSQL DB harus menerbitkan log ke Log CloudWatch](#)

- [\[Redshift.3\] Cluster Amazon Redshift harus mengaktifkan snapshot otomatis](#)
- [\[Redshift.8\] Cluster Amazon Redshift tidak boleh menggunakan nama pengguna Admin default](#)
- [\[Redshift.9\] Cluster Redshift tidak boleh menggunakan nama database default](#)
- [\[RedshiftServerless.1\] Grup kerja Amazon Redshift Tanpa Server harus menggunakan perutean VPC yang disempurnakan](#)
- [\[RedshiftServerless.2\] Koneksi ke grup kerja Redshift Serverless harus diperlukan untuk menggunakan SSL](#)
- [\[Route53.1\] Pemeriksaan kesehatan rute 53 harus ditandai](#)
- [\[Route53.2\] Route 53 zona yang dihosting publik harus mencatat kueri DNS](#)
- [\[S3.24\] Poin Akses Multi-Wilayah S3 harus mengaktifkan pengaturan akses publik blok](#)
- [\[SageMaker.1\] Instans SageMaker notebook Amazon seharusnya tidak memiliki akses internet langsung](#)
- [\[SageMaker.2\] instance SageMaker notebook harus diluncurkan dalam VPC khusus](#)
- [\[SageMaker.3\] Pengguna seharusnya tidak memiliki akses root ke instance SageMaker notebook](#)
- [\[SageMaker.5\] SageMaker model harus memblokir lalu lintas masuk](#)
- [\[ServiceCatalog.1\] Portofolio Service Catalog harus dibagikan hanya dalam suatu organisasi AWS](#)
- [\[SQS.1\] Antrian Amazon SQS harus dienkripsi saat istirahat](#)
- [\[SQS.2\] Antrian SQS harus ditandai](#)
- [\[SQS.3\] Kebijakan akses antrian SQS seharusnya tidak mengizinkan akses publik](#)
- [\[SSM.3\] EC2 Instans Amazon yang dikelola oleh Systems Manager harus memiliki status kepatuhan asosiasi COMPLIANT](#)
- [\[SSM.4\] Dokumen SSM seharusnya tidak bersifat publik](#)
- [\[StepFunctions.1\] Mesin status Step Functions seharusnya mengaktifkan logging](#)
- [\[Transfer.3\] Konektor Transfer Family seharusnya mengaktifkan logging](#)
- [\[Transfer.4\] Perjanjian Transfer Family harus ditandai](#)
- [\[WAF.1\] Pencatatan ACL Web Global AWS WAF Klasik harus diaktifkan](#)
- [\[WAF.3\] Kelompok aturan Regional AWS WAF Klasik harus memiliki setidaknya satu aturan](#)
- [\[WAF.6\] Aturan global AWS WAF klasik harus memiliki setidaknya satu syarat](#)
- [\[WAF.7\] Kelompok aturan global AWS WAF klasik harus memiliki setidaknya satu aturan](#)
- [\[WAF.8\] Web global AWS WAF klasik ACLs harus memiliki setidaknya satu aturan atau kelompok aturan](#)

- [\[WAF.11\] pencatatan ACL AWS WAF web harus diaktifkan](#)
- [\[WorkSpaces.1\] volume WorkSpaces pengguna harus dienkrpsi saat istirahat](#)
- [\[WorkSpaces.2\] volume WorkSpaces root harus dienkrpsi saat istirahat](#)

Meksiko (Tengah)

Kontrol berikut tidak didukung di Wilayah Meksiko (Tengah).

- [\[ACM.1\] Sertifikat yang diimpor dan diterbitkan ACM harus diperbarui setelah jangka waktu tertentu](#)
- [\[ACM.2\] Sertifikat RSA yang dikelola oleh ACM harus menggunakan panjang kunci minimal 2.048 bit](#)
- [\[ACM.3\] Sertifikat ACM harus ditandai](#)
- [\[Akun.1\] Informasi kontak keamanan harus disediakan untuk Akun AWS](#)
- [\[Akun.2\] Akun AWS harus menjadi bagian dari organisasi AWS Organizations](#)
- [\[APIGateway.1\] API Gateway REST dan pencatatan eksekusi WebSocket API harus diaktifkan](#)
- [\[APIGateway.2\] Tahapan API Gateway REST API harus dikonfigurasi untuk menggunakan sertifikat SSL untuk otentikasi backend](#)
- [\[APIGateway.3\] Tahapan API Gateway REST API harus mengaktifkan AWS X-Ray penelusuran](#)
- [\[APIGateway.4\] API Gateway harus dikaitkan dengan ACL Web WAF](#)
- [\[APIGateway.5\] Data cache API Gateway REST API harus dienkrpsi saat istirahat](#)
- [\[APIGateway.8\] Rute API Gateway harus menentukan jenis otorisasi](#)
- [\[APIGateway.9\] Pencatatan akses harus dikonfigurasi untuk Tahap API Gateway V2](#)
- [\[Amplify.1\] Aplikasi Amplify harus diberi tag](#)
- [\[Amplify.2\] Amplify branch harus diberi tag](#)
- [\[AppConfig.1\] AWS AppConfig aplikasi harus diberi tag](#)
- [\[AppConfig.2\] profil AWS AppConfig konfigurasi harus ditandai](#)
- [\[AppConfig.3\] AWS AppConfig lingkungan harus ditandai](#)
- [\[AppConfig.4\] asosiasi AWS AppConfig ekstensi harus ditandai](#)
- [\[AppFlow.1\] AppFlow Aliran Amazon harus ditandai](#)
- [\[AppRunner.1\] Layanan App Runner harus diberi tag](#)
- [\[AppRunner.2\] Konektor VPC App Runner harus diberi tag](#)
- [\[AppSync.1\] Cache AWS AppSync API harus dienkrpsi saat istirahat](#)

- [\[AppSync.2\] AWS AppSync harus mengaktifkan logging tingkat lapangan](#)
- [\[AppSync.4\] AWS AppSync APIs GraphQL harus diberi tag](#)
- [\[AppSync.5\] AWS AppSync APIs GraphQL tidak boleh diautentikasi dengan kunci API](#)
- [\[AppSync.6\] Cache AWS AppSync API harus dienkripsi saat transit](#)
- [\[Athena.2\] Katalog data Athena harus ditandai](#)
- [\[Athena.3\] Kelompok kerja Athena harus ditandai](#)
- [\[Athena.4\] Kelompok kerja Athena seharusnya mengaktifkan logging](#)
- [\[AutoScaling.2\] Grup EC2 Auto Scaling Amazon harus mencakup beberapa Availability Zone](#)
- [\[AutoScaling.3\] Konfigurasi peluncuran grup Auto Scaling harus EC2 mengonfigurasi instance agar memerlukan Layanan Metadata Instance Versi 2 \(\) IMDSv2](#)
- [\[AutoScaling.6\] Grup Auto Scaling harus menggunakan beberapa jenis instance di beberapa Availability Zone](#)
- [\[AutoScaling.9\] Grup EC2 Auto Scaling Amazon harus menggunakan templat peluncuran Amazon EC2](#)
- [\[AutoScaling.10\] Grup EC2 Auto Scaling harus diberi tag](#)
- [\[Backup.1\] titik AWS Backup pemulihan harus dienkripsi saat istirahat](#)
- [\[Backup.2\] poin AWS Backup pemulihan harus ditandai](#)
- [\[Backup.3\] AWS Backup brankas harus ditandai](#)
- [\[Backup.4\] rencana AWS Backup laporan harus ditandai](#)
- [\[Backup.5\] rencana AWS Backup cadangan harus ditandai](#)
- [\[Batch.1\] Antrian pekerjaan batch harus ditandai](#)
- [\[Batch.2\] Kebijakan penjadwalan batch harus ditandai](#)
- [\[Batch.3\] Lingkungan komputasi Batch harus ditandai](#)
- [\[Batch.4\] Properti sumber daya komputasi di lingkungan komputasi Batch dikelola harus ditandai](#)
- [\[CloudFormation.2\] CloudFormation tumpukan harus ditandai](#)
- [\[CloudFront.1\] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi](#)
- [\[CloudFront.3\] CloudFront distribusi harus memerlukan enkripsi dalam perjalanan](#)
- [\[CloudFront.4\] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi](#)
- [\[CloudFront.5\] CloudFront distribusi seharusnya mengaktifkan logging](#)
- [\[CloudFront.6\] CloudFront distribusi harus mengaktifkan WAF](#)

- [\[CloudFront.7\] CloudFront distribusi harus menggunakan sertifikat SSL/TLS khusus](#)
- [\[CloudFront.8\] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS](#)
- [\[CloudFront.9\] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus](#)
- [\[CloudFront.10\] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal kustom](#)
- [\[CloudFront.12\] CloudFront distribusi seharusnya tidak menunjukkan asal S3 yang tidak ada](#)
- [\[CloudFront.13\] CloudFront distribusi harus menggunakan kontrol akses asal](#)
- [\[CloudFront.14\] CloudFront distribusi harus ditandai](#)
- [\[CloudTrail.6\] Pastikan bucket S3 yang digunakan untuk menyimpan CloudTrail log tidak dapat diakses publik](#)
- [\[CloudTrail.7\] Pastikan pencatatan akses bucket S3 diaktifkan pada bucket CloudTrail S3](#)
- [\[CloudTrail.9\] CloudTrail jejak harus ditandai](#)
- [\[CloudTrail.10\] Penyimpanan data acara CloudTrail danau harus dienkripsi dengan pelanggan yang dikelola AWS KMS keys](#)
- [\[CloudWatch.17\] tindakan CloudWatch alarm harus diaktifkan](#)
- [\[CodeArtifact.1\] CodeArtifact repositori harus ditandai](#)
- [\[CodeBuild.1\] Repositori sumber CodeBuild Bitbucket tidak URLs boleh berisi kredensial sensitif](#)
- [\[CodeBuild.2\] variabel lingkungan CodeBuild proyek tidak boleh berisi kredensial teks yang jelas](#)
- [\[CodeBuild.3\] Log CodeBuild S3 harus dienkripsi](#)
- [\[CodeBuild.4\] lingkungan CodeBuild proyek harus memiliki urasi logging AWS Config](#)
- [\[CodeBuild.7\] ekspor kelompok CodeBuild laporan harus dienkripsi saat istirahat](#)
- [\[CodeGuruProfiler.1\] Grup CodeGuru profil profiler harus diberi tag](#)
- [\[CodeGuruReviewer.1\] Asosiasi CodeGuru repositori peninjau harus diberi tag](#)
- [\[Cognito.1\] Kumpulan pengguna Cognito harus mengaktifkan perlindungan ancaman dengan mode penegakan fungsi penuh untuk otentikasi standar](#)
- [\[Connect.1\] Jenis objek Amazon Connect Customer Profiles harus diberi tag](#)
- [\[Connect.2\] Instans Amazon Connect seharusnya mengaktifkan logging CloudWatch](#)
- [\[DataFirehose.1\] Aliran pengiriman Firehose harus dienkripsi saat istirahat](#)
- [\[DataSync.1\] DataSync tugas harus mengaktifkan logging](#)
- [\[DataSync.2\] DataSync tugas harus ditandai](#)
- [\[Detective.1\] Grafik perilaku detektif harus diberi tag](#)

- [\[DMS.1\] Instans replikasi Layanan Migrasi Database tidak boleh bersifat publik](#)
- [\[DMS.2\] Sertifikat DMS harus ditandai](#)
- [\[DMS.3\] Langganan acara DMS harus ditandai](#)
- [\[DMS.4\] Contoh replikasi DMS harus ditandai](#)
- [\[DMS.5\] Grup subnet replikasi DMS harus ditandai](#)
- [\[DMS.6\] Instans replikasi DMS harus mengaktifkan peningkatan versi minor otomatis](#)
- [\[DMS.7\] Tugas replikasi DMS untuk database target seharusnya mengaktifkan logging](#)
- [\[DMS.8\] Tugas replikasi DMS untuk database sumber seharusnya mengaktifkan logging](#)
- [\[DMS.9\] Titik akhir DMS harus menggunakan SSL](#)
- [\[DMS.10\] Titik akhir DMS untuk database Neptune harus mengaktifkan otorisasi IAM](#)
- [\[DMS.11\] Titik akhir DMS untuk MongoDB harus mengaktifkan mekanisme otentikasi](#)
- [\[DMS.12\] Titik akhir DMS untuk Redis OSS seharusnya mengaktifkan TLS](#)
- [\[DocumentDB.1\] Cluster Amazon DocumentDB harus dienkripsi saat istirahat](#)
- [\[DocumentDB.2\] Cluster Amazon DocumentDB harus memiliki periode retensi cadangan yang memadai](#)
- [\[DocumentDB.3\] Cuplikan cluster manual Amazon DocumentDB seharusnya tidak bersifat publik](#)
- [\[DocumentDB.4\] Cluster Amazon DocumentDB harus mempublikasikan log audit ke Log CloudWatch](#)
- [\[DocumentDB.5\] Cluster Amazon DocumentDB harus mengaktifkan perlindungan penghapusan](#)
- [\[DocumentDB.6\] Cluster Amazon DocumentDB harus dienkripsi saat transit](#)
- [\[DynamoDB.3\] Cluster DynamoDB Accelerator \(DAX\) harus dienkripsi saat istirahat](#)
- [\[DynamoDB.4\] Tabel DynamoDB harus ada dalam rencana cadangan](#)
- [\[DynamoDB.5\] Tabel DynamoDB harus diberi tag](#)
- [\[DynamoDB.6\] Tabel DynamoDB harus mengaktifkan perlindungan penghapusan](#)
- [\[DynamoDB.7\] Cluster DynamoDB Accelerator harus dienkripsi saat transit](#)
- [\[EC2.4\] EC2 Instans yang dihentikan harus dihapus setelah periode waktu tertentu](#)
- [\[EC2.21\] Jaringan ACLs seharusnya tidak mengizinkan masuknya dari 0.0.0.0/0 ke port 22 atau port 3389.](#)
- [\[EC2.22\] Grup EC2 keamanan Amazon yang tidak digunakan harus dihapus](#)
- [\[EC2.23\] Amazon EC2 Transit Gateways seharusnya tidak secara otomatis menerima permintaan lampiran VPC](#)

- [\[EC2.24\] Jenis instance EC2 paravirtual Amazon tidak boleh digunakan](#)
- [\[EC2.25\] Templat EC2 peluncuran Amazon tidak boleh menetapkan publik IPs ke antarmuka jaringan](#)
- [\[EC2.28\] Volume EBS harus dicakup oleh rencana cadangan](#)
- [\[EC2.33\] lampiran gateway EC2 transit harus ditandai](#)
- [\[EC2.34\] tabel rute gateway EC2 transit harus ditandai](#)
- [\[EC2.35\] antarmuka EC2 jaringan harus ditandai](#)
- [\[EC2.36\] gateway EC2 pelanggan harus ditandai](#)
- [\[EC2.37\] Alamat IP EC2 elastis harus ditandai](#)
- [\[EC2.38\] EC2 instance harus ditandai](#)
- [\[EC2.39\] gateway EC2 internet harus ditandai](#)
- [\[EC2.40\] Gateway EC2 NAT harus ditandai](#)
- [\[EC2.41\] EC2 jaringan ACLs harus ditandai](#)
- [\[EC2.42\] tabel EC2 rute harus ditandai](#)
- [\[EC2.43\] grup EC2 keamanan harus ditandai](#)
- [\[EC2.44\] EC2 subnet harus ditandai](#)
- [\[EC2.45\] EC2 volume harus ditandai](#)
- [\[EC2.46\] Amazon VPCs harus diberi tag](#)
- [\[EC2.47\] Layanan titik akhir Amazon VPC harus diberi tag](#)
- [\[EC2.48\] Log aliran VPC Amazon harus diberi tag](#)
- [\[EC2.49\] Koneksi peering VPC Amazon harus ditandai](#)
- [\[EC2.50\] Gateway EC2 VPN harus diberi tag](#)
- [\[EC2.51\] Titik akhir EC2 Client VPN harus mengaktifkan pencatatan koneksi klien](#)
- [\[EC2.52\] gateway EC2 transit harus ditandai](#)
- [\[EC2.53\] grup EC2 keamanan seharusnya tidak mengizinkan masuknya dari 0.0.0.0/0 ke port administrasi server jarak jauh](#)
- [\[EC2.54\] grup EC2 keamanan tidak boleh mengizinkan masuknya dari :/0 ke port administrasi server jarak jauh](#)
- [\[EC2.55\] VPCs harus dikonfigurasi dengan titik akhir antarmuka untuk ECR API](#)
- [\[EC2.56\] VPCs harus dikonfigurasi dengan titik akhir antarmuka untuk Docker Registry](#)
- [\[EC2.57\] VPCs harus dikonfigurasi dengan titik akhir antarmuka untuk Systems Manager](#)

- [\[EC2.58\] VPCs harus dikonfigurasi dengan titik akhir antarmuka untuk Kontak Manajer Insiden Systems Manager](#)
- [\[EC2.60\] VPCs harus dikonfigurasi dengan titik akhir antarmuka untuk Systems Manager Incident Manager](#)
- [\[EC2.170\] templat EC2 peluncuran harus menggunakan Layanan Metadata Instance Versi 2 \(\) IMDSv2](#)
- [\[EC2.171\] Koneksi EC2 VPN seharusnya mengaktifkan logging](#)
- [\[EC2.172\] Pengaturan Akses Publik Blok EC2 VPC harus memblokir lalu lintas gateway internet](#)
- [\[EC2.173\] Permintaan Armada EC2 Spot harus mengaktifkan enkripsi untuk volume EBS terlampir](#)
- [\[EC2.174\] Set opsi EC2 DHCP harus ditandai](#)
- [\[EC2.175\] templat EC2 peluncuran harus diberi tag](#)
- [\[EC2.176\] daftar EC2 awalan harus ditandai](#)
- [\[EC2.177\] Sesi cermin EC2 lalu lintas harus ditandai](#)
- [\[EC2.178\] Filter cermin EC2 lalu lintas harus ditandai](#)
- [\[EC2.179\] Target cermin EC2 lalu lintas harus ditandai](#)
- [\[ECR.1\] Repositori pribadi ECR harus memiliki pemindaian gambar yang dikonfigurasi](#)
- [\[ECR.2\] Repositori pribadi ECR harus memiliki kekekalan tag yang dikonfigurasi](#)
- [\[ECR.3\] Repositori ECR harus memiliki setidaknya satu kebijakan siklus hidup yang dikonfigurasi](#)
- [\[ECR.4\] Repositori publik ECR harus ditandai](#)
- [\[ECR.5\] Repositori ECR harus dienkripsi dengan pelanggan yang dikelola AWS KMS keys](#)
- [\[ECS.2\] Layanan ECS seharusnya tidak memiliki alamat IP publik yang ditetapkan kepadanya secara otomatis](#)
- [\[ECS.3\] Definisi tugas ECS tidak boleh membagikan namespace proses host](#)
- [\[ECS.4\] Kontainer ECS harus berjalan sebagai non-hak istimewa](#)
- [\[ECS.5\] Wadah ECS harus dibatasi pada akses hanya-baca ke sistem file root](#)
- [\[ECS.8\] Rahasia tidak boleh diteruskan sebagai variabel lingkungan kontainer](#)
- [\[ECS.9\] Definisi tugas ECS harus memiliki konfigurasi logging](#)
- [\[ECS.10\] Layanan ECS Fargate harus berjalan pada versi platform Fargate terbaru](#)
- [\[ECS.12\] Cluster ECS harus menggunakan Wawasan Kontainer](#)
- [\[ECS.13\] Layanan ECS harus ditandai](#)
- [\[ECS.14\] Cluster ECS harus ditandai](#)

- [\[ECS.15\] Definisi tugas ECS harus ditandai](#)
- [\[ECS.16\] Set tugas ECS seharusnya tidak secara otomatis menetapkan alamat IP publik](#)
- [\[ECS.17\] Definisi tugas ECS tidak boleh menggunakan mode jaringan host](#)
- [\[EFS.1\] Sistem File Elastis harus dikonfigurasi untuk mengenkripsi data file saat istirahat menggunakan AWS KMS](#)
- [\[EFS.2\] Volume Amazon EFS harus dalam rencana cadangan](#)
- [\[EFS.3\] Titik akses EFS harus menegakkan direktori root](#)
- [\[EFS.4\] Titik akses EFS harus menegakkan identitas pengguna](#)
- [\[EFS.5\] Titik akses EFS harus ditandai](#)
- [\[EFS.6\] Target pemasangan EFS tidak boleh dikaitkan dengan subnet publik](#)
- [\[EFS.7\] Sistem file EFS harus mengaktifkan pencadangan otomatis](#)
- [\[EFS.8\] Sistem file EFS harus dienkripsi saat istirahat](#)
- [\[EKS.2\] Kluster EKS harus berjalan pada versi Kubernetes yang didukung](#)
- [\[EKS.3\] Kluster EKS harus menggunakan rahasia Kubernetes terenkripsi](#)
- [\[EKS.6\] Kluster EKS harus ditandai](#)
- [\[EKS.7\] Konfigurasi penyedia identitas EKS harus ditandai](#)
- [\[EKS.8\] Kluster EKS harus mengaktifkan pencatatan audit](#)
- [\[ELB.7\] Classic Load Balancers harus mengaktifkan pengurusan koneksi](#)
- [\[ELB.10\] Classic Load Balancer harus menjangkau beberapa Availability Zone](#)
- [\[ELB.12\] Application Load Balancer harus dikonfigurasi dengan mode mitigasi desync defensif atau paling ketat](#)
- [\[ELB.13\] Penyeimbang Beban Aplikasi, Jaringan, dan Gateway harus mencakup beberapa Availability Zone](#)
- [\[ELB.14\] Classic Load Balancer harus dikonfigurasi dengan mode mitigasi desync defensif atau paling ketat](#)
- [\[ELB.17\] Aplikasi dan Penyeimbang Beban Jaringan dengan pendengar harus menggunakan kebijakan keamanan yang direkomendasikan](#)
- [\[ElastiCache.1\] Cluster ElastiCache \(Redis OSS\) harus mengaktifkan pencadangan otomatis](#)
- [\[ElastiCache.2\] ElastiCache cluster harus mengaktifkan peningkatan versi minor otomatis](#)
- [\[ElastiCache.3\] grup ElastiCache replikasi harus mengaktifkan failover otomatis](#)
- [\[ElastiCache.4\] grup ElastiCache replikasi harus dienkripsi saat istirahat](#)

- [\[ElastiCache.5\] grup ElastiCache replikasi harus dienkrpsi saat transit](#)
- [\[ElastiCache.6\] ElastiCache \(Redis OSS\) grup replikasi dari versi sebelumnya harus mengaktifkan Redis OSS AUTH](#)
- [\[ElastiCache.7\] ElastiCache cluster tidak boleh menggunakan grup subnet default](#)
- [\[ElasticBeanstalk.1\] Lingkungan Elastic Beanstalk seharusnya mengaktifkan pelaporan kesehatan yang ditingkatkan](#)
- [\[ElasticBeanstalk.2\] Pembaruan platform yang dikelola Elastic Beanstalk harus diaktifkan](#)
- [\[ElasticBeanstalk.3\] Elastic Beanstalk harus mengalirkan log ke CloudWatch](#)
- [\[EMR.1\] Node primer klaster EMR Amazon seharusnya tidak memiliki alamat IP publik](#)
- [\[EMR.2\] Pengaturan akses publik blok EMR Amazon harus diaktifkan](#)
- [\[EMR.3\] Konfigurasi keamanan Amazon EMR harus dienkrpsi saat istirahat](#)
- [\[EMR.4\] Konfigurasi keamanan Amazon EMR harus dienkrpsi saat transit](#)
- [\[ES.3\] Domain Elasticsearch harus mengenkripsi data yang dikirim antar node](#)
- [\[ES.4\] Kesalahan domain Elasticsearch yang masuk ke CloudWatch Log harus diaktifkan](#)
- [\[ES.5\] Domain Elasticsearch harus mengaktifkan pencatatan audit](#)
- [\[ES.6\] Domain Elasticsearch harus memiliki setidaknya tiga node data](#)
- [\[ES.7\] Domain Elasticsearch harus dikonfigurasi dengan setidaknya tiga node master khusus](#)
- [\[ES.8\] Koneksi ke domain Elasticsearch harus dienkrpsi menggunakan kebijakan keamanan TLS terbaru](#)
- [\[ES.9\] Domain Elasticsearch harus diberi tag](#)
- [\[EventBridge.2\] bus EventBridge acara harus diberi tag](#)
- [\[EventBridge.3\] bus acara EventBridge khusus harus memiliki kebijakan berbasis sumber daya terlampir](#)
- [\[EventBridge.4\] titik akhir EventBridge global harus mengaktifkan replikasi acara](#)
- [\[FraudDetector.1\] Jenis entitas Amazon Fraud Detector harus diberi tag](#)
- [\[FraudDetector.2\] Label Amazon Fraud Detector harus diberi tag](#)
- [\[FraudDetector.3\] Hasil Amazon Fraud Detector harus ditandai](#)
- [\[FraudDetector.4\] Variabel Amazon Fraud Detector harus diberi tag](#)
- [\[FSx.1\] FSx untuk sistem file OpenZFS harus dikonfigurasi untuk menyalin tag ke cadangan dan volume](#)
- [\[FSx.2\] FSx untuk sistem file Lustre harus dikonfigurasi untuk menyalin tag ke cadangan](#)

- [\[FSx.3\] FSx untuk sistem file OpenZFS harus dikonfigurasi untuk penyebaran Multi-AZ](#)
- [\[FSx.4\] FSx untuk sistem file NetApp ONTAP harus dikonfigurasi untuk penyebaran Multi-AZ](#)
- [\[FSx.5\] FSx untuk sistem file Windows File Server harus dikonfigurasi untuk penyebaran Multi-AZ](#)
- [\[GlobalAccelerator.1\] Akselerator Akselerator Global harus diberi tag](#)
- [AWS Glue Pekerjaan \[Glue.1\] harus ditandai](#)
- [\[Glue.3\] transformasi pembelajaran AWS Glue mesin harus dienkripsi saat istirahat](#)
- [\[Glue.4\] Pekerjaan AWS Glue percikan harus berjalan pada versi yang didukung AWS Glue](#)
- [\[GuardDuty.1\] GuardDuty harus diaktifkan](#)
- [\[GuardDuty.2\] GuardDuty filter harus diberi tag](#)
- [\[GuardDuty.3\] GuardDuty IPSets harus ditandai](#)
- [\[GuardDuty.4\] GuardDuty detektor harus diberi tag](#)
- [\[GuardDuty.5\] Pemantauan Log Audit GuardDuty EKS harus diaktifkan](#)
- [\[GuardDuty.6\] Perlindungan GuardDuty Lambda harus diaktifkan](#)
- [\[GuardDuty.7\] GuardDuty EKS Runtime Monitoring harus diaktifkan](#)
- [\[GuardDuty.8\] Perlindungan GuardDuty Malware untuk EC2 harus diaktifkan](#)
- [\[GuardDuty.9\] Perlindungan GuardDuty RDS harus diaktifkan](#)
- [\[GuardDuty.10\] Perlindungan GuardDuty S3 harus diaktifkan](#)
- [\[GuardDuty.11\] GuardDuty Runtime Monitoring harus diaktifkan](#)
- [\[GuardDuty.12\] GuardDuty ECS Runtime Monitoring harus diaktifkan](#)
- [\[GuardDuty.13\] GuardDuty EC2 Runtime Monitoring harus diaktifkan](#)
- [\[IAM.1\] Kebijakan IAM seharusnya tidak mengizinkan hak administratif “*” penuh](#)
- [\[IAM.2\] Pengguna IAM seharusnya tidak memiliki kebijakan IAM yang dilampirkan](#)
- [\[IAM.3\] Kunci akses pengguna IAM harus diputar setiap 90 hari atau kurang](#)
- [\[IAM.4\] Kunci akses pengguna root IAM seharusnya tidak ada](#)
- [\[IAM.5\] MFA harus diaktifkan untuk semua pengguna IAM yang memiliki kata sandi konsol](#)
- [\[IAM.6\] MFA perangkat keras harus diaktifkan untuk pengguna root](#)
- [\[IAM.7\] Kebijakan kata sandi untuk pengguna IAM harus memiliki konfigurasi yang kuat](#)
- [\[IAM.8\] Kredensi pengguna IAM yang tidak digunakan harus dihapus](#)
- [\[IAM.9\] MFA harus diaktifkan untuk pengguna root](#)
- [\[IAM.10\] Kebijakan kata sandi untuk pengguna IAM harus memiliki konfigurasi yang kuat](#)

- [\[IAM.11\] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu huruf besar](#)
- [\[IAM.12\] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu huruf kecil](#)
- [\[IAM.13\] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu simbol](#)
- [\[IAM.14\] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu nomor](#)
- [\[IAM.15\] Pastikan kebijakan kata sandi IAM membutuhkan panjang kata sandi minimum 14 atau lebih](#)
- [\[IAM.16\] Pastikan kebijakan kata sandi IAM mencegah penggunaan kembali kata sandi](#)
- [\[IAM.17\] Pastikan kebijakan kata sandi IAM kedaluwarsa kata sandi dalam waktu 90 hari atau kurang](#)
- [\[IAM.18\] Memastikan peran dukungan telah dibuat untuk mengelola insiden dengan AWS Dukungan](#)
- [\[IAM.19\] MFA harus diaktifkan untuk semua pengguna IAM](#)
- [\[IAM.21\] Kebijakan terkelola pelanggan IAM yang Anda buat seharusnya tidak mengizinkan tindakan wildcard untuk layanan](#)
- [\[IAM.22\] Kredensi pengguna IAM yang tidak digunakan selama 45 hari harus dihapus](#)
- [\[IAM.23\] Penganalisis Akses IAM harus ditandai](#)
- [\[IAM.24\] Peran IAM harus ditandai](#)
- [\[IAM.25\] Pengguna IAM harus diberi tag](#)
- [\[IAM.26\] Sertifikat SSL/TLS kedaluwarsa yang dikelola di IAM harus dihapus](#)
- [\[IAM.27\] Identitas IAM seharusnya tidak memiliki kebijakan yang dilampirkan AWSCloud ShellFullAccess](#)
- [\[IAM.28\] IAM Access Analyzer penganalisis akses eksternal harus diaktifkan](#)
- [\[Inspektor.1\] Pemindaian Amazon Inspector harus diaktifkan EC2](#)
- [\[Inspektor.2\] Pemindaian ECR Amazon Inspector harus diaktifkan](#)
- [\[Inspektor.3\] Pemindaian kode Amazon Inspector Lambda harus diaktifkan](#)
- [\[Inspektor.4\] Pemindaian standar Amazon Inspector Lambda harus diaktifkan](#)
- [\[IoT.1\] profil AWS IoT Device Defender keamanan harus ditandai](#)
- [\[IoT.2\] tindakan AWS IoT Core mitigasi harus ditandai](#)
- [AWS IoT Core Dimensi \[IoT.3\] harus ditandai](#)
- [\[IoT.4\] AWS IoT Core otorisasi harus diberi tag](#)
- [\[IoT.5\] alias AWS IoT Core peran harus ditandai](#)

- [AWS IoT Core Kebijakan \[IoT.6\] harus ditandai](#)
- [\[IoTEvents .1\] Input Peristiwa AWS IoT harus diberi tag](#)
- [\[IoTEvents .2\] Model detektor Acara AWS IoT harus diberi tag](#)
- [\[IoTEvents .3\] Model alarm AWS IoT Events harus diberi tag](#)
- [\[IoTSiteWise.1\] Model aset AWS IoT harus ditandai SiteWise](#)
- [\[IoTSiteWise.2\] Dasbor AWS IoT harus diberi tag SiteWise](#)
- [\[IoTSiteWise.3\] Gateway AWS IoT harus diberi tag SiteWise](#)
- [\[IoTSiteWise.4\] Portal AWS IoT harus diberi tag SiteWise](#)
- [\[IoTSiteWise.5\] Proyek AWS IoT harus diberi tag SiteWise](#)
- [\[IoT TwinMaker.1\] Pekerjaan sinkronisasi AWS IoT harus ditandai TwinMaker](#)
- [\[IoT TwinMaker.2\] Ruang kerja AWS IoT harus diberi tag TwinMaker](#)
- [\[IoT TwinMaker.3\] Adegan AWS IoT harus diberi tag TwinMaker](#)
- [\[IoT TwinMaker.4\] Entitas AWS IoT harus diberi tag TwinMaker](#)
- [\[IoTWireless .1\] Grup multicast Nirkabel AWS IoT harus diberi tag](#)
- [\[IoTWireless .2\] Profil layanan AWS IoT Wireless harus diberi tag](#)
- [\[IoTWireless .3\] Tugas AWS IoT FUOTA harus ditandai](#)
- [\[IVS.1\] Pasangan kunci pemutaran IVS harus ditandai](#)
- [\[IVS.2\] Konfigurasi perekaman IVS harus ditandai](#)
- [\[IVS.3\] Saluran IVS harus ditandai](#)
- [\[Keyspaces.1\] Ruang kunci Amazon Keyspaces harus diberi tag](#)
- [\[Kinesis.1\] Aliran kinesis harus dienkripsi saat istirahat](#)
- [\[Kinesis.2\] Aliran kinesis harus ditandai](#)
- [\[Kinesis.3\] Aliran kinesis harus memiliki periode retensi data yang memadai](#)
- [\[KMS.1\] Kebijakan yang dikelola pelanggan IAM tidak boleh mengizinkan tindakan dekripsi pada semua kunci KMS](#)
- [\[KMS.2\] Prinsipal IAM tidak boleh memiliki kebijakan inline IAM yang memungkinkan tindakan dekripsi pada semua kunci KMS](#)
- [\[KMS.3\] tidak AWS KMS keys boleh dihapus secara tidak sengaja](#)
- [\[KMS.5\] Kunci KMS tidak boleh diakses publik](#)
- [\[Lambda.5\] Fungsi VPC Lambda harus beroperasi di beberapa Availability Zone](#)
- [\[Lambda.6\] Fungsi Lambda harus ditandai](#)

- [\[Macie.1\] Amazon Macie harus diaktifkan](#)
- [\[Macie.2\] Penemuan data sensitif otomatis Macie harus diaktifkan](#)
- [\[MQ.2\] Broker ActiveMQ harus mengalirkan log audit ke CloudWatch](#)
- [\[MQ.3\] Broker Amazon MQ harus mengaktifkan peningkatan versi minor otomatis](#)
- [\[MQ.4\] Broker Amazon MQ harus diberi tag](#)
- [\[MQ.5\] Broker ActiveMQ harus menggunakan mode penerapan aktif/siaga](#)
- [\[MQ.6\] Broker RabbitMQ harus menggunakan mode penerapan cluster](#)
- [\[MSK.1\] Kluster MSK harus dienkripsi saat transit di antara node broker](#)
- [\[MSK.2\] Kluster MSK seharusnya telah meningkatkan pemantauan yang dikonfigurasi](#)
- [\[MSK.3\] Konektor MSK Connect harus dienkripsi saat transit](#)
- [\[Neptunus.1\] Cluster DB Neptunus harus dienkripsi saat istirahat](#)
- [\[Neptune.2\] Cluster DB Neptunus harus menerbitkan log audit ke Log CloudWatch](#)
- [\[Neptune.3\] Snapshot cluster Neptunus DB seharusnya tidak publik](#)
- [\[Neptunus.4\] Cluster DB Neptunus harus mengaktifkan perlindungan penghapusan](#)
- [\[Neptunus.5\] Cluster DB Neptunus harus mengaktifkan cadangan otomatis](#)
- [\[Neptune.6\] Snapshot cluster Neptunus DB harus dienkripsi saat istirahat](#)
- [\[Neptune.7\] Cluster DB Neptunus harus mengaktifkan otentikasi basis data IAM](#)
- [\[Neptunus.8\] Cluster DB Neptunus harus dikonfigurasi untuk menyalin tag ke snapshot](#)
- [\[Neptunus.9\] Cluster DB Neptunus harus digunakan di beberapa Availability Zone](#)
- [\[NetworkFirewall.1\] Firewall Jaringan harus digunakan di beberapa Availability Zone](#)
- [\[NetworkFirewall.2\] Pencatatan Firewall Jaringan harus diaktifkan](#)
- [\[NetworkFirewall.3\] Kebijakan Network Firewall harus memiliki setidaknya satu kelompok aturan yang terkait](#)
- [\[NetworkFirewall.4\] Tindakan stateless default untuk kebijakan Network Firewall harus drop atau forward untuk paket penuh](#)
- [\[NetworkFirewall.5\] Tindakan stateless default untuk kebijakan Network Firewall harus drop atau forward untuk paket yang terfragmentasi](#)
- [\[NetworkFirewall.6\] Grup aturan Stateless Network Firewall tidak boleh kosong](#)
- [\[NetworkFirewall.7\] Firewall Jaringan harus diberi tag](#)
- [\[NetworkFirewall.8\] Kebijakan firewall Network Firewall harus ditandai](#)
- [\[NetworkFirewall.9\] Firewall Jaringan harus mengaktifkan perlindungan penghapusan](#)

- [\[NetworkFirewall.10\] Firewall Jaringan harus mengaktifkan perlindungan perubahan subnet](#)
- [\[Opensearch.1\] OpenSearch domain harus mengaktifkan enkripsi saat istirahat](#)
- [\[Opensearch.2\] OpenSearch domain tidak boleh diakses publik](#)
- [\[Opensearch.3\] OpenSearch domain harus mengenkripsi data yang dikirim antar node](#)
- [\[Opensearch.4\] login kesalahan OpenSearch domain ke Log harus diaktifkan CloudWatch](#)
- [\[Opensearch.5\] OpenSearch domain harus mengaktifkan pencatatan audit](#)
- [\[Opensearch.6\] OpenSearch domain harus memiliki setidaknya tiga node data](#)
- [\[Opensearch.7\] OpenSearch domain harus mengaktifkan kontrol akses berbutir halus](#)
- [\[Opensearch.8\] Koneksi ke OpenSearch domain harus dienkripsi menggunakan kebijakan keamanan TLS terbaru](#)
- [\[Opensearch.9\] domain harus ditandai OpenSearch](#)
- [\[Opensearch.10\] OpenSearch domain harus menginstal pembaruan perangkat lunak terbaru](#)
- [\[Opensearch.11\] OpenSearch domain harus memiliki setidaknya tiga node primer khusus](#)
- [\[PCA.1\] otoritas sertifikat AWS Private CA root harus dinonaktifkan](#)
- [\[PCA.2\] Otoritas sertifikat CA AWS swasta harus ditandai](#)
- [\[RDS.14\] Cluster Amazon Aurora seharusnya mengaktifkan backtracking](#)
- [\[RDS.16\] Cluster RDS DB harus dikonfigurasi untuk menyalin tag ke snapshot](#)
- [\[RDS.17\] Instans RDS DB harus dikonfigurasi untuk menyalin tag ke snapshot](#)
- [\[RDS.18\] Instans RDS harus digunakan di VPC](#)
- [\[RDS.19\] Langganan pemberitahuan acara RDS yang ada harus dikonfigurasi untuk peristiwa kluster penting](#)
- [\[RDS.20\] Langganan pemberitahuan acara RDS yang ada harus dikonfigurasi untuk peristiwa instance basis data penting](#)
- [\[RDS.21\] Langganan pemberitahuan acara RDS harus dikonfigurasi untuk peristiwa grup parameter basis data penting](#)
- [\[RDS.22\] Langganan pemberitahuan acara RDS harus dikonfigurasi untuk acara grup keamanan basis data penting](#)
- [\[RDS.23\] Instans RDS tidak boleh menggunakan port default mesin database](#)
- [\[RDS.24\] Kluster Database RDS harus menggunakan nama pengguna administrator khusus](#)
- [\[RDS.25\] Instans database RDS harus menggunakan nama pengguna administrator khusus](#)
- [\[RDS.26\] Instans RDS DB harus dilindungi oleh rencana cadangan](#)

- [\[RDS.27\] Cluster RDS DB harus dienkripsi saat istirahat](#)
- [\[RDS.28\] Cluster RDS DB harus ditandai](#)
- [\[RDS.29\] Snapshot cluster RDS DB harus ditandai](#)
- [\[RDS.30\] Instans RDS DB harus ditandai](#)
- [\[RDS.31\] Grup keamanan RDS DB harus ditandai](#)
- [\[RDS.32\] Snapshot RDS DB harus ditandai](#)
- [\[RDS.33\] Grup subnet RDS DB harus ditandai](#)
- [\[RDS.34\] Kluster Aurora MySQL DB harus menerbitkan log audit ke Log CloudWatch](#)
- [\[RDS.35\] Cluster RDS DB harus mengaktifkan peningkatan versi minor otomatis](#)
- [\[RDS.36\] RDS untuk instance PostgreSQL DB harus menerbitkan log ke Log CloudWatch](#)
- [\[RDS.37\] Cluster Aurora PostgreSQL DB harus menerbitkan log ke Log CloudWatch](#)
- [\[RDS.38\] RDS untuk instance PostgreSQL DB harus dienkripsi saat transit](#)
- [\[RDS.39\] RDS untuk instance MySQL DB harus dienkripsi saat transit](#)
- [\[RDS.40\] RDS untuk instance SQL Server DB harus menerbitkan log ke Log CloudWatch](#)
- [\[RDS.41\] RDS untuk instance SQL Server DB harus dienkripsi saat transit](#)
- [\[RDS.42\] RDS untuk instance MariaDB DB harus menerbitkan log ke Log CloudWatch](#)
- [\[RDS.44\] RDS untuk instance MariaDB DB harus dienkripsi saat transit](#)
- [\[Redshift.1\] Cluster Amazon Redshift harus melarang akses publik](#)
- [\[Redshift.2\] Koneksi ke cluster Amazon Redshift harus dienkripsi saat transit](#)
- [\[Redshift.3\] Cluster Amazon Redshift harus mengaktifkan snapshot otomatis](#)
- [\[Redshift.4\] Cluster Amazon Redshift harus mengaktifkan pencatatan audit](#)
- [\[Redshift.6\] Amazon Redshift harus mengaktifkan peningkatan otomatis ke versi utama](#)
- [\[Redshift.7\] Cluster Redshift harus menggunakan perutean VPC yang ditingkatkan](#)
- [\[Redshift.8\] Cluster Amazon Redshift tidak boleh menggunakan nama pengguna Admin default](#)
- [\[Redshift.9\] Cluster Redshift tidak boleh menggunakan nama database default](#)
- [\[Redshift.10\] Cluster Redshift harus dienkripsi saat istirahat](#)
- [\[Redshift.11\] Cluster Redshift harus ditandai](#)
- [\[Redshift.12\] Langganan pemberitahuan acara Redshift harus ditandai](#)
- [\[Redshift.13\] Snapshot cluster Redshift harus ditandai](#)
- [\[Redshift.14\] Grup subnet cluster Redshift harus ditandai](#)

- [\[Redshift.15\] Grup keamanan Redshift harus mengizinkan masuknya port cluster hanya dari asal yang dibatasi](#)
- [\[Redshift.16\] Grup subnet cluster Redshift harus memiliki subnet dari beberapa Availability Zone](#)
- [\[Redshift.17\] Grup parameter cluster Redshift harus ditandai](#)
- [\[RedshiftServerless.1\] Grup kerja Amazon Redshift Tanpa Server harus menggunakan perutean VPC yang disempurnakan](#)
- [\[RedshiftServerless.2\] Koneksi ke grup kerja Redshift Serverless harus diperlukan untuk menggunakan SSL](#)
- [\[RedshiftServerless.3\] Kelompok kerja Redshift Tanpa Server harus melarang akses publik](#)
- [\[RedshiftServerless.4\] Ruang nama Redshift Tanpa Server harus dienkripsi dengan pengelolaan pelanggan AWS KMS keys](#)
- [\[RedshiftServerless.5\] Ruang nama Redshift Tanpa Server tidak boleh menggunakan nama pengguna admin default](#)
- [\[RedshiftServerless.6\] Ruang nama Redshift Tanpa Server harus mengeksport log ke Log CloudWatch](#)
- [\[RedshiftServerless.7\] Ruang nama Redshift Tanpa Server seharusnya tidak menggunakan nama database default](#)
- [\[Route53.1\] Pemeriksaan kesehatan rute 53 harus ditandai](#)
- [\[Route53.2\] Route 53 zona yang dihosting publik harus mencatat kueri DNS](#)
- [\[S3.7\] Ember tujuan umum S3 harus menggunakan replikasi lintas wilayah](#)
- [\[S3.10\] Bucket tujuan umum S3 dengan versi diaktifkan harus memiliki konfigurasi Siklus Hidup](#)
- [\[S3.11\] Bucket tujuan umum S3 harus mengaktifkan pemberitahuan acara](#)
- [\[S3.12\] tidak ACLs boleh digunakan untuk mengelola akses pengguna ke bucket tujuan umum S3](#)
- [\[S3.13\] Bucket tujuan umum S3 harus memiliki konfigurasi Siklus Hidup](#)
- [\[S3.19\] Titik akses S3 harus mengaktifkan pengaturan akses publik blok](#)
- [\[S3.20\] Bucket tujuan umum S3 harus mengaktifkan penghapusan MFA](#)
- [\[S3.22\] Bucket tujuan umum S3 harus mencatat peristiwa penulisan tingkat objek](#)
- [\[S3.23\] Bucket tujuan umum S3 harus mencatat peristiwa pembacaan tingkat objek](#)
- [\[S3.24\] Poin Akses Multi-Wilayah S3 harus mengaktifkan pengaturan akses publik blok](#)
- [\[SageMaker.1\] Instans SageMaker notebook Amazon seharusnya tidak memiliki akses internet langsung](#)
- [\[SageMaker.2\] instance SageMaker notebook harus diluncurkan dalam VPC khusus](#)

- [\[SageMaker.3\] Pengguna seharusnya tidak memiliki akses root ke instance SageMaker notebook](#)
- [\[SageMaker.4\] varian produksi SageMaker titik akhir harus memiliki jumlah instance awal yang lebih besar dari 1](#)
- [\[SageMaker.5\] SageMaker model harus memblokir lalu lintas masuk](#)
- [\[SageMaker.6\] konfigurasi gambar SageMaker aplikasi harus ditandai](#)
- [\[SageMaker.7\] SageMaker gambar harus diberi tag](#)
- [\[SageMaker.8\] instance SageMaker notebook harus berjalan pada platform yang didukung](#)
- [\[SES.1\] Daftar kontak SES harus ditandai](#)
- [\[SES.2\] Set konfigurasi SES harus ditandai](#)
- [\[SecretsManager.1\] Rahasia Secrets Manager harus mengaktifkan rotasi otomatis](#)
- [\[SecretsManager.2\] Rahasia Secrets Manager yang dikonfigurasi dengan rotasi otomatis harus berhasil diputar](#)
- [\[SecretsManager.3\] Hapus rahasia Secrets Manager yang tidak digunakan](#)
- [\[SecretsManager.4\] Rahasia Secrets Manager harus diputar dalam jumlah hari tertentu](#)
- [\[SecretsManager.5\] Rahasia Secrets Manager harus ditandai](#)
- [\[ServiceCatalog.1\] Portofolio Service Catalog harus dibagikan hanya dalam suatu organisasi AWS](#)
- [\[SNS.3\] Topik SNS harus ditandai](#)
- [\[SNS.4\] Kebijakan akses topik SNS seharusnya tidak mengizinkan akses publik](#)
- [\[SQS.1\] Antrian Amazon SQS harus dienkripsi saat istirahat](#)
- [\[SQS.2\] Antrian SQS harus ditandai](#)
- [\[SQS.3\] Kebijakan akses antrian SQS seharusnya tidak mengizinkan akses publik](#)
- [\[SSM.3\] EC2 Instans Amazon yang dikelola oleh Systems Manager harus memiliki status kepatuhan asosiasi COMPLIANT](#)
- [\[SSM.4\] Dokumen SSM seharusnya tidak bersifat publik](#)
- [\[SSM.5\] Dokumen SSM harus ditandai](#)
- [\[StepFunctions.1\] Mesin status Step Functions seharusnya mengaktifkan logging](#)
- [\[StepFunctions.2\] Aktivitas Step Functions harus diberi tag](#)
- [\[Transfer.1\] AWS Transfer Family alur kerja harus ditandai](#)
- [\[Transfer.2\] Server Transfer Family tidak boleh menggunakan protokol FTP untuk koneksi titik akhir](#)
- [\[Transfer.3\] Konektor Transfer Family seharusnya mengaktifkan logging](#)
- [\[Transfer.4\] Perjanjian Transfer Family harus ditandai](#)

- [\[Transfer.5\] Sertifikat Transfer Family harus diberi tag](#)
- [\[Transfer.6\] Konektor Transfer Family harus diberi tag](#)
- [\[Transfer.7\] Profil Transfer Family harus diberi tag](#)
- [\[WAF.1\] Pencatatan ACL Web Global AWS WAF Klasik harus diaktifkan](#)
- [\[WAF.2\] Aturan Regional AWS WAF Klasik harus memiliki setidaknya satu syarat](#)
- [\[WAF.3\] Kelompok aturan Regional AWS WAF Klasik harus memiliki setidaknya satu aturan](#)
- [\[WAF.4\] Web Regional AWS WAF Klasik ACLs harus memiliki setidaknya satu aturan atau kelompok aturan](#)
- [\[WAF.6\] Aturan global AWS WAF klasik harus memiliki setidaknya satu syarat](#)
- [\[WAF.7\] Kelompok aturan global AWS WAF klasik harus memiliki setidaknya satu aturan](#)
- [\[WAF.8\] Web global AWS WAF klasik ACLs harus memiliki setidaknya satu aturan atau kelompok aturan](#)
- [\[WAF.10\] AWS WAF web ACLs harus memiliki setidaknya satu aturan atau kelompok aturan](#)
- [\[WAF.11\] pencatatan ACL AWS WAF web harus diaktifkan](#)
- [AWS WAF Aturan \[WAF.12\] harus mengaktifkan metrik CloudWatch](#)
- [\[WorkSpaces.1\] volume WorkSpaces pengguna harus dienkrpsi saat istirahat](#)
- [\[WorkSpaces.2\] volume WorkSpaces root harus dienkrpsi saat istirahat](#)

Timur Tengah (Bahrain)

Kontrol berikut tidak didukung di Wilayah Timur Tengah (Bahrain).

- [\[AppFlow.1\] AppFlow Aliran Amazon harus ditandai](#)
- [\[AppRunner.1\] Layanan App Runner harus diberi tag](#)
- [\[AppRunner.2\] Konektor VPC App Runner harus diberi tag](#)
- [\[CloudFront.1\] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi](#)
- [\[CloudFront.3\] CloudFront distribusi harus memerlukan enkripsi dalam perjalanan](#)
- [\[CloudFront.4\] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi](#)
- [\[CloudFront.5\] CloudFront distribusi seharusnya mengaktifkan logging](#)
- [\[CloudFront.6\] CloudFront distribusi harus mengaktifkan WAF](#)
- [\[CloudFront.7\] CloudFront distribusi harus menggunakan sertifikat SSL/TLS khusus](#)
- [\[CloudFront.8\] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS](#)

- [\[CloudFront.9\] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus](#)
- [\[CloudFront.10\] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal kustom](#)
- [\[CloudFront.12\] CloudFront distribusi seharusnya tidak menunjukkan asal S3 yang tidak ada](#)
- [\[CloudFront.13\] CloudFront distribusi harus menggunakan kontrol akses asal](#)
- [\[CloudFront.14\] CloudFront distribusi harus ditandai](#)
- [\[CloudTrail.10\] Penyimpanan data acara CloudTrail harus dienkripsi dengan pelanggan yang dikelola AWS KMS keys](#)
- [\[CodeArtifact.1\] CodeArtifact repositori harus ditandai](#)
- [\[CodeGuruProfiler.1\] Grup CodeGuru profil profiler harus diberi tag](#)
- [\[CodeGuruReviewer.1\] Asosiasi CodeGuru repositori peninjau harus diberi tag](#)
- [\[Connect.1\] Jenis objek Amazon Connect Customer Profiles harus diberi tag](#)
- [\[Connect.2\] Instans Amazon Connect seharusnya mengaktifkan logging CloudWatch](#)
- [\[DocumentDB.1\] Cluster Amazon DocumentDB harus dienkripsi saat istirahat](#)
- [\[DocumentDB.2\] Cluster Amazon DocumentDB harus memiliki periode retensi cadangan yang memadai](#)
- [\[DocumentDB.3\] Cuplikan cluster manual Amazon DocumentDB seharusnya tidak bersifat publik](#)
- [\[DocumentDB.4\] Cluster Amazon DocumentDB harus mempublikasikan log audit ke Log CloudWatch](#)
- [\[DocumentDB.5\] Cluster Amazon DocumentDB harus mengaktifkan perlindungan penghapusan](#)
- [\[DocumentDB.6\] Cluster Amazon DocumentDB harus dienkripsi saat transit](#)
- [\[DynamoDB.3\] Cluster DynamoDB Accelerator \(DAX\) harus dienkripsi saat istirahat](#)
- [\[DynamoDB.7\] Cluster DynamoDB Accelerator harus dienkripsi saat transit](#)
- [\[EC2.20\] Kedua terowongan VPN untuk koneksi AWS Site-to-Site VPN harus siap](#)
- [\[EC2.24\] Jenis instance EC2 paravirtual Amazon tidak boleh digunakan](#)
- [\[EC2.58\] VPCs harus dikonfigurasi dengan titik akhir antarmuka untuk Kontak Manajer Insiden Systems Manager](#)
- [\[EC2.60\] VPCs harus dikonfigurasi dengan titik akhir antarmuka untuk Systems Manager Incident Manager](#)
- [\[EC2.173\] Permintaan Armada EC2 Spot harus mengaktifkan enkripsi untuk volume EBS terlampir](#)
- [\[ECR.4\] Repositori publik ECR harus ditandai](#)

- [\[ECR.5\] Repositori ECR harus dienkripsi dengan pelanggan yang dikelola AWS KMS keys](#)
- [\[ECS.17\] Definisi tugas ECS tidak boleh menggunakan mode jaringan host](#)
- [\[ELB.17\] Aplikasi dan Penyeimbang Beban Jaringan dengan pendengar harus menggunakan kebijakan keamanan yang direkomendasikan](#)
- [\[EventBridge.4\] titik akhir EventBridge global harus mengaktifkan replikasi acara](#)
- [\[FraudDetector.1\] Jenis entitas Amazon Fraud Detector harus diberi tag](#)
- [\[FraudDetector.2\] Label Amazon Fraud Detector harus diberi tag](#)
- [\[FraudDetector.3\] Hasil Amazon Fraud Detector harus ditandai](#)
- [\[FraudDetector.4\] Variabel Amazon Fraud Detector harus diberi tag](#)
- [\[FSx.3\] FSx untuk sistem file OpenZFS harus dikonfigurasi untuk penyebaran Multi-AZ](#)
- [\[FSx.4\] FSx untuk sistem file NetApp ONTAP harus dikonfigurasi untuk penyebaran Multi-AZ](#)
- [\[FSx.5\] FSx untuk sistem file Windows File Server harus dikonfigurasi untuk penyebaran Multi-AZ](#)
- [\[GlobalAccelerator.1\] Akselerator Akselerator Global harus diberi tag](#)
- [\[Glue.4\] Pekerjaan AWS Glue percikan harus berjalan pada versi yang didukung AWS Glue](#)
- [\[GuardDuty.11\] GuardDuty Runtime Monitoring harus diaktifkan](#)
- [\[GuardDuty.12\] GuardDuty ECS Runtime Monitoring harus diaktifkan](#)
- [\[GuardDuty.13\] GuardDuty EC2 Runtime Monitoring harus diaktifkan](#)
- [\[IAM.26\] Sertifikat SSL/TLS kedaluwarsa yang dikelola di IAM harus dihapus](#)
- [\[Inspektor.3\] Pemindaian kode Amazon Inspector Lambda harus diaktifkan](#)
- [\[IoTEvents.1\] Input Peristiwa AWS IoT harus diberi tag](#)
- [\[IoTEvents.2\] Model detektor Acara AWS IoT harus diberi tag](#)
- [\[IoTEvents.3\] Model alarm AWS IoT Events harus diberi tag](#)
- [\[IoTSiteWise.1\] Model aset AWS IoT harus ditandai SiteWise](#)
- [\[IoTSiteWise.2\] Dasbor AWS IoT harus diberi tag SiteWise](#)
- [\[IoTSiteWise.3\] Gateway AWS IoT harus diberi tag SiteWise](#)
- [\[IoTSiteWise.4\] Portal AWS IoT harus diberi tag SiteWise](#)
- [\[IoTSiteWise.5\] Proyek AWS IoT harus diberi tag SiteWise](#)
- [\[IoTThingMaker.1\] Pekerjaan sinkronisasi AWS IoT harus ditandai TwinMaker](#)
- [\[IoTThingMaker.2\] Ruang kerja AWS IoT harus diberi tag TwinMaker](#)
- [\[IoTThingMaker.3\] Adegan AWS IoT harus diberi tag TwinMaker](#)

- [\[IoT Twin Maker.4\] Entitas AWS IoT harus diberi tag TwinMaker](#)
- [\[IoT Wireless .1\] Grup multicast Nirkabel AWS IoT harus diberi tag](#)
- [\[IoT Wireless .2\] Profil layanan AWS IoT Wireless harus diberi tag](#)
- [\[IoT Wireless .3\] Tugas AWS IoT FUOTA harus ditandai](#)
- [\[IVS.1\] Pasangan kunci pemutaran IVS harus ditandai](#)
- [\[IVS.2\] Konfigurasi perekaman IVS harus ditandai](#)
- [\[IVS.3\] Saluran IVS harus ditandai](#)
- [\[MSK.3\] Konektor MSK Connect harus dienkripsi saat transit](#)
- [\[NetworkFirewall.10\] Firewall Jaringan harus mengaktifkan perlindungan perubahan subnet](#)
- [\[RDS.14\] Cluster Amazon Aurora seharusnya mengaktifkan backtracking](#)
- [\[RDS.31\] Grup keamanan RDS DB harus ditandai](#)
- [\[RDS.41\] RDS untuk instance SQL Server DB harus dienkripsi saat transit](#)
- [\[RDS.42\] RDS untuk instance MariaDB DB harus menerbitkan log ke Log CloudWatch](#)
- [\[RDS.44\] RDS untuk instance MariaDB DB harus dienkripsi saat transit](#)
- [\[RedshiftServerless.1\] Grup kerja Amazon Redshift Tanpa Server harus menggunakan perutean VPC yang disempurnakan](#)
- [\[RedshiftServerless.2\] Koneksi ke grup kerja Redshift Serverless harus diperlukan untuk menggunakan SSL](#)
- [\[RedshiftServerless.3\] Kelompok kerja Redshift Tanpa Server harus melarang akses publik](#)
- [\[RedshiftServerless.4\] Ruang nama Redshift Tanpa Server harus dienkripsi dengan pengelolaan pelanggan AWS KMS keys](#)
- [\[RedshiftServerless.5\] Ruang nama Redshift Tanpa Server tidak boleh menggunakan nama pengguna admin default](#)
- [\[RedshiftServerless.6\] Ruang nama Redshift Tanpa Server harus mengeksport log ke Log CloudWatch](#)
- [\[RedshiftServerless.7\] Ruang nama Redshift Tanpa Server seharusnya tidak menggunakan nama database default](#)
- [\[Route53.1\] Pemeriksaan kesehatan rute 53 harus ditandai](#)
- [\[Route53.2\] Route 53 zona yang dihosting publik harus mencatat kueri DNS](#)
- [\[S3.24\] Poin Akses Multi-Wilayah S3 harus mengaktifkan pengaturan akses publik blok](#)
- [\[SageMaker.8\] instance SageMaker notebook harus berjalan pada platform yang didukung](#)

- [\[SQS.3\] Kebijakan akses antrian SQS seharusnya tidak mengizinkan akses publik](#)
- [\[Transfer.3\] Konektor Transfer Family seharusnya mengaktifkan logging](#)
- [\[WAF.1\] Pencatatan ACL Web Global AWS WAF Klasik harus diaktifkan](#)
- [\[WAF.6\] Aturan global AWS WAF klasik harus memiliki setidaknya satu syarat](#)
- [\[WAF.7\] Kelompok aturan global AWS WAF klasik harus memiliki setidaknya satu aturan](#)
- [\[WAF.8\] Web global AWS WAF klasik ACLs harus memiliki setidaknya satu aturan atau kelompok aturan](#)
- [\[WorkSpaces.1\] volume WorkSpaces pengguna harus dienkrpsi saat istirahat](#)
- [\[WorkSpaces.2\] volume WorkSpaces root harus dienkrpsi saat istirahat](#)

Timur Tengah (UEA)

Kontrol berikut tidak didukung di Wilayah Timur Tengah (UEA).

- [\[APIGateway.8\] Rute API Gateway harus menentukan jenis otorisasi](#)
- [\[APIGateway.9\] Pencatatan akses harus dikonfigurasi untuk Tahap API Gateway V2](#)
- [\[Amplify.1\] Aplikasi Amplify harus diberi tag](#)
- [\[Amplify.2\] Amplify branch harus diberi tag](#)
- [\[AppConfig.1\] AWS AppConfig aplikasi harus diberi tag](#)
- [\[AppConfig.2\] profil AWS AppConfig konfigurasi harus ditandai](#)
- [\[AppConfig.3\] AWS AppConfig lingkungan harus ditandai](#)
- [\[AppFlow.1\] AppFlow Aliran Amazon harus ditandai](#)
- [\[AppRunner.1\] Layanan App Runner harus diberi tag](#)
- [\[AppRunner.2\] Konektor VPC App Runner harus diberi tag](#)
- [\[AppSync.1\] Cache AWS AppSync API harus dienkrpsi saat istirahat](#)
- [\[AppSync.6\] Cache AWS AppSync API harus dienkrpsi saat transit](#)
- [\[AutoScaling.1\] Grup Auto Scaling yang terkait dengan penyeimbang beban harus menggunakan pemeriksaan kesehatan ELB](#)
- [\[Backup.1\] titik AWS Backup pemulihan harus dienkrpsi saat istirahat](#)
- [\[Backup.4\] rencana AWS Backup laporan harus ditandai](#)
- [\[CloudFront.1\] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi](#)
- [\[CloudFront.3\] CloudFront distribusi harus memerlukan enkripsi dalam perjalanan](#)

- [\[CloudFront.4\] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi](#)
- [\[CloudFront.5\] CloudFront distribusi seharusnya mengaktifkan logging](#)
- [\[CloudFront.6\] CloudFront distribusi harus mengaktifkan WAF](#)
- [\[CloudFront.7\] CloudFront distribusi harus menggunakan sertifikat SSL/TLS khusus](#)
- [\[CloudFront.8\] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS](#)
- [\[CloudFront.9\] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus](#)
- [\[CloudFront.10\] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal kustom](#)
- [\[CloudFront.12\] CloudFront distribusi seharusnya tidak menunjukkan asal S3 yang tidak ada](#)
- [\[CloudFront.13\] CloudFront distribusi harus menggunakan kontrol akses asal](#)
- [\[CloudFront.14\] CloudFront distribusi harus ditandai](#)
- [\[CloudTrail.1\] CloudTrail harus diaktifkan dan dikonfigurasi dengan setidaknya satu jejak Multi-wilayah yang mencakup acara manajemen baca dan tulis](#)
- [\[CloudTrail.6\] Pastikan bucket S3 yang digunakan untuk menyimpan CloudTrail log tidak dapat diakses publik](#)
- [\[CloudWatch.16\] grup CloudWatch log harus dipertahankan untuk jangka waktu tertentu](#)
- [\[CodeArtifact.1\] CodeArtifact repositori harus ditandai](#)
- [\[CodeGuruProfiler.1\] Grup CodeGuru profil profiler harus diberi tag](#)
- [\[CodeGuruReviewer.1\] Asosiasi CodeGuru repositori peninjau harus diberi tag](#)
- [\[Cognito.1\] Kumpulan pengguna Cognito harus mengaktifkan perlindungan ancaman dengan mode penegakan fungsi penuh untuk otentikasi standar](#)
- [\[Connect.1\] Jenis objek Amazon Connect Customer Profiles harus diberi tag](#)
- [\[Connect.2\] Instans Amazon Connect seharusnya mengaktifkan logging CloudWatch](#)
- [\[Detective.1\] Grafik perilaku detektif harus diberi tag](#)
- [\[DMS.2\] Sertifikat DMS harus ditandai](#)
- [\[DMS.3\] Langganan acara DMS harus ditandai](#)
- [\[DMS.4\] Contoh replikasi DMS harus ditandai](#)
- [\[DMS.5\] Grup subnet replikasi DMS harus ditandai](#)
- [\[DMS.6\] Instans replikasi DMS harus mengaktifkan peningkatan versi minor otomatis](#)
- [\[DMS.7\] Tugas replikasi DMS untuk database target seharusnya mengaktifkan logging](#)
- [\[DMS.8\] Tugas replikasi DMS untuk database sumber seharusnya mengaktifkan logging](#)

- [\[DMS.9\] Titik akhir DMS harus menggunakan SSL](#)
- [\[DMS.10\] Titik akhir DMS untuk database Neptune harus mengaktifkan otorisasi IAM](#)
- [\[DMS.11\] Titik akhir DMS untuk MongoDB harus mengaktifkan mekanisme otentikasi](#)
- [\[DMS.12\] Titik akhir DMS untuk Redis OSS seharusnya mengaktifkan TLS](#)
- [\[DynamoDB.3\] Cluster DynamoDB Accelerator \(DAX\) harus dienkripsi saat istirahat](#)
- [\[DynamoDB.4\] Tabel DynamoDB harus ada dalam rencana cadangan](#)
- [\[DynamoDB.7\] Cluster DynamoDB Accelerator harus dienkripsi saat transit](#)
- [\[EC2.4\] EC2 Instans yang dihentikan harus dihapus setelah periode waktu tertentu](#)
- [\[EC2.8\] EC2 instans harus menggunakan Instance Metadata Service Versi 2 \(\) IMDSv2](#)
- [\[EC2.12\] Amazon yang tidak terpakai EC2 EIPs harus dihapus](#)
- [\[EC2.14\] Grup keamanan seharusnya tidak mengizinkan masuknya dari 0.0.0.0/0 atau :/0 ke port 3389](#)
- [\[EC2.22\] Grup EC2 keamanan Amazon yang tidak digunakan harus dihapus](#)
- [\[EC2.24\] Jenis instance EC2 paravirtual Amazon tidak boleh digunakan](#)
- [\[EC2.25\] Templat EC2 peluncuran Amazon tidak boleh menetapkan publik IPs ke antarmuka jaringan](#)
- [\[EC2.28\] Volume EBS harus dicakup oleh rencana cadangan](#)
- [\[EC2.51\] Titik akhir EC2 Client VPN harus mengaktifkan pencatatan koneksi klien](#)
- [\[EC2.58\] VPCs harus dikonfigurasi dengan titik akhir antarmuka untuk Kontak Manajer Insiden Systems Manager](#)
- [\[EC2.60\] VPCs harus dikonfigurasi dengan titik akhir antarmuka untuk Systems Manager Incident Manager](#)
- [\[EC2.170\] templat EC2 peluncuran harus menggunakan Layanan Metadata Instance Versi 2 \(\) IMDSv2](#)
- [\[EC2.173\] Permintaan Armada EC2 Spot harus mengaktifkan enkripsi untuk volume EBS terlampir](#)
- [\[EC2.175\] templat EC2 peluncuran harus diberi tag](#)
- [\[EC2.177\] Sesi cermin EC2 lalu lintas harus ditandai](#)
- [\[EC2.179\] Target cermin EC2 lalu lintas harus ditandai](#)
- [\[ECR.4\] Repositori publik ECR harus ditandai](#)
- [\[ECS.1\] Definisi tugas Amazon ECS harus memiliki mode jaringan yang aman dan definisi pengguna](#)

- [\[EFS.1\] Sistem File Elastis harus dikonfigurasi untuk mengenkripsi data file saat istirahat menggunakan AWS KMS](#)
- [\[EFS.2\] Volume Amazon EFS harus dalam rencana cadangan](#)
- [\[ELB.3\] Pendengar Classic Load Balancer harus dikonfigurasi dengan penghentian HTTPS atau TLS](#)
- [\[ELB.14\] Classic Load Balancer harus dikonfigurasi dengan mode mitigasi desync defensif atau paling ketat](#)
- [\[ELB.17\] Aplikasi dan Penyeimbang Beban Jaringan dengan pendengar harus menggunakan kebijakan keamanan yang direkomendasikan](#)
- [\[ElastiCache.1\] Cluster ElastiCache \(Redis OSS\) harus mengaktifkan pencadangan otomatis](#)
- [\[ElastiCache.2\] ElastiCache cluster harus mengaktifkan peningkatan versi minor otomatis](#)
- [\[ElastiCache.3\] grup ElastiCache replikasi harus mengaktifkan failover otomatis](#)
- [\[ElastiCache.4\] grup ElastiCache replikasi harus dienkripsi saat istirahat](#)
- [\[ElastiCache.5\] grup ElastiCache replikasi harus dienkripsi saat transit](#)
- [\[ElastiCache.6\] ElastiCache \(Redis OSS\) grup replikasi dari versi sebelumnya harus mengaktifkan Redis OSS AUTH](#)
- [\[ElastiCache.7\] ElastiCache cluster tidak boleh menggunakan grup subnet default](#)
- [\[ElasticBeanstalk.1\] Lingkungan Elastic Beanstalk seharusnya mengaktifkan pelaporan kesehatan yang ditingkatkan](#)
- [\[ElasticBeanstalk.2\] Pembaruan platform yang dikelola Elastic Beanstalk harus diaktifkan](#)
- [\[ElasticBeanstalk.3\] Elastic Beanstalk harus mengalirkan log ke CloudWatch](#)
- [\[EMR.1\] Node primer kluster EMR Amazon seharusnya tidak memiliki alamat IP publik](#)
- [\[EventBridge.4\] titik akhir EventBridge global harus mengaktifkan replikasi acara](#)
- [\[FraudDetector.1\] Jenis entitas Amazon Fraud Detector harus diberi tag](#)
- [\[FraudDetector.2\] Label Amazon Fraud Detector harus diberi tag](#)
- [\[FraudDetector.3\] Hasil Amazon Fraud Detector harus ditandai](#)
- [\[FraudDetector.4\] Variabel Amazon Fraud Detector harus diberi tag](#)
- [\[GlobalAccelerator.1\] Akselerator Akselerator Global harus diberi tag](#)
- [\[Glue.4\] Pekerjaan AWS Glue percikan harus berjalan pada versi yang didukung AWS Glue](#)
- [\[GuardDuty.2\] GuardDuty filter harus diberi tag](#)
- [\[IAM.1\] Kebijakan IAM seharusnya tidak mengizinkan hak administratif “*” penuh](#)

- [\[IAM.2\] Pengguna IAM seharusnya tidak memiliki kebijakan IAM yang dilampirkan](#)
- [\[IAM.3\] Kunci akses pengguna IAM harus diputar setiap 90 hari atau kurang](#)
- [\[IAM.4\] Kunci akses pengguna root IAM seharusnya tidak ada](#)
- [\[IAM.5\] MFA harus diaktifkan untuk semua pengguna IAM yang memiliki kata sandi konsol](#)
- [\[IAM.6\] MFA perangkat keras harus diaktifkan untuk pengguna root](#)
- [\[IAM.8\] Kredensi pengguna IAM yang tidak digunakan harus dihapus](#)
- [\[IAM.9\] MFA harus diaktifkan untuk pengguna root](#)
- [\[IAM.18\] Memastikan peran dukungan telah dibuat untuk mengelola insiden dengan AWS Dukungan](#)
- [\[IAM.19\] MFA harus diaktifkan untuk semua pengguna IAM](#)
- [\[IAM.21\] Kebijakan terkelola pelanggan IAM yang Anda buat seharusnya tidak mengizinkan tindakan wildcard untuk layanan](#)
- [\[IAM.22\] Kredensi pengguna IAM yang tidak digunakan selama 45 hari harus dihapus](#)
- [\[IAM.24\] Peran IAM harus ditandai](#)
- [\[IAM.25\] Pengguna IAM harus diberi tag](#)
- [\[IAM.26\] Sertifikat SSL/TLS kedaluwarsa yang dikelola di IAM harus dihapus](#)
- [\[IAM.27\] Identitas IAM seharusnya tidak memiliki kebijakan yang dilampirkan AWSCloud ShellFullAccess](#)
- [\[Inspektor.1\] Pemindaian Amazon Inspector harus diaktifkan EC2](#)
- [\[Inspektor.2\] Pemindaian ECR Amazon Inspector harus diaktifkan](#)
- [\[Inspektor.3\] Pemindaian kode Amazon Inspector Lambda harus diaktifkan](#)
- [\[Inspektor.4\] Pemindaian standar Amazon Inspector Lambda harus diaktifkan](#)
- [\[IoT Events .1\] Input Peristiwa AWS IoT harus diberi tag](#)
- [\[IoT Events .2\] Model detektor Acara AWS IoT harus diberi tag](#)
- [\[IoT Events .3\] Model alarm AWS IoT Events harus diberi tag](#)
- [\[IoT Site Wise.1\] Model aset AWS IoT harus ditandai SiteWise](#)
- [\[IoT Site Wise.2\] Dasbor AWS IoT harus diberi tag SiteWise](#)
- [\[IoT Site Wise.3\] Gateway AWS IoT harus diberi tag SiteWise](#)
- [\[IoT Site Wise.4\] Portal AWS IoT harus diberi tag SiteWise](#)
- [\[IoT Site Wise.5\] Proyek AWS IoT harus diberi tag SiteWise](#)
- [\[IoT Twin Maker.1\] Pekerjaan sinkronisasi AWS IoT harus ditandai TwinMaker](#)

- [\[Io TTwin Maker.2\] Ruang kerja AWS IoT harus diberi tag TwinMaker](#)
- [\[Io TTwin Maker.3\] Adegan AWS IoT harus diberi tag TwinMaker](#)
- [\[Io TTwin Maker.4\] Entitas AWS IoT harus diberi tag TwinMaker](#)
- [\[Io TWireless .1\] Grup multicast Nirkabel AWS IoT harus diberi tag](#)
- [\[Io TWireless .2\] Profil layanan AWS IoT Wireless harus diberi tag](#)
- [\[Io TWireless .3\] Tugas AWS IoT FUOTA harus ditandai](#)
- [\[IVS.1\] Pasangan kunci pemutaran IVS harus ditandai](#)
- [\[IVS.2\] Konfigurasi perekaman IVS harus ditandai](#)
- [\[IVS.3\] Saluran IVS harus ditandai](#)
- [\[Keyspaces.1\] Ruang kunci Amazon Keyspaces harus diberi tag](#)
- [\[KMS.1\] Kebijakan yang dikelola pelanggan IAM tidak boleh mengizinkan tindakan dekripsi pada semua kunci KMS](#)
- [\[KMS.2\] Prinsipal IAM tidak boleh memiliki kebijakan inline IAM yang memungkinkan tindakan dekripsi pada semua kunci KMS](#)
- [\[KMS.4\] rotasi AWS KMS tombol harus diaktifkan](#)
- [\[Macie.1\] Amazon Macie harus diaktifkan](#)
- [\[Macie.2\] Penemuan data sensitif otomatis Macie harus diaktifkan](#)
- [\[MSK.3\] Konektor MSK Connect harus dienkripsi saat transit](#)
- [\[Opensearch.1\] OpenSearch domain harus mengaktifkan enkripsi saat istirahat](#)
- [\[Opensearch.2\] OpenSearch domain tidak boleh diakses publik](#)
- [\[Opensearch.3\] OpenSearch domain harus mengenkripsi data yang dikirim antar node](#)
- [\[Opensearch.4\] login kesalahan OpenSearch domain ke Log harus diaktifkan CloudWatch](#)
- [\[Opensearch.5\] OpenSearch domain harus mengaktifkan pencatatan audit](#)
- [\[Opensearch.6\] OpenSearch domain harus memiliki setidaknya tiga node data](#)
- [\[Opensearch.7\] OpenSearch domain harus mengaktifkan kontrol akses berbutir halus](#)
- [\[Opensearch.8\] Koneksi ke OpenSearch domain harus dienkripsi menggunakan kebijakan keamanan TLS terbaru](#)
- [\[Opensearch.9\] domain harus ditandai OpenSearch](#)
- [\[Opensearch.10\] OpenSearch domain harus menginstal pembaruan perangkat lunak terbaru](#)
- [\[Opensearch.11\] OpenSearch domain harus memiliki setidaknya tiga node primer khusus](#)
- [\[RDS.14\] Cluster Amazon Aurora seharusnya mengaktifkan backtracking](#)

- [\[RDS.26\] Instans RDS DB harus dilindungi oleh rencana cadangan](#)
- [\[RDS.31\] Grup keamanan RDS DB harus ditandai](#)
- [\[RDS.35\] Cluster RDS DB harus mengaktifkan peningkatan versi minor otomatis](#)
- [\[RedshiftServerless.1\] Grup kerja Amazon Redshift Tanpa Server harus menggunakan perutean VPC yang disempurnakan](#)
- [\[RedshiftServerless.2\] Koneksi ke grup kerja Redshift Serverless harus diperlukan untuk menggunakan SSL](#)
- [\[Route53.1\] Pemeriksaan kesehatan rute 53 harus ditandai](#)
- [\[Route53.2\] Route 53 zona yang dihosting publik harus mencatat kueri DNS](#)
- [\[S3.24\] Poin Akses Multi-Wilayah S3 harus mengaktifkan pengaturan akses publik blok](#)
- [\[SageMaker.1\] Instans SageMaker notebook Amazon seharusnya tidak memiliki akses internet langsung](#)
- [\[SageMaker.2\] instance SageMaker notebook harus diluncurkan dalam VPC khusus](#)
- [\[SageMaker.3\] Pengguna seharusnya tidak memiliki akses root ke instance SageMaker notebook](#)
- [\[SageMaker.5\] SageMaker model harus memblokir lalu lintas masuk](#)
- [\[SES.1\] Daftar kontak SES harus ditandai](#)
- [\[SES.2\] Set konfigurasi SES harus ditandai](#)
- [\[SQS.1\] Antrian Amazon SQS harus dienkripsi saat istirahat](#)
- [\[SQS.2\] Antrian SQS harus ditandai](#)
- [\[SQS.3\] Kebijakan akses antrian SQS seharusnya tidak mengizinkan akses publik](#)
- [\[SSM.1\] EC2 Instans Amazon harus dikelola oleh AWS Systems Manager](#)
- [\[WAF.1\] Pencatatan ACL Web Global AWS WAF Klasik harus diaktifkan](#)
- [\[WAF.3\] Kelompok aturan Regional AWS WAF Klasik harus memiliki setidaknya satu aturan](#)
- [\[WAF.6\] Aturan global AWS WAF klasik harus memiliki setidaknya satu syarat](#)
- [\[WAF.7\] Kelompok aturan global AWS WAF klasik harus memiliki setidaknya satu aturan](#)
- [\[WAF.8\] Web global AWS WAF klasik ACLs harus memiliki setidaknya satu aturan atau kelompok aturan](#)
- [\[WAF.10\] AWS WAF web ACLs harus memiliki setidaknya satu aturan atau kelompok aturan](#)
- [\[WAF.11\] pencatatan ACL AWS WAF web harus diaktifkan](#)
- [\[WorkSpaces.1\] volume WorkSpaces pengguna harus dienkripsi saat istirahat](#)
- [\[WorkSpaces.2\] volume WorkSpaces root harus dienkripsi saat istirahat](#)

Amerika Selatan (Sao Paulo)

Kontrol berikut tidak didukung di Wilayah Amerika Selatan (São Paulo).

- [\[AppRunner.1\] Layanan App Runner harus diberi tag](#)
- [\[AppRunner.2\] Konektor VPC App Runner harus diberi tag](#)
- [\[CloudFront.1\] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi](#)
- [\[CloudFront.3\] CloudFront distribusi harus memerlukan enkripsi dalam perjalanan](#)
- [\[CloudFront.4\] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi](#)
- [\[CloudFront.5\] CloudFront distribusi seharusnya mengaktifkan logging](#)
- [\[CloudFront.6\] CloudFront distribusi harus mengaktifkan WAF](#)
- [\[CloudFront.7\] CloudFront distribusi harus menggunakan sertifikat SSL/TLS khusus](#)
- [\[CloudFront.8\] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS](#)
- [\[CloudFront.9\] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus](#)
- [\[CloudFront.10\] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal kustom](#)
- [\[CloudFront.12\] CloudFront distribusi seharusnya tidak menunjukkan asal S3 yang tidak ada](#)
- [\[CloudFront.13\] CloudFront distribusi harus menggunakan kontrol akses asal](#)
- [\[CloudFront.14\] CloudFront distribusi harus ditandai](#)
- [\[CodeArtifact.1\] CodeArtifact repositori harus ditandai](#)
- [\[CodeGuruProfiler.1\] Grup CodeGuru profil profiler harus diberi tag](#)
- [\[CodeGuruReviewer.1\] Asosiasi CodeGuru repositori peninjau harus diberi tag](#)
- [\[Connect.1\] Jenis objek Amazon Connect Customer Profiles harus diberi tag](#)
- [\[Connect.2\] Instans Amazon Connect seharusnya mengaktifkan logging CloudWatch](#)
- [\[EC2.173\] Permintaan Armada EC2 Spot harus mengaktifkan enkripsi untuk volume EBS terlampir](#)
- [\[ECR.4\] Repositori publik ECR harus ditandai](#)
- [\[FraudDetector.1\] Jenis entitas Amazon Fraud Detector harus diberi tag](#)
- [\[FraudDetector.2\] Label Amazon Fraud Detector harus diberi tag](#)
- [\[FraudDetector.3\] Hasil Amazon Fraud Detector harus ditandai](#)
- [\[FraudDetector.4\] Variabel Amazon Fraud Detector harus diberi tag](#)
- [\[GlobalAccelerator.1\] Akselerator Akselerator Global harus diberi tag](#)

- [\[IAM.26\] Sertifikat SSL/TLS kedaluwarsa yang dikelola di IAM harus dihapus](#)
- [\[Inspektor.3\] Pemindaian kode Amazon Inspector Lambda harus diaktifkan](#)
- [\[IoT.1\] profil AWS IoT Device Defender keamanan harus ditandai](#)
- [\[IoT.2\] tindakan AWS IoT Core mitigasi harus ditandai](#)
- [AWS IoT Core Dimensi \[IoT.3\] harus ditandai](#)
- [\[IoT TEEvents .1\] Input Peristiwa AWS IoT harus diberi tag](#)
- [\[IoT TEEvents .2\] Model detektor Acara AWS IoT harus diberi tag](#)
- [\[IoT TEEvents .3\] Model alarm AWS IoT Events harus diberi tag](#)
- [\[IoT TSite Wise.1\] Model aset AWS IoT harus ditandai SiteWise](#)
- [\[IoT TSite Wise.2\] Dasbor AWS IoT harus diberi tag SiteWise](#)
- [\[IoT TSite Wise.3\] Gateway AWS IoT harus diberi tag SiteWise](#)
- [\[IoT TSite Wise.4\] Portal AWS IoT harus diberi tag SiteWise](#)
- [\[IoT TSite Wise.5\] Proyek AWS IoT harus diberi tag SiteWise](#)
- [\[IoT TTwin Maker.1\] Pekerjaan sinkronisasi AWS IoT harus ditandai TwinMaker](#)
- [\[IoT TTwin Maker.2\] Ruang kerja AWS IoT harus diberi tag TwinMaker](#)
- [\[IoT TTwin Maker.3\] Adegan AWS IoT harus diberi tag TwinMaker](#)
- [\[IoT TTwin Maker.4\] Entitas AWS IoT harus diberi tag TwinMaker](#)
- [\[IVS.1\] Pasangan kunci pemutaran IVS harus ditandai](#)
- [\[IVS.2\] Konfigurasi perekaman IVS harus ditandai](#)
- [\[IVS.3\] Saluran IVS harus ditandai](#)
- [\[RDS.14\] Cluster Amazon Aurora seharusnya mengaktifkan backtracking](#)
- [\[RedshiftServerless.1\] Grup kerja Amazon Redshift Tanpa Server harus menggunakan perutean VPC yang disempurnakan](#)
- [\[RedshiftServerless.2\] Koneksi ke grup kerja Redshift Serverless harus diperlukan untuk menggunakan SSL](#)
- [\[Route53.1\] Pemeriksaan kesehatan rute 53 harus ditandai](#)
- [\[Route53.2\] Route 53 zona yang dihosting publik harus mencatat kueri DNS](#)
- [\[S3.24\] Poin Akses Multi-Wilayah S3 harus mengaktifkan pengaturan akses publik blok](#)
- [\[WAF.1\] Pencatatan ACL Web Global AWS WAF Klasik harus diaktifkan](#)
- [\[WAF.6\] Aturan global AWS WAF klasik harus memiliki setidaknya satu syarat](#)
- [\[WAF.7\] Kelompok aturan global AWS WAF klasik harus memiliki setidaknya satu aturan](#)

- [\[WAF.8\] Web global AWS WAF klasik ACLs harus memiliki setidaknya satu aturan atau kelompok aturan](#)

AWS GovCloud (AS-Timur)

Kontrol berikut tidak didukung di Wilayah AWS GovCloud (AS-Timur).

- [\[ACM.2\] Sertifikat RSA yang dikelola oleh ACM harus menggunakan panjang kunci minimal 2.048 bit](#)
- [\[Akun.1\] Informasi kontak keamanan harus disediakan untuk Akun AWS](#)
- [\[Akun.2\] Akun AWS harus menjadi bagian dari organisasi AWS Organizations](#)
- [\[APIGateway.2\] Tahapan API Gateway REST API harus dikonfigurasi untuk menggunakan sertifikat SSL untuk otentikasi backend](#)
- [\[APIGateway.8\] Rute API Gateway harus menentukan jenis otorisasi](#)
- [\[APIGateway.9\] Pencatatan akses harus dikonfigurasi untuk Tahap API Gateway V2](#)
- [\[Amplify.1\] Aplikasi Amplify harus diberi tag](#)
- [\[Amplify.2\] Amplify branch harus diberi tag](#)
- [\[AppConfig.1\] AWS AppConfig aplikasi harus diberi tag](#)
- [\[AppConfig.2\] profil AWS AppConfig konfigurasi harus ditandai](#)
- [\[AppConfig.3\] AWS AppConfig lingkungan harus ditandai](#)
- [\[AppConfig.4\] asosiasi AWS AppConfig ekstensi harus ditandai](#)
- [\[AppFlow.1\] AppFlow Aliran Amazon harus ditandai](#)
- [\[AppRunner.1\] Layanan App Runner harus diberi tag](#)
- [\[AppRunner.2\] Konektor VPC App Runner harus diberi tag](#)
- [\[AppSync.1\] Cache AWS AppSync API harus dienkrpsi saat istirahat](#)
- [\[AppSync.2\] AWS AppSync harus mengaktifkan logging tingkat lapangan](#)
- [\[AppSync.4\] AWS AppSync APIs GraphQL harus diberi tag](#)
- [\[AppSync.5\] AWS AppSync APIs GraphQL tidak boleh diautentikasi dengan kunci API](#)
- [\[AppSync.6\] Cache AWS AppSync API harus dienkrpsi saat transit](#)
- [\[AutoScaling.2\] Grup EC2 Auto Scaling Amazon harus mencakup beberapa Availability Zone](#)
- [\[AutoScaling.3\] Konfigurasi peluncuran grup Auto Scaling harus EC2 mengonfigurasi instance agar memerlukan Layanan Metadata Instance Versi 2 \(\) IMDSv2](#)

- [\[AutoScaling.6\] Grup Auto Scaling harus menggunakan beberapa jenis instance di beberapa Availability Zone](#)
- [\[AutoScaling.9\] Grup EC2 Auto Scaling Amazon harus menggunakan templat peluncuran Amazon EC2](#)
- [\[Backup.4\] rencana AWS Backup laporan harus ditandai](#)
- [\[Batch.1\] Antrian pekerjaan batch harus ditandai](#)
- [\[Batch.2\] Kebijakan penjadwalan batch harus ditandai](#)
- [\[Batch.3\] Lingkungan komputasi Batch harus ditandai](#)
- [\[Batch.4\] Properti sumber daya komputasi di lingkungan komputasi Batch terkelola harus ditandai](#)
- [\[CloudFront.1\] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi](#)
- [\[CloudFront.3\] CloudFront distribusi harus memerlukan enkripsi dalam perjalanan](#)
- [\[CloudFront.4\] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi](#)
- [\[CloudFront.5\] CloudFront distribusi seharusnya mengaktifkan logging](#)
- [\[CloudFront.6\] CloudFront distribusi harus mengaktifkan WAF](#)
- [\[CloudFront.7\] CloudFront distribusi harus menggunakan sertifikat SSL/TLS khusus](#)
- [\[CloudFront.8\] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS](#)
- [\[CloudFront.9\] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus](#)
- [\[CloudFront.10\] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal kustom](#)
- [\[CloudFront.12\] CloudFront distribusi seharusnya tidak menunjukkan asal S3 yang tidak ada](#)
- [\[CloudFront.13\] CloudFront distribusi harus menggunakan kontrol akses asal](#)
- [\[CloudFront.14\] CloudFront distribusi harus ditandai](#)
- [\[CloudWatch.17\] tindakan CloudWatch alarm harus diaktifkan](#)
- [\[CodeArtifact.1\] CodeArtifact repositori harus ditandai](#)
- [\[CodeBuild.3\] Log CodeBuild S3 harus dienkripsi](#)
- [\[CodeBuild.4\] lingkungan CodeBuild proyek harus memiliki urasi logging AWS Config](#)
- [\[CodeGuruProfiler.1\] Grup CodeGuru profil profiler harus diberi tag](#)
- [\[CodeGuruReviewer.1\] Asosiasi CodeGuru repositori peninjau harus diberi tag](#)
- [\[Cognito.1\] Kumpulan pengguna Cognito harus mengaktifkan perlindungan ancaman dengan mode penegakan fungsi penuh untuk otentikasi standar](#)
- [\[Connect.1\] Jenis objek Amazon Connect Customer Profiles harus diberi tag](#)

- [\[Connect.2\] Instans Amazon Connect seharusnya mengaktifkan logging CloudWatch](#)
- [\[DataSync.2\] DataSync tugas harus ditandai](#)
- [\[DMS.2\] Sertifikat DMS harus ditandai](#)
- [\[DMS.6\] Instans replikasi DMS harus mengaktifkan peningkatan versi minor otomatis](#)
- [\[DMS.7\] Tugas replikasi DMS untuk database target seharusnya mengaktifkan logging](#)
- [\[DMS.8\] Tugas replikasi DMS untuk database sumber seharusnya mengaktifkan logging](#)
- [\[DMS.9\] Titik akhir DMS harus menggunakan SSL](#)
- [\[DocumentDB.1\] Cluster Amazon DocumentDB harus dienkripsi saat istirahat](#)
- [\[DocumentDB.2\] Cluster Amazon DocumentDB harus memiliki periode retensi cadangan yang memadai](#)
- [\[DocumentDB.3\] Cuplikan cluster manual Amazon DocumentDB seharusnya tidak bersifat publik](#)
- [\[DocumentDB.4\] Cluster Amazon DocumentDB harus mempublikasikan log audit ke Log CloudWatch](#)
- [\[DocumentDB.5\] Cluster Amazon DocumentDB harus mengaktifkan perlindungan penghapusan](#)
- [\[DynamoDB.3\] Cluster DynamoDB Accelerator \(DAX\) harus dienkripsi saat istirahat](#)
- [\[DynamoDB.7\] Cluster DynamoDB Accelerator harus dienkripsi saat transit](#)
- [\[EC2.21\] Jaringan ACLs seharusnya tidak mengizinkan masuknya dari 0.0.0.0/0 ke port 22 atau port 3389.](#)
- [\[EC2.22\] Grup EC2 keamanan Amazon yang tidak digunakan harus dihapus](#)
- [\[EC2.23\] Amazon EC2 Transit Gateways seharusnya tidak secara otomatis menerima permintaan lampiran VPC](#)
- [\[EC2.24\] Jenis instance EC2 paravirtual Amazon tidak boleh digunakan](#)
- [\[EC2.25\] Templat EC2 peluncuran Amazon tidak boleh menetapkan publik IPs ke antarmuka jaringan](#)
- [\[EC2.47\] Layanan titik akhir Amazon VPC harus diberi tag](#)
- [\[EC2.52\] gateway EC2 transit harus ditandai](#)
- [\[EC2.58\] VPCs harus dikonfigurasi dengan titik akhir antarmuka untuk Kontak Manajer Insiden Systems Manager](#)
- [\[EC2.60\] VPCs harus dikonfigurasi dengan titik akhir antarmuka untuk Systems Manager Incident Manager](#)
- [\[EC2.170\] templat EC2 peluncuran harus menggunakan Layanan Metadata Instance Versi 2 \(\) IMDSv2](#)

- [\[EC2.173\] Permintaan Armada EC2 Spot harus mengaktifkan enkripsi untuk volume EBS terlampir](#)
- [\[EC2.174\] Set opsi EC2 DHCP harus ditandai](#)
- [\[EC2.175\] templat EC2 peluncuran harus diberi tag](#)
- [\[EC2.176\] daftar EC2 awalan harus ditandai](#)
- [\[EC2.177\] Sesi cermin EC2 lalu lintas harus ditandai](#)
- [\[EC2.178\] Filter cermin EC2 lalu lintas harus ditandai](#)
- [\[EC2.179\] Target cermin EC2 lalu lintas harus ditandai](#)
- [\[ECR.1\] Repositori pribadi ECR harus memiliki pemindaian gambar yang dikonfigurasi](#)
- [\[ECR.2\] Repositori pribadi ECR harus memiliki kekekalan tag yang dikonfigurasi](#)
- [\[ECR.3\] Repositori ECR harus memiliki setidaknya satu kebijakan siklus hidup yang dikonfigurasi](#)
- [\[ECR.4\] Repositori publik ECR harus ditandai](#)
- [\[ECS.3\] Definisi tugas ECS tidak boleh membagikan namespace proses host](#)
- [\[ECS.4\] Kontainer ECS harus berjalan sebagai non-hak istimewa](#)
- [\[ECS.5\] Wadah ECS harus dibatasi pada akses hanya-baca ke sistem file root](#)
- [\[ECS.8\] Rahasia tidak boleh diteruskan sebagai variabel lingkungan kontainer](#)
- [\[ECS.9\] Definisi tugas ECS harus memiliki konfigurasi logging](#)
- [\[ECS.10\] Layanan ECS Fargate harus berjalan pada versi platform Fargate terbaru](#)
- [\[ECS.12\] Cluster ECS harus menggunakan Wawasan Kontainer](#)
- [\[EFS.3\] Titik akses EFS harus menegakkan direktori root](#)
- [\[EFS.4\] Titik akses EFS harus menegakkan identitas pengguna](#)
- [\[EKS.2\] Kluster EKS harus berjalan pada versi Kubernetes yang didukung](#)
- [\[EKS.8\] Kluster EKS harus mengaktifkan pencatatan audit](#)
- [\[ELB.10\] Classic Load Balancer harus menjangkau beberapa Availability Zone](#)
- [\[ELB.12\] Application Load Balancer harus dikonfigurasi dengan mode mitigasi desync defensif atau paling ketat](#)
- [\[ELB.13\] Penyeimbang Beban Aplikasi, Jaringan, dan Gateway harus mencakup beberapa Availability Zone](#)
- [\[ELB.14\] Classic Load Balancer harus dikonfigurasi dengan mode mitigasi desync defensif atau paling ketat](#)
- [\[ELB.16\] Application Load Balancers harus dikaitkan dengan ACL web AWS WAF](#)
- [\[ElastiCache.1\] Cluster ElastiCache \(Redis OSS\) harus mengaktifkan pencadangan otomatis](#)

- [\[ElastiCache.2\] ElastiCache cluster harus mengaktifkan peningkatan versi minor otomatis](#)
- [\[ElastiCache.3\] grup ElastiCache replikasi harus mengaktifkan failover otomatis](#)
- [\[ElastiCache.4\] grup ElastiCache replikasi harus dienkripsi saat istirahat](#)
- [\[ElastiCache.5\] grup ElastiCache replikasi harus dienkripsi saat transit](#)
- [\[ElastiCache.6\] ElastiCache \(Redis OSS\) grup replikasi dari versi sebelumnya harus mengaktifkan Redis OSS AUTH](#)
- [\[ElastiCache.7\] ElastiCache cluster tidak boleh menggunakan grup subnet default](#)
- [\[ElasticBeanstalk.1\] Lingkungan Elastic Beanstalk seharusnya mengaktifkan pelaporan kesehatan yang ditingkatkan](#)
- [\[ElasticBeanstalk.2\] Pembaruan platform yang dikelola Elastic Beanstalk harus diaktifkan](#)
- [\[ElasticBeanstalk.3\] Elastic Beanstalk harus mengalirkan log ke CloudWatch](#)
- [\[EMR.2\] Pengaturan akses publik blok EMR Amazon harus diaktifkan](#)
- [\[EMR.3\] Konfigurasi keamanan Amazon EMR harus dienkripsi saat istirahat](#)
- [\[EMR.4\] Konfigurasi keamanan Amazon EMR harus dienkripsi saat transit](#)
- [\[ES.4\] Kesalahan domain Elasticsearch yang masuk ke CloudWatch Log harus diaktifkan](#)
- [\[EventBridge.3\] bus acara EventBridge khusus harus memiliki kebijakan berbasis sumber daya terlampir](#)
- [\[EventBridge.4\] titik akhir EventBridge global harus mengaktifkan replikasi acara](#)
- [\[FraudDetector.1\] Jenis entitas Amazon Fraud Detector harus diberi tag](#)
- [\[FraudDetector.2\] Label Amazon Fraud Detector harus diberi tag](#)
- [\[FraudDetector.3\] Hasil Amazon Fraud Detector harus ditandai](#)
- [\[FraudDetector.4\] Variabel Amazon Fraud Detector harus diberi tag](#)
- [\[FSx.1\] FSx untuk sistem file OpenZFS harus dikonfigurasi untuk menyalin tag ke cadangan dan volume](#)
- [\[FSx.2\] FSx untuk sistem file Lustre harus dikonfigurasi untuk menyalin tag ke cadangan](#)
- [\[GlobalAccelerator.1\] Akselerator Akselerator Global harus diberi tag](#)
- [\[Glue.3\] transformasi pembelajaran AWS Glue mesin harus dienkripsi saat istirahat](#)
- [\[GuardDuty.7\] GuardDuty EKS Runtime Monitoring harus diaktifkan](#)
- [\[GuardDuty.8\] Perlindungan GuardDuty Malware untuk EC2 harus diaktifkan](#)
- [\[GuardDuty.9\] Perlindungan GuardDuty RDS harus diaktifkan](#)
- [\[GuardDuty.11\] GuardDuty Runtime Monitoring harus diaktifkan](#)

- [\[GuardDuty.12\] GuardDuty ECS Runtime Monitoring harus diaktifkan](#)
- [\[GuardDuty.13\] GuardDuty EC2 Runtime Monitoring harus diaktifkan](#)
- [\[IAM.6\] MFA perangkat keras harus diaktifkan untuk pengguna root](#)
- [\[IAM.9\] MFA harus diaktifkan untuk pengguna root](#)
- [\[IAM.21\] Kebijakan terkelola pelanggan IAM yang Anda buat seharusnya tidak mengizinkan tindakan wildcard untuk layanan](#)
- [\[IAM.24\] Peran IAM harus ditandai](#)
- [\[IAM.25\] Pengguna IAM harus diberi tag](#)
- [\[IAM.26\] Sertifikat SSL/TLS kedaluwarsa yang dikelola di IAM harus dihapus](#)
- [\[IAM.28\] IAM Access Analyzer penganalisis akses eksternal harus diaktifkan](#)
- [\[Inspektor.3\] Pemindaian kode Amazon Inspector Lambda harus diaktifkan](#)
- [\[IoT Events .1\] Input Peristiwa AWS IoT harus diberi tag](#)
- [\[IoT Events .2\] Model detektor Acara AWS IoT harus diberi tag](#)
- [\[IoT Events .3\] Model alarm AWS IoT Events harus diberi tag](#)
- [\[IoT Site Wise.1\] Model aset AWS IoT harus ditandai SiteWise](#)
- [\[IoT Site Wise.2\] Dasbor AWS IoT harus diberi tag SiteWise](#)
- [\[IoT Site Wise.3\] Gateway AWS IoT harus diberi tag SiteWise](#)
- [\[IoT Site Wise.4\] Portal AWS IoT harus diberi tag SiteWise](#)
- [\[IoT Site Wise.5\] Proyek AWS IoT harus diberi tag SiteWise](#)
- [\[IoT Twin Maker.1\] Pekerjaan sinkronisasi AWS IoT harus ditandai TwinMaker](#)
- [\[IoT Twin Maker.2\] Ruang kerja AWS IoT harus diberi tag TwinMaker](#)
- [\[IoT Twin Maker.3\] Adegan AWS IoT harus diberi tag TwinMaker](#)
- [\[IoT Twin Maker.4\] Entitas AWS IoT harus diberi tag TwinMaker](#)
- [\[IoT Wireless .1\] Grup multicast Nirkabel AWS IoT harus diberi tag](#)
- [\[IoT Wireless .2\] Profil layanan AWS IoT Wireless harus diberi tag](#)
- [\[IoT Wireless .3\] Tugas AWS IoT FUOTA harus ditandai](#)
- [\[IVS.1\] Pasangan kunci pemutaran IVS harus ditandai](#)
- [\[IVS.2\] Konfigurasi perekaman IVS harus ditandai](#)
- [\[IVS.3\] Saluran IVS harus ditandai](#)
- [\[Keyspaces.1\] Ruang kunci Amazon Keyspaces harus diberi tag](#)

- [\[Kinesis.1\] Aliran kinesis harus dienkripsi saat istirahat](#)
- [\[KMS.5\] Kunci KMS tidak boleh diakses publik](#)
- [\[Lambda.5\] Fungsi VPC Lambda harus beroperasi di beberapa Availability Zone](#)
- [\[Macie.1\] Amazon Macie harus diaktifkan](#)
- [\[Macie.2\] Penemuan data sensitif otomatis Macie harus diaktifkan](#)
- [\[MQ.3\] Broker Amazon MQ harus mengaktifkan peningkatan versi minor otomatis](#)
- [\[MQ.5\] Broker ActiveMQ harus menggunakan mode penerapan aktif/siaga](#)
- [\[MQ.6\] Broker RabbitMQ harus menggunakan mode penerapan cluster](#)
- [\[MSK.1\] Kluster MSK harus dienkripsi saat transit di antara node broker](#)
- [\[MSK.2\] Kluster MSK seharusnya telah meningkatkan pemantauan yang dikonfigurasi](#)
- [\[MSK.3\] Konektor MSK Connect harus dienkripsi saat transit](#)
- [\[Neptunus.1\] Cluster DB Neptunus harus dienkripsi saat istirahat](#)
- [\[Neptune.2\] Cluster DB Neptunus harus menerbitkan log audit ke Log CloudWatch](#)
- [\[Neptune.3\] Snapshot cluster Neptunus DB seharusnya tidak publik](#)
- [\[Neptunus.4\] Cluster DB Neptunus harus mengaktifkan perlindungan penghapusan](#)
- [\[Neptunus.5\] Cluster DB Neptunus harus mengaktifkan cadangan otomatis](#)
- [\[Neptune.6\] Snapshot cluster Neptunus DB harus dienkripsi saat istirahat](#)
- [\[Neptune.7\] Cluster DB Neptunus harus mengaktifkan otentikasi basis data IAM](#)
- [\[Neptunus.8\] Cluster DB Neptunus harus dikonfigurasi untuk menyalin tag ke snapshot](#)
- [\[Neptunus.9\] Cluster DB Neptunus harus digunakan di beberapa Availability Zone](#)
- [\[NetworkFirewall.1\] Firewall Jaringan harus digunakan di beberapa Availability Zone](#)
- [\[NetworkFirewall.2\] Pencatatan Firewall Jaringan harus diaktifkan](#)
- [\[NetworkFirewall.3\] Kebijakan Network Firewall harus memiliki setidaknya satu kelompok aturan yang terkait](#)
- [\[NetworkFirewall.4\] Tindakan stateless default untuk kebijakan Network Firewall harus drop atau forward untuk paket penuh](#)
- [\[NetworkFirewall.5\] Tindakan stateless default untuk kebijakan Network Firewall harus drop atau forward untuk paket yang terfragmentasi](#)
- [\[NetworkFirewall.6\] Grup aturan Stateless Network Firewall tidak boleh kosong](#)
- [\[NetworkFirewall.9\] Firewall Jaringan harus mengaktifkan perlindungan penghapusan](#)
- [\[Opensearch.1\] OpenSearch domain harus mengaktifkan enkripsi saat istirahat](#)

- [\[Opensearch.2\] OpenSearch domain tidak boleh diakses publik](#)
- [\[Opensearch.3\] OpenSearch domain harus mengenkripsi data yang dikirim antar node](#)
- [\[Opensearch.4\] login kesalahan OpenSearch domain ke Log harus diaktifkan CloudWatch](#)
- [\[Opensearch.5\] OpenSearch domain harus mengaktifkan pencatatan audit](#)
- [\[Opensearch.6\] OpenSearch domain harus memiliki setidaknya tiga node data](#)
- [\[Opensearch.7\] OpenSearch domain harus mengaktifkan kontrol akses berbutir halus](#)
- [\[Opensearch.8\] Koneksi ke OpenSearch domain harus dienkripsi menggunakan kebijakan keamanan TLS terbaru](#)
- [\[PCA.1\] otoritas sertifikat AWS Private CA root harus dinonaktifkan](#)
- [\[PCA.2\] Otoritas sertifikat CA AWS swasta harus ditandai](#)
- [\[RDS.14\] Cluster Amazon Aurora seharusnya mengaktifkan backtracking](#)
- [\[RDS.15\] Cluster RDS DB harus dikonfigurasi untuk beberapa Availability Zone](#)
- [\[RDS.24\] Kluster Database RDS harus menggunakan nama pengguna administrator khusus](#)
- [\[RDS.25\] Instans database RDS harus menggunakan nama pengguna administrator khusus](#)
- [\[RDS.27\] Cluster RDS DB harus dienkripsi saat istirahat](#)
- [\[RDS.31\] Grup keamanan RDS DB harus ditandai](#)
- [\[RDS.34\] Kluster Aurora MySQL DB harus menerbitkan log audit ke Log CloudWatch](#)
- [\[RDS.35\] Cluster RDS DB harus mengaktifkan peningkatan versi minor otomatis](#)
- [\[Redshift.8\] Cluster Amazon Redshift tidak boleh menggunakan nama pengguna Admin default](#)
- [\[Redshift.9\] Cluster Redshift tidak boleh menggunakan nama database default](#)
- [\[Redshift.10\] Cluster Redshift harus dienkripsi saat istirahat](#)
- [\[Redshift.17\] Grup parameter cluster Redshift harus ditandai](#)
- [\[RedshiftServerless.1\] Grup kerja Amazon Redshift Tanpa Server harus menggunakan perutean VPC yang disempurnakan](#)
- [\[RedshiftServerless.2\] Koneksi ke grup kerja Redshift Serverless harus diperlukan untuk menggunakan SSL](#)
- [\[RedshiftServerless.3\] Kelompok kerja Redshift Tanpa Server harus melarang akses publik](#)
- [\[RedshiftServerless.6\] Ruang nama Redshift Tanpa Server harus mengeksport log ke Log CloudWatch](#)
- [\[Route53.1\] Pemeriksaan kesehatan rute 53 harus ditandai](#)
- [\[Route53.2\] Route 53 zona yang dihosting publik harus mencatat kueri DNS](#)

- [\[S3.10\] Bucket tujuan umum S3 dengan versi diaktifkan harus memiliki konfigurasi Siklus Hidup](#)
- [\[S3.11\] Bucket tujuan umum S3 harus mengaktifkan pemberitahuan acara](#)
- [\[S3.12\] tidak ACLs boleh digunakan untuk mengelola akses pengguna ke bucket tujuan umum S3](#)
- [\[S3.13\] Bucket tujuan umum S3 harus memiliki konfigurasi Siklus Hidup](#)
- [\[S3.20\] Bucket tujuan umum S3 harus mengaktifkan penghapusan MFA](#)
- [\[S3.24\] Poin Akses Multi-Wilayah S3 harus mengaktifkan pengaturan akses publik blok](#)
- [\[SageMaker.1\] Instans SageMaker notebook Amazon seharusnya tidak memiliki akses internet langsung](#)
- [\[SageMaker.2\] instance SageMaker notebook harus diluncurkan dalam VPC khusus](#)
- [\[SageMaker.3\] Pengguna seharusnya tidak memiliki akses root ke instance SageMaker notebook](#)
- [\[SageMaker.5\] SageMaker model harus memblokir lalu lintas masuk](#)
- [\[SageMaker.6\] konfigurasi gambar SageMaker aplikasi harus ditandai](#)
- [\[SageMaker.7\] SageMaker gambar harus diberi tag](#)
- [\[SES.1\] Daftar kontak SES harus ditandai](#)
- [\[SES.2\] Set konfigurasi SES harus ditandai](#)
- [\[SNS.4\] Kebijakan akses topik SNS seharusnya tidak mengizinkan akses publik](#)
- [\[SQS.3\] Kebijakan akses antrian SQS seharusnya tidak mengizinkan akses publik](#)
- [\[SSM.4\] Dokumen SSM seharusnya tidak bersifat publik](#)
- [\[SSM.5\] Dokumen SSM harus ditandai](#)
- [\[StepFunctions.1\] Mesin status Step Functions seharusnya mengaktifkan logging](#)
- [\[StepFunctions.2\] Aktivitas Step Functions harus diberi tag](#)
- [\[Transfer.4\] Perjanjian Transfer Family harus ditandai](#)
- [\[Transfer.5\] Sertifikat Transfer Family harus diberi tag](#)
- [\[Transfer.6\] Konektor Transfer Family harus diberi tag](#)
- [\[Transfer.7\] Profil Transfer Family harus diberi tag](#)
- [\[WAF.1\] Pencatatan ACL Web Global AWS WAF Klasik harus diaktifkan](#)
- [\[WAF.2\] Aturan Regional AWS WAF Klasik harus memiliki setidaknya satu syarat](#)
- [\[WAF.3\] Kelompok aturan Regional AWS WAF Klasik harus memiliki setidaknya satu aturan](#)
- [\[WAF.4\] Web Regional AWS WAF Klasik ACLs harus memiliki setidaknya satu aturan atau kelompok aturan](#)
- [\[WAF.6\] Aturan global AWS WAF klasik harus memiliki setidaknya satu syarat](#)

- [\[WAF.7\] Kelompok aturan global AWS WAF klasik harus memiliki setidaknya satu aturan](#)
- [\[WAF.8\] Web global AWS WAF klasik ACLs harus memiliki setidaknya satu aturan atau kelompok aturan](#)
- [\[WAF.10\] AWS WAF web ACLs harus memiliki setidaknya satu aturan atau kelompok aturan](#)
- [AWS WAF Aturan \[WAF.12\] harus mengaktifkan metrik CloudWatch](#)
- [\[WorkSpaces.1\] volume WorkSpaces pengguna harus dienkripsi saat istirahat](#)
- [\[WorkSpaces.2\] volume WorkSpaces root harus dienkripsi saat istirahat](#)

AWS GovCloud (AS-Barat)

Kontrol berikut tidak didukung di Wilayah AWS GovCloud (AS-Barat).

- [\[ACM.2\] Sertifikat RSA yang dikelola oleh ACM harus menggunakan panjang kunci minimal 2.048 bit](#)
- [\[Akun.1\] Informasi kontak keamanan harus disediakan untuk Akun AWS](#)
- [\[Akun.2\] Akun AWS harus menjadi bagian dari organisasi AWS Organizations](#)
- [\[APIGateway.2\] Tahapan API Gateway REST API harus dikonfigurasi untuk menggunakan sertifikat SSL untuk otentikasi backend](#)
- [\[APIGateway.8\] Rute API Gateway harus menentukan jenis otorisasi](#)
- [\[APIGateway.9\] Pencatatan akses harus dikonfigurasi untuk Tahap API Gateway V2](#)
- [\[Amplify.1\] Aplikasi Amplify harus diberi tag](#)
- [\[Amplify.2\] Amplify branch harus diberi tag](#)
- [\[AppConfig.1\] AWS AppConfig aplikasi harus diberi tag](#)
- [\[AppConfig.2\] profil AWS AppConfig konfigurasi harus ditandai](#)
- [\[AppConfig.3\] AWS AppConfig lingkungan harus ditandai](#)
- [\[AppConfig.4\] asosiasi AWS AppConfig ekstensi harus ditandai](#)
- [\[AppFlow.1\] AppFlow Aliran Amazon harus ditandai](#)
- [\[AppRunner.1\] Layanan App Runner harus diberi tag](#)
- [\[AppRunner.2\] Konektor VPC App Runner harus diberi tag](#)
- [\[AppSync.1\] Cache AWS AppSync API harus dienkripsi saat istirahat](#)
- [\[AppSync.2\] AWS AppSync harus mengaktifkan logging tingkat lapangan](#)
- [\[AppSync.4\] AWS AppSync APIs GraphQL harus diberi tag](#)

- [\[AppSync.5\] AWS AppSync APIs GraphQL tidak boleh diautentikasi dengan kunci API](#)
- [\[AppSync.6\] Cache AWS AppSync API harus dienkripsi saat transit](#)
- [\[AutoScaling.2\] Grup EC2 Auto Scaling Amazon harus mencakup beberapa Availability Zone](#)
- [\[AutoScaling.3\] Konfigurasi peluncuran grup Auto Scaling harus EC2 mengonfigurasi instance agar memerlukan Layanan Metadata Instance Versi 2 \(\) IMDSv2](#)
- [\[AutoScaling.6\] Grup Auto Scaling harus menggunakan beberapa jenis instance di beberapa Availability Zone](#)
- [\[AutoScaling.9\] Grup EC2 Auto Scaling Amazon harus menggunakan templat peluncuran Amazon EC2](#)
- [\[Backup.4\] rencana AWS Backup laporan harus ditandai](#)
- [\[Batch.1\] Antrian pekerjaan batch harus ditandai](#)
- [\[Batch.2\] Kebijakan penjadwalan batch harus ditandai](#)
- [\[Batch.3\] Lingkungan komputasi Batch harus ditandai](#)
- [\[Batch.4\] Properti sumber daya komputasi di lingkungan komputasi Batch terkelola harus ditandai](#)
- [\[CloudFront.1\] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi](#)
- [\[CloudFront.3\] CloudFront distribusi harus memerlukan enkripsi dalam perjalanan](#)
- [\[CloudFront.4\] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi](#)
- [\[CloudFront.5\] CloudFront distribusi seharusnya mengaktifkan logging](#)
- [\[CloudFront.6\] CloudFront distribusi harus mengaktifkan WAF](#)
- [\[CloudFront.7\] CloudFront distribusi harus menggunakan sertifikat SSL/TLS khusus](#)
- [\[CloudFront.8\] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS](#)
- [\[CloudFront.9\] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus](#)
- [\[CloudFront.10\] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal kustom](#)
- [\[CloudFront.12\] CloudFront distribusi seharusnya tidak menunjukkan asal S3 yang tidak ada](#)
- [\[CloudFront.13\] CloudFront distribusi harus menggunakan kontrol akses asal](#)
- [\[CloudFront.14\] CloudFront distribusi harus ditandai](#)
- [\[CloudWatch.17\] tindakan CloudWatch alarm harus diaktifkan](#)
- [\[CodeArtifact.1\] CodeArtifact repositori harus ditandai](#)
- [\[CodeBuild.3\] Log CodeBuild S3 harus dienkripsi](#)
- [\[CodeBuild.4\] lingkungan CodeBuild proyek harus memiliki urasi logging AWS Config](#)

- [\[CodeGuruProfiler.1\] Grup CodeGuru profil profiler harus diberi tag](#)
- [\[CodeGuruReviewer.1\] Asosiasi CodeGuru repositori peninjau harus diberi tag](#)
- [\[Cognito.1\] Kumpulan pengguna Cognito harus mengaktifkan perlindungan ancaman dengan mode penegakan fungsi penuh untuk otentikasi standar](#)
- [\[Connect.1\] Jenis objek Amazon Connect Customer Profiles harus diberi tag](#)
- [\[DataSync.2\] DataSync tugas harus ditandai](#)
- [\[DMS.2\] Sertifikat DMS harus ditandai](#)
- [\[DMS.6\] Instans replikasi DMS harus mengaktifkan peningkatan versi minor otomatis](#)
- [\[DMS.7\] Tugas replikasi DMS untuk database target seharusnya mengaktifkan logging](#)
- [\[DMS.8\] Tugas replikasi DMS untuk database sumber seharusnya mengaktifkan logging](#)
- [\[DMS.9\] Titik akhir DMS harus menggunakan SSL](#)
- [\[DocumentDB.1\] Cluster Amazon DocumentDB harus dienkripsi saat istirahat](#)
- [\[DocumentDB.2\] Cluster Amazon DocumentDB harus memiliki periode retensi cadangan yang memadai](#)
- [\[DocumentDB.3\] Cuplikan cluster manual Amazon DocumentDB seharusnya tidak bersifat publik](#)
- [\[DocumentDB.4\] Cluster Amazon DocumentDB harus mempublikasikan log audit ke Log CloudWatch](#)
- [\[DocumentDB.5\] Cluster Amazon DocumentDB harus mengaktifkan perlindungan penghapusan](#)
- [\[DynamoDB.3\] Cluster DynamoDB Accelerator \(DAX\) harus dienkripsi saat istirahat](#)
- [\[DynamoDB.7\] Cluster DynamoDB Accelerator harus dienkripsi saat transit](#)
- [\[EC2.21\] Jaringan ACLs seharusnya tidak mengizinkan masuknya dari 0.0.0.0/0 ke port 22 atau port 3389.](#)
- [\[EC2.22\] Grup EC2 keamanan Amazon yang tidak digunakan harus dihapus](#)
- [\[EC2.23\] Amazon EC2 Transit Gateways seharusnya tidak secara otomatis menerima permintaan lampiran VPC](#)
- [\[EC2.24\] Jenis instance EC2 paravirtual Amazon tidak boleh digunakan](#)
- [\[EC2.25\] Templat EC2 peluncuran Amazon tidak boleh menetapkan publik IPs ke antarmuka jaringan](#)
- [\[EC2.28\] Volume EBS harus dicakup oleh rencana cadangan](#)
- [\[EC2.38\] EC2 instance harus ditandai](#)
- [\[EC2.58\] VPCs harus dikonfigurasi dengan titik akhir antarmuka untuk Kontak Manajer Insiden Systems Manager](#)

- [\[EC2.60\] VPCs harus dikonfigurasi dengan titik akhir antarmuka untuk Systems Manager Incident Manager](#)
- [\[EC2.170\] templat EC2 peluncuran harus menggunakan Layanan Metadata Instance Versi 2 \(\) IMDSv2](#)
- [\[EC2.173\] Permintaan Armada EC2 Spot harus mengaktifkan enkripsi untuk volume EBS terlampir](#)
- [\[EC2.174\] Set opsi EC2 DHCP harus ditandai](#)
- [\[EC2.175\] templat EC2 peluncuran harus diberi tag](#)
- [\[EC2.176\] daftar EC2 awalan harus ditandai](#)
- [\[EC2.177\] Sesi cermin EC2 lalu lintas harus ditandai](#)
- [\[EC2.178\] Filter cermin EC2 lalu lintas harus ditandai](#)
- [\[EC2.179\] Target cermin EC2 lalu lintas harus ditandai](#)
- [\[ECR.1\] Repositori pribadi ECR harus memiliki pemindaian gambar yang dikonfigurasi](#)
- [\[ECR.2\] Repositori pribadi ECR harus memiliki kekekalan tag yang dikonfigurasi](#)
- [\[ECR.3\] Repositori ECR harus memiliki setidaknya satu kebijakan siklus hidup yang dikonfigurasi](#)
- [\[ECR.4\] Repositori publik ECR harus ditandai](#)
- [\[ECS.3\] Definisi tugas ECS tidak boleh membagikan namespace proses host](#)
- [\[ECS.4\] Kontainer ECS harus berjalan sebagai non-hak istimewa](#)
- [\[ECS.5\] Wadah ECS harus dibatasi pada akses hanya-baca ke sistem file root](#)
- [\[ECS.8\] Rahasia tidak boleh diteruskan sebagai variabel lingkungan kontainer](#)
- [\[ECS.9\] Definisi tugas ECS harus memiliki konfigurasi logging](#)
- [\[ECS.10\] Layanan ECS Fargate harus berjalan pada versi platform Fargate terbaru](#)
- [\[ECS.12\] Cluster ECS harus menggunakan Wawasan Kontainer](#)
- [\[EFS.3\] Titik akses EFS harus menegakkan direktori root](#)
- [\[EFS.4\] Titik akses EFS harus menegakkan identitas pengguna](#)
- [\[EKS.2\] Kluster EKS harus berjalan pada versi Kubernetes yang didukung](#)
- [\[EKS.8\] Kluster EKS harus mengaktifkan pencatatan audit](#)
- [\[ELB.10\] Classic Load Balancer harus menjangkau beberapa Availability Zone](#)
- [\[ELB.12\] Application Load Balancer harus dikonfigurasi dengan mode mitigasi desync defensif atau paling ketat](#)
- [\[ELB.13\] Penyeimbang Beban Aplikasi, Jaringan, dan Gateway harus mencakup beberapa Availability Zone](#)

- [\[ELB.14\] Classic Load Balancer harus dikonfigurasi dengan mode mitigasi desync defensif atau paling ketat](#)
- [\[ELB.16\] Application Load Balancers harus dikaitkan dengan ACL web AWS WAF](#)
- [\[ElastiCache.1\] Cluster ElastiCache \(Redis OSS\) harus mengaktifkan pencadangan otomatis](#)
- [\[ElastiCache.2\] ElastiCache cluster harus mengaktifkan peningkatan versi minor otomatis](#)
- [\[ElastiCache.3\] grup ElastiCache replikasi harus mengaktifkan failover otomatis](#)
- [\[ElastiCache.4\] grup ElastiCache replikasi harus dienkripsi saat istirahat](#)
- [\[ElastiCache.5\] grup ElastiCache replikasi harus dienkripsi saat transit](#)
- [\[ElastiCache.6\] ElastiCache \(Redis OSS\) grup replikasi dari versi sebelumnya harus mengaktifkan Redis OSS AUTH](#)
- [\[ElastiCache.7\] ElastiCache cluster tidak boleh menggunakan grup subnet default](#)
- [\[ElasticBeanstalk.1\] Lingkungan Elastic Beanstalk seharusnya mengaktifkan pelaporan kesehatan yang ditingkatkan](#)
- [\[ElasticBeanstalk.2\] Pembaruan platform yang dikelola Elastic Beanstalk harus diaktifkan](#)
- [\[ElasticBeanstalk.3\] Elastic Beanstalk harus mengalirkan log ke CloudWatch](#)
- [\[EMR.2\] Pengaturan akses publik blok EMR Amazon harus diaktifkan](#)
- [\[EMR.3\] Konfigurasi keamanan Amazon EMR harus dienkripsi saat istirahat](#)
- [\[EMR.4\] Konfigurasi keamanan Amazon EMR harus dienkripsi saat transit](#)
- [\[ES.4\] Kesalahan domain Elasticsearch yang masuk ke CloudWatch Log harus diaktifkan](#)
- [\[EventBridge.3\] bus acara EventBridge khusus harus memiliki kebijakan berbasis sumber daya terlampir](#)
- [\[EventBridge.4\] titik akhir EventBridge global harus mengaktifkan replikasi acara](#)
- [\[FraudDetector.1\] Jenis entitas Amazon Fraud Detector harus diberi tag](#)
- [\[FraudDetector.2\] Label Amazon Fraud Detector harus diberi tag](#)
- [\[FraudDetector.3\] Hasil Amazon Fraud Detector harus ditandai](#)
- [\[FraudDetector.4\] Variabel Amazon Fraud Detector harus diberi tag](#)
- [\[FSx.1\] FSx untuk sistem file OpenZFS harus dikonfigurasi untuk menyalin tag ke cadangan dan volume](#)
- [\[FSx.2\] FSx untuk sistem file Lustre harus dikonfigurasi untuk menyalin tag ke cadangan](#)
- [\[GlobalAccelerator.1\] Akselerator Akselerator Global harus diberi tag](#)
- [\[GuardDuty.7\] GuardDuty EKS Runtime Monitoring harus diaktifkan](#)

- [\[GuardDuty.8\] Perlindungan GuardDuty Malware untuk EC2 harus diaktifkan](#)
- [\[GuardDuty.9\] Perlindungan GuardDuty RDS harus diaktifkan](#)
- [\[GuardDuty.11\] GuardDuty Runtime Monitoring harus diaktifkan](#)
- [\[GuardDuty.12\] GuardDuty ECS Runtime Monitoring harus diaktifkan](#)
- [\[GuardDuty.13\] GuardDuty EC2 Runtime Monitoring harus diaktifkan](#)
- [\[IAM.6\] MFA perangkat keras harus diaktifkan untuk pengguna root](#)
- [\[IAM.9\] MFA harus diaktifkan untuk pengguna root](#)
- [\[IAM.21\] Kebijakan terkelola pelanggan IAM yang Anda buat seharusnya tidak mengizinkan tindakan wildcard untuk layanan](#)
- [\[IAM.24\] Peran IAM harus ditandai](#)
- [\[IAM.25\] Pengguna IAM harus diberi tag](#)
- [\[IAM.28\] IAM Access Analyzer peng analisis akses eksternal harus diaktifkan](#)
- [\[Inspektor.3\] Pemindaian kode Amazon Inspector Lambda harus diaktifkan](#)
- [\[IoT Events .1\] Input Peristiwa AWS IoT harus diberi tag](#)
- [\[IoT Events .2\] Model detektor Acara AWS IoT harus diberi tag](#)
- [\[IoT Events .3\] Model alarm AWS IoT Events harus diberi tag](#)
- [\[IoT Site Wise.1\] Model aset AWS IoT harus ditandai SiteWise](#)
- [\[IoT Site Wise.2\] Dasbor AWS IoT harus diberi tag SiteWise](#)
- [\[IoT Site Wise.3\] Gateway AWS IoT harus diberi tag SiteWise](#)
- [\[IoT Site Wise.4\] Portal AWS IoT harus diberi tag SiteWise](#)
- [\[IoT Site Wise.5\] Proyek AWS IoT harus diberi tag SiteWise](#)
- [\[IoT Twin Maker.1\] Pekerjaan sinkronisasi AWS IoT harus ditandai TwinMaker](#)
- [\[IoT Twin Maker.2\] Ruang kerja AWS IoT harus diberi tag TwinMaker](#)
- [\[IoT Twin Maker.3\] Adegan AWS IoT harus diberi tag TwinMaker](#)
- [\[IoT Twin Maker.4\] Entitas AWS IoT harus diberi tag TwinMaker](#)
- [\[IoT Wireless .1\] Grup multicast Nirkabel AWS IoT harus diberi tag](#)
- [\[IoT Wireless .2\] Profil layanan AWS IoT Wireless harus diberi tag](#)
- [\[IoT Wireless .3\] Tugas AWS IoT FUOTA harus ditandai](#)
- [\[IVS.1\] Pasangan kunci pemutaran IVS harus ditandai](#)
- [\[IVS.2\] Konfigurasi perekaman IVS harus ditandai](#)

- [\[IVS.3\] Saluran IVS harus ditandai](#)
- [\[Keyspaces.1\] Ruang kunci Amazon Keyspaces harus diberi tag](#)
- [\[Kinesis.1\] Aliran kinesis harus dienkripsi saat istirahat](#)
- [\[KMS.5\] Kunci KMS tidak boleh diakses publik](#)
- [\[Lambda.5\] Fungsi VPC Lambda harus beroperasi di beberapa Availability Zone](#)
- [\[Macie.1\] Amazon Macie harus diaktifkan](#)
- [\[Macie.2\] Penemuan data sensitif otomatis Macie harus diaktifkan](#)
- [\[MQ.3\] Broker Amazon MQ harus mengaktifkan peningkatan versi minor otomatis](#)
- [\[MQ.5\] Broker ActiveMQ harus menggunakan mode penerapan aktif/siaga](#)
- [\[MQ.6\] Broker RabbitMQ harus menggunakan mode penerapan cluster](#)
- [\[MSK.1\] Kluster MSK harus dienkripsi saat transit di antara node broker](#)
- [\[MSK.2\] Kluster MSK seharusnya telah meningkatkan pemantauan yang dikonfigurasi](#)
- [\[MSK.3\] Konektor MSK Connect harus dienkripsi saat transit](#)
- [\[Neptunus.1\] Cluster DB Neptunus harus dienkripsi saat istirahat](#)
- [\[Neptune.2\] Cluster DB Neptunus harus menerbitkan log audit ke Log CloudWatch](#)
- [\[Neptune.3\] Snapshot cluster Neptunus DB seharusnya tidak publik](#)
- [\[Neptunus.4\] Cluster DB Neptunus harus mengaktifkan perlindungan penghapusan](#)
- [\[Neptunus.5\] Cluster DB Neptunus harus mengaktifkan cadangan otomatis](#)
- [\[Neptune.6\] Snapshot cluster Neptunus DB harus dienkripsi saat istirahat](#)
- [\[Neptune.7\] Cluster DB Neptunus harus mengaktifkan otentikasi basis data IAM](#)
- [\[Neptunus.8\] Cluster DB Neptunus harus dikonfigurasi untuk menyalin tag ke snapshot](#)
- [\[Neptunus.9\] Cluster DB Neptunus harus digunakan di beberapa Availability Zone](#)
- [\[NetworkFirewall.1\] Firewall Jaringan harus digunakan di beberapa Availability Zone](#)
- [\[NetworkFirewall.2\] Pencatatan Firewall Jaringan harus diaktifkan](#)
- [\[NetworkFirewall.3\] Kebijakan Network Firewall harus memiliki setidaknya satu kelompok aturan yang terkait](#)
- [\[NetworkFirewall.4\] Tindakan stateless default untuk kebijakan Network Firewall harus drop atau forward untuk paket penuh](#)
- [\[NetworkFirewall.5\] Tindakan stateless default untuk kebijakan Network Firewall harus drop atau forward untuk paket yang terfragmentasi](#)
- [\[NetworkFirewall.6\] Grup aturan Stateless Network Firewall tidak boleh kosong](#)

- [\[NetworkFirewall.9\] Firewall Jaringan harus mengaktifkan perlindungan penghapusan](#)
- [\[Opensearch.1\] OpenSearch domain harus mengaktifkan enkripsi saat istirahat](#)
- [\[Opensearch.2\] OpenSearch domain tidak boleh diakses publik](#)
- [\[Opensearch.3\] OpenSearch domain harus mengenkripsi data yang dikirim antar node](#)
- [\[Opensearch.4\] login kesalahan OpenSearch domain ke Log harus diaktifkan CloudWatch](#)
- [\[Opensearch.5\] OpenSearch domain harus mengaktifkan pencatatan audit](#)
- [\[Opensearch.6\] OpenSearch domain harus memiliki setidaknya tiga node data](#)
- [\[Opensearch.7\] OpenSearch domain harus mengaktifkan kontrol akses berbutir halus](#)
- [\[Opensearch.8\] Koneksi ke OpenSearch domain harus dienkripsi menggunakan kebijakan keamanan TLS terbaru](#)
- [\[PCA.1\] otoritas sertifikat AWS Private CA root harus dinonaktifkan](#)
- [\[PCA.2\] Otoritas sertifikat CA AWS swasta harus ditandai](#)
- [\[RDS.14\] Cluster Amazon Aurora seharusnya mengaktifkan backtracking](#)
- [\[RDS.15\] Cluster RDS DB harus dikonfigurasi untuk beberapa Availability Zone](#)
- [\[RDS.24\] Kluster Database RDS harus menggunakan nama pengguna administrator khusus](#)
- [\[RDS.25\] Instans database RDS harus menggunakan nama pengguna administrator khusus](#)
- [\[RDS.27\] Cluster RDS DB harus dienkripsi saat istirahat](#)
- [\[RDS.34\] Kluster Aurora MySQL DB harus menerbitkan log audit ke Log CloudWatch](#)
- [\[RDS.35\] Cluster RDS DB harus mengaktifkan peningkatan versi minor otomatis](#)
- [\[Redshift.7\] Cluster Redshift harus menggunakan perutean VPC yang ditingkatkan](#)
- [\[Redshift.8\] Cluster Amazon Redshift tidak boleh menggunakan nama pengguna Admin default](#)
- [\[Redshift.9\] Cluster Redshift tidak boleh menggunakan nama database default](#)
- [\[Redshift.10\] Cluster Redshift harus dienkripsi saat istirahat](#)
- [\[Redshift.11\] Cluster Redshift harus ditandai](#)
- [\[Redshift.13\] Snapshot cluster Redshift harus ditandai](#)
- [\[Redshift.17\] Grup parameter cluster Redshift harus ditandai](#)
- [\[RedshiftServerless.1\] Grup kerja Amazon Redshift Tanpa Server harus menggunakan perutean VPC yang disempurnakan](#)
- [\[RedshiftServerless.2\] Koneksi ke grup kerja Redshift Serverless harus diperlukan untuk menggunakan SSL](#)
- [\[RedshiftServerless.3\] Kelompok kerja Redshift Tanpa Server harus melarang akses publik](#)

- [\[RedshiftServerless.6\] Ruang nama Redshift Tanpa Server harus mengekspor log ke Log CloudWatch](#)
- [\[Route53.1\] Pemeriksaan kesehatan rute 53 harus ditandai](#)
- [\[Route53.2\] Route 53 zona yang dihosting publik harus mencatat kueri DNS](#)
- [\[S3.10\] Bucket tujuan umum S3 dengan versi diaktifkan harus memiliki konfigurasi Siklus Hidup](#)
- [\[S3.11\] Bucket tujuan umum S3 harus mengaktifkan pemberitahuan acara](#)
- [\[S3.12\] tidak ACLs boleh digunakan untuk mengelola akses pengguna ke bucket tujuan umum S3](#)
- [\[S3.13\] Bucket tujuan umum S3 harus memiliki konfigurasi Siklus Hidup](#)
- [\[S3.20\] Bucket tujuan umum S3 harus mengaktifkan penghapusan MFA](#)
- [\[S3.24\] Poin Akses Multi-Wilayah S3 harus mengaktifkan pengaturan akses publik blok](#)
- [\[SageMaker.2\] instance SageMaker notebook harus diluncurkan dalam VPC khusus](#)
- [\[SageMaker.3\] Pengguna seharusnya tidak memiliki akses root ke instance SageMaker notebook](#)
- [\[SageMaker.5\] SageMaker model harus memblokir lalu lintas masuk](#)
- [\[SageMaker.6\] konfigurasi gambar SageMaker aplikasi harus ditandai](#)
- [\[SageMaker.7\] SageMaker gambar harus diberi tag](#)
- [\[SNS.4\] Kebijakan akses topik SNS seharusnya tidak mengizinkan akses publik](#)
- [\[SQS.3\] Kebijakan akses antrian SQS seharusnya tidak mengizinkan akses publik](#)
- [\[SSM.4\] Dokumen SSM seharusnya tidak bersifat publik](#)
- [\[SSM.5\] Dokumen SSM harus ditandai](#)
- [\[StepFunctions.1\] Mesin status Step Functions seharusnya mengaktifkan logging](#)
- [\[StepFunctions.2\] Aktivitas Step Functions harus diberi tag](#)
- [\[Transfer.4\] Perjanjian Transfer Family harus ditandai](#)
- [\[Transfer.5\] Sertifikat Transfer Family harus diberi tag](#)
- [\[Transfer.6\] Konektor Transfer Family harus diberi tag](#)
- [\[Transfer.7\] Profil Transfer Family harus diberi tag](#)
- [\[WAF.1\] Pencatatan ACL Web Global AWS WAF Klasik harus diaktifkan](#)
- [\[WAF.2\] Aturan Regional AWS WAF Klasik harus memiliki setidaknya satu syarat](#)
- [\[WAF.3\] Kelompok aturan Regional AWS WAF Klasik harus memiliki setidaknya satu aturan](#)
- [\[WAF.4\] Web Regional AWS WAF Klasik ACLs harus memiliki setidaknya satu aturan atau kelompok aturan](#)
- [\[WAF.6\] Aturan global AWS WAF klasik harus memiliki setidaknya satu syarat](#)

- [\[WAF.7\] Kelompok aturan global AWS WAF klasik harus memiliki setidaknya satu aturan](#)
- [\[WAF.8\] Web global AWS WAF klasik ACLs harus memiliki setidaknya satu aturan atau kelompok aturan](#)
- [\[WAF.10\] AWS WAF web ACLs harus memiliki setidaknya satu aturan atau kelompok aturan](#)
- [AWS WAF Aturan \[WAF.12\] harus mengaktifkan metrik CloudWatch](#)

Membuat sumber daya CSPM Security Hub dengan CloudFormation

AWS Security Hub Cloud Security Posture Management (CSPM) terintegrasi dengan AWS CloudFormation, yang merupakan layanan yang membantu Anda memodelkan dan mengatur AWS sumber daya sehingga Anda dapat menghabiskan lebih sedikit waktu untuk membuat dan mengelola sumber daya dan infrastruktur Anda. Anda membuat templat yang menjelaskan semua AWS sumber daya yang Anda inginkan (seperti aturan otomatisasi), dan AWS CloudFormation ketentuan serta mengonfigurasi sumber daya tersebut untuk Anda.

Bila Anda menggunakan AWS CloudFormation, Anda dapat menggunakan kembali template Anda untuk mengatur sumber daya CSPM Security Hub Anda secara konsisten dan berulang kali. Jelaskan sumber daya Anda sekali, lalu sediakan sumber daya yang sama berulang-ulang di beberapa Akun AWS dan Wilayah.

CSPM dan template Security Hub AWS CloudFormation

Untuk menyediakan dan mengonfigurasi sumber daya untuk CSPM Security Hub dan layanan terkait, Anda harus memahami cara kerja [AWS CloudFormation templat](#). Template adalah file teks dalam format JSON atau YAMM. Template ini menjelaskan sumber daya yang ingin Anda sediakan di AWS CloudFormation tumpukan Anda.

Jika Anda tidak terbiasa dengan JSON atau YAMM, Anda dapat menggunakan AWS CloudFormation Designer untuk membantu Anda memulai dengan template. AWS CloudFormation Untuk informasi lebih lanjut, lihat [Apa itu AWS CloudFormation Desainer?](#) dalam AWS CloudFormation User Guide.

Anda dapat membuat AWS CloudFormation template untuk jenis sumber daya CSPM Security Hub berikut:

- Mengaktifkan Security Hub CSPM
- Menunjuk administrator CSPM Security Hub yang didelegasikan untuk sebuah organisasi
- Tentukan cara organisasi Anda dikonfigurasi di Security Hub CSPM
- Mengaktifkan standar keamanan
- Mengaktifkan agregasi lintas wilayah
- Membuat kebijakan konfigurasi pusat dan mengaitkannya dengan akun, unit organisasi (OUs), atau root

- Membuat wawasan khusus
- Membuat aturan otomatisasi
- Menyesuaikan parameter kontrol
- Berlangganan integrasi produk pihak ketiga

Untuk informasi selengkapnya, termasuk contoh template JSON dan YAMAL untuk sumber daya, lihat [referensi jenis sumber daya AWS Security Hub Cloud Security Posture Management \(CSPM\) Security Hub di Panduan Pengguna](#).AWS CloudFormation

Pelajari lebih lanjut tentang AWS CloudFormation

Untuk mempelajari selengkapnya AWS CloudFormation, lihat sumber daya berikut:

- [AWS CloudFormation](#)
- [AWS CloudFormation Panduan Pengguna](#)
- [AWS CloudFormation Referensi API](#)
- [AWS CloudFormation Panduan Pengguna Antarmuka Baris Perintah](#)

Berlangganan pengumuman CSPM Security Hub dengan Amazon SNS

Bagian ini memberikan informasi tentang berlangganan pengumuman AWS Security Hub Cloud Security Posture Management (CSPM) dengan Amazon Simple Notification Service (Amazon SNS) untuk menerima pemberitahuan tentang Security Hub CSPM.

Setelah berlangganan, Anda akan menerima pemberitahuan tentang acara berikut (perhatikan yang sesuai `AnnouncementType` untuk setiap acara):

- **GENERAL**— Pemberitahuan umum tentang layanan CSPM Security Hub.
- **UPCOMING_STANDARDS_CONTROLS**— Kontrol atau standar CSPM Security Hub yang ditentukan akan segera dirilis. Jenis pengumuman ini membantu Anda mempersiapkan alur kerja respons dan remediasi sebelum rilis.
- **NEW_REGIONS**— Support for Security Hub CSPM tersedia dalam versi baru. Wilayah AWS
- **NEW_STANDARDS_CONTROLS**— Kontrol atau standar CSPM Security Hub baru telah ditambahkan.
- **UPDATED_STANDARDS_CONTROLS**— Kontrol atau standar CSPM Security Hub yang ada telah diperbarui.
- **RETIRED_STANDARDS_CONTROLS**— Kontrol atau standar CSPM Security Hub yang ada telah dihentikan.
- **UPDATED_ASFF**— Sintaks, bidang, atau nilai AWS Security Finding Format (ASFF) telah diperbarui.
- **NEW_INTEGRATION**— Integrasi baru dengan AWS layanan lain atau produk pihak ketiga tersedia.
- **NEW_FEATURE**— Fitur CSPM Security Hub baru tersedia.
- **UPDATED_FEATURE**— Fitur CSPM Security Hub yang ada telah diperbarui.

Notifikasi tersedia dalam semua format yang didukung Amazon SNS. Anda dapat berlangganan pengumuman CSPM Security Hub di semua tempat [CSPM Security Wilayah AWS Hub tersedia](#).

Pengguna harus memiliki `Subscribe` izin untuk berlangganan topik Amazon SNS. Anda dapat mencapai ini dengan kebijakan Amazon SNS, kebijakan IAM, atau keduanya. Untuk informasi selengkapnya, lihat [kebijakan IAM dan Amazon SNS bersama-sama di Panduan](#) Pengembang Layanan Pemberitahuan Sederhana Amazon.

Note

Security Hub CSPM mengirimkan pengumuman Amazon SNS tentang pembaruan ke layanan CSPM Security Hub ke semua yang berlangganan. Akun AWS Untuk menerima pemberitahuan tentang temuan CSPM Security Hub, lihat. [Meninjau detail dan riwayat penemuan di Security Hub CSPM](#)

Anda dapat berlangganan antrian Amazon Simple Queue Service (Amazon SQS) untuk topik Amazon SNS, tetapi Anda harus menggunakan topik Amazon SNS Nama Sumber Daya Amazon (ARN) yang ada di Wilayah yang sama. Untuk informasi selengkapnya, lihat [Berlangganan antrian ke topik Amazon SNS](#) di Panduan Pengembang Layanan Antrian Sederhana Amazon.

Anda juga dapat menggunakan AWS Lambda fungsi untuk memanggil acara saat Anda menerima pemberitahuan. Untuk informasi selengkapnya, termasuk kode fungsi contoh, lihat [Tutorial: Menggunakan AWS Lambda dengan Amazon Simple Notification Service](#) di Panduan AWS Lambda Pengembang.

Topik Amazon SNS ARNs untuk setiap Wilayah adalah sebagai berikut.

Wilayah AWS	ARN topik Amazon SNS
AS Timur (Ohio)	arn:aws:sns:us-east-2:291342846459:SecurityHubAnnouncements
AS Timur (Virginia Utara)	arn:aws:sns:us-east-1:088139225913:SecurityHubAnnouncements
AS Barat (California Utara)	arn:aws:sns:us-west-1:137690824926:SecurityHubAnnouncements
AS Barat (Oregon)	arn:aws:sns:us-west-2:393883065485:SecurityHubAnnouncements

Wilayah AWS	ARN topik Amazon SNS
Afrika (Cape Town)	<code>arn:aws:sns:af-south-1:463142546776:SecurityHubAnnouncements</code>
Asia Pasifik (Hong Kong)	<code>arn:aws:sns:ap-east-1:464812404305:SecurityHubAnnouncements</code>
Asia Pasifik (Hyderabad)	<code>arn:aws:sns:ap-south-2:849907286123:SecurityHubAnnouncements</code>
Asia Pasifik (Jakarta)	<code>arn:aws:sns:ap-southeast-3:627843640627:SecurityHubAnnouncements</code>
Asia Pasifik (Mumbai)	<code>arn:aws:sns:ap-south-1:707356269775:SecurityHubAnnouncements</code>
Asia Pasifik (Osaka)	<code>arn:aws:sns:ap-northeast-3:633550238216:SecurityHubAnnouncements</code>
Asia Pasifik (Seoul)	<code>arn:aws:sns:ap-northeast-2:374299265323:SecurityHubAnnouncements</code>
Asia Pasifik (Singapura)	<code>arn:aws:sns:ap-southeast-1:512267288502:SecurityHubAnnouncements</code>
Asia Pasifik (Sydney)	<code>arn:aws:sns:ap-southeast-2:475730049140:SecurityHubAnnouncements</code>

Wilayah AWS	ARN topik Amazon SNS
Asia Pasifik (Tokyo)	<code>arn:aws:sns:ap-northeast-1:592469075483:SecurityHubAnnouncements</code>
Kanada (Pusat)	<code>arn:aws:sns:ca-central-1:137749997395:SecurityHubAnnouncements</code>
Tiongkok (Beijing)	<code>arn:aws-cn:sns:cn-north-1:672341567257:SecurityHubAnnouncements</code>
Tiongkok (Ningxia)	<code>arn:aws-cn:sns:cn-northwest-1:672534482217:SecurityHubAnnouncements</code>
Eropa (Frankfurt)	<code>arn:aws:sns:eu-central-1:871975303681:SecurityHubAnnouncements</code>
Eropa (Irlandia)	<code>arn:aws:sns:eu-west-1:705756202095:SecurityHubAnnouncements</code>
Eropa (London)	<code>arn:aws:sns:eu-west-2:883600840440:SecurityHubAnnouncements</code>
Eropa (Milan)	<code>arn:aws:sns:eu-south-1:151363035580:SecurityHubAnnouncements</code>
Eropa (Paris)	<code>arn:aws:sns:eu-west-3:313420042571:SecurityHubAnnouncements</code>

Wilayah AWS	ARN topik Amazon SNS
Eropa (Spanyol)	<code>arn:aws:sns:eu-south-2:777487947751:SecurityHubAnnouncements</code>
Eropa (Stockholm)	<code>arn:aws:sns:eu-north-1:191971010772:SecurityHubAnnouncements</code>
Eropa (Zürich)	<code>arn:aws:sns:eu-central-2:704347005078:SecurityHubAnnouncements</code>
Israel (Tel Aviv)	<code>arn:aws:sns:il-central-1:726652212146:SecurityHubAnnouncements</code>
Timur Tengah (Bahrain)	<code>arn:aws:sns:me-south-1:585146626860:SecurityHubAnnouncements</code>
Timur Tengah (UEA)	<code>arn:aws:sns:me-central-1:431548502100:SecurityHubAnnouncements</code>
Amerika Selatan (Sao Paulo)	<code>arn:aws:sns:sa-east-1:359811883282:SecurityHubAnnouncements</code>
AWS GovCloud (AS-Timur)	<code>arn:aws-us-gov:sns:us-gov-east-1:239368469855:SecurityHubAnnouncements</code>
AWS GovCloud (AS-Barat)	<code>arn:aws-us-gov:sns:us-gov-west-1:239334163374:SecurityHubAnnouncements</code>

Pesan biasanya sama di seluruh Wilayah dalam [partisi](#), sehingga Anda dapat berlangganan satu Wilayah di setiap partisi untuk menerima pengumuman yang memengaruhi semua Wilayah di partisi tersebut. Pengumuman yang terkait dengan akun anggota tidak direplikasi di akun administrator. Akibatnya, setiap akun, termasuk akun administrator, hanya akan memiliki satu salinan dari setiap pengumuman. Anda dapat memutuskan akun mana yang ingin Anda gunakan untuk berlangganan pengumuman CSPM Security Hub.

[Untuk informasi tentang biaya berlangganan pengumuman CSPM Security Hub, lihat harga Amazon SNS.](#)

Berlangganan pengumuman CSPM Security Hub (konsol)

1. [Buka konsol Amazon SNS di https://console.aws.amazon.com/sns/v3/home](https://console.aws.amazon.com/sns/v3/home).
2. Dalam daftar Wilayah, pilih Wilayah tempat Anda ingin berlangganan pengumuman CSPM Security Hub. Contoh ini menggunakan Wilayah us-west-2.
3. Di panel navigasi, pilih Langganan, lalu pilih Buat langganan.
4. Masukkan topik ARN ke dalam topik ARN kotak. Misalnya, `arn:aws:sns:us-west-2:393883065485:SecurityHubAnnouncements`.
5. Untuk Protokol, pilih cara Anda ingin menerima pengumuman CSPM Security Hub. Jika Anda memilih Email, untuk Endpoint, masukkan alamat email yang ingin Anda gunakan untuk menerima pengumuman.
6. Pilih Buat langganan.
7. Konfirmasi langganan. Misalnya, jika Anda memilih protokol email, Amazon SNS akan mengirim pesan konfirmasi berlangganan ke email yang Anda berikan.

Berlangganan pengumuman CSPM Security Hub (AWS CLI)

1. Jalankan perintah berikut:

```
aws sns --region us-west-2 subscribe --topic-arn arn:aws:sns:us-west-2:393883065485:SecurityHubAnnouncements --protocol email --notification-endpoint your_email@your_domain.com
```

2. Konfirmasi langganan. Misalnya, jika Anda memilih protokol email, Amazon SNS akan mengirim pesan konfirmasi berlangganan ke email yang Anda berikan.

Format pesan Amazon SNS

Contoh berikut menunjukkan pengumuman CSPM Security Hub dari Amazon SNS tentang pengenalan kontrol keamanan baru. Konten pesan bervariasi berdasarkan jenis pengumuman, tetapi formatnya sama untuk semua jenis pengumuman. Secara opsional, Link bidang yang memberikan rincian tentang pengumuman dapat disertakan.

Contoh: Pengumuman CSPM Security Hub untuk kontrol baru (protokol email)

```
{
  "AnnouncementType": "NEW_STANDARDS_CONTROLS",
  "Title": "[New Controls] 36 new Security Hub CSPM controls added to the AWS Foundational Security Best Practices standard",
  "Description": "We have added 36 new controls to the AWS Foundational Security Best Practices standard. These include controls for Amazon Auto Scaling (AutoScaling.3, AutoScaling.4, AutoScaling.6), AWS CloudFormation (CloudFormation.1), Amazon CloudFront (CloudFront.10), Amazon Elastic Compute Cloud (Amazon EC2) (EC2.23, EC2.24, EC2.27), Amazon Elastic Container Registry (Amazon ECR) (ECR.1, ECR.2), Amazon Elastic Container Service (Amazon ECS) (ECS.3, ECS.4, ECS.5, ECS.8, ECS.10, ECS.12), Amazon Elastic File System (Amazon EFS) (EFS.3, EFS.4), Amazon Elastic Kubernetes Service (Amazon EKS) (EKS.2), Elastic Load Balancing (ELB.12, ELB.13, ELB.14), Amazon Kinesis (Kinesis.1), AWS Network Firewall (NetworkFirewall.3, NetworkFirewall.4, NetworkFirewall.5), Amazon OpenSearch Service (OpenSearch.7), Amazon Redshift (Redshift.9), Amazon Simple Storage Service (Amazon S3) (S3.13), Amazon Simple Notification Service (SNS.2), AWS WAF (WAF.2, WAF.3, WAF.4, WAF.6, WAF.7, WAF.8). If you enabled the AWS Foundational Security Best Practices standard in an account and configured Security Hub CSPM to automatically enable new controls, these controls are enabled by default. Availability of controls can vary by Region. "
}
```

Contoh: Pengumuman CSPM Security Hub untuk kontrol baru (protokol Email-JSON)

```
{
  "Type" : "Notification",
  "MessageId" : "d124c9cf-326a-5931-9263-92a92e7af49f",
  "TopicArn" : "arn:aws:sns:us-west-2:393883065485:SecurityHubAnnouncements",
  "Message" : "{\"AnnouncementType\":\"NEW_STANDARDS_CONTROLS\",\"Title\":\"[New Controls] 36 new Security Hub CSPM controls added to the AWS Foundational Security Best Practices standard\",\"Description\":\"We have added 36 new controls to the AWS Foundational Security Best Practices standard. These include controls for Amazon Auto Scaling (AutoScaling.3, AutoScaling.4, AutoScaling.6), AWS CloudFormation
```

```
(CloudFormation.1), Amazon CloudFront (CloudFront.10), Amazon Elastic Compute Cloud
(Amazon EC2) (EC2.23, EC2.24, EC2.27), Amazon Elastic Container Registry (Amazon ECR)
(ECR.1, ECR.2), Amazon Elastic Container Service (Amazon ECS) (ECS.3, ECS.4, ECS.5,
ECS.8, ECS.10, ECS.12), Amazon Elastic File System (Amazon EFS) (EFS.3, EFS.4), Amazon
Elastic Kubernetes Service (Amazon EKS) (EKS.2), Elastic Load Balancing (ELB.12,
ELB.13, ELB.14), Amazon Kinesis (Kinesis.1), AWS Network Firewall (NetworkFirewall.1.3,
NetworkFirewall.1.4, NetworkFirewall.1.5), Amazon OpenSearch Service (OpenSearch.7),
Amazon Redshift (Redshift.9),
Amazon Simple Storage Service (Amazon S3) (S3.13), Amazon Simple Notification Service
(SNS.2), AWS WAF (WAF.2, WAF.3, WAF.4, WAF.6, WAF.7, WAF.8). If you enabled the AWS
Foundational Security Best Practices standard in an account and configured SSecurity
Hub CSPM to automatically enable new controls, these controls are enabled by default.
Availability of controls can vary by Region. \"}",
  "Timestamp" : "2022-08-04T19:11:12.652Z",
  "SignatureVersion" : "1",
  "Signature" :
    "HTHgNFRYMetCvisulgLM4CVySvK9qCXFPHQDxYl9tuCFQuIrd7Y04m4YFR28XKMgzqrF20YP
+EilipUm2S0TpEEt0TekU5bn74+YmNZfwr4aPFx0vUuQCV0shmHl37hjkilJhCg/t53QQiLfp7MH
+MTXIUPR37k5SuFCXvjpRQ8ynV532AH3Wpv0HmojDLMg+eg51V1fUs0G8yiJVCBEJhJ1yS
+gkwJdhRk2UQab9RcAmE6COK3hRWcjDwqTXz5nR6Ywv1ZqZfLI17gYKslt+jsyd/k+7k0qGm0JRDr7qhE7H
+7vaGRL0ptsQnbW8VmeYnDbahE08FV+Mp1rpV+7Qg==",
  "SigningCertURL" : "https://sns.us-west-2.amazonaws.com/
SimpleNotificationService-56e67fcb41f6fec09b0196692625d385.pem",
  "UnsubscribeURL" : "https://sns.us-west-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-
west-2:393883065485:SecurityHubAnnouncements:9d0230d7-d582-451d-9f15-0c32818bf61f"
}
```

Menonaktifkan CSPM Security Hub

Anda dapat menonaktifkan AWS Security Hub Cloud Security Posture Management (CSPM) dengan menggunakan konsol CSPM Security Hub atau Security Hub API. Jika Anda menonaktifkan Security Hub CSPM, Anda dapat mengaktifkannya lagi nanti.

Jika organisasi Anda menggunakan konfigurasi pusat, administrator CSPM Security Hub yang didelegasikan dapat membuat kebijakan konfigurasi yang menonaktifkan CSPM Security Hub untuk akun tertentu dan unit organisasi (OUs), dan tetap mengaktifkan CSPM Security Hub untuk orang lain. Kebijakan konfigurasi memengaruhi Wilayah asal dan semua Wilayah yang ditautkan. Untuk informasi selengkapnya, lihat [Memahami konfigurasi pusat di Security Hub CSPM](#).

Jika Anda menonaktifkan CSPM Security Hub untuk sebuah akun, hal berikut akan terjadi:

- Semua standar dan kontrol dinonaktifkan untuk akun.
- Security Hub CSPM berhenti menghasilkan dan menelan temuan baru untuk akun tersebut.
- Setelah 30 hari, Security Hub CSPM secara permanen menghapus semua temuan arsip yang ada untuk akun tersebut. Temuan ini tidak dapat dipulihkan dengan menggunakan Security Hub CSPM.
- Setelah 90 hari, Security Hub CSPM secara permanen menghapus semua temuan aktif yang ada untuk akun tersebut. Temuan ini tidak dapat dipulihkan dengan menggunakan Security Hub CSPM.
- Setelah 90 hari, Security Hub CSPM secara permanen menghapus semua wawasan yang ada dan pengaturan konfigurasi CSPM Security Hub untuk akun tersebut. Data dan pengaturan tidak dapat dipulihkan.

Untuk mempertahankan temuan yang ada, Anda dapat mengekspor temuan ke bucket S3 sebelum menonaktifkan CSPM Security Hub. Anda dapat melakukan ini dengan menggunakan tindakan kustom dengan EventBridge aturan Amazon. Untuk informasi selengkapnya, lihat [Menggunakan EventBridge untuk respon otomatis dan remediasi](#).

Jika Anda mengaktifkan kembali CSPM Security Hub dalam waktu 90 hari setelah menonaktifkannya untuk akun, Anda mendapatkan kembali akses ke temuan aktif yang ada, serta wawasan dan pengaturan konfigurasi CSPM Security Hub untuk akun tersebut. Jika Anda mengaktifkan kembali CSPM Security Hub dalam waktu 30 hari, Anda juga mendapatkan kembali akses ke temuan arsip yang ada untuk akun tersebut. Namun, temuan yang ada mungkin tidak akurat karena akan mencerminkan keadaan AWS lingkungan Anda saat Anda menonaktifkan CSPM Security Hub. Selain itu, saat Anda mengaktifkan kembali standar dan kontrol individual, Security Hub CSPM mungkin

awalnya menghasilkan temuan duplikat untuk AWS sumber daya tertentu, tergantung pada standar dan kontrol yang Anda aktifkan. Untuk alasan ini, kami menyarankan Anda melakukan salah satu hal berikut:

- Ubah status alur kerja dari semua temuan yang ada RESOLVED sebelum Anda menonaktifkan CSPM Security Hub. Untuk informasi selengkapnya, lihat [Menetapkan status alur kerja temuan di Security Hub CSPM](#).
- Nonaktifkan semua standar setidaknya enam hari sebelum Anda menonaktifkan Security Hub CSPM. Security Hub CSPM kemudian mengarsipkan semua temuan yang ada berdasarkan upaya terbaik, biasanya dalam waktu tiga hingga lima hari. Untuk informasi selengkapnya, lihat [Menonaktifkan standar keamanan](#).

Anda tidak dapat menonaktifkan CSPM Security Hub dalam kasus berikut:

- Akun Anda adalah akun administrator CSPM Security Hub yang didelegasikan untuk organisasi. Jika Anda menggunakan konfigurasi pusat, Anda tidak dapat mengaitkan kebijakan konfigurasi yang menonaktifkan CSPM Security Hub untuk akun administrator yang didelegasikan. Asosiasi dapat berhasil untuk akun lain, tetapi CSPM Security Hub tidak menerapkan kebijakan tersebut ke akun administrator yang didelegasikan.
- Akun Anda adalah akun administrator CSPM Security Hub berdasarkan undangan, dan Anda memiliki akun anggota. Sebelum Anda dapat menonaktifkan Security Hub CSPM, Anda harus memisahkan semua akun anggota Anda. Untuk mempelajari caranya, lihat [the section called “Memutuskan akun anggota”](#).

Sebelum pemilik akun anggota dapat menonaktifkan CSPM Security Hub, akun tersebut harus memisahkan diri dari akun administratornya. Untuk akun organisasi, hanya akun administrator yang dapat memisahkan akun anggota. Untuk informasi selengkapnya, lihat [the section called “Memutuskan akun anggota organisasi”](#). Untuk akun yang diundang secara manual, akun administrator atau akun anggota dapat memisahkan akun. Untuk informasi selengkapnya, lihat [the section called “Memutuskan akun anggota”](#) atau [the section called “Memutuskan hubungan dari akun administrator”](#). Pemutusan tidak diperlukan jika Anda menggunakan konfigurasi pusat karena administrator CSPM Security Hub dapat membuat kebijakan yang menonaktifkan CSPM Security Hub untuk akun anggota tertentu.

Saat Anda menonaktifkan CSPM Security Hub untuk sebuah akun, CSPM hanya dinonaktifkan saat ini. Wilayah AWS Namun, jika Anda menggunakan konfigurasi pusat untuk menonaktifkan CSPM

Security Hub untuk akun tertentu, itu dinonaktifkan di Wilayah beranda dan semua Wilayah yang ditautkan.

Untuk menonaktifkan CSPM Security Hub, pilih metode pilihan Anda dan ikuti langkah-langkahnya.

Security Hub CSPM console

Ikuti langkah-langkah ini untuk menonaktifkan CSPM Security Hub dengan menggunakan konsol.

Untuk menonaktifkan CSPM Security Hub

1. Buka konsol AWS Security Hub Cloud Security Posture Management (CSPM) di <https://console.aws.amazon.com/securityhub/>
2. Di panel navigasi, pada Pengaturan, pilih Umum.
3. Di bagian Nonaktifkan CSPM Security Hub, pilih Nonaktifkan CSPM Security Hub.
4. Saat diminta konfirmasi, pilih Nonaktifkan CSPM Security Hub.

Security Hub API

Untuk menonaktifkan Security Hub CSPM secara terprogram, gunakan [DisableSecurityHub](#) pengoperasian Security Hub AWS API. Atau, jika Anda menggunakan AWS CLI, jalankan [disable-security-hub](#) perintah. Misalnya, perintah berikut menonaktifkan CSPM Security Hub saat ini: Wilayah AWS

```
$ aws securityhub disable-security-hub
```


Keamanan di AWS Security Hub

Keamanan cloud di AWS adalah prioritas tertinggi. Sebagai AWS pelanggan, Anda mendapat manfaat dari pusat data dan arsitektur jaringan yang dibangun untuk memenuhi persyaratan organisasi yang paling sensitif terhadap keamanan.

Keamanan adalah tanggung jawab bersama antara Anda AWS dan Anda. [Model tanggung jawab bersama](#) menggambarkan hal ini sebagai keamanan dari cloud dan keamanan di cloud:

- Keamanan cloud — AWS bertanggung jawab untuk melindungi infrastruktur yang menjalankan AWS layanan di AWS Cloud. AWS juga memberi Anda layanan yang dapat Anda gunakan dengan aman. Auditor pihak ketiga menguji dan memverifikasi efektivitas keamanan kami sebagai bagian dari [program kepatuhan AWS](#). Untuk mempelajari program kepatuhan yang berlaku di AWS Security Hub, lihat [Cakupan Layanan Menurut Program Kepatuhan AWS](#).
- Keamanan di cloud — Tanggung jawab Anda ditentukan oleh AWS layanan yang Anda gunakan. Anda juga bertanggung jawab atas faktor lain, yang mencakup sensitivitas data Anda, persyaratan perusahaan Anda, serta undang-undang dan peraturan yang berlaku.

Dokumentasi ini membantu Anda memahami cara menerapkan model tanggung jawab bersama saat menggunakan Security Hub. Topik berikut menunjukkan cara mengonfigurasi Security Hub untuk memenuhi tujuan keamanan dan kepatuhan Anda. Anda juga mempelajari cara menggunakan AWS layanan lain yang membantu Anda memantau dan mengamankan sumber daya Security Hub Anda.

Topik

- [Perlindungan data di AWS Security Hub](#)
- [AWS Identity and Access Management untuk Security Hub](#)
- [Validasi Kepatuhan untuk AWS Security Hub](#)
- [Ketahanan di Security Hub AWS](#)
- [Keamanan infrastruktur di AWS Security Hub](#)
- [AWS Security Hub dan titik akhir VPC antarmuka \(AWS PrivateLink\)](#)

Perlindungan data di AWS Security Hub

[Model tanggung jawab AWS bersama model](#) berlaku untuk perlindungan data di AWS Security Hub. Seperti yang dijelaskan dalam model AWS ini, bertanggung jawab untuk melindungi infrastruktur

global yang menjalankan semua AWS Cloud. Anda bertanggung jawab untuk mempertahankan kendali atas konten yang di-host pada infrastruktur ini. Anda juga bertanggung jawab atas tugas-tugas konfigurasi dan manajemen keamanan untuk Layanan AWS yang Anda gunakan. Lihat informasi yang lebih lengkap tentang privasi data dalam [Pertanyaan Umum Privasi Data](#). Lihat informasi tentang perlindungan data di Eropa di pos blog [Model Tanggung Jawab Bersama dan GDPR AWS](#) di Blog Keamanan AWS .

Untuk tujuan perlindungan data, kami menyarankan Anda melindungi Akun AWS kredensial dan mengatur pengguna individu dengan AWS IAM Identity Center atau AWS Identity and Access Management (IAM). Dengan cara itu, setiap pengguna hanya diberi izin yang diperlukan untuk memenuhi tanggung jawab tugasnya. Kami juga menyarankan supaya Anda mengamankan data dengan cara-cara berikut:

- Gunakan autentikasi multi-faktor (MFA) pada setiap akun.
- Gunakan SSL/TLS untuk berkomunikasi dengan sumber daya. AWS Kami mensyaratkan TLS 1.2 dan menganjurkan TLS 1.3.
- Siapkan API dan pencatatan aktivitas pengguna dengan AWS CloudTrail. Untuk informasi tentang penggunaan CloudTrail jejak untuk menangkap AWS aktivitas, lihat [Bekerja dengan CloudTrail jejak](#) di AWS CloudTrail Panduan Pengguna.
- Gunakan solusi AWS enkripsi, bersama dengan semua kontrol keamanan default di dalamnya Layanan AWS.
- Gunakan layanan keamanan terkelola tingkat lanjut seperti Amazon Macie, yang membantu menemukan dan mengamankan data sensitif yang disimpan di Amazon S3.
- Jika Anda memerlukan modul kriptografi tervalidasi FIPS 140-3 saat mengakses AWS melalui antarmuka baris perintah atau API, gunakan titik akhir FIPS. Lihat informasi selengkapnya tentang titik akhir FIPS yang tersedia di [Standar Pemrosesan Informasi Federal \(FIPS\) 140-3](#).

Kami sangat merekomendasikan agar Anda tidak pernah memasukkan informasi identifikasi yang sensitif, seperti nomor rekening pelanggan Anda, ke dalam tanda atau bidang isian bebas seperti bidang Nama. Ini termasuk saat Anda bekerja dengan Security Hub atau lainnya Layanan AWS menggunakan konsol, API AWS CLI, atau AWS SDKs. Data apa pun yang Anda masukkan ke dalam tanda atau bidang isian bebas yang digunakan untuk nama dapat digunakan untuk log penagihan atau log diagnostik. Saat Anda memberikan URL ke server eksternal, kami sangat menganjurkan supaya Anda tidak menyertakan informasi kredensial di dalam URL untuk memvalidasi permintaan Anda ke server itu.

Security Hub adalah penawaran layanan multi-tenant. Untuk memastikan perlindungan data, Security Hub mengenkripsi data saat istirahat dan data dalam perjalanan antar layanan komponen.

AWS Identity and Access Management untuk Security Hub

AWS Identity and Access Management (IAM) adalah Layanan AWS yang membantu administrator mengontrol akses ke AWS sumber daya dengan aman. Administrator IAM mengontrol siapa yang dapat diautentikasi (masuk) dan diberi wewenang (memiliki izin) untuk menggunakan sumber daya Security Hub. IAM adalah Layanan AWS yang dapat Anda gunakan tanpa biaya tambahan.

Topik

- [Audiens](#)
- [Mengautentikasi dengan identitas](#)
- [Mengelola akses menggunakan kebijakan](#)
- [Bagaimana Security Hub bekerja dengan IAM](#)
- [Contoh kebijakan berbasis identitas untuk AWS Security Hub](#)
- [Peran terkait layanan untuk AWS Security Hub](#)
- [AWS kebijakan terkelola untuk Security Hub](#)
- [Memecahkan masalah AWS Security Hub identitas dan akses](#)

Audiens

Cara Anda menggunakan AWS Identity and Access Management (IAM) berbeda, tergantung pada pekerjaan yang Anda lakukan di Security Hub.

Pengguna layanan — Jika Anda menggunakan layanan Security Hub untuk melakukan pekerjaan Anda, administrator Anda memberi Anda kredensi dan izin yang Anda butuhkan. Saat Anda menggunakan lebih banyak fitur Security Hub untuk melakukan pekerjaan Anda, Anda mungkin memerlukan izin tambahan. Memahami cara akses dikelola dapat membantu Anda meminta izin yang tepat dari administrator Anda. Jika Anda tidak dapat mengakses fitur di Security Hub, lihat [Memecahkan masalah AWS Security Hub identitas dan akses](#).

Administrator layanan - Jika Anda bertanggung jawab atas sumber daya Security Hub di perusahaan Anda, Anda mungkin memiliki akses penuh ke Security Hub. Tugas Anda adalah menentukan fitur dan sumber daya Security Hub mana yang harus diakses pengguna layanan Anda. Kemudian, Anda

harus mengirimkan permintaan kepada administrator IAM untuk mengubah izin pengguna layanan Anda. Tinjau informasi di halaman ini untuk memahami konsep dasar IAM. Untuk mempelajari lebih lanjut tentang cara perusahaan Anda dapat menggunakan IAM dengan Security Hub, lihat [Bagaimana Security Hub bekerja dengan IAM](#).

Administrator IAM — Jika Anda administrator IAM, Anda mungkin ingin mempelajari detail tentang cara menulis kebijakan untuk mengelola akses ke Security Hub. Untuk melihat contoh kebijakan berbasis identitas Security Hub yang dapat Anda gunakan di IAM, lihat [Contoh kebijakan berbasis identitas untuk AWS Security Hub](#)

Mengautentikasi dengan identitas

Otentikasi adalah cara Anda masuk AWS menggunakan kredensi identitas Anda. Anda harus diautentikasi (masuk ke AWS) sebagai Pengguna root akun AWS, sebagai pengguna IAM, atau dengan mengasumsikan peran IAM.

Anda dapat masuk AWS sebagai identitas federasi dengan menggunakan kredensial yang disediakan melalui sumber identitas. AWS IAM Identity Center Pengguna (IAM Identity Center), autentikasi masuk tunggal perusahaan Anda, dan kredensi Google atau Facebook Anda adalah contoh identitas federasi. Saat Anda masuk sebagai identitas terfederasi, administrator Anda sebelumnya menyiapkan federasi identitas menggunakan peran IAM. Ketika Anda mengakses AWS dengan menggunakan federasi, Anda secara tidak langsung mengambil peran.

Bergantung pada jenis pengguna Anda, Anda dapat masuk ke AWS Management Console atau portal AWS akses. Untuk informasi selengkapnya tentang masuk AWS, lihat [Cara masuk ke Panduan AWS Sign-In Pengguna Anda Akun AWS](#).

Jika Anda mengakses AWS secara terprogram, AWS sediakan kit pengembangan perangkat lunak (SDK) dan antarmuka baris perintah (CLI) untuk menandatangani permintaan Anda secara kriptografis dengan menggunakan kredensial Anda. Jika Anda tidak menggunakan AWS alat, Anda harus menandatangani permintaan sendiri. Guna mengetahui informasi selengkapnya tentang penggunaan metode yang disarankan untuk menandatangani permintaan sendiri, lihat [AWS Signature Version 4 untuk permintaan API](#) dalam Panduan Pengguna IAM.

Apa pun metode autentikasi yang digunakan, Anda mungkin diminta untuk menyediakan informasi keamanan tambahan. Misalnya, AWS merekomendasikan agar Anda menggunakan otentikasi multi-faktor (MFA) untuk meningkatkan keamanan akun Anda. Untuk mempelajari selengkapnya, lihat [Autentikasi multi-faktor](#) dalam Panduan Pengguna AWS IAM Identity Center dan [Autentikasi multi-faktor AWS di IAM](#) dalam Panduan Pengguna IAM.

Akun AWS pengguna root

Saat Anda membuat Akun AWS, Anda mulai dengan satu identitas masuk yang memiliki akses lengkap ke semua Layanan AWS dan sumber daya di akun. Identitas ini disebut pengguna Akun AWS root dan diakses dengan masuk dengan alamat email dan kata sandi yang Anda gunakan untuk membuat akun. Kami sangat menyarankan agar Anda tidak menggunakan pengguna root untuk tugas sehari-hari. Lindungi kredensial pengguna root Anda dan gunakan kredensial tersebut untuk melakukan tugas yang hanya dapat dilakukan pengguna root. Untuk daftar lengkap tugas yang mengharuskan Anda masuk sebagai pengguna root, lihat [Tugas yang memerlukan kredensial pengguna root](#) dalam Panduan Pengguna IAM.

Identitas gabungan

Sebagai praktik terbaik, mewajibkan pengguna manusia, termasuk pengguna yang memerlukan akses administrator, untuk menggunakan federasi dengan penyedia identitas untuk mengakses Layanan AWS dengan menggunakan kredensi sementara.

Identitas federasi adalah pengguna dari direktori pengguna perusahaan Anda, penyedia identitas web, direktori Pusat Identitas AWS Directory Service, atau pengguna mana pun yang mengakses Layanan AWS dengan menggunakan kredensial yang disediakan melalui sumber identitas. Ketika identitas federasi mengakses Akun AWS, mereka mengambil peran, dan peran memberikan kredensi sementara.

Untuk manajemen akses terpusat, kami sarankan Anda menggunakan AWS IAM Identity Center. Anda dapat membuat pengguna dan grup di Pusat Identitas IAM, atau Anda dapat menghubungkan dan menyinkronkan ke sekumpulan pengguna dan grup di sumber identitas Anda sendiri untuk digunakan di semua aplikasi Akun AWS dan aplikasi Anda. Untuk informasi tentang Pusat Identitas IAM, lihat [Apakah itu Pusat Identitas IAM?](#) dalam Panduan Pengguna AWS IAM Identity Center .

Pengguna dan grup IAM

[Pengguna IAM](#) adalah identitas dalam diri Anda Akun AWS yang memiliki izin khusus untuk satu orang atau aplikasi. Jika memungkinkan, kami merekomendasikan untuk mengandalkan kredensial sementara, bukan membuat pengguna IAM yang memiliki kredensial jangka panjang seperti kata sandi dan kunci akses. Namun, jika Anda memiliki kasus penggunaan tertentu yang memerlukan kredensial jangka panjang dengan pengguna IAM, kami merekomendasikan Anda merotasi kunci akses. Untuk informasi selengkapnya, lihat [Merotasi kunci akses secara teratur untuk kasus penggunaan yang memerlukan kredensial jangka panjang](#) dalam Panduan Pengguna IAM.

[Grup IAM](#) adalah identitas yang menentukan sekumpulan pengguna IAM. Anda tidak dapat masuk sebagai grup. Anda dapat menggunakan grup untuk menentukan izin bagi beberapa pengguna sekaligus. Grup mempermudah manajemen izin untuk sejumlah besar pengguna sekaligus. Misalnya, Anda dapat meminta kelompok untuk menyebutkan IAMAdmins dan memberikan izin kepada grup tersebut untuk mengelola sumber daya IAM.

Pengguna berbeda dari peran. Pengguna secara unik terkait dengan satu orang atau aplikasi, tetapi peran dimaksudkan untuk dapat digunakan oleh siapa pun yang membutuhkannya. Pengguna memiliki kredensial jangka panjang permanen, tetapi peran memberikan kredensial sementara. Untuk mempelajari selengkapnya, lihat [Kasus penggunaan untuk pengguna IAM](#) dalam Panduan Pengguna IAM.

Peran IAM

[Peran IAM](#) adalah identitas dalam diri Anda Akun AWS yang memiliki izin khusus. Peran ini mirip dengan pengguna IAM, tetapi tidak terkait dengan orang tertentu. Untuk mengambil peran IAM sementara AWS Management Console, Anda dapat [beralih dari pengguna ke peran IAM \(konsol\)](#). Anda dapat mengambil peran dengan memanggil operasi AWS CLI atau AWS API atau dengan menggunakan URL kustom. Untuk informasi selengkapnya tentang cara menggunakan peran, lihat [Metode untuk mengambil peran](#) dalam Panduan Pengguna IAM.

Peran IAM dengan kredensial sementara berguna dalam situasi berikut:

- Akses pengguna terfederasi – Untuk menetapkan izin ke identitas terfederasi, Anda membuat peran dan menentukan izin untuk peran tersebut. Ketika identitas terfederasi mengautentikasi, identitas tersebut terhubung dengan peran dan diberi izin yang ditentukan oleh peran. Untuk informasi tentang peran untuk federasi, lihat [Buat peran untuk penyedia identitas pihak ketiga](#) dalam Panduan Pengguna IAM. Jika menggunakan Pusat Identitas IAM, Anda harus mengonfigurasi set izin. Untuk mengontrol apa yang dapat diakses identitas Anda setelah identitas tersebut diautentikasi, Pusat Identitas IAM akan mengorelasikan set izin ke peran dalam IAM. Untuk informasi tentang set izin, lihat [Set izin](#) dalam Panduan Pengguna AWS IAM Identity Center .
- Izin pengguna IAM sementara – Pengguna atau peran IAM dapat mengambil peran IAM guna mendapatkan berbagai izin secara sementara untuk tugas tertentu.
- Akses lintas akun – Anda dapat menggunakan peran IAM untuk mengizinkan seseorang (prinsipal tepercaya) di akun lain untuk mengakses sumber daya di akun Anda. Peran adalah cara utama untuk memberikan akses lintas akun. Namun, dengan beberapa Layanan AWS, Anda dapat melampirkan kebijakan secara langsung ke sumber daya (alih-alih menggunakan peran sebagai

proxy). Untuk mempelajari perbedaan antara peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat [Akses sumber daya lintas akun di IAM](#) dalam Panduan Pengguna IAM.

- Akses lintas layanan — Beberapa Layanan AWS menggunakan fitur lain Layanan AWS. Misalnya, saat Anda melakukan panggilan dalam suatu layanan, biasanya layanan tersebut menjalankan aplikasi di Amazon EC2 atau menyimpan objek di Amazon S3. Sebuah layanan mungkin melakukannya menggunakan izin prinsipal yang memanggil, menggunakan peran layanan, atau peran terkait layanan.
- Sesi akses teruskan (FAS) — Saat Anda menggunakan pengguna atau peran IAM untuk melakukan tindakan AWS, Anda dianggap sebagai prinsipal. Ketika Anda menggunakan beberapa layanan, Anda mungkin melakukan sebuah tindakan yang kemudian menginisiasi tindakan lain di layanan yang berbeda. FAS menggunakan izin dari pemanggilan utama Layanan AWS, dikombinasikan dengan permintaan Layanan AWS untuk membuat permintaan ke layanan hilir. Permintaan FAS hanya dibuat ketika layanan menerima permintaan yang memerlukan interaksi dengan orang lain Layanan AWS atau sumber daya untuk menyelesaikannya. Dalam hal ini, Anda harus memiliki izin untuk melakukan kedua tindakan tersebut. Untuk detail kebijakan ketika mengajukan permintaan FAS, lihat [Sesi akses maju](#).
- Peran layanan – Peran layanan adalah [peran IAM](#) yang dijalankan oleh layanan untuk melakukan tindakan atas nama Anda. Administrator IAM dapat membuat, mengubah, dan menghapus peran layanan dari dalam IAM. Untuk informasi selengkapnya, lihat [Buat sebuah peran untuk mendelegasikan izin ke Layanan AWS](#) dalam Panduan pengguna IAM.
- Peran terkait layanan — Peran terkait layanan adalah jenis peran layanan yang ditautkan ke peran layanan. Layanan AWS Layanan tersebut dapat menjalankan peran untuk melakukan tindakan atas nama Anda. Peran terkait layanan muncul di Anda Akun AWS dan dimiliki oleh layanan. Administrator IAM dapat melihat, tetapi tidak dapat mengedit izin untuk peran terkait layanan.
- Aplikasi yang berjalan di Amazon EC2 — Anda dapat menggunakan peran IAM untuk mengelola kredensi sementara untuk aplikasi yang berjalan pada EC2 instance dan membuat AWS CLI atau AWS permintaan API. Ini lebih baik untuk menyimpan kunci akses dalam EC2 instance. Untuk menetapkan AWS peran ke EC2 instance dan membuatnya tersedia untuk semua aplikasinya, Anda membuat profil instance yang dilampirkan ke instance. Profil instance berisi peran dan memungkinkan program yang berjalan pada EC2 instance untuk mendapatkan kredensi sementara. Untuk informasi selengkapnya, lihat [Menggunakan peran IAM untuk memberikan izin ke aplikasi yang berjalan di EC2 instans Amazon di Panduan Pengguna](#) IAM.

Mengelola akses menggunakan kebijakan

Anda mengontrol akses AWS dengan membuat kebijakan dan melampirkannya ke AWS identitas atau sumber daya. Kebijakan adalah objek AWS yang, ketika dikaitkan dengan identitas atau sumber daya, menentukan izinnya. AWS mengevaluasi kebijakan ini ketika prinsipal (pengguna, pengguna root, atau sesi peran) membuat permintaan. Izin dalam kebijakan menentukan apakah permintaan diizinkan atau ditolak. Sebagian besar kebijakan disimpan AWS sebagai dokumen JSON. Untuk informasi selengkapnya tentang struktur dan isi dokumen kebijakan JSON, lihat [Gambaran umum kebijakan JSON](#) dalam Panduan Pengguna IAM.

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Artinya, prinsipal manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan kondisi apa.

Secara default, pengguna dan peran tidak memiliki izin. Untuk memberikan izin kepada pengguna untuk melakukan tindakan di sumber daya yang mereka perlukan, administrator IAM dapat membuat kebijakan IAM. Administrator kemudian dapat menambahkan kebijakan IAM ke peran, dan pengguna dapat mengambil peran.

Kebijakan IAM mendefinisikan izin untuk suatu tindakan terlepas dari metode yang Anda gunakan untuk melakukan operasinya. Misalnya, anggaplah Anda memiliki kebijakan yang mengizinkan tindakan `iam:GetRole`. Pengguna dengan kebijakan tersebut bisa mendapatkan informasi peran dari AWS Management Console, API AWS CLI, atau AWS API.

Kebijakan berbasis identitas

Kebijakan berbasis identitas adalah dokumen kebijakan izin JSON yang dapat Anda lampirkan ke sebuah identitas, seperti pengguna IAM, grup pengguna IAM, atau peran IAM. Kebijakan ini mengontrol jenis tindakan yang dapat dilakukan oleh pengguna dan peran, di sumber daya mana, dan berdasarkan kondisi seperti apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, lihat [Tentukan izin IAM kustom dengan kebijakan terkelola pelanggan](#) dalam Panduan Pengguna IAM.

Kebijakan berbasis identitas dapat dikategorikan lebih lanjut sebagai kebijakan inline atau kebijakan yang dikelola. Kebijakan inline disematkan langsung ke satu pengguna, grup, atau peran. Kebijakan terkelola adalah kebijakan mandiri yang dapat Anda lampirkan ke beberapa pengguna, grup, dan peran dalam Akun AWS. Kebijakan AWS terkelola mencakup kebijakan terkelola dan kebijakan yang dikelola pelanggan. Untuk mempelajari cara memilih antara kebijakan yang dikelola atau kebijakan inline, lihat [Pilih antara kebijakan yang dikelola dan kebijakan inline](#) dalam Panduan Pengguna IAM.

Kebijakan berbasis sumber daya

Kebijakan berbasis sumber daya adalah dokumen kebijakan JSON yang Anda lampirkan ke sumber daya. Contoh kebijakan berbasis sumber daya adalah kebijakan kepercayaan peran IAM dan kebijakan bucket Amazon S3. Dalam layanan yang mendukung kebijakan berbasis sumber daya, administrator layanan dapat menggunakannya untuk mengontrol akses ke sumber daya tertentu. Untuk sumber daya tempat kebijakan dilampirkan, kebijakan menentukan tindakan apa yang dapat dilakukan oleh prinsipal tertentu pada sumber daya tersebut dan dalam kondisi apa. Anda harus [menentukan prinsipal](#) dalam kebijakan berbasis sumber daya. Prinsipal dapat mencakup akun, pengguna, peran, pengguna federasi, atau Layanan AWS

Kebijakan berbasis sumber daya merupakan kebijakan inline yang terletak di layanan tersebut. Anda tidak dapat menggunakan kebijakan AWS terkelola dari IAM dalam kebijakan berbasis sumber daya.

Daftar kontrol akses (ACLs)

Access control lists (ACLs) mengontrol prinsipal mana (anggota akun, pengguna, atau peran) yang memiliki izin untuk mengakses sumber daya. ACLs mirip dengan kebijakan berbasis sumber daya, meskipun mereka tidak menggunakan format dokumen kebijakan JSON.

Amazon S3, AWS WAF, dan Amazon VPC adalah contoh layanan yang mendukung ACLs. Untuk mempelajari selengkapnya ACLs, lihat [Ringkasan daftar kontrol akses \(ACL\)](#) di Panduan Pengembang Layanan Penyimpanan Sederhana Amazon.

Jenis-jenis kebijakan lain

AWS mendukung jenis kebijakan tambahan yang kurang umum. Jenis-jenis kebijakan ini dapat mengatur izin maksimum yang diberikan kepada Anda oleh jenis kebijakan yang lebih umum.

- **Batasan izin** – Batasan izin adalah fitur lanjutan tempat Anda mengatur izin maksimum yang dapat diberikan oleh kebijakan berbasis identitas ke entitas IAM (pengguna IAM atau peran IAM). Anda dapat menetapkan batasan izin untuk suatu entitas. Izin yang dihasilkan adalah perpotongan antara kebijakan berbasis identitas milik entitas dan batasan izinnya. Kebijakan berbasis sumber daya yang menentukan pengguna atau peran dalam bidang `Principal` tidak dibatasi oleh batasan izin. Penolakan eksplisit dalam salah satu kebijakan ini akan menggantikan pemberian izin. Untuk informasi selengkapnya tentang batasan izin, lihat [Batasan izin untuk entitas IAM](#) dalam Panduan Pengguna IAM.
- **Kebijakan kontrol layanan (SCPs)** — SCPs adalah kebijakan JSON yang menentukan izin maksimum untuk organisasi atau unit organisasi (OU) di AWS Organizations

adalah layanan untuk mengelompokkan dan mengelola secara terpusat beberapa Akun AWS yang dimiliki bisnis Anda. Jika Anda mengaktifkan semua fitur dalam suatu organisasi, maka Anda dapat menerapkan kebijakan kontrol layanan (SCPs) ke salah satu atau semua akun Anda. SCP membatasi izin untuk entitas di akun anggota, termasuk masing-masing. Pengguna root akun AWS Untuk informasi selengkapnya tentang Organizations dan SCPs, lihat [Kebijakan kontrol layanan](#) di Panduan AWS Organizations Pengguna.

- Kebijakan kontrol sumber daya (RCPs) — RCPs adalah kebijakan JSON yang dapat Anda gunakan untuk menetapkan izin maksimum yang tersedia untuk sumber daya di akun Anda tanpa memperbarui kebijakan IAM yang dilampirkan ke setiap sumber daya yang Anda miliki. RCP membatasi izin untuk sumber daya di akun anggota dan dapat memengaruhi izin efektif untuk identitas, termasuk Pengguna root akun AWS, terlepas dari apakah itu milik organisasi Anda. Untuk informasi selengkapnya tentang Organizations dan RCPs, termasuk daftar dukungan Layanan AWS tersebut RCPs, lihat [Kebijakan kontrol sumber daya \(RCPs\)](#) di Panduan AWS Organizations Pengguna.
- Kebijakan sesi – Kebijakan sesi adalah kebijakan lanjutan yang Anda berikan sebagai parameter ketika Anda membuat sesi sementara secara programatis untuk peran atau pengguna terfederasi. Izin sesi yang dihasilkan adalah perpotongan antara kebijakan berbasis identitas pengguna atau peran dan kebijakan sesi. Izin juga bisa datang dari kebijakan berbasis sumber daya. Penolakan eksplisit dalam salah satu kebijakan ini akan menggantikan pemberian izin. Untuk informasi selengkapnya, lihat [Kebijakan sesi](#) dalam Panduan Pengguna IAM.

Berbagai jenis kebijakan

Ketika beberapa jenis kebijakan berlaku pada suatu permintaan, izin yang dihasilkan lebih rumit untuk dipahami. Untuk mempelajari cara AWS menentukan apakah akan mengizinkan permintaan saat beberapa jenis kebijakan terlibat, lihat [Logika evaluasi kebijakan](#) di Panduan Pengguna IAM.

Bagaimana Security Hub bekerja dengan IAM

Sebelum Anda menggunakan AWS Identity and Access Management (IAM) untuk mengelola akses AWS Security Hub, pelajari fitur IAM mana yang tersedia untuk digunakan dengan Security Hub.

Fitur IAM yang dapat Anda gunakan AWS Security Hub

Fitur IAM	Dukungan Security Hub
Kebijakan berbasis identitas	Ya

Fitur IAM	Dukungan Security Hub
Kebijakan berbasis sumber daya	Tidak
Tindakan kebijakan	Ya
Sumber daya kebijakan	Tidak
Kunci kondisi kebijakan	Ya
Daftar kontrol akses (ACLs)	Tidak
Kontrol akses berbasis atribut (ABAC) — tag dalam kebijakan	Ya
Kredensial sementara	Ya
Sesi akses teruskan (FAS)	Ya
Peran layanan	Tidak
Peran terkait layanan	Ya

Untuk tampilan tingkat tinggi tentang cara Layanan AWS kerja Security Hub dan fitur lainnya dengan sebagian besar fitur IAM, lihat fitur [Layanan AWS tersebut bekerja dengan IAM di Panduan Pengguna IAM](#).

Kebijakan berbasis identitas untuk Security Hub

Mendukung kebijakan berbasis identitas: Ya

Kebijakan berbasis identitas adalah dokumen kebijakan izin JSON yang dapat Anda lampirkan ke sebuah identitas, seperti pengguna IAM, grup pengguna IAM, atau peran IAM. Kebijakan ini mengontrol jenis tindakan yang dapat dilakukan oleh pengguna dan peran, di sumber daya mana, dan berdasarkan kondisi seperti apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, lihat [Tentukan izin IAM kustom dengan kebijakan terkelola pelanggan](#) dalam Panduan Pengguna IAM.

Dengan kebijakan berbasis identitas IAM, Anda dapat menentukan secara spesifik apakah tindakan dan sumber daya diizinkan atau ditolak, serta kondisi yang menjadi dasar dikabulkan atau ditolaknya

tindakan tersebut. Anda tidak dapat menentukan secara spesifik prinsipal dalam sebuah kebijakan berbasis identitas karena prinsipal berlaku bagi pengguna atau peran yang melekat kepadanya. Untuk mempelajari semua elemen yang dapat Anda gunakan dalam kebijakan JSON, lihat [Referensi elemen kebijakan JSON IAM](#) dalam Panduan Pengguna IAM.

Security Hub mendukung kebijakan berbasis identitas. Untuk informasi selengkapnya, lihat [Contoh kebijakan berbasis identitas untuk AWS Security Hub](#).

Kebijakan berbasis sumber daya untuk Security Hub

Mendukung kebijakan berbasis sumber daya: Tidak

Kebijakan berbasis sumber daya adalah dokumen kebijakan JSON yang Anda lampirkan ke sumber daya. Contoh kebijakan berbasis sumber daya adalah kebijakan kepercayaan peran IAM dan kebijakan bucket Amazon S3. Dalam layanan yang mendukung kebijakan berbasis sumber daya, administrator layanan dapat menggunakannya untuk mengontrol akses ke sumber daya tertentu. Untuk sumber daya tempat kebijakan dilampirkan, kebijakan menentukan tindakan apa yang dapat dilakukan oleh prinsipal tertentu pada sumber daya tersebut dan dalam kondisi apa. Anda harus [menentukan prinsipal](#) dalam kebijakan berbasis sumber daya. Prinsipal dapat mencakup akun, pengguna, peran, pengguna federasi, atau. Layanan AWS

Untuk mengaktifkan akses lintas akun, Anda dapat menentukan secara spesifik seluruh akun atau entitas IAM di akun lain sebagai prinsipal dalam kebijakan berbasis sumber daya. Menambahkan prinsipal akun silang ke kebijakan berbasis sumber daya hanya setengah dari membangun hubungan kepercayaan. Ketika prinsipal dan sumber daya berbeda Akun AWS, administrator IAM di akun tepercaya juga harus memberikan izin entitas utama (pengguna atau peran) untuk mengakses sumber daya. Mereka memberikan izin dengan melampirkan kebijakan berbasis identitas kepada entitas. Namun, jika kebijakan berbasis sumber daya memberikan akses ke principal dalam akun yang sama, tidak diperlukan kebijakan berbasis identitas tambahan. Untuk informasi selengkapnya, lihat [Akses sumber daya lintas akun di IAM](#) dalam Panduan Pengguna IAM.

Security Hub tidak mendukung kebijakan berbasis sumber daya. Anda tidak dapat melampirkan kebijakan IAM secara langsung ke sumber daya Security Hub.

Tindakan kebijakan untuk Security Hub

Mendukung tindakan kebijakan: Ya

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Artinya, prinsipal manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan kondisi apa.

Elemen `Action` dari kebijakan JSON menjelaskan tindakan yang dapat Anda gunakan untuk mengizinkan atau menolak akses dalam sebuah kebijakan. Tindakan kebijakan biasanya memiliki nama yang sama dengan operasi AWS API terkait. Ada beberapa pengecualian, misalnya tindakan hanya izin yang tidak memiliki operasi API yang cocok. Ada juga beberapa operasi yang memerlukan beberapa tindakan dalam suatu kebijakan. Tindakan tambahan ini disebut tindakan dependen.

Sertakan tindakan dalam kebijakan untuk memberikan izin untuk melakukan operasi terkait.

Tindakan kebijakan di Security Hub menggunakan awalan berikut sebelum tindakan:

```
securityhub:
```

Misalnya, untuk memberikan izin kepada pengguna untuk mengaktifkan Security Hub, yang merupakan tindakan yang sesuai dengan `EnableSecurityHub` pengoperasian API Security Hub, sertakan `securityhub:EnableSecurityHub` tindakan tersebut dalam kebijakan mereka. Pernyataan kebijakan harus memuat elemen `Action` atau `NotAction`. Security Hub mendefinisikan serangkaian tindakannya sendiri yang menjelaskan tugas yang dapat Anda lakukan dengan layanan ini.

```
"Action": "securityhub:EnableSecurityHub"
```

Untuk menetapkan secara spesifik beberapa tindakan dalam satu pernyataan, pisahkan tindakan tersebut dengan koma. Misalnya:

```
"Action": [  
    "securityhub:EnableSecurityHub",  
    "securityhub:BatchEnableStandards"
```

Anda juga dapat menentukan beberapa tindakan menggunakan wildcard (*). Sebagai contoh, untuk menentukan semua tindakan yang dimulai dengan kata `Get`, sertakan tindakan berikut:

```
"Action": "securityhub:Get*"
```

Namun, sebagai praktik terbaik, Anda harus membuat kebijakan yang mengikuti prinsip hak istimewa paling sedikit. Dengan kata lain, Anda harus membuat kebijakan yang hanya menyertakan izin yang diperlukan untuk melakukan tugas tertentu.

Pengguna harus memiliki akses ke `DescribeStandardsControl` operasi untuk memiliki akses ke `BatchGetSecurityControls`, `BatchGetStandardsControlAssociations`, dan `ListStandardsControlAssociations`.

Pengguna harus memiliki akses ke `UpdateStandardsControls` operasi untuk memiliki akses ke `BatchUpdateStandardsControlAssociations`, dan `UpdateSecurityControl`.

Untuk daftar tindakan Security Hub, lihat [Tindakan yang ditentukan oleh AWS Security Hub](#) dalam Referensi Otorisasi Layanan. Untuk contoh kebijakan yang menentukan tindakan Security Hub, lihat [Contoh kebijakan berbasis identitas untuk AWS Security Hub](#).

Sumber daya kebijakan untuk Security Hub

Mendukung sumber daya kebijakan: Tidak

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Artinya, prinsipal manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan kondisi apa.

Elemen kebijakan JSON `Resource` menentukan objek yang menjadi target penerapan tindakan. Pernyataan harus menyertakan elemen `Resource` atau `NotResource`. Praktik terbaiknya, tentukan sumber daya menggunakan [Amazon Resource Name \(ARN\)](#). Anda dapat melakukan ini untuk tindakan yang mendukung jenis sumber daya tertentu, yang dikenal sebagai izin tingkat sumber daya.

Untuk tindakan yang tidak mendukung izin di tingkat sumber daya, misalnya operasi pencantuman, gunakan wildcard (*) untuk menunjukkan bahwa pernyataan tersebut berlaku untuk semua sumber daya.

```
"Resource": "*"

```

Security Hub mendefinisikan jenis sumber daya berikut:

- Hub
- Produk
- Menemukan agregator, juga disebut sebagai agregator lintas wilayah

- Aturan otomatisasi
- Kebijakan konfigurasi

Anda dapat menentukan jenis sumber daya ini dalam kebijakan dengan menggunakan ARNs.

Untuk daftar jenis sumber daya Security Hub dan sintaks ARN untuk masing-masing, lihat [Jenis sumber daya yang ditentukan oleh AWS Security Hub](#) dalam Referensi Otorisasi Layanan. Untuk mempelajari tindakan yang dapat Anda tentukan untuk setiap jenis sumber daya, lihat [Tindakan yang ditentukan oleh AWS Security Hub](#) dalam Referensi Otorisasi Layanan. Untuk contoh kebijakan yang menentukan sumber daya, lihat [Contoh kebijakan berbasis identitas untuk AWS Security Hub](#).

Kunci kondisi kebijakan untuk Security Hub

Mendukung kunci kondisi kebijakan khusus layanan: Yes

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Artinya, prinsipal manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan kondisi apa.

Elemen Condition (atau blok Condition) akan memungkinkan Anda menentukan kondisi yang menjadi dasar suatu pernyataan berlaku. Elemen Condition bersifat opsional. Anda dapat membuat ekspresi bersyarat yang menggunakan [operator kondisi](#), misalnya sama dengan atau kurang dari, untuk mencocokkan kondisi dalam kebijakan dengan nilai-nilai yang diminta.

Jika Anda menentukan beberapa elemen Condition dalam sebuah pernyataan, atau beberapa kunci dalam elemen Condition tunggal, maka AWS akan mengevaluasinya menggunakan operasi AND logis. Jika Anda menentukan beberapa nilai untuk satu kunci kondisi, AWS mengevaluasi kondisi menggunakan OR operasi logis. Semua kondisi harus dipenuhi sebelum izin pernyataan diberikan.

Anda juga dapat menggunakan variabel placeholder saat menentukan kondisi. Sebagai contoh, Anda dapat memberikan izin kepada pengguna IAM untuk mengakses sumber daya hanya jika izin tersebut mempunyai tanda yang sesuai dengan nama pengguna IAM mereka. Untuk informasi selengkapnya, lihat [Elemen kebijakan IAM: variabel dan tanda](#) dalam Panduan Pengguna IAM.

AWS mendukung kunci kondisi global dan kunci kondisi khusus layanan. Untuk melihat semua kunci kondisi AWS global, lihat [kunci konteks kondisi AWS global](#) di Panduan Pengguna IAM.

Untuk daftar kunci kondisi Security Hub, lihat [Kunci kondisi untuk AWS Security Hub](#) Referensi Otorisasi Layanan. Untuk mempelajari tindakan dan sumber daya yang dapat digunakan untuk menggunakan kunci kondisi, lihat [Tindakan yang ditentukan oleh AWS Security Hub](#). Untuk contoh

kebijakan yang menggunakan kunci kondisi, lihat [Contoh kebijakan berbasis identitas untuk AWS Security Hub](#).

Daftar kontrol akses (ACLs) di Security Hub

Mendukung ACLs: Tidak

Access control lists (ACLs) mengontrol prinsipal mana (anggota akun, pengguna, atau peran) yang memiliki izin untuk mengakses sumber daya. ACLs mirip dengan kebijakan berbasis sumber daya, meskipun mereka tidak menggunakan format dokumen kebijakan JSON.

Security Hub tidak mendukung ACLs, yang berarti Anda tidak dapat melampirkan ACL ke sumber daya Security Hub.

Kontrol akses berbasis atribut (ABAC) dengan Security Hub

Mendukung ABAC (tanda dalam kebijakan): Ya

Kontrol akses berbasis atribut (ABAC) adalah strategi otorisasi yang menentukan izin berdasarkan atribut. Dalam AWS, atribut ini disebut tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke banyak AWS sumber daya. Penandaan ke entitas dan sumber daya adalah langkah pertama dari ABAC. Kemudian rancanglah kebijakan ABAC untuk mengizinkan operasi ketika tanda milik prinsipal cocok dengan tanda yang ada di sumber daya yang ingin diakses.

ABAC sangat berguna di lingkungan yang berkembang dengan cepat dan berguna di situasi saat manajemen kebijakan menjadi rumit.

Untuk mengendalikan akses berdasarkan tanda, berikan informasi tentang tanda di [elemen kondisi](#) dari kebijakan menggunakan kunci kondisi `aws:ResourceTag/key-name`, `aws:RequestTag/key-name`, atau `aws:TagKeys`.

Jika sebuah layanan mendukung ketiga kunci kondisi untuk setiap jenis sumber daya, nilainya adalah Ya untuk layanan tersebut. Jika suatu layanan mendukung ketiga kunci kondisi untuk hanya beberapa jenis sumber daya, nilainya adalah Parsial.

Untuk informasi selengkapnya tentang ABAC, lihat [Tentukan izin dengan otorisasi ABAC](#) dalam Panduan Pengguna IAM. Untuk melihat tutorial yang menguraikan langkah-langkah pengaturan ABAC, lihat [Menggunakan kontrol akses berbasis atribut \(ABAC\)](#) dalam Panduan Pengguna IAM.

Anda dapat melampirkan tag ke sumber daya Security Hub. Anda juga dapat mengontrol akses ke sumber daya dengan memberikan informasi tag dalam `Condition` elemen kebijakan.

Untuk informasi tentang menandai sumber daya Security Hub, lihat [Menandai sumber daya CSPM Security Hub](#). Untuk contoh kebijakan berbasis identitas yang mengontrol akses ke sumber daya berdasarkan tag, lihat [Contoh kebijakan berbasis identitas untuk AWS Security Hub](#)

Menggunakan kredensi sementara dengan Security Hub

Mendukung kredensial sementara: Ya

Beberapa Layanan AWS tidak berfungsi saat Anda masuk menggunakan kredensi sementara. Untuk informasi tambahan, termasuk yang Layanan AWS bekerja dengan kredensi sementara, lihat [Layanan AWS yang bekerja dengan IAM di Panduan Pengguna IAM](#).

Anda menggunakan kredensi sementara jika Anda masuk AWS Management Console menggunakan metode apa pun kecuali nama pengguna dan kata sandi. Misalnya, ketika Anda mengakses AWS menggunakan tautan masuk tunggal (SSO) perusahaan Anda, proses tersebut secara otomatis membuat kredensial sementara. Anda juga akan secara otomatis membuat kredensial sementara ketika Anda masuk ke konsol sebagai seorang pengguna lalu beralih peran. Untuk informasi selengkapnya tentang peralihan peran, lihat [Beralih dari pengguna ke peran IAM \(konsol\)](#) dalam Panduan Pengguna IAM.

Anda dapat membuat kredensial sementara secara manual menggunakan API AWS CLI atau AWS . Anda kemudian dapat menggunakan kredensi sementara tersebut untuk mengakses AWS . AWS merekomendasikan agar Anda secara dinamis menghasilkan kredensi sementara alih-alih menggunakan kunci akses jangka panjang. Untuk informasi selengkapnya, lihat [Kredensial keamanan sementara di IAM](#).

Anda dapat menggunakan kredensial sementara untuk masuk dengan gabungan, menjalankan IAM role, atau menjalankan peran lintas akun. Anda memperoleh kredensial keamanan sementara dengan memanggil operasi AWS STS API seperti [AssumeRole](#) atau [GetFederationToken](#)

Security Hub mendukung penggunaan kredensi sementara.

Teruskan sesi akses untuk Security Hub

Mendukung sesi akses maju (FAS): Ya

Saat Anda menggunakan pengguna atau peran IAM untuk melakukan tindakan AWS, Anda dianggap sebagai prinsipal. Ketika Anda menggunakan beberapa layanan, Anda mungkin melakukan sebuah tindakan yang kemudian menginisiasi tindakan lain di layanan yang berbeda. FAS menggunakan izin dari pemanggilan utama Layanan AWS, dikombinasikan dengan permintaan Layanan AWS untuk membuat permintaan ke layanan hilir. Permintaan FAS hanya dibuat ketika layanan menerima

permintaan yang memerlukan interaksi dengan orang lain Layanan AWS atau sumber daya untuk menyelesaikannya. Dalam hal ini, Anda harus memiliki izin untuk melakukan kedua tindakan tersebut. Untuk detail kebijakan ketika mengajukan permintaan FAS, lihat [Sesi akses maju](#).

Misalnya, Security Hub membuat permintaan FAS ke hilir Layanan AWS saat Anda mengintegrasikan Security Hub dengan AWS Organizations dan saat Anda menetapkan akun administrator Security Hub yang didelegasikan untuk organisasi di Organizations.

Untuk tugas lain, Security Hub menggunakan peran terkait layanan untuk melakukan tindakan atas nama Anda. Untuk detail tentang peran ini, lihat [Peran terkait layanan untuk AWS Security Hub](#).

Peran layanan untuk Security Hub

Security Hub tidak mengasumsikan atau menggunakan peran layanan. Untuk melakukan tindakan atas nama Anda, Security Hub menggunakan peran terkait layanan. Untuk detail tentang peran ini, lihat [Peran terkait layanan untuk AWS Security Hub](#).

Warning

Mengubah izin untuk peran layanan dapat menimbulkan masalah operasional dengan penggunaan Security Hub. Edit peran layanan hanya jika Security Hub memberikan panduan untuk melakukannya.

Peran terkait layanan untuk Security Hub

Mendukung peran terkait layanan: Ya

Peran terkait layanan adalah jenis peran layanan yang ditautkan ke Layanan AWS. Layanan tersebut dapat menjalankan peran untuk melakukan tindakan atas nama Anda. Peran terkait layanan muncul di Anda Akun AWS dan dimiliki oleh layanan. Administrator IAM dapat melihat, tetapi tidak dapat mengedit izin untuk peran terkait layanan.

Security Hub menggunakan peran terkait layanan untuk melakukan tindakan atas nama Anda. Untuk detail tentang peran ini, lihat [Peran terkait layanan untuk AWS Security Hub](#).

Contoh kebijakan berbasis identitas untuk AWS Security Hub

Secara default, pengguna dan peran tidak memiliki izin untuk membuat atau memodifikasi sumber daya Security Hub. Mereka juga tidak dapat melakukan tugas menggunakan AWS Management

Console, AWS CLI, atau AWS API. Administrator harus membuat kebijakan IAM yang memberikan izin kepada pengguna dan peran untuk melakukan operasi API tertentu pada sumber daya tertentu yang mereka butuhkan. Administrator kemudian harus melampirkan kebijakan tersebut ke pengguna atau grup yang memerlukan izin tersebut.

Untuk mempelajari cara membuat kebijakan berbasis identitas IAM menggunakan contoh dokumen kebijakan JSON ini, lihat [Membuat Kebijakan pada Tab JSON](#) dalam Panduan Pengguna IAM.

Topik

- [Praktik terbaik kebijakan](#)
- [Menggunakan konsol Security Hub](#)
- [Contoh: Izinkan pengguna untuk melihat izin mereka sendiri](#)
- [Contoh: Izinkan pengguna membuat dan mengelola kebijakan konfigurasi](#)
- [Contoh: Izinkan pengguna untuk melihat temuan](#)
- [Contoh: Izinkan pengguna membuat dan mengelola aturan otomatisasi](#)

Praktik terbaik kebijakan

Kebijakan berbasis identitas menentukan apakah seseorang dapat membuat, mengakses, atau menghapus sumber daya Security Hub di akun Anda. Tindakan ini membuat Akun AWS Anda dikenai biaya. Ketika Anda membuat atau mengedit kebijakan berbasis identitas, ikuti panduan dan rekomendasi ini:

- Mulailah dengan kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit — Untuk mulai memberikan izin kepada pengguna dan beban kerja Anda, gunakan kebijakan AWS terkelola yang memberikan izin untuk banyak kasus penggunaan umum. Mereka tersedia di Akun AWS. Kami menyarankan Anda mengurangi izin lebih lanjut dengan menentukan kebijakan yang dikelola AWS pelanggan yang khusus untuk kasus penggunaan Anda. Untuk informasi selengkapnya, lihat [Kebijakan yang dikelola AWS](#) atau [Kebijakan yang dikelola AWS untuk fungsi tugas](#) dalam Panduan Pengguna IAM.
- Menerapkan izin dengan hak akses paling rendah – Ketika Anda menetapkan izin dengan kebijakan IAM, hanya berikan izin yang diperlukan untuk melakukan tugas. Anda melakukannya dengan mendefinisikan tindakan yang dapat diambil pada sumber daya tertentu dalam kondisi tertentu, yang juga dikenal sebagai izin dengan hak akses paling rendah. Untuk informasi selengkapnya tentang cara menggunakan IAM untuk mengajukan izin, lihat [Kebijakan dan izin dalam IAM](#) dalam Panduan Pengguna IAM.

- Gunakan kondisi dalam kebijakan IAM untuk membatasi akses lebih lanjut – Anda dapat menambahkan suatu kondisi ke kebijakan Anda untuk membatasi akses ke tindakan dan sumber daya. Sebagai contoh, Anda dapat menulis kondisi kebijakan untuk menentukan bahwa semua permintaan harus dikirim menggunakan SSL. Anda juga dapat menggunakan ketentuan untuk memberikan akses ke tindakan layanan jika digunakan melalui yang spesifik Layanan AWS, seperti AWS CloudFormation. Untuk informasi selengkapnya, lihat [Elemen kebijakan JSON IAM: Kondisi](#) dalam Panduan Pengguna IAM.
- Gunakan IAM Access Analyzer untuk memvalidasi kebijakan IAM Anda untuk memastikan izin yang aman dan fungsional – IAM Access Analyzer memvalidasi kebijakan baru dan yang sudah ada sehingga kebijakan tersebut mematuhi bahasa kebijakan IAM (JSON) dan praktik terbaik IAM. IAM Access Analyzer menyediakan lebih dari 100 pemeriksaan kebijakan dan rekomendasi yang dapat ditindaklanjuti untuk membantu Anda membuat kebijakan yang aman dan fungsional. Untuk informasi selengkapnya, lihat [Validasi kebijakan dengan IAM Access Analyzer](#) dalam Panduan Pengguna IAM.
- Memerlukan otentikasi multi-faktor (MFA) - Jika Anda memiliki skenario yang mengharuskan pengguna IAM atau pengguna root di Anda, Akun AWS aktifkan MFA untuk keamanan tambahan. Untuk meminta MFA ketika operasi API dipanggil, tambahkan kondisi MFA pada kebijakan Anda. Untuk informasi selengkapnya, lihat [Amankan akses API dengan MFA](#) dalam Panduan Pengguna IAM.

Untuk informasi selengkapnya tentang praktik terbaik dalam IAM, lihat [Praktik terbaik keamanan di IAM](#) dalam Panduan Pengguna IAM.

Menggunakan konsol Security Hub

Untuk mengakses AWS Security Hub konsol, Anda harus memiliki set izin minimum. Izin ini harus memungkinkan Anda untuk membuat daftar dan melihat detail tentang sumber daya Security Hub di situs Anda Akun AWS. Jika Anda membuat kebijakan berbasis identitas yang lebih ketat daripada izin minimum yang diperlukan, konsol tidak akan berfungsi sebagaimana mestinya untuk entitas (pengguna atau peran) dengan kebijakan tersebut.

Anda tidak perlu mengizinkan izin konsol minimum untuk pengguna yang melakukan panggilan hanya ke AWS CLI atau AWS API. Sebagai gantinya, izinkan akses hanya ke tindakan yang sesuai dengan operasi API yang coba mereka lakukan.

Untuk memastikan bahwa pengguna dan peran tersebut dapat menggunakan konsol Security Hub, lampirkan juga kebijakan AWS terkelola berikut ke entitas. Untuk informasi selengkapnya, lihat [Menambahkan izin ke pengguna](#) dalam Panduan Pengguna IAM:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "securityhub:*",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "iam:CreateServiceLinkedRole",
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "iam:AWSServiceName": "securityhub.amazonaws.com"
        }
      }
    }
  ]
}
```

Contoh: Izinkan pengguna untuk melihat izin mereka sendiri

Contoh ini menunjukkan cara membuat kebijakan yang mengizinkan pengguna IAM melihat kebijakan inline dan terkelola yang dilampirkan ke identitas pengguna mereka. Kebijakan ini mencakup izin untuk menyelesaikan tindakan ini di konsol atau menggunakan API atau secara terprogram. AWS CLI AWS

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ViewOwnUserInfo",
      "Effect": "Allow",
      "Action": [
        "iam:GetUserPolicy",
        "iam:ListGroupsForUser",
        "iam:ListAttachedUserPolicies",

```

```

        "iam:ListUserPolicies",
        "iam:GetUser"
    ],
    "Resource": ["arn:aws:iam::*:user/${aws:username}"]
},
{
    "Sid": "NavigateInConsole",
    "Effect": "Allow",
    "Action": [
        "iam:GetGroupPolicy",
        "iam:GetPolicyVersion",
        "iam:GetPolicy",
        "iam:ListAttachedGroupPolicies",
        "iam:ListGroupPolicies",
        "iam:ListPolicyVersions",
        "iam:ListPolicies",
        "iam:ListUsers"
    ],
    "Resource": "*"
}
]
}

```

Contoh: Izinkan pengguna membuat dan mengelola kebijakan konfigurasi

Contoh ini menunjukkan cara membuat kebijakan IAM yang memungkinkan pengguna membuat, melihat, memperbarui, dan menghapus kebijakan konfigurasi. Kebijakan contoh ini juga memungkinkan pengguna untuk memulai, menghentikan, dan melihat asosiasi kebijakan. Agar kebijakan IAM ini berfungsi, pengguna harus menjadi administrator Security Hub yang didelegasikan untuk organisasi.

```

{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "CreateAndUpdateConfigurationPolicy",
            "Effect": "Allow",
            "Action": [
                "securityhub:CreateConfigurationPolicy",
                "securityhub:UpdateConfigurationPolicy"
            ],
            "Resource": "*"
        },
    ],
}

```

```

{
  "Sid": "ViewConfigurationPolicy",
  "Effect": "Allow",
  "Action": [
    "securityhub:GetConfigurationPolicy",
    "securityhub:ListConfigurationPolicies"
  ],
  "Resource": "*"
},
{
  "Sid": "DeleteConfigurationPolicy",
  "Effect": "Allow",
  "Action": [
    "securityhub:DeleteConfigurationPolicy"
  ],
  "Resource": "*"
},
{
  "Sid": "ViewConfigurationPolicyAssociation",
  "Effect": "Allow",
  "Action": [
    "securityhub:BatchGetConfigurationPolicyAssociations",
    "securityhub:GetConfigurationPolicyAssociation",
    "securityhub:ListConfigurationPolicyAssociations"
  ],
  "Resource": "*"
},
{
  "Sid": "UpdateConfigurationPolicyAssociation",
  "Effect": "Allow",
  "Action": [
    "securityhub:StartConfigurationPolicyAssociation",
    "securityhub:StartConfigurationPolicyDisassociation"
  ],
  "Resource": "*"
}
]
}

```

Contoh: Izinkan pengguna untuk melihat temuan

Contoh ini menunjukkan cara Anda membuat kebijakan IAM yang memungkinkan pengguna melihat temuan Security Hub.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ReviewFindings",
      "Effect": "Allow",
      "Action": [
        "securityhub:GetFindings"
      ],
      "Resource": "*"
    }
  ]
}
```

Contoh: Izinkan pengguna membuat dan mengelola aturan otomatisasi

Contoh ini menunjukkan cara membuat kebijakan IAM yang memungkinkan pengguna membuat, melihat, memperbarui, dan menghapus aturan otomatisasi Security Hub. Agar kebijakan IAM ini berfungsi, pengguna harus menjadi administrator Security Hub. Untuk membatasi izin — misalnya, untuk mengizinkan pengguna hanya melihat aturan otomatisasi — Anda dapat menghapus izin buat, perbarui, dan hapus.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "CreateAndUpdateAutomationRules",
      "Effect": "Allow",
      "Action": [
        "securityhub:CreateAutomationRule",
        "securityhub:BatchUpdateAutomationRules"
      ],
      "Resource": "*"
    },
    {
      "Sid": "ViewAutomationRules",
      "Effect": "Allow",
      "Action": [
        "securityhub:BatchGetAutomationRules",
        "securityhub:ListAutomationRules"
      ],
      "Resource": "*"
    }
  ]
}
```



```
    },  
    {  
      "Sid": "DeleteAutomationRules",  
      "Effect": "Allow",  
      "Action": [  
        "securityhub:BatchDeleteAutomationRules"  
      ],  
      "Resource": "*"   
    }  
  ]  
}
```

Peran terkait layanan untuk AWS Security Hub

AWS Security Hub menggunakan peran [terkait layanan AWS Identity and Access Management](#) (IAM) bernama `AWSServiceRoleForSecurityHub`. Peran terkait layanan ini adalah peran IAM yang ditautkan langsung ke Security Hub. Ini telah ditentukan sebelumnya oleh Security Hub, dan mencakup semua izin yang diperlukan Security Hub untuk memanggil sumber daya lain Layanan AWS dan memantau AWS sumber daya atas nama Anda. Security Hub menggunakan peran terkait layanan ini di semua Wilayah AWS tempat Security Hub tersedia.

Peran terkait layanan membuat pengaturan Security Hub lebih mudah karena Anda tidak perlu menambahkan izin yang diperlukan secara manual. Security Hub mendefinisikan izin peran terkait layanan, dan kecuali izin ditentukan sebaliknya, hanya Security Hub yang dapat mengambil peran tersebut. Izin yang ditentukan mencakup kebijakan kepercayaan dan kebijakan izin, dan Anda tidak dapat melampirkan kebijakan izin tersebut ke entitas IAM lainnya.

Untuk melihat detail peran terkait layanan, pada halaman Pengaturan konsol Security Hub, pilih Umum, lalu Lihat izin layanan.

Anda dapat menghapus peran terkait layanan Security Hub hanya setelah pertama kali menonaktifkan Security Hub di semua Wilayah yang diaktifkan. Ini melindungi sumber daya Security Hub karena Anda tidak dapat secara tidak sengaja menghapus izin untuk mengaksesnya.

Untuk informasi tentang layanan lain yang mendukung peran terkait layanan, lihat [AWS layanan yang bekerja dengan IAM di Panduan Pengguna IAM](#) dan temukan layanan yang memiliki Ya di kolom Peran Tertaut Layanan. Pilih Ya dengan sebuah tautan untuk melihat dokumentasi peran terkait layanan untuk layanan tersebut.

Topik

- [Izin peran terkait layanan untuk Security Hub](#)
- [Membuat peran terkait layanan untuk Security Hub](#)
- [Mengedit peran terkait layanan untuk Security Hub](#)
- [Menghapus peran terkait layanan untuk Security Hub](#)

Izin peran terkait layanan untuk Security Hub

Security Hub menggunakan peran terkait layanan bernama `AWSServiceRoleForSecurityHub`. Ini adalah peran terkait layanan yang diperlukan AWS Security Hub untuk mengakses sumber daya Anda. Peran terkait layanan memungkinkan Security Hub menerima temuan dari yang lain Layanan AWS dan mengonfigurasi AWS Config infrastruktur yang diperlukan untuk menjalankan pemeriksaan keamanan untuk kontrol.

Peran terkait layanan `AWSServiceRoleForSecurityHub` memercayai layanan berikut untuk mengambil peran tersebut:

- `securityhub.amazonaws.com`

`AWSServiceRoleForSecurityHub` Peran terkait layanan menggunakan kebijakan terkelola. [AWSSecurityHubServiceRolePolicy](#)

Anda harus memberikan izin untuk mengizinkan identitas IAM (seperti peran, grup, atau pengguna) untuk membuat, mengedit, atau menghapus peran terkait layanan. Agar peran `AWSServiceRoleForSecurityHub` terkait layanan berhasil dibuat, identitas IAM yang Anda gunakan untuk mengakses Security Hub harus memiliki izin yang diperlukan. Untuk memberikan izin yang diperlukan, lampirkan kebijakan berikut ke peran, grup, atau pengguna.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "securityhub:*",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "iam:CreateServiceLinkedRole",
      "Resource": "*",
    }
  ]
}
```

```
    "Condition": {
      "StringLike": {
        "iam:AWSServiceName": "securityhub.amazonaws.com"
      }
    }
  }
]
```

Membuat peran terkait layanan untuk Security Hub

Peran `AWSServiceRoleForSecurityHub` terkait layanan dibuat secara otomatis saat Anda mengaktifkan Security Hub untuk pertama kalinya atau mengaktifkan Security Hub di Wilayah yang didukung yang sebelumnya tidak mengaktifkannya. Anda juga dapat membuat peran terkait layanan `AWSServiceRoleForSecurityHub` secara manual menggunakan konsol IAM, CLI IAM, atau API IAM.

Important

Peran terkait layanan yang dibuat untuk akun administrator Security Hub tidak berlaku untuk akun anggota Security Hub.

Untuk informasi selengkapnya tentang membuat peran secara manual, lihat [Membuat peran terkait layanan](#) dalam Panduan Pengguna IAM.

Mengedit peran terkait layanan untuk Security Hub

Security Hub tidak mengizinkan Anda mengedit peran `AWSServiceRoleForSecurityHub` terkait layanan. Setelah membuat peran terkait layanan, Anda tidak dapat mengubah nama peran karena berbagai entitas mungkin mereferensikan peran tersebut. Namun, Anda dapat mengubah deskripsi peran dengan menggunakan IAM. Untuk informasi selengkapnya, lihat [Mengedit peran terkait layanan](#) dalam Panduan Pengguna IAM.

Menghapus peran terkait layanan untuk Security Hub

Jika Anda tidak perlu lagi menggunakan fitur atau layanan yang memerlukan peran terkait layanan, sebaiknya hapus peran tersebut. Dengan begitu, Anda tidak memiliki entitas yang tidak terpakai yang tidak dipantau atau dipelihara secara aktif.

⚠ Important

Untuk menghapus peran `AWSServiceRoleForSecurityHub` terkait layanan, Anda harus menonaktifkan Security Hub terlebih dahulu di semua Wilayah yang diaktifkan.

Jika Security Hub tidak dinonaktifkan saat Anda mencoba menghapus peran terkait layanan, penghapusan akan gagal. Untuk informasi selengkapnya, lihat [Menonaktifkan CSPM Security Hub](#).

Saat Anda menonaktifkan Security Hub, peran `AWSServiceRoleForSecurityHub` terkait layanan tidak akan dihapus secara otomatis. Jika Anda mengaktifkan Security Hub lagi, Security Hub akan mulai menggunakan peran `AWSServiceRoleForSecurityHub` terkait layanan yang ada.

Untuk menghapus peran terkait layanan secara manual menggunakan IAM

Gunakan konsol IAM, CLI IAM, atau API CLI untuk menghapus peran terkait layanan `AWSServiceRoleForSecurityHub`. Untuk informasi selengkapnya, lihat [Menghapus peran terkait layanan](#) dalam Panduan Pengguna IAM.

AWS kebijakan terkelola untuk Security Hub

Kebijakan AWS terkelola adalah kebijakan mandiri yang dibuat dan dikelola oleh AWS. AWS Kebijakan terkelola dirancang untuk memberikan izin bagi banyak kasus penggunaan umum sehingga Anda dapat mulai menetapkan izin kepada pengguna, grup, dan peran.

Perlu diingat bahwa kebijakan AWS terkelola mungkin tidak memberikan izin hak istimewa paling sedikit untuk kasus penggunaan spesifik Anda karena tersedia untuk digunakan semua pelanggan. AWS Kami menyarankan Anda untuk mengurangi izin lebih lanjut dengan menentukan [kebijakan yang dikelola pelanggan](#) yang khusus untuk kasus penggunaan Anda.

Anda tidak dapat mengubah izin yang ditentukan dalam kebijakan AWS terkelola. Jika AWS memperbarui izin yang ditentukan dalam kebijakan AWS terkelola, pembaruan akan memengaruhi semua identitas utama (pengguna, grup, dan peran) yang dilampirkan kebijakan tersebut. AWS kemungkinan besar akan memperbarui kebijakan AWS terkelola saat baru Layanan AWS diluncurkan atau operasi API baru tersedia untuk layanan yang ada.

Untuk informasi selengkapnya, lihat [Kebijakan terkelola AWS](#) dalam Panduan Pengguna IAM.

AWS kebijakan terkelola: AWSSecurityHubFullAccess

Anda dapat melampirkan kebijakan `AWSSecurityHubFullAccess` ke identitas IAM Anda.

Kebijakan ini memberikan izin administratif yang memungkinkan akses penuh utama ke semua tindakan CSPM Security Hub. Kebijakan ini harus dilampirkan pada prinsipal sebelum mengaktifkan Security Hub CSPM secara manual untuk akun mereka. Misalnya, kepala sekolah dengan izin ini dapat melihat dan memperbarui status temuan. Mereka dapat mengonfigurasi wawasan khusus, dan mengaktifkan integrasi. Mereka dapat mengaktifkan dan menonaktifkan standar dan kontrol. Prinsipal untuk akun administrator juga dapat mengelola akun anggota.

Detail izin

Kebijakan ini mencakup izin berikut.

- `securityhub`— Memungkinkan kepala sekolah akses penuh ke semua tindakan CSPM Security Hub.
- `guardduty`— Memungkinkan kepala sekolah untuk mendapatkan informasi tentang status akun di Amazon. GuardDuty
- `iam`— Memungkinkan kepala sekolah untuk membuat peran terkait layanan untuk Security Hub CSPM dan Security Hub.
- `inspector`— Memungkinkan kepala sekolah untuk mendapatkan informasi tentang status akun di Amazon Inspector.
- `pricing`— Memungkinkan kepala sekolah untuk mendapatkan daftar harga dan produk. Layanan AWS

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "SecurityHubAllowAll",
      "Effect": "Allow",
      "Action": "securityhub:*",
      "Resource": "*"
    },
    {
      "Sid": "SecurityHubServiceLinkedRole",
      "Effect": "Allow",
```

```

    "Action": "iam:CreateServiceLinkedRole",
    "Resource": "*",
    "Condition": {
      "StringLike": {
        "iam:AWSServiceName": [
          "securityhub.amazonaws.com",
          "securityhubv2.amazonaws.com"
        ]
      }
    }
  },
  {
    "Sid": "OtherServicePermission",
    "Effect": "Allow",
    "Action": [
      "guardduty:GetDetector",
      "guardduty:ListDetectors",
      "inspector2:BatchGetAccountStatus",
      "pricing:GetProducts"
    ],
    "Resource": "*"
  }
]
}

```

Kebijakan terkelola CSPM Security Hub: AWSSecurityHubReadOnlyAccess

Anda dapat melampirkan kebijakan AWSSecurityHubReadOnlyAccess ke identitas IAM Anda.

Kebijakan ini memberikan izin hanya-baca yang memungkinkan pengguna melihat informasi di CSPM Security Hub. Prinsipal dengan kebijakan ini terlampir tidak dapat melakukan pembaruan apa pun di Security Hub CSPM. Misalnya, kepala sekolah dengan izin ini dapat melihat daftar temuan yang terkait dengan akun mereka, tetapi tidak dapat mengubah status temuan. Mereka dapat melihat hasil wawasan, tetapi tidak dapat membuat atau mengonfigurasi wawasan khusus. Mereka tidak dapat mengonfigurasi kontrol atau integrasi produk.

Detail izin

Kebijakan ini mencakup izin berikut.

- **securityhub** – Mengizinkan pengguna melakukan tindakan yang mengembalikan daftar item atau detail tentang item. Ini termasuk operasi API yang dimulai dengan `Get`, `List`, atau `Describe`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSSecurityHubReadOnlyAccess",
      "Effect": "Allow",
      "Action": [
        "securityhub:Get*",
        "securityhub:List*",
        "securityhub:BatchGet*",
        "securityhub:Describe*"
      ],
      "Resource": "*"
    }
  ]
}
```

AWS kebijakan terkelola: AWSSecurityHubOrganizationsAccess

Anda dapat melampirkan kebijakan AWSSecurityHubOrganizationsAccess ke identitas IAM Anda.

Kebijakan ini memberikan izin administratif untuk mengaktifkan dan mengelola Security Hub dan Security Hub CSPM dalam suatu organisasi.

Izin kebijakan ini memungkinkan akun manajemen organisasi menunjuk akun administrator yang didelegasikan untuk Security Hub dan Security Hub CSPM. Mereka juga mengizinkan akun administrator yang didelegasikan untuk mengaktifkan akun organisasi sebagai akun anggota.

Kebijakan ini hanya memberikan izin untuk Organizations. Akun manajemen organisasi dan akun administrator yang didelegasikan juga memerlukan izin untuk tindakan terkait. Izin ini dapat diberikan menggunakan kebijakan AWSSecurityHubFullAccess terkelola.

Detail izin

Kebijakan ini mencakup izin berikut.

- **organizations:ListAccounts**— Memungkinkan kepala sekolah untuk mengambil daftar akun yang merupakan bagian dari organisasi.
- **organizations:DescribeOrganization**— Memungkinkan kepala sekolah untuk mengambil informasi tentang organisasi.

- `organizations:ListRoots`— Memungkinkan kepala sekolah untuk membuat daftar akar organisasi.
- `organizations:ListDelegatedAdministrators`— Memungkinkan kepala sekolah untuk membuat daftar administrator yang didelegasikan dari suatu organisasi.
- `organizations:ListAWSServiceAccessForOrganization`— Memungkinkan kepala sekolah untuk membuat daftar Layanan AWS yang digunakan organisasi.
- `organizations:ListOrganizationalUnitsForParent`— Memungkinkan kepala sekolah untuk membuat daftar unit organisasi anak (OU) dari OU orang tua.
- `organizations:ListAccountsForParent`— Memungkinkan kepala sekolah untuk membuat daftar akun anak dari OU orang tua.
- `organizations:ListParents`— Daftar root atau unit organisasi (OUs) yang berfungsi sebagai induk langsung dari OU atau akun anak yang ditentukan.
- `organizations:DescribeAccount` – Memungkinkan principal mengambil informasi tentang akun di organisasi.
- `organizations:DescribeOrganizationalUnit`— Memungkinkan kepala sekolah untuk mengambil informasi tentang OU dalam organisasi.
- `organizations:ListPolicies`— Mengambil daftar semua kebijakan dalam organisasi dari jenis tertentu.
- `organizations:ListPoliciesForTarget`— Daftar kebijakan yang secara langsung dilampirkan ke root target yang ditentukan, unit organisasi (OU), atau akun.
- `organizations:ListTargetsForPolicy`— Daftar semua akar, unit organisasi (OUs), dan akun yang dilampirkan kebijakan yang ditentukan.
- `organizations:EnableAWSServiceAccess`— Memungkinkan prinsipal untuk mengaktifkan integrasi dengan Organizations.
- `organizations:RegisterDelegatedAdministrator`— Memungkinkan kepala sekolah untuk menunjuk akun administrator yang didelegasikan.
- `organizations:DeregisterDelegatedAdministrator`— Memungkinkan kepala sekolah untuk menghapus akun administrator yang didelegasikan.
- `organizations:DescribePolicy`— Mengambil informasi tentang kebijakan.
- `organizations:DescribeEffectivePolicy`— Mengembalikan isi kebijakan efektif untuk jenis kebijakan dan akun tertentu.
- `organizations:CreatePolicy`— Membuat kebijakan dari jenis tertentu yang dapat Anda lampirkan ke root, unit organisasi (OU), atau AWS akun individu.

- `organizations:UpdatePolicy`— Memperbarui kebijakan yang ada dengan nama, deskripsi, atau konten baru.
- `organizations>DeletePolicy`— Menghapus kebijakan yang ditentukan dari organisasi Anda.
- `organizations:AttachPolicy`— Melampirkan kebijakan ke root, unit organisasi (OU), atau akun individu.
- `organizations:DetachPolicy`— Melepaskan kebijakan dari akar target, unit organisasi (OU), atau akun.
- `organizations:EnablePolicyType`— Mengaktifkan jenis kebijakan di root.
- `organizations:DisablePolicyType`— Menonaktifkan jenis kebijakan organisasi di root.
- `organizations:TagResource`— Menambahkan satu atau lebih tag ke sumber daya yang ditentukan.
- `organizations:UntagResource`— Menghapus tag apa pun dengan kunci yang ditentukan dari sumber daya yang ditentukan.
- `organizations:ListTagsForResource`— Daftar tag yang dilampirkan ke sumber daya yang ditentukan.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "OrganizationPermissions",
      "Effect": "Allow",
      "Action": [
        "organizations:ListAccounts",
        "organizations:DescribeOrganization",
        "organizations:ListRoots",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListAccountsForParent",
        "organizations:ListParents",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganizationalUnit",
        "organizations:ListPolicies",
        "organizations:ListPoliciesForTarget",
        "organizations:ListTargetsForPolicy"
      ],
      "Resource": "*"
    }
  ]
}
```

```

    },
    {
      "Sid": "OrganizationPermissionsEnable",
      "Effect": "Allow",
      "Action": "organizations:EnableAWSServiceAccess",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "organizations:ServicePrincipal": "securityhub.amazonaws.com"
        }
      }
    },
    {
      "Sid": "OrganizationPermissionsDelegatedAdmin",
      "Effect": "Allow",
      "Action": [
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator"
      ],
      "Resource": "arn:aws:organizations::*:account/o-*/*",
      "Condition": {
        "StringEquals": {
          "organizations:ServicePrincipal": "securityhub.amazonaws.com"
        }
      }
    },
    {
      "Sid": "OrganizationPolicyPermissions",
      "Effect": "Allow",
      "Action": [
        "organizations:DescribePolicy",
        "organizations:DescribeEffectivePolicy",
        "organizations:CreatePolicy",
        "organizations:UpdatePolicy",
        "organizations>DeletePolicy",
        "organizations:AttachPolicy",
        "organizations:DetachPolicy",
        "organizations:EnablePolicyType",
        "organizations:DisablePolicyType"
      ],
      "Resource": [
        "arn:aws:organizations::*:root/o-*/*",
        "arn:aws:organizations::*:account/o-*/*",
        "arn:aws:organizations::*:ou/o-*/*",

```

```

        "arn:aws:organizations::*:policy/o-*/securityhub_policy/*"
    ],
    "Condition": {
        "StringLikeIfExists": {
            "organizations:PolicyType": "SECURITYHUB_POLICY"
        }
    }
},
{
    "Sid": "OrganizationPolicyTaggingPermissions",
    "Effect": "Allow",
    "Action": [
        "organizations:TagResource",
        "organizations:UntagResource",
        "organizations:ListTagsForResource"
    ],
    "Resource": [
        "arn:aws:organizations::*:policy/o-*/securityhub_policy/*"
    ]
}
]
}

```

AWS kebijakan terkelola: AWSSecurityHubServiceRolePolicy

Anda tidak dapat melampirkan AWSSecurityHubServiceRolePolicy ke entitas IAM Anda. Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan CSPM Security Hub melakukan tindakan atas nama Anda. Untuk informasi selengkapnya, lihat [the section called “Peran terkait layanan”](#).

Kebijakan ini memberikan izin administratif yang memungkinkan peran terkait layanan untuk melakukan pemeriksaan keamanan untuk kontrol CSPM Security Hub.

Detail izin

Kebijakan ini mencakup izin untuk melakukan hal berikut:

- `cloudtrail`— Ambil informasi tentang jalan CloudTrail setiapak.
- `cloudwatch`— Ambil CloudWatch alarm saat ini.
- `logs`— Ambil filter metrik untuk CloudWatch log.
- `sns`— Ambil daftar langganan ke topik SNS.

- **config**— Mengambil informasi tentang perekam konfigurasi, sumber daya, dan AWS Config aturan. Juga memungkinkan peran terkait layanan untuk membuat dan menghapus AWS Config aturan, dan menjalankan evaluasi terhadap aturan.
- **iam**— Dapatkan dan buat laporan kredensi untuk akun.
- **organizations**— Mengambil informasi akun dan unit organisasi (OU) untuk suatu organisasi.
- **securityhub**— Mengambil informasi tentang bagaimana layanan, standar, dan kontrol CSPM Security Hub dikonfigurasi.
- **tag**— Mengambil informasi tentang tag sumber daya.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "SecurityHubServiceRolePermissions",
      "Effect": "Allow",
      "Action": [
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:GetEventSelectors",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeAlarmsForMetric",
        "logs:DescribeMetricFilters",
        "sns:ListSubscriptionsByTopic",
        "config:DescribeConfigurationRecorders",
        "config:DescribeConfigurationRecorderStatus",
        "config:DescribeConfigRules",
        "config:DescribeConfigRuleEvaluationStatus",
        "config:BatchGetResourceConfig",
        "config:SelectResourceConfig",
        "iam:GenerateCredentialReport",
        "organizations:ListAccounts",
        "config:PutEvaluations",
        "tag:GetResources",
        "iam:GetCredentialReport",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListChildren",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganizationalUnit",
        "securityhub:BatchDisableStandards",

```

```

        "securityhub:BatchEnableStandards",
        "securityhub:BatchUpdateStandardsControlAssociations",
        "securityhub:BatchGetSecurityControls",
        "securityhub:BatchGetStandardsControlAssociations",
        "securityhub:CreateMembers",
        "securityhub>DeleteMembers",
        "securityhub:DescribeHub",
        "securityhub:DescribeOrganizationConfiguration",
        "securityhub:DescribeStandards",
        "securityhub:DescribeStandardsControls",
        "securityhub:DisassociateFromAdministratorAccount",
        "securityhub:DisassociateMembers",
        "securityhub:DisableSecurityHub",
        "securityhub:EnableSecurityHub",
        "securityhub:GetEnabledStandards",
        "securityhub:ListStandardsControlAssociations",
        "securityhub:ListSecurityControlDefinitions",
        "securityhub:UpdateOrganizationConfiguration",
        "securityhub:UpdateSecurityControl",
        "securityhub:UpdateSecurityHubConfiguration",
        "securityhub:UpdateStandardsControl",
        "tag:GetResources"
    ],
    "Resource": "*"
},
{
    "Sid": "SecurityHubServiceRoleConfigPermissions",
    "Effect": "Allow",
    "Action": [
        "config:PutConfigRule",
        "config>DeleteConfigRule",
        "config:GetComplianceDetailsByConfigRule"
    ],
    "Resource": "arn:aws:config:*:*:config-rule/aws-service-rule/*securityhub*"
},
{
    "Sid": "SecurityHubServiceRoleOrganizationsPermissions",
    "Effect": "Allow",
    "Action": [
        "organizations:ListDelegatedAdministrators"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {

```

```

        "organizations:ServicePrincipal": [
            "securityhub.amazonaws.com"
        ]
    }
}

```

AWS kebijakan terkelola: AWSSecurityHubV2ServiceRolePolicy

Note

Security Hub dalam rilis pratinjau dan dapat berubah sewaktu-waktu.

Kebijakan ini memungkinkan Security Hub mengelola AWS Config aturan dan sumber daya Security Hub di organisasi Anda dan atas nama Anda. Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda. Untuk informasi selengkapnya, lihat [the section called “Peran terkait layanan”](#).

Detail izin

Kebijakan ini mencakup izin untuk melakukan hal berikut:

- **config**— Mengelola perekam konfigurasi terkait layanan untuk sumber daya Security Hub.
- **iam**— Menciptakan peran terkait layanan untuk. AWS Config
- **organizations**— Mengambil informasi akun dan unit organisasi (OU) untuk suatu organisasi.
- **securityhub**— Mengelola konfigurasi Security Hub.
- **tag**— Mengambil informasi tentang tag sumber daya.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "SecurityHubV2ServiceRoleAssetsConfig",
      "Effect": "Allow",
      "Action": [

```

```

        "config:DeleteServiceLinkedConfigurationRecorder",
        "config:DescribeConfigurationRecorders",
        "config:DescribeConfigurationRecorderStatus",
        "config:PutServiceLinkedConfigurationRecorder"
    ],
    "Resource": "arn:aws:config:*:*:configuration-recorder/
AWSConfigurationRecorderForSecurityHubAssets/*"
},
{
    "Sid": "SecurityHubV2ServiceRoleAssetsIamPermissions",
    "Effect": "Allow",
    "Action": [
        "iam:CreateServiceLinkedRole"
    ],
    "Resource": "arn:aws:iam:*:*:role/aws-service-role/config.amazonaws.com/
AWSServiceRoleForConfig",
    "Condition": {
        "StringEquals": {
            "iam:AWSServiceName": "config.amazonaws.com"
        }
    }
},
{
    "Sid": "SecurityHubV2ServiceRoleSecurityHubPermissions",
    "Effect": "Allow",
    "Action": [
        "securityhub:DisableSecurityHubV2",
        "securityhub:EnableSecurityHubV2",
        "securityhub:DescribeSecurityHubV2"
    ],
    "Resource": "arn:aws:securityhub:*:*:hubv2/*",
    "Condition": {
        "StringEquals": {
            "aws:ResourceAccount": "${aws:PrincipalAccount}"
        }
    }
},
{
    "Sid": "SecurityHubV2ServiceRoleTagPermissions",
    "Effect": "Allow",
    "Action": [
        "tag:GetResources"
    ],
    "Resource": "*"
}

```

```

    },
    {
      "Sid": "SecurityHubV2ServiceRoleOrganizationsPermissionsOnResources",
      "Effect": "Allow",
      "Action": [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganizationalUnit"
      ],
      "Resource": "arn:aws:organizations::*:*"
    },
    {
      "Sid": "SecurityHubV2ServiceRoleOrganizationsPermissionsWithoutResources",
      "Effect": "Allow",
      "Action": [
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListChildren"
      ],
      "Resource": "*"
    },
    {
      "Sid": "SecurityHubV2ServiceRoleDelegatedAdminPermissions",
      "Effect": "Allow",
      "Action": [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "organizations:ServicePrincipal": [
            "securityhub.amazonaws.com"
          ]
        }
      }
    }
  ]
}

```


Pembaruan CSPM Security Hub ke AWS kebijakan terkelola

Lihat detail tentang pembaruan kebijakan AWS terkelola untuk CSPM Security Hub sejak layanan ini mulai melacak perubahan ini. [Untuk peringatan otomatis tentang perubahan pada halaman ini, berlangganan umpan RSS di halaman riwayat Dokumen CSPM Security Hub.](#)

Perubahan	Deskripsi	Tanggal
AWSSecurityHubOrganizationsAccess – Pembaruan ke kebijakan yang sudah ada	Security Hub CSPM menambahkan izin baru ke. <code>AWSSecurityHubOrganizationsAccess</code> Izin ini memungkinkan manajemen organisasi untuk mengaktifkan dan mengelola Security Hub dan Security Hub CSPM dalam suatu organisasi.	Juni 17, 2025
AWSSecurityHubOrganizationsAccess – Pembaruan ke kebijakan yang ada	Menambahkan izin baru yang memungkinkan manajemen organisasi mengaktifkan dan mengelola Security Hub dan Security Hub CSPM dalam suatu organisasi.	Juni 17, 2025
AWSSecurityHubFullAccess – Pembaruan ke kebijakan yang ada	Security Hub CSPM menambahkan izin baru yang memungkinkan prinsipal membuat peran terkait layanan untuk Security Hub.	Juni 17, 2025
AWSSecurityHUBv2ServiceRolePolicy - Kebijakan baru	Security Hub menambahkan kebijakan baru untuk memungkinkan Security Hub mengelola AWS Config aturan dan sumber daya Security	Juni 17, 2025

Perubahan	Deskripsi	Tanggal
	Hub di organisasi pelanggan dan atas nama pelanggan . Security Hub dalam rilis pratinjau dan dapat berubah sewaktu-waktu.	
AWSSecurityHubFullAccess — Perbarui ke kebijakan yang ada	Security Hub CSPM memperbarui kebijakan untuk mendapatkan detail harga Layanan AWS dan produk.	April 24, 2024
AWSSecurityHubReadOnlyAccess — Perbarui ke kebijakan yang ada	Security Hub CSPM memperbarui kebijakan terkelola ini dengan menambahkan kolom. Sid	Februari 22, 2024
AWSSecurityHubFullAccess — Perbarui ke kebijakan yang ada	Security Hub CSPM memperbarui kebijakan sehingga dapat menentukan apakah Amazon GuardDuty dan Amazon Inspector diaktifkan di akun. Ini membantu pelanggan menyatukan informasi terkait keamanan dari beberapa. Layanan AWS	16 November 2023

Perubahan	Deskripsi	Tanggal
AWSSecurityHubOrganizationsAccess — Perbarui ke kebijakan yang ada	Security Hub CSPM memperbarui kebijakan untuk memberikan izin tambahan guna mengizinkan akses hanya-baca ke fungsionalitas administrator yang didelegasikan. AWS Organizations Ini termasuk detail seperti root, unit organisasi (OUs), akun, struktur organisasi, dan akses layanan.	16 November 2023
AWSSecurityHubServiceRolePolicy – Pembaruan ke kebijakan yang ada	Security Hub CSPM menambahkan <code>BatchGetSecurityControls</code> , <code>DisassociateFromAdministratorAccount</code> , dan <code>UpdateSecurityControl</code> izin untuk membaca dan memperbarui properti kontrol keamanan yang dapat disesuaikan.	26 November 2023
AWSSecurityHubServiceRolePolicy – Pembaruan ke kebijakan yang ada	Security Hub CSPM menambahkan <code>tag:GetResources</code> izin untuk membaca tag sumber daya yang terkait dengan temuan.	7 November 2023

Perubahan	Deskripsi	Tanggal
AWSSecurityHubServiceRolePolicy – Pembaruan ke kebijakan yang ada	Security Hub CSPM menambahkan BatchGetStandardsControlAssociations izin untuk mendapatkan informasi tentang status pemberdayaan kontrol dalam standar.	27 September 2023
AWSSecurityHubServiceRolePolicy – Pembaruan ke kebijakan yang ada	Security Hub CSPM menambahkan izin baru untuk mendapatkan AWS Organizations data dan membaca serta memperbarui konfigurasi CSPM Security Hub, termasuk standar dan kontrol.	20 September 2023
AWSSecurityHubServiceRolePolicy – Pembaruan ke kebijakan yang ada	Security Hub CSPM memindahkan config:DescribeConfigRuleEvaluationStatus izin yang ada ke pernyataan yang berbeda dalam kebijakan. config:DescribeConfigRuleEvaluationStatus Izin sekarang diterapkan ke semua sumber daya.	Maret 17, 2023

Perubahan	Deskripsi	Tanggal
AWSSecurityHubServiceRolePolicy – Pembaruan ke kebijakan yang ada	Security Hub CSPM memindahkan <code>config:PutEvaluations</code> izin yang ada ke pernyataan yang berbeda dalam kebijakan. <code>config:PutEvaluations</code> izin sekarang diterapkan ke semua sumber daya.	14 Juli 2021
AWSSecurityHubServiceRolePolicy – Pembaruan ke kebijakan yang ada	Security Hub CSPM menambahkan izin baru untuk memungkinkan peran terkait layanan memberikan hasil evaluasi. AWS Config	29 Juni 2021
AWSSecurityHubServiceRolePolicy — Ditambahkan ke daftar kebijakan terkelola	Menambahkan informasi tentang kebijakan terkelola <code>AWSSecurityHubServiceRolePolicy</code> , yang digunakan oleh peran terkait layanan CSPM Security Hub.	11 Juni 2021
AWSSecurityHubOrganizationsAccess — Kebijakan baru	Security Hub CSPM menambahkan kebijakan baru yang memberikan izin yang diperlukan untuk integrasi CSPM Security Hub dengan Organizations.	15 Maret 2021
Security Hub CSPM mulai melacak perubahan	Security Hub CSPM mulai melacak perubahan untuk kebijakan yang AWS dikelola.	15 Maret 2021

Memecahkan masalah AWS Security Hub identitas dan akses

Gunakan informasi berikut untuk membantu Anda mendiagnosis dan memperbaiki masalah umum yang mungkin Anda temui saat bekerja dengan AWS Security Hub dan IAM.

Topik

- [Saya tidak berwenang untuk melakukan tindakan di Security Hub](#)
- [Saya tidak berwenang untuk melakukan iam: PassRole](#)
- [Saya ingin akses terprogram ke Security Hub](#)
- [Saya seorang administrator dan ingin mengizinkan orang lain mengakses Security Hub](#)
- [Saya ingin mengizinkan orang di luar saya Akun AWS untuk mengakses sumber daya Security Hub saya](#)

Saya tidak berwenang untuk melakukan tindakan di Security Hub

Jika AWS Management Console memberitahu Anda bahwa Anda tidak berwenang untuk melakukan tindakan, maka Anda harus menghubungi administrator Anda untuk bantuan. Administrator Anda adalah orang yang memberi Anda kredensial masuk.

Contoh kesalahan berikut terjadi ketika pengguna mateojackson mencoba menggunakan konsol untuk melihat detail tentang *widget* tetapi tidak memiliki `securityhub:GetWidget` izin.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform: securityhub:GetWidget on resource: my-example-widget
```

Dalam hal ini, Mateo meminta administratornya untuk memperbarui kebijakannya untuk mengizinkan dia mengakses sumber daya *my-example-widget* menggunakan tindakan `securityhub:GetWidget`.

Saya tidak berwenang untuk melakukan iam: PassRole

Jika Anda menerima kesalahan yang tidak diizinkan untuk melakukan `iam:PassRole` tindakan, kebijakan Anda harus diperbarui agar Anda dapat meneruskan peran ke Security Hub.

Beberapa Layanan AWS memungkinkan Anda untuk meneruskan peran yang ada ke layanan tersebut alih-alih membuat peran layanan baru atau peran terkait layanan. Untuk melakukannya, Anda harus memiliki izin untuk meneruskan peran ke layanan.

Contoh kesalahan berikut terjadi ketika pengguna IAM bernama `marymajor` mencoba menggunakan konsol untuk melakukan tindakan di Security Hub. Namun, tindakan tersebut memerlukan layanan untuk mendapatkan izin yang diberikan oleh peran layanan. Mary tidak memiliki izin untuk meneruskan peran tersebut pada layanan.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
iam:PassRole
```

Dalam kasus ini, kebijakan Mary harus diperbarui agar dia mendapatkan izin untuk melakukan tindakan `iam:PassRole` tersebut.

Jika Anda memerlukan bantuan, hubungi AWS administrator Anda. Administrator Anda adalah orang yang memberi Anda kredensial masuk.

Saya ingin akses terprogram ke Security Hub

Pengguna membutuhkan akses terprogram jika mereka ingin berinteraksi dengan AWS luar. AWS Management Console Cara untuk memberikan akses terprogram tergantung pada jenis pengguna yang mengakses AWS.

Untuk memberi pengguna akses programatis, pilih salah satu opsi berikut.

Pengguna mana yang membutuhkan akses programatis?	Untuk	Oleh
Identitas tenaga kerja (Pengguna yang dikelola di Pusat Identitas IAM)	Gunakan kredensi sementara untuk menandatangani permintaan terprogram ke AWS CLI,, AWS SDKs atau. AWS APIs	Mengikuti petunjuk untuk antarmuka yang ingin Anda gunakan. • Untuk AWS CLI, lihat Mengkonfigurasi yang akan AWS CLI digunakan AWS IAM Identity Center dalam Panduan AWS Command Line Interface Pengguna. • Untuk AWS SDKs, alat, dan AWS APIs, lihat Autentikasi Pusat Identitas IAM di

Pengguna mana yang membutuhkan akses programatis?	Untuk	Oleh
		Panduan Referensi Alat AWS SDKs dan Alat.
IAM	Gunakan kredensi sementara untuk menandatangani permintaan terprogram ke AWS CLI,, AWS SDKs atau. AWS APIs	Mengikuti petunjuk dalam Menggunakan kredensi sementara dengan AWS sumber daya di Panduan Pengguna IAM.
IAM	(Tidak direkomendasikan) Gunakan kredensi jangka panjang untuk menandatangani permintaan terprogram ke AWS CLI,, AWS SDKs atau. AWS APIs	Mengikuti petunjuk untuk antarmuka yang ingin Anda gunakan. • Untuk mengetahui AWS CLI, lihat Mengautentikasi menggunakan kredensi pengguna IAM di Panduan Pengguna. AWS Command Line Interface • Untuk AWS SDKs dan alat, lihat Mengautentikasi menggunakan kredensi jangka panjang di Panduan Referensi Alat AWS SDKs dan Alat. • Untuk AWS APIs, lihat Mengelola kunci akses untuk pengguna IAM di Panduan Pengguna IAM.

Saya seorang administrator dan ingin mengizinkan orang lain mengakses Security Hub

Untuk memberikan akses dan menambahkan izin bagi pengguna, grup, atau peran Anda:

- Pengguna dan grup di AWS IAM Identity Center:

Buat rangkaian izin. Ikuti instruksi di [Buat rangkaian izin](#) di Panduan Pengguna AWS IAM Identity Center .

- Pengguna yang dikelola di IAM melalui penyedia identitas:

Buat peran untuk federasi identitas. Ikuti instruksi dalam [Buat peran untuk penyedia identitas pihak ketiga \(federasi\)](#) dalam Panduan Pengguna IAM.

- Pengguna IAM:

- Buat peran yang dapat diambil pengguna Anda. Ikuti instruksi dalam [Buat peran untuk pengguna IAM](#) dalam Panduan Pengguna IAM.
- (Tidak disarankan) Lampirkan kebijakan langsung ke pengguna atau tambahkan pengguna ke grup pengguna. Ikuti petunjuk dalam [Menambahkan izin ke pengguna \(konsol\)](#) dalam Panduan Pengguna IAM.

Saya ingin mengizinkan orang di luar saya Akun AWS untuk mengakses sumber daya Security Hub saya

Anda dapat membuat peran yang dapat digunakan pengguna di akun lain atau orang-orang di luar organisasi Anda untuk mengakses sumber daya Anda. Anda dapat menentukan siapa saja yang dipercaya untuk mengambil peran tersebut. Untuk layanan yang mendukung kebijakan berbasis sumber daya atau daftar kontrol akses (ACLs), Anda dapat menggunakan kebijakan tersebut untuk memberi orang akses ke sumber daya Anda.

Untuk mempelajari selengkapnya, periksa referensi berikut:

- Untuk mengetahui apakah Security Hub mendukung fitur-fitur ini, lihat [Bagaimana Security Hub bekerja dengan IAM](#).
- Untuk mempelajari cara menyediakan akses ke sumber daya Anda di seluruh sumber daya Akun AWS yang Anda miliki, lihat [Menyediakan akses ke pengguna IAM di pengguna lain Akun AWS yang Anda miliki](#) di Panduan Pengguna IAM.
- Untuk mempelajari cara menyediakan akses ke sumber daya Anda kepada pihak ketiga Akun AWS, lihat [Menyediakan akses yang Akun AWS dimiliki oleh pihak ketiga](#) dalam Panduan Pengguna IAM.
- Untuk mempelajari cara memberikan akses melalui federasi identitas, lihat [Menyediakan akses ke pengguna terautentikasi eksternal \(federasi identitas\)](#) dalam Panduan Pengguna IAM.

- Untuk mempelajari perbedaan antara menggunakan peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat [Akses sumber daya lintas akun di IAM di Panduan Pengguna IAM](#).

Validasi Kepatuhan untuk AWS Security Hub

Untuk mempelajari apakah program kepatuhan spesifik, lihat [Layanan AWS di Cakupan Menurut Program Layanan AWS Kepatuhan](#) yang Kepatuhan yang Anda minati. Layanan AWS Untuk informasi umum, lihat [Program AWS Kepatuhan Program AWS](#).

Anda bisa mengunduh laporan audit pihak ketiga menggunakan AWS Artifact. Untuk informasi selengkapnya, lihat [Mengunduh Laporan di AWS Artifact](#).

Tanggung jawab kepatuhan Anda saat menggunakan Layanan AWS ditentukan oleh sensitivitas data Anda, tujuan kepatuhan perusahaan Anda, serta undang-undang dan peraturan yang berlaku. AWS menyediakan sumber daya berikut untuk membantu kepatuhan:

- [Kepatuhan dan Tata Kelola Keamanan](#) – Panduan implementasi solusi ini membahas pertimbangan arsitektur serta memberikan langkah-langkah untuk menerapkan fitur keamanan dan kepatuhan.
- [Referensi Layanan yang Memenuhi Syarat HIPAA](#) — Daftar layanan yang memenuhi syarat HIPAA. Tidak semua memenuhi Layanan AWS syarat HIPAA.
- [AWS Sumber Daya AWS](#) — Kumpulan buku kerja dan panduan ini mungkin berlaku untuk industri dan lokasi Anda.
- [AWS Panduan Kepatuhan Pelanggan](#) - Memahami model tanggung jawab bersama melalui lensa kepatuhan. Panduan ini merangkum praktik terbaik untuk mengamankan Layanan AWS dan memetakan panduan untuk kontrol keamanan di berbagai kerangka kerja (termasuk Institut Standar dan Teknologi Nasional (NIST), Dewan Standar Keamanan Industri Kartu Pembayaran (PCI), dan Organisasi Internasional untuk Standardisasi (ISO)).
- [Mengevaluasi Sumber Daya dengan Aturan](#) di Panduan AWS Config Developer — AWS Config Layanan menilai seberapa baik konfigurasi sumber daya Anda sesuai dengan praktik internal, pedoman industri, dan peraturan.
- [AWS Security Hub](#)— Ini Layanan AWS memberikan pandangan komprehensif tentang status keamanan Anda di dalam AWS. Security Hub menggunakan kontrol keamanan untuk sumber daya AWS Anda serta untuk memeriksa kepatuhan Anda terhadap standar industri keamanan dan praktik terbaik. Untuk daftar layanan dan kontrol yang didukung, lihat [Referensi kontrol Security Hub](#).

- [Amazon GuardDuty](#) — Ini Layanan AWS mendeteksi potensi ancaman terhadap beban kerja Akun AWS, kontainer, dan data Anda dengan memantau lingkungan Anda untuk aktivitas mencurigakan dan berbahaya. GuardDuty dapat membantu Anda mengatasi berbagai persyaratan kepatuhan, seperti PCI DSS, dengan memenuhi persyaratan deteksi intrusi yang diamanatkan oleh kerangka kerja kepatuhan tertentu.
- [AWS Audit Manager](#)— Ini akan Layanan AWS membantu Anda dalam meng-audit AWS Anda secara berkelanjutan untuk menyederhanakan cara Anda mengelola risiko dan kepatuhan terhadap peraturan dan standar industri.

Ketahanan di Security Hub AWS

Infrastruktur AWS global dibangun di sekitar Wilayah AWS dan Availability Zones. Wilayah memberikan beberapa Zona Ketersediaan yang terpisah dan terisolasi secara fisik, yang terkoneksi melalui jaringan latensi rendah, throughput tinggi, dan sangat redundan. Dengan Zona Ketersediaan, Anda dapat merancang serta mengoperasikan aplikasi dan basis data yang secara otomatis melakukan fail over di antara zona tanpa gangguan. Zona Ketersediaan memiliki ketersediaan dan toleransi kesalahan yang lebih baik, dan dapat diskalakan dibandingkan infrastruktur pusat data tunggal atau multi tradisional.

Untuk informasi selengkapnya tentang Wilayah AWS dan Availability Zone, lihat [Infrastruktur AWS Global](#).

Keamanan infrastruktur di AWS Security Hub

Sebagai layanan terkelola, AWS Security Hub dilindungi oleh keamanan jaringan AWS global. Untuk informasi tentang layanan AWS keamanan dan cara AWS melindungi infrastruktur, lihat [Keamanan AWS Cloud](#). Untuk mendesain AWS lingkungan Anda menggunakan praktik terbaik untuk keamanan infrastruktur, lihat [Perlindungan Infrastruktur dalam Kerangka Kerja](#) yang AWS Diarsiteksikan dengan Baik Pilar Keamanan.

Anda menggunakan panggilan API yang AWS dipublikasikan untuk mengakses Security Hub melalui jaringan. Klien harus mendukung hal-hal berikut:

- Keamanan Lapisan Pengangkutan (TLS). Kami mensyaratkan TLS 1.2 dan menganjurkan TLS 1.3.
- Sandi cocok dengan sistem kerahasiaan maju sempurna (perfect forward secrecy, PFS) seperti DHE (Ephemeral Diffie-Hellman) atau ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Sebagian besar sistem modern seperti Java 7 dan versi lebih baru mendukung mode-mode ini.

Selain itu, permintaan harus ditandatangani menggunakan ID kunci akses dan kunci akses rahasia yang terkait dengan prinsipal IAM. Atau Anda bisa menggunakan [AWS Security Token Service](#) (AWS STS) untuk membuat kredensial keamanan sementara guna menandatangani permintaan.

AWS Security Hub dan titik akhir VPC antarmuka (AWS PrivateLink)

Anda dapat membangun koneksi privat antara VPC Anda dan AWS Security Hub dengan membuat VPC endpoint antarmuka. Titik akhir antarmuka didukung oleh [AWS PrivateLink](#), teknologi yang memungkinkan Anda mengakses Security Hub APIs tanpa gateway internet, perangkat NAT, koneksi VPN, atau koneksi Direct AWS Connect. Instans dalam VPC Anda tidak memerlukan alamat IP publik untuk berkomunikasi dengan Security Hub. APIs Lalu lintas antara VPC Anda dan Security Hub tidak meninggalkan jaringan Amazon.

Setiap titik akhir antarmuka diwakili oleh satu atau beberapa [Antarmuka Jaringan Elastis](#) di subnet Anda. Untuk informasi selengkapnya, lihat [Mengakses titik akhir VPC antarmuka Layanan AWS menggunakan](#) antarmuka di Panduan Amazon Virtual Private Cloud.

Pertimbangan untuk titik akhir VPC Security Hub

[Sebelum Anda menyiapkan VPC endpoint antarmuka untuk Security Hub, pastikan bahwa Anda meninjau prasyarat dan informasi lainnya dalam Panduan Amazon Virtual Private Cloud.](#)

Security Hub mendukung pembuatan panggilan ke semua tindakan API-nya dari VPC Anda.

Membuat VPC endpoint antarmuka untuk Security Hub

Anda dapat membuat VPC endpoint untuk layanan Security Hub menggunakan konsol Amazon VPC atau (). AWS Command Line Interface AWS CLI Untuk informasi selengkapnya, lihat [Membuat VPC endpoint](#) dalam Panduan Amazon Virtual Private Cloud.

Buat VPC endpoint untuk Security Hub menggunakan nama layanan berikut:

`com.amazonaws.region.securityhub`

Di **region** mana kode Wilayah untuk yang berlaku Wilayah AWS.

Jika mengaktifkan DNS privat untuk titik akhir, Anda dapat mengajukan permintaan API ke Security Hub menggunakan nama DNS default untuk Wilayah, misalnya `securityhub.us-east-1.amazonaws.com` untuk Wilayah AS Timur (Virginia).

Membuat kebijakan VPC endpoint untuk Security Hub

Anda dapat melampirkan kebijakan titik akhir ke VPC endpoint yang mengendalikan akses ke Security Hub. Kebijakan titik akhir menentukan informasi berikut:

- Prinsipal yang dapat melakukan tindakan.
- Tindakan yang dapat dilakukan.
- Sumber daya yang menjadi target tindakan.

Untuk informasi selengkapnya, lihat [Mengontrol akses ke titik akhir VPC menggunakan kebijakan titik akhir](#) di Panduan Amazon Virtual Private Cloud.

Contoh: Kebijakan VPC endpoint untuk tindakan Security Hub

Berikut adalah contoh kebijakan titik akhir untuk Security Hub. Jika dilampirkan ke titik akhir, kebijakan ini memberikan akses ke tindakan Security Hub untuk semua yang utama di semua sumber daya.

```
{
  "Statement": [
    {
      "Principal": "*",
      "Effect": "Allow",
      "Action": [
        "securityhub:getFindings",
        "securityhub:getEnabledStandards",
        "securityhub:getInsights"
      ],
      "Resource": "*"
    }
  ]
}
```

Subnet bersama

Anda tidak dapat membuat, mendeskripsikan, memodifikasi, atau menghapus titik akhir VPC di subnet yang dibagikan dengan Anda. Namun, Anda dapat menggunakan titik akhir VPC di subnet yang dibagikan dengan Anda. Untuk informasi tentang berbagi VPC, lihat [Membagikan subnet VPC Anda dengan akun lain di Panduan Amazon Virtual Private Cloud](#).

Pencatatan panggilan API CSPM Security Hub dengan CloudTrail

AWS Security Hub Cloud Security Posture Management (CSPM) terintegrasi dengan AWS CloudTrail, layanan yang menyediakan catatan tindakan yang diambil oleh pengguna, peran, atau AWS layanan di Security Hub CSPM. CloudTrail menangkap panggilan API untuk Security Hub CSPM sebagai peristiwa. Panggilan yang ditangkap termasuk panggilan dari konsol CSPM Security Hub dan panggilan kode ke operasi API CSPM Security Hub. Jika Anda membuat jejak, Anda dapat mengaktifkan pengiriman CloudTrail acara secara terus menerus ke bucket Amazon S3, termasuk peristiwa untuk Security Hub CSPM. Jika Anda tidak mengonfigurasi jejak, Anda masih dapat melihat peristiwa terbaru di CloudTrail konsol dalam Riwayat acara. Dengan menggunakan informasi yang CloudTrail dikumpulkan, Anda dapat menentukan permintaan yang dibuat ke Security Hub CSPM, alamat IP tempat permintaan dibuat, siapa yang membuat permintaan, kapan dibuat, dan detail tambahan.

Untuk mempelajari selengkapnya CloudTrail, termasuk cara mengonfigurasi dan mengaktifkannya, lihat [Panduan AWS CloudTrail Pengguna](#).

Informasi CSPM Security Hub di CloudTrail

CloudTrail diaktifkan pada Akun AWS saat Anda membuat akun. Ketika aktivitas peristiwa yang didukung terjadi di Security Hub CSPM, aktivitas tersebut direkam dalam suatu CloudTrail peristiwa bersama dengan peristiwa AWS layanan lainnya dalam riwayat Acara. Anda dapat melihat, mencari, dan mengunduh peristiwa terbaru di akun. Untuk informasi selengkapnya, lihat [Melihat peristiwa dengan riwayat CloudTrail acara](#).

Untuk catatan peristiwa yang sedang berlangsung di akun Anda, termasuk acara untuk Security Hub CSPM, buat jejak. Jejak memungkinkan CloudTrail untuk mengirimkan file log ke bucket Amazon S3. Secara default, ketika Anda membuat jejak pada konsol tersebut, jejak diterapkan ke semua Wilayah AWS. Jejak mencatat peristiwa dari semua Wilayah di AWS partisi dan mengirimkan file log ke bucket Amazon S3 yang Anda tentukan. Selain itu, Anda dapat mengonfigurasi AWS layanan lain untuk menganalisis lebih lanjut dan menindaklanjuti data peristiwa yang dikumpulkan dalam CloudTrail log. Untuk informasi selengkapnya, lihat berikut:

- [Gambaran umum untuk membuat jejak](#)
- [CloudTrail layanan dan integrasi yang didukung](#)

- [Mengonfigurasi notifikasi Amazon SNS untuk CloudTrail](#)
- [Menerima file CloudTrail log dari beberapa wilayah](#) dan [Menerima file CloudTrail log dari beberapa akun](#)

Security Hub CSPM mendukung pencatatan semua tindakan Security Hub CSPM API sebagai peristiwa dalam log. CloudTrail Untuk melihat daftar operasi CSPM Security Hub, lihat Referensi API [CSPM Security Hub](#).

Saat aktivitas untuk tindakan berikut dicatat CloudTrail, nilai untuk `responseElements` disetel ke `null`. Ini memastikan bahwa informasi sensitif tidak disertakan dalam CloudTrail log.

- `BatchImportFindings`
- `GetFindings`
- `GetInsights`
- `GetMembers`
- `UpdateFindings`

Setiap entri peristiwa atau log berisi informasi tentang entitas yang membuat permintaan tersebut. Informasi identitas membantu Anda menentukan hal berikut ini:

- Apakah permintaan dibuat dengan root atau AWS Identity and Access Management (IAM) kredensial pengguna
- Baik permintaan tersebut dibuat dengan kredensial keamanan sementara untuk peran atau pengguna gabungan
- Apakah permintaan itu dibuat oleh AWS layanan lain

Untuk informasi selengkapnya, lihat [Elemen userIdentity CloudTrail](#).

Contoh: Entri file log CSPM Security Hub

Trail adalah konfigurasi yang memungkinkan pengiriman peristiwa sebagai file log ke bucket Amazon S3 yang Anda tentukan. CloudTrail file log berisi satu atau lebih entri log. Peristiwa mewakili permintaan tunggal dari sumber manapun dan mencakup informasi tentang tindakan yang diminta, tanggal dan waktu tindakan, parameter permintaan, dan sebagainya. CloudTrail file log bukanlah

jejak tumpukan yang diurutkan dari panggilan API publik, jadi file tersebut tidak muncul dalam urutan tertentu.

Contoh berikut menunjukkan entri CloudTrail log yang menunjukkan CreateInsight tindakan. Dalam contoh ini, wawasan yang Test Insight disebut dibuat. ResourceIdAtribut ditetapkan sebagai Grup menurut agregator, dan tidak ada filter opsional untuk wawasan ini yang ditentukan. Untuk informasi selengkapnya tentang wawasan, lihat [Melihat wawasan di Security Hub CSPM](#).

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDAJK6U5DS22IAVUI7BW",
    "arn": "arn:aws:iam::012345678901:user/TestUser",
    "accountId": "012345678901",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "userName": "TestUser"
  },
  "eventTime": "2018-11-25T01:02:18Z",
  "eventSource": "securityhub.amazonaws.com",
  "eventName": "CreateInsight",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "205.251.233.179",
  "userAgent": "aws-cli/1.11.76 Python/2.7.10 Darwin/17.7.0 botocore/1.5.39",
  "requestParameters": {
    "Filters": {},
    "ResultField": "ResourceId",
    "Name": "Test Insight"
  },
  "responseElements": {
    "InsightArn": "arn:aws:securityhub:us-west-2:0123456789010:insight/custom/f4c4890b-ac6b-4c26-95f9-e62cc46f3055"
  },
  "requestID": "c0ffffccd-f04d-11e8-93fc-ddcd14710066",
  "eventID": "3dabcebf-35b0-443f-a1a2-26e186ce23bf",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "recipientAccountId": "012345678901"
}
```


Menandai sumber daya CSPM Security Hub

Tag adalah label opsional yang dapat Anda tentukan dan tetapkan ke AWS sumber daya, termasuk jenis sumber daya AWS Security Hub Cloud Security Posture Management (CSPM) tertentu. Tag dapat membantu Anda mengidentifikasi, mengkategorikan, dan mengelola sumber daya dengan cara yang berbeda, seperti berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Misalnya, Anda dapat menggunakan tag untuk membedakan sumber daya, mengidentifikasi sumber daya yang mendukung persyaratan kepatuhan atau alur kerja tertentu, atau mengalokasikan biaya.

Anda dapat menambahkan tag ke jenis sumber daya CSPM Security Hub berikut:

- Aturan otomatisasi
- Kebijakan konfigurasi
- Sumber daya Hub

Menandai dasar-dasar

Sumber daya dapat memiliki sebanyak 50 tag. Setiap tag terdiri dari kunci tag yang diperlukan dan nilai tag opsional, yang keduanya Anda tentukan. Kunci tag adalah label umum yang bertindak sebagai kategori untuk nilai tag yang lebih spesifik. Nilai tag bertindak sebagai deskriptor untuk kunci tag.

Misalnya, jika Anda membuat aturan otomatisasi yang berbeda untuk lingkungan yang berbeda (satu set aturan otomatisasi untuk akun pengujian dan satu lagi untuk akun produksi), Anda dapat menetapkan kunci `Environment` tag untuk aturan tersebut. Nilai tag terkait mungkin `Test` untuk aturan yang terkait dengan akun pengujian, dan `Prod` untuk aturan yang terkait dengan akun produksi dan OUs.

Saat Anda menentukan dan menetapkan tag ke sumber daya AWS Security Hub Cloud Security Posture Management (CSPM) Security Hub, ingatlah hal berikut:

- Setiap sumber daya dapat memiliki maksimum 50 tag.
- Untuk setiap sumber daya, setiap kunci tag harus unik dan hanya dapat memiliki satu nilai tag.
- Kunci dan nilai tanda peka huruf besar-kecil. Sebagai praktik terbaik, kami menyarankan Anda menentukan strategi untuk memanfaatkan tag dan menerapkan strategi itu secara konsisten di seluruh sumber daya Anda.

- Tombol tag dapat memiliki maksimal 128 karakter UTF-8. Nilai tag dapat memiliki maksimal 256 karakter UTF-8. Karakter dapat berupa huruf, angka, spasi, atau simbol berikut: `_./= + - @`
- `aws` :Awalan dicadangkan untuk digunakan oleh AWS. Anda tidak dapat menggunakannya dalam kunci tag atau nilai apa pun yang Anda tentukan. Selain itu, Anda tidak dapat mengubah atau menghapus kunci tag atau nilai yang menggunakan awalan ini. Tag yang menggunakan awalan ini tidak dihitung terhadap kuota 50 tag per sumber daya.
- Setiap tag yang Anda tetapkan hanya tersedia untuk Anda Akun AWS dan hanya Wilayah AWS di mana Anda menetapkannya.
- Jika Anda menetapkan tag ke sumber daya menggunakan CSPM Security Hub, tag hanya diterapkan ke sumber daya yang disimpan langsung di CSPM Security Hub di yang berlaku. Wilayah AWS Mereka tidak diterapkan pada sumber daya pendukung terkait yang dibuat, digunakan, atau dikelola oleh Security Hub CSPM untuk Anda di tempat lain. Layanan AWS Misalnya, jika Anda menetapkan tag ke aturan otomatisasi yang memperbarui temuan yang terkait dengan Amazon Simple Storage Service (Amazon S3), tag hanya diterapkan ke aturan otomatisasi di CSPM Security Hub untuk Wilayah yang ditentukan. Mereka tidak diterapkan ke ember S3 Anda. Untuk juga menetapkan tag ke sumber daya terkait, Anda dapat menggunakan AWS Resource Groups atau Layanan AWS yang menyimpan sumber daya—misalnya, Amazon S3 untuk bucket S3. Menetapkan tag ke sumber daya terkait dapat membantu Anda mengidentifikasi sumber daya pendukung untuk sumber daya CSPM Security Hub Anda.
- Jika Anda menghapus sumber daya, tag apa pun yang ditetapkan ke sumber daya juga akan dihapus.

 Important

Jangan menyimpan rahasia atau jenis data sensitif lainnya dalam tag. Tag dapat diakses dari banyak orang Layanan AWS, termasuk AWS Manajemen Penagihan dan Biaya. Mereka tidak dimaksudkan untuk digunakan untuk data sensitif.

Untuk menambahkan dan mengelola tag untuk sumber daya CSPM Security Hub, Anda dapat menggunakan konsol CSPM Security Hub, Security Hub CSPM API, atau API Tagging. AWS Resource Groups Dengan Security Hub CSPM, Anda dapat menambahkan tag ke sumber daya saat membuat sumber daya. Anda juga dapat menambahkan dan mengelola tag untuk sumber daya individual yang ada. Dengan Resource Groups, Anda dapat menambahkan dan mengelola tag

secara massal untuk beberapa sumber daya yang ada mencakup beberapa Layanan AWS, termasuk Security Hub CSPM.

Untuk tips penandaan tambahan dan praktik terbaik, lihat [Menandai AWS sumber daya Anda di Panduan Pengguna](#) Tagging AWS Resources.

Menggunakan tag dalam kebijakan IAM

Setelah mulai menandai sumber daya, Anda dapat menentukan izin tingkat sumber daya berbasis tag dalam kebijakan (IAM). AWS Identity and Access Management Dengan menggunakan tag dengan cara ini, Anda dapat menerapkan kontrol terperinci tentang pengguna dan peran mana yang Akun AWS memiliki izin untuk membuat dan menandai sumber daya, dan pengguna dan peran mana yang memiliki izin untuk menambahkan, mengedit, dan menghapus tag secara lebih umum. Untuk mengontrol akses berdasarkan tag, Anda dapat menggunakan [kunci kondisi terkait tag](#) di [elemen Kondisi kebijakan](#) IAM.

Misalnya, Anda dapat membuat kebijakan IAM yang memungkinkan pengguna memiliki akses penuh ke semua sumber daya AWS Security Hub Cloud Security Posture Management (CSPM) Security Hub, jika Owner tag untuk sumber daya menentukan nama pengguna mereka:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ModifyResourceIfOwner",
      "Effect": "Allow",
      "Action": "securityhub:*",
      "Resource": "*",
      "Condition": {
        "StringEqualsIgnoreCase": {"aws:ResourceTag/Owner": "${aws:username}"}
      }
    }
  ]
}
```

Jika Anda menentukan izin tingkat sumber daya berbasis tag, izin akan segera berlaku. Ini berarti bahwa sumber daya Anda lebih aman segera setelah dibuat, dan Anda dapat dengan cepat mulai menerapkan penggunaan tag untuk sumber daya baru. Anda juga dapat menggunakan izin tingkat sumber daya untuk mengontrol kunci dan nilai tag mana yang dapat dikaitkan dengan sumber daya

baru dan yang sudah ada. Untuk informasi selengkapnya, lihat [Mengontrol akses ke AWS sumber daya menggunakan tag](#) di Panduan Pengguna IAM.

Menambahkan tag ke sumber daya CSPM Security Hub

Tag adalah label yang dapat Anda tentukan dan tetapkan ke AWS sumber daya, termasuk jenis sumber daya AWS Security Hub Cloud Security Posture Management (CSPM) tertentu. Dengan menggunakan tag, Anda dapat mengidentifikasi, mengkategorikan, dan mengelola sumber daya dengan cara yang berbeda, seperti berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Misalnya, Anda dapat menggunakan tag untuk: menerapkan kebijakan, mengalokasikan biaya, membedakan antara versi sumber daya, atau mengidentifikasi sumber daya yang mendukung persyaratan kepatuhan atau alur kerja tertentu.

Anda dapat menambahkan tag ke jenis sumber daya CSPM Security Hub berikut:

- Aturan otomatisasi
- Kebijakan konfigurasi
- Sumber daya Hub

Sumber daya dapat memiliki sebanyak 50 tag. Setiap tag terdiri dari kunci tag yang diperlukan dan nilai tag opsional. Kunci tag adalah label umum yang bertindak sebagai kategori untuk nilai tag yang lebih spesifik. Nilai tag bertindak sebagai deskriptor untuk kunci tag. Untuk informasi selengkapnya tentang opsi dan persyaratan penandaan, lihat [Menandai dasar-dasar](#).

Untuk menambahkan tag ke sumber daya CSPM Security Hub, Anda dapat menggunakan konsol CSPM Security Hub atau Security Hub CSPM API. Namun, konsol tidak mendukung penambahan tag ke Hub sumber daya.

Setelah menambahkan tag, Anda dapat mengedit tag dan mengubah kunci tag atau nilai tag.

[Untuk menambahkan atau mengedit tag untuk beberapa sumber daya CSPM Security Hub secara bersamaan, gunakan operasi penandaan API Penandaan.AWS Resource Groups](#)

Important

Menambahkan tag ke sumber daya dapat memengaruhi akses ke sumber daya. Sebelum menambahkan tag ke sumber daya, tinjau kebijakan AWS Identity and Access Management (IAM) apa pun yang mungkin menggunakan tag untuk mengontrol akses ke sumber daya.

Console

Untuk menambahkan tag ke sumber daya CSPM Security Hub (konsol)

Saat Anda membuat aturan otomatisasi atau kebijakan konfigurasi, konsol CSPM Security Hub menyediakan opsi untuk menambahkan tag ke dalamnya. Anda dapat memberikan kunci tag dan nilai tag di bagian Tag.

Security Hub CSPM API

Untuk menambahkan tag ke sumber daya CSPM Security Hub (API)

Untuk membuat sumber daya dan menambahkan satu atau beberapa tag ke dalamnya secara terprogram, gunakan operasi yang sesuai untuk jenis sumber daya yang ingin Anda buat:

- Untuk membuat kebijakan konfigurasi dan menambahkan satu atau beberapa tag ke dalamnya, panggil [CreateConfigurationPolicy](#) API atau, jika Anda menggunakan AWS CLI, jalankan [create-configuration-policy](#) perintah.
- Untuk membuat aturan otomatisasi dan menambahkan satu atau beberapa tag ke dalamnya, panggil [CreateAutomationRule](#) API atau, jika Anda menggunakan AWS CLI, jalankan [create-automation-rule](#) perintah.
- Untuk mengaktifkan CSPM Security Hub dan menambahkan satu atau beberapa tag ke Hub sumber daya Anda, jalankan [EnableSecurityHub](#) API atau, jika Anda menggunakan AWS Command Line Interface (AWS CLI), jalankan perintah [enable-security-hub](#).

Dalam permintaan Anda, gunakan `tags` parameter untuk menentukan kunci tag dan nilai tag opsional untuk setiap tag untuk ditambahkan ke sumber daya. `tagsParameter` menentukan array objek. Setiap objek menentukan kunci tag dan nilai tag yang terkait.

Untuk menambahkan satu atau beberapa tag ke sumber daya yang ada, gunakan [TagResource](#) pengoperasian API CSPM Security Hub atau, jika Anda menggunakan AWS CLI, jalankan perintah [tag-resource](#). Dalam permintaan Anda, tentukan Nama Sumber Daya Amazon (ARN) dari sumber daya yang ingin Anda tambahkan tag. Gunakan `tags` parameter untuk menentukan kunci tag (`key`) dan nilai tag opsional (`value`) untuk setiap tag yang akan ditambahkan. `tagsParameter` menentukan array objek, satu objek untuk setiap kunci tag dan nilai tag terkait.

Misalnya, AWS CLI perintah berikut menambahkan kunci `Environment` tag dengan nilai `Prod` tag ke kebijakan konfigurasi yang ditentukan. Contoh ini diformat untuk Linux, macOS, atau Unix, dan menggunakan karakter garis miring terbalik (`\`) untuk meningkatkan keterbacaan.

Contoh perintah CLI:

```
$ aws securityhub tag-resource \  
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/  
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \  
--tags '{"Environment":"Prod"}'
```

Di mana:

- **resource-arn** menentukan ARN dari kebijakan konfigurasi untuk menambahkan tag ke.
- **Environment** adalah kunci tag untuk ditambahkan ke aturan.
- **Prod** adalah nilai tag untuk kunci tag yang ditentukan (**Environment**).

Dalam contoh berikut, perintah menambahkan beberapa tag ke kebijakan konfigurasi.

```
$ aws securityhub tag-resource \  
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/  
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \  
--tags '{"Environment":"Prod", "CostCenter":"12345", "Owner":"jane-doe"}'
```

Untuk setiap objek dalam tags array, keduanya key dan value argumen diperlukan. Namun, nilai untuk value argumen dapat berupa string kosong. Jika Anda tidak ingin mengaitkan nilai tag dengan kunci tag, jangan tentukan nilai untuk value argumen tersebut. Misalnya, perintah berikut menambahkan kunci Owner tag tanpa nilai tag terkait:

```
$ aws securityhub tag-resource \  
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/  
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \  
--tags '{"Owner":""}'
```

Jika operasi penandaan berhasil, Security Hub CSPM mengembalikan respons HTTP 200 kosong. Jika tidak, Security Hub CSPM mengembalikan respons HTTP 4 xx atau 500 yang menunjukkan mengapa operasi gagal.

Mengedit tag untuk sumber daya CSPM Security Hub

Karena lingkungan atau persyaratan Anda berubah seiring waktu, Anda dapat mengevaluasi tag yang ada untuk sumber daya AWS Security Hub Cloud Security Posture Management (CSPM)

Security Hub dan mengubah tag seperlunya. Tag adalah label yang Anda tentukan dan tetapkan ke satu atau beberapa AWS sumber daya, termasuk jenis sumber daya Macie tertentu. Setiap tag terdiri dari kunci tag yang diperlukan dan nilai tag opsional. Kunci tag adalah label umum yang bertindak sebagai kategori untuk nilai tag yang lebih spesifik. Nilai tag bertindak sebagai deskriptor untuk kunci tag.

Tag dapat membantu Anda mengidentifikasi, mengkategorikan, dan mengelola sumber daya dengan cara yang berbeda, seperti berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Misalnya, Anda dapat menggunakan tag untuk: menerapkan kebijakan, mengalokasikan biaya, membedakan antara versi sumber daya, atau mengidentifikasi sumber daya yang mendukung persyaratan kepatuhan atau alur kerja tertentu.

Anda dapat menambahkan tag ke jenis sumber daya CSPM Security Hub berikut:

- Aturan otomatisasi
- Kebijakan konfigurasi
- Sumber daya Hub

Untuk mengedit kunci tag atau nilai tag untuk sumber daya CSPM Security Hub, Anda dapat menggunakan Security Hub CSPM API. Konsol CSPM Security Hub saat ini tidak mendukung pengeditan tag.

Important

Mengedit tag untuk sumber daya dapat memengaruhi akses ke sumber daya. Sebelum Anda mengedit tag untuk sumber daya, tinjau kebijakan AWS Identity and Access Management (IAM) apa pun yang mungkin menggunakan tag untuk mengontrol akses ke sumber daya.

Security Hub CSPM API

Untuk mengedit tag untuk sumber daya CSPM Security Hub (API)

Saat Anda mengedit tag untuk sumber daya secara terprogram, Anda menerima tag yang ada dengan nilai baru. Oleh karena itu, cara terbaik untuk mengedit tag tergantung pada apakah Anda ingin mengedit kunci tag, nilai tag, atau keduanya. Untuk mengedit kunci tag, [hapus tag saat ini](#) dan [tambahkan tag baru](#).

Untuk mengedit atau menghapus hanya nilai tag yang terkait dengan kunci tag, timpa nilai yang ada dengan menggunakan [TagResource](#) pengoperasian Security Hub CSPM API. Jika Anda menggunakan AWS CLI, jalankan perintah [tag-resource](#). Dalam permintaan Anda, tentukan Nama Sumber Daya Amazon (ARN) sumber daya yang nilai tagnya ingin Anda edit atau hapus.

Untuk mengedit nilai tag, gunakan `tags` parameter untuk menentukan kunci tag yang nilai tag yang ingin Anda ubah. Anda juga harus menentukan nilai tag baru untuk kunci tersebut. Misalnya, AWS CLI perintah berikut mengubah nilai tag dari `Prod` menjadi kunci `Test Environment` tag yang ditetapkan ke aturan otomatisasi yang ditentukan. Contoh ini diformat untuk Linux, macOS, atau Unix, dan menggunakan karakter garis miring terbalik (`\`) untuk meningkatkan keterbacaan.

```
$ aws securityhub tag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tags '{"Environment":"Test"}'
```

Di mana:

- `resource-arn` menentukan ARN dari kebijakan konfigurasi.
- `Environment` adalah kunci tag yang terkait dengan nilai tag yang akan diubah.
- `Test` adalah nilai tag baru untuk kunci tag yang ditentukan (`Environment`).

Untuk menghapus nilai tag dari kunci tag, jangan tentukan nilai untuk `value` argumen kunci dalam `tags` parameter. Misalnya:

```
$ aws securityhub tag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tags '{"Owner":""}'
```

Jika operasi berhasil, Security Hub CSPM mengembalikan respons HTTP 200 kosong. Jika tidak, Security Hub CSPM mengembalikan respons HTTP 4 xx atau 500 yang menunjukkan mengapa operasi gagal.

Meninjau tag untuk sumber daya CSPM Security Hub

Setelah menambahkan atau mengedit tag untuk sumber daya AWS Security Hub Cloud Security Posture Management (CSPM) Security Hub, Anda dapat melihat kunci tag dan nilai tag yang dimiliki

sumber daya saat ini. Tag adalah label yang Anda tentukan dan tetapkan ke satu atau beberapa AWS sumber daya, termasuk jenis sumber daya Macie tertentu. Setiap tag terdiri dari kunci tag yang diperlukan dan nilai tag opsional. Kunci tag adalah label umum yang bertindak sebagai kategori untuk nilai tag yang lebih spesifik. Nilai tag bertindak sebagai deskriptor untuk kunci tag.

Tag dapat membantu Anda mengidentifikasi, mengkategorikan, dan mengelola sumber daya dengan cara yang berbeda, seperti berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Misalnya, Anda dapat menggunakan tag untuk: menerapkan kebijakan, mengalokasikan biaya, membedakan antara versi sumber daya, atau mengidentifikasi sumber daya yang mendukung persyaratan kepatuhan atau alur kerja tertentu.

Anda dapat menambahkan tag ke jenis sumber daya CSPM Security Hub berikut:

- Aturan otomatisasi
- Kebijakan konfigurasi
- Sumber daya Hub

Anda dapat meninjau tag untuk aturan otomatisasi CSPM Security Hub atau kebijakan konfigurasi dengan menggunakan konsol CSPM Security Hub atau Security Hub CSPM API. Konsol tidak mendukung tag peninjauan untuk Hub sumber daya. Secara terprogram, Anda dapat meninjau tag untuk sumber daya apa pun.

[Untuk meninjau tag untuk beberapa sumber daya CSPM Security Hub secara bersamaan, gunakan operasi penandaan API Penandaan.AWS Resource Groups](#)

Console

Untuk meninjau tag untuk sumber daya CSPM Security Hub (konsol)

1. Menggunakan kredensi administrator CSPM Security Hub, buka konsol Security Hub AWS Cloud Security Posture Management (CSPM) di <https://console.aws.amazon.com/securityhub/>
2. Bergantung pada jenis sumber daya yang ingin Anda tambahkan tag, lakukan salah satu hal berikut:
 - Untuk meninjau tag untuk aturan otomatisasi, pilih Otomasi di panel navigasi. Kemudian, pilih aturan otomatisasi.

- Untuk meninjau tag untuk kebijakan konfigurasi, pilih Konfigurasi di panel navigasi. Kemudian, pada tab Kebijakan, pilih opsi di sebelah kebijakan konfigurasi. Panel samping terbuka yang menunjukkan jumlah tag yang ditetapkan ke kebijakan. Anda dapat memperluas header Tag untuk melihat kunci tag dan nilai tag.

Bagian Tag mencantumkan semua tag yang saat ini ditetapkan ke sumber daya.

Security Hub CSPM API

Untuk meninjau tag untuk sumber daya CSPM Security Hub (API)

Untuk mengambil dan meninjau tag untuk sumber daya yang ada, panggil API.

[ListTagsForResource](#) Dalam permintaan Anda, gunakan `resourceArn` parameter untuk menentukan Nama Sumber Daya Amazon (ARN) sumber daya.

Jika Anda menggunakan AWS CLI, jalankan [list-tags-for-resource](#) perintah dan gunakan `resource-arn` parameter untuk menentukan ARN sumber daya. Misalnya:

```
$ aws securityhub list-tags-for-resource --resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Jika operasi berhasil, Security Hub CSPM mengembalikan array. `tags` Setiap objek dalam array menentukan tag (baik kunci tag dan nilai tag) yang saat ini ditetapkan ke sumber daya. Misalnya:

```
{
  "tags": [
    {
      "key": "Environment",
      "value": "Prod"
    },
    {
      "key": "CostCenter",
      "value": "12345"
    },
    {
      "key": "Owner",
      "value": ""
    }
  ]
}
```

Di mana `EnvironmentCostCenter`, dan `Owner` merupakan kunci tag yang ditetapkan ke sumber daya. `Prod` adalah nilai tag yang terkait dengan kunci `Environment` tag. `12345` adalah nilai tag yang terkait dengan kunci `CostCenter` tag. Kunci `Owner` tag tidak memiliki nilai tag terkait.

Untuk mengambil daftar semua sumber daya CSPM Security Hub yang memiliki tag dan semua tag yang ditetapkan ke masing-masing sumber daya tersebut, gunakan [GetResources](#) pengoperasian API Tagging. AWS Resource Groups Dalam permintaan Anda, tetapkan nilai untuk `ResourceTypeFilters` parameter `kesecurityhub`. Untuk melakukan ini menggunakan AWS CLI, jalankan perintah [get-resources](#) dan atur nilai untuk `resource-type-filters` parameter ke. `securityhub` Misalnya:

```
$ aws resourcegroupstaggingapi get-resources --resource-type-filters "securityhub"
```

Jika operasi berhasil, Resource Groups mengembalikan `ResourceTagMappingList` array. Array berisi satu objek untuk setiap sumber daya CSPM Security Hub yang memiliki tag. Setiap objek menentukan ARN sumber daya CSPM Security Hub, dan kunci tag serta nilai yang ditetapkan ke sumber daya.

Menghapus tag dari sumber daya CSPM Security Hub

Jika Anda menambahkan tag ke sumber daya AWS Security Hub Cloud Security Posture Management (CSPM) Security Hub, Anda selanjutnya dapat menghapus satu atau beberapa tag. Tag adalah label yang Anda tentukan dan tetapkan ke AWS sumber daya, termasuk jenis sumber daya CSPM Security Hub tertentu. Anda dapat menambahkan, mengedit, dan menghapus tag dari jenis sumber daya CSPM Security Hub berikut: aturan otomatisasi, kebijakan konfigurasi, dan sumber daya. Hub

Untuk menghapus tag dari sumber daya AWS Security Hub Cloud Security Posture Management (CSPM) individual, Anda dapat menggunakan Security Hub CSPM API. Konsol CSPM Security Hub saat ini tidak mendukung penghapusan tag.

[Untuk menghapus tag dari beberapa sumber daya CSPM Security Hub secara bersamaan, gunakan operasi penandaan API Penandaan.AWS Resource Groups](#)

⚠ Important

Menghapus tag dari sumber daya dapat memengaruhi akses ke sumber daya. Sebelum Anda menghapus tag, tinjau kebijakan AWS Identity and Access Management (IAM) apa pun yang mungkin menggunakan tag untuk mengontrol akses ke sumber daya.

Security Hub CSPM API

Untuk menghapus tag dari sumber daya CSPM Security Hub (API)

Untuk menghapus satu atau beberapa tag dari sumber daya secara terprogram, gunakan [UntagResource](#) pengoperasian Security Hub CSPM API. Dalam permintaan Anda, gunakan `resourceArn` parameter untuk menentukan Nama Sumber Daya Amazon (ARN) sumber daya untuk menghapus tag. Gunakan `tagKeys` parameter untuk menentukan kunci tag tag yang akan dihapus. Untuk menghapus beberapa tag, tambahkan `tagKeys` parameter dan argumen untuk setiap tag yang akan dihapus, dipisahkan oleh ampersand (&) —misalnya, `tagKeys=key1&tagKeys=key2` Untuk menghapus hanya nilai tag tertentu (bukan kunci tag) dari sumber daya, [edit tag](#) alih-alih menghapus tag.

Jika Anda menggunakan AWS CLI, jalankan perintah [untag-resource](#) untuk menghapus satu atau beberapa tag dari sumber daya. Untuk `resource-arn` parameter, tentukan ARN sumber daya untuk menghapus tag dari. Gunakan `tag-keys` parameter untuk menentukan kunci tag tag yang akan dihapus. Misalnya, perintah berikut menghapus `Environment` tag (kunci tag dan nilai tag) dari kebijakan konfigurasi yang ditentukan:

```
$ aws securityhub untag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tag-keys Environment
```

Di mana `resource-arn` menentukan ARN dari kebijakan konfigurasi untuk menghapus tag dari, `Environment` dan merupakan kunci tag tag untuk dihapus.

Untuk menghapus beberapa tag dari sumber daya, tambahkan setiap kunci tag tambahan sebagai argumen untuk `tag-keys` parameter. Misalnya:

```
$ aws securityhub untag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
```

```
--tag-keys Environment Owner
```

Jika operasi berhasil, Security Hub CSPM mengembalikan respons HTTP 200 kosong. Jika tidak, Security Hub CSPM mengembalikan respons HTTP 4 xx atau 500 yang menunjukkan mengapa operasi gagal.

Kuota untuk Security Hub CSPM

Anda Akun AWS memiliki kuota default tertentu, sebelumnya disebut sebagai batas, untuk masing-masing. Layanan AWS Kuota ini merupakan jumlah maksimum layanan sumber daya atau operasi untuk akun Anda. Topik ini menautkan ke kuota yang berlaku untuk sumber daya dan operasi AWS Security Hub Cloud Security Posture Management (CSPM) Security Hub untuk akun Anda. Kecuali sebaliknya dinyatakan lain, setiap kuota berlaku untuk akun Anda di setiap Wilayah AWS.

Beberapa kuota dapat ditingkatkan, sementara yang lain tidak bisa. Untuk meminta peningkatan kuota, gunakan [konsol Service Quotas](#). Untuk mempelajari selengkapnya cara menyampaikan permintaan kenaikan kuota, lihat [Meminta kenaikan kuota](#) dalam Panduan Pengguna Service Quotas. Jika kuota tidak tersedia di konsol Service Quotas, gunakan formulir [peningkatan batas layanan](#) untuk meminta kenaikan kuota. AWS Support Center Console

Kuota maksimum

Untuk daftar kuota yang berlaku untuk sumber daya CSPM Security Hub, lihat titik [akhir dan kuota AWS Security Hub Cloud Security Posture Management \(CSPM\) Security Hub](#) di. Referensi Umum AWS

Nilai kuota

Untuk daftar kuota yang berlaku untuk operasi API CSPM Security Hub, lihat Referensi API [AWS Security Hub Cloud Security Posture Management \(CSPM\) Security Hub](#).

Jika Anda menyiapkan [agregasi Lintas wilayah di CSPM Security Hub](#), satu panggilan ke BatchImportFindings dan BatchUpdateFindings berdampak pada Wilayah yang ditautkan dan Wilayah agregasi. GetFindingsOperasi mengambil temuan dari Wilayah terkait dan Wilayah agregasi. Namun, BatchEnableStandards dan UpdateStandardsControl operasinya spesifik Wilayah.

Riwayat dokumen untuk Panduan Pengguna AWS Security Hub

Tabel berikut menjelaskan perubahan penting pada dokumentasi sejak rilis terakhir AWS Security Hub dan Security Hub CSPM. Untuk rilis kontrol keamanan CSPM baru, tanggal menentukan kapan kontrol mulai tersedia di didukung. Wilayah AWS Diperlukan waktu 1-2 minggu agar kontrol tersedia di semua Wilayah yang didukung.

Untuk pemberitahuan tentang pembaruan Panduan Pengguna AWS Security Hub, Anda dapat berlangganan umpan RSS.

Perubahan	Deskripsi	Tanggal
Pembaruan untuk menemukan retensi	Security Hub CSPM sekarang menyimpan temuan yang diarsipkan selama 30 hari, bukan 90 hari, yang dapat mengurangi kebisingan temuan. Untuk retensi jangka panjang, Anda dapat mengekspor temuan ke bucket S3 dengan menggunakan tindakan kustom dengan aturan Amazon . EventBridge	Juni 20, 2025
Memperbarui ke kebijakan terkelola yang ada	Security Hub CSPM menambahkan izin baru ke. <code>AWSecurityHubOrganizationsAccess</code> Izin ini memungkinkan manajemen organisasi untuk mengaktifkan dan mengelola Security Hub dan Security Hub CSPM dalam suatu organisasi.	Juni 17, 2025

Memperbarui ke kebijakan terkelola yang ada	Security Hub CSPM menambahkan izin baru ke. <code>AWSecurityHubFullAccess</code> Izin ini memungkinkan kepala sekolah untuk membuat peran terkait layanan untuk Security Hub.	Juni 17, 2025
Rilis pratinjau publik dari AWS Security Hub	Rilis pratinjau publik yang diterbitkan dari Panduan Pengguna AWS Security Hub .	Juni 17, 2025
Kebijakan terkelola baru untuk Security Hub	Kebijakan terkelola baru <code>AWSecurityHubV2ServiceRolePolicy</code> , memungkinkan Security Hub mengelola AWS Config aturan dan sumber daya Security Hub di organisasi pelanggan dan atas nama pelanggan . Security Hub dalam rilis pratinjau dan dapat berubah sewaktu-waktu.	Juni 17, 2025

[Pembaruan untuk standar keamanan dan kontrol](#)

Kami menghapus [kontrol IAM.10](#) dari standar [PCI DSS v4.0.1](#). Kontrol ini memeriksa apakah kebijakan kata sandi akun untuk pengguna IAM memenuhi persyaratan minimum, termasuk panjang kata sandi minimum 7 karakter. PCI DSS v4.0.1 sekarang membutuhkan kata sandi untuk memiliki minimal 8 karakter. Kontrol IAM.10 terus berlaku untuk standar PCI DSS v3.2.1, yang memiliki persyaratan kata sandi yang berbeda.

30 Mei 2025

[Standar keamanan baru](#)

Security Hub CSPM sekarang menyediakan [standar keamanan](#) yang selaras dengan kerangka kerja keamanan siber dan kepatuhan NIST SP 800-171 Revisi 2. Standar baru ini mencakup lebih dari 60 kontrol keamanan yang ada. Kontrol melakukan pemeriksaan otomatis yang mengevaluasi sumber daya tertentu Layanan AWS dan untuk kepatuhan dengan subset dari persyaratan yang ditentukan oleh kerangka kerja.

29 Mei 2025

[Pembaruan untuk kontrol keamanan](#)

Security Hub CSPM mengembalikan rilis kontrol berikut secara keseluruhan an Wilayah AWS: [RDS.46] Instans RDS DB tidak boleh digunakan di subnet publik dengan rute ke gateway internet. Sebelumnya, kontrol ini mendukung standar AWS Foundational Security Best Practices (FSBP).

8 Mei 2025

[Kontrol keamanan baru](#)

Security Hub CSPM merilis 9 kontrol baru. Sebagian besar kontrol mendukung standar [Praktik Terbaik Keamanan AWS Dasar \(FSBP\)](#). Beberapa kontrol mendukung persyaratan [NIST SP 800-53 Rev. 5](#).

7 Mei 2025

- [Untuk standar AWS FSBP, IDs untuk kontrol yang berlaku adalah: DocumentDb.6, RDS.44, RedshiftServerless.2, .3, .5, .6, dan .7. RedshiftServerless](#)
- [Untuk NIST SP 800-53 Rev. 5, IDs untuk kontrol yang berlaku adalah: CloudTrail.10, .4, RedshiftServerless dan .7. RedshiftServerless](#)

Kontrol keamanan baru

Security Hub CSPM dirilis 24 April 16, 2025

kontrol baru. Sebagian besar kontrol mendukung standar [AWS Foundational Security Best Practices \(FSBP\)](#) atau [AWS Resource Tagging](#). Beberapa kontrol mendukung persyaratan [NIST SP 800-53 Rev. 5](#).

- [Untuk standar AWS FSBP, IDs untuk kontrol yang berlaku adalah: EC2.173, RDS.41, RDS.42, dan .8. SageMaker](#)
- [Untuk standar Penandaan AWS Sumber Daya, IDs untuk kontrol yang berlaku adalah: Amplify.1, Amplify.2, Batch.4, .2, .174, EC2 .175, .176, .177, .178, DataSync EC2 .179, Redshift.17, EC2 .6, .7, SSM.5, Transfer.4, EC2Transfer.5, EC2 EC2 SageMaker SageMaker <https://docs.aws.amazon.com/securityhub/latest/userguide/transfer-controls.html#transfer-6>Transfer.6, dan Transfer.7.](#)
- [Untuk NIST SP 800-53 Rev. 5, IDs untuk kontrol yang berlaku adalah: ECS.17 dan RDS.42.](#)

Kontrol keamanan baru

Security Hub CSPM merilis empat kontrol baru untuk standar [AWS Praktik Terbaik Keamanan Dasar](#). Kontrolnya adalah:

Maret 18, 2025

- [the section called “\[FSx.3\] FSx untuk sistem file OpenZFS harus dikonfigurasi untuk penyebaran Multi-AZ”](#)
- [the section called “\[FSx.4\] FSx untuk sistem file NetApp ONTAP harus dikonfigurasi untuk penyebaran Multi-AZ”](#)
- [the section called “\[FSx.5\] FSx untuk sistem file Windows File Server harus dikonfigurasi untuk penyebaran Multi-AZ”](#)
- [the section called “\[RedshiftServerless.1\] Grup kerja Amazon Redshift Tanpa Server harus menggunakan perutean VPC yang disempurnakan”](#)

[Pembaruan untuk standar keamanan dan kontrol](#)

Kami menghapus [kontrol keamanan RDS.18](#) dari [standar Praktik Terbaik Keamanan](#) AWS Dasar dan pemeriksaan otomatis untuk persyaratan NIST SP 800-53 Rev. 5. Sejak jaringan Amazon EC2 -Classic dihentikan, instans Amazon Relational Database Service (Amazon RDS) tidak dapat lagi digunakan di luar VPC. Kontrol terus menjadi bagian dari standar yang [AWS Control Tower dikelola layanan](#).

7 Maret 2025

[Pembaruan untuk mengontrol temuan](#)

Security Hub CSPM sekarang menghasilkan WARNING temuan untuk kontrol yang diaktifkan jika [perekaman sumber daya](#) tidak diaktifkan AWS Config untuk jenis sumber daya yang diperiksa kontrol. Ini dapat membantu Anda mengidentifikasi dan mengatasi potensi kesenjangan konfigurasi dalam pemeriksaan kontrol keamanan Anda.

Februari 25, 2025

Kontrol keamanan baru

Security Hub CSPM merilis 11 kontrol baru. Kontrolnya adalah:

Februari 24, 2025

- [the section called “\[Connect .2\] Instans Amazon Connect seharusnya mengaktifkan logging CloudWatch ”](#)
- [the section called “\[ECR.5\] Repositori ECR harus dienkripsi dengan pelanggan yang dikelola AWS KMS keys”](#)
- [the section called “\[ELB.17\] Aplikasi dan Penyeimbangan Beban Jaringan dengan pendengar harus menggunakan kebijakan keamanan yang direkomendasikan”](#)
- [the section called “\[Glue.4\] Pekerjaan AWS Glue percikan harus berjalan pada versi yang didukung AWS Glue”](#)
- [the section called “\[GuardDuty.11\] GuardDuty Runtime Monitoring harus diaktifkan”](#)
- [the section called “\[GuardDuty.12\] GuardDuty ECS Runtime Monitoring harus diaktifkan”](#)
- [the section called “\[GuardDuty.13\] GuardDuty EC2](#)

Runtime Monitoring harus diaktifkan”

- the section called “[Network Firewall.10] Firewall Jaringan harus mengaktifkan perlindungan perubahan subnet”
- the section called “[RDS.40] RDS untuk instance SQL Server DB harus menerbitkan log ke Log CloudWatch ”
- the section called “[SQS.3] Kebijakan akses antrian SQS seharusnya tidak mengizinkan akses publik”
- the section called “[Transfer.3] Konektor Transfer Family seharusnya mengaktifkan logging”

Kontrol keamanan baru

Security Hub CSPM merilis 37 kontrol baru untuk Standar [Penandaan AWS Sumber Daya](#). Security Hub CSPM juga merilis kontrol baru berikut:

Januari 22, 2025

- [the section called “\[EMR.3\] Konfigurasi keamanan Amazon EMR harus dienkripsi saat istirahat”](#)
- [the section called “\[EMR.4\] Konfigurasi keamanan Amazon EMR harus dienkripsi saat transit”](#)
- [the section called “\[SageMaker.5\] SageMaker model harus memblokir lalu lintas masuk”](#)

Kontrol keamanan baru

Security Hub CSPM merilis [EC2.172 Pengaturan Akses Publik Blok EC2 VPC harus memblokir lalu lintas gateway internet](#).

Januari 15, 2025

[Kontrol keamanan baru](#)

Kontrol CSPM Security Hub baru berikut ini tersedia.

Desember 17, 2024

- [the section called “\[Cognito.1\] Kumpulan pengguna Cognito harus mengaktifkan perlindungan ancaman dengan mode penegakan fungsi penuh untuk otentikasi standar”](#)
- [the section called “\[RDS.38\] RDS untuk instance PostgreSQL DB harus dienkripsi saat transit”](#)
- [the section called “\[RDS.39\] RDS untuk instance MySQL DB harus dienkripsi saat transit”](#)
- [the section called “\[Redshift.16\] Grup subnet cluster Redshift harus memiliki subnet dari beberapa Availability Zone”](#)

[Security Hub CSPM mendukung PCI DSS v4.0.1](#)

Security Hub CSPM sekarang mendukung v4.0.1 dari Payment Card Industry Data Security Standard (PCI DSS). Untuk informasi selengkapnya tentang standar dan kontrol yang berlaku padanya, lihat [PCI DSS di Security Hub CSPM](#).

Desember 11, 2024

[Security Hub CSPM menerima temuan urutan GuardDuty serangan](#)

Security Hub CSPM sekarang menerima temuan urutan serangan dari Amazon GuardDuty Extended Threat Detection. Detail pencarian urutan serangan tersedia di objek [Deteksi](#) dari AWS Security Finding Format (ASFF).

Desember 1, 2024

[Security Hub CSPM didukung di baru Wilayah AWS](#)

Security Hub CSPM sekarang tersedia di Wilayah Asia Pasifik (Malaysia). Beberapa kontrol keamanan memiliki batasan Regional. Untuk daftar kontrol yang tidak tersedia di Wilayah ini, lihat [Batas Regional pada kontrol CSPM Security Hub](#).

November 22, 2024

[Perubahan pada Config.1](#)

Security Hub CSPM meningkatkan tingkat keparahan kontrol Config.1 dari MEDIUM keCRITICAL, dan menambahkan kode status baru dan alasan status untuk temuan Config.1 yang gagal. Untuk informasi selengkapnya tentang perubahan, lihat entri untuk 20 November 2024 di [log Perubahan untuk kontrol CSPM Security Hub](#).

November 20, 2024

Kontrol keamanan baru

Kontrol CSPM Security Hub

November 15, 2024

baru berikut ini tersedia.

Kontrol ini merupakan bagian dari Praktik Terbaik Keamanan AWS Dasar dan NIST SP 800-53 Rev. 5, dan mereka mengevaluasi apakah cloud pribadi virtual (VPC) yang Anda kelola memiliki titik akhir VPC antarmuka untuk sumber daya atau sumber daya. Layanan AWS AWS

- [the section called “\[EC2.55\] VPCs harus dikonfigurasi dengan titik akhir antarmuka untuk ECR API”](#)
- [the section called “\[EC2.56\] VPCs harus dikonfigurasi dengan titik akhir antarmuka untuk Docker Registry”](#)
- [the section called “\[EC2.57\] VPCs harus dikonfigurasi dengan titik akhir antarmuka untuk Systems Manager”](#)
- [the section called “\[EC2.58\] VPCs harus dikonfigurasi dengan titik akhir antarmuka untuk Kontak Manajer Insiden Systems Manager”](#)
- [the section called “\[EC2.60\] VPCs harus dikonfigurasi dengan titik akhir antarmuka untuk Systems Manager Incident Manager”](#)

Kontrol keamanan baru

Kontrol CSPM Security Hub baru berikut ini tersedia.

Oktober 18, 2024

- [the section called “\[AppSync .1\] Cache AWS AppSync API harus dienkripsi saat istirahat”](#)
- [the section called “\[AppSync .6\] Cache AWS AppSync API harus dienkripsi saat transit”](#)
- [the section called “\[EC2.170\] templat EC2 peluncuran harus menggunakan Layanan Metadata Instance Versi 2 \(\) IMDSv2”](#)
- [the section called “\[EC2.171\] Koneksi EC2 VPN seharusnya mengaktifkan logging”](#)
- [the section called “\[EFS.8\] Sistem file EFS harus dienkripsi saat istirahat”](#)
- [the section called “\[KMS.5\] Kunci KMS tidak boleh diakses publik”](#)
- [the section called “\[SNS.4\] Kebijakan akses topik SNS seharusnya tidak mengizinkan akses publik”](#)

Kontrol keamanan baru

Kontrol CSPM Security Hub baru berikut ini tersedia.

Oktober 3, 2024

- the section called “[ECS.16] Set tugas ECS seharusnya tidak secara otomatis menetapkan alamat IP publik”
- the section called “[GuardDuty.7] GuardDuty EKS Runtime Monitoring harus diaktifkan”
- the section called “[Kinesis.3] Aliran kinesis harus memiliki periode retensi data yang memadai”
- the section called “[MSK.3] Konektor MSK Connect harus dienkripsi saat transit”
- the section called “[RDS.36] RDS untuk instance PostgreSQL DB harus menerbitkan log ke Log CloudWatch ”
- the section called “[RDS.37] Cluster Aurora PostgreSQL DB harus menerbitkan log ke Log CloudWatch ”
- the section called “[S3.24] Poin Akses Multi-Wilayah S3 harus mengaktifkan pengaturan akses publik blok”

Kontrol keamanan baru

Kontrol CSPM Security Hub baru berikut ini tersedia.

Agustus 30, 2024

- [the section called “\[Athena.4\] Kelompok kerja Athena seharusnya mengaktifkan logging”](#)
- [the section called “\[CodeBuild.7\] ekspor kelompok CodeBuild laporan harus dienkripsi saat istirahat”](#)
- [the section called “\[DataSync.1\] DataSync tugas harus mengaktifkan logging”](#)
- [the section called “\[EFS.7\] Sistem file EFS harus mengaktifkan pencadangan otomatis”](#)
- Lem. 2 (pensiun)
- [the section called “\[Glue.3\] transformasi pembelajaran AWS Glue mesin harus dienkripsi saat istirahat”](#)
- [the section called “\[WorkSpaces.1\] volume WorkSpaces pengguna harus dienkripsi saat istirahat”](#)
- [the section called “\[WorkSpaces.2\] volume Workspace root harus dienkripsi saat istirahat”](#)

[Panel temuan baru](#)

[Panel temuan baru](#) di konsol CSPM Security Hub membantu Anda dengan cepat mengambil tindakan atas temuan, meninjau detail sumber daya dan menemukan riwayat, dan menemukan informasi terkait lainnya tentang temuan.

Agustus 16, 2024

[Perbarui ke kontrol Config.1](#)

[Kontrol Config.1](#) memeriksa apakah AWS Config diaktifkan, menggunakan peran terkait layanan, dan merekam sumber daya untuk kontrol yang diaktifkan. Security Hub CSPM menambahkan parameter kontrol kustom bernama `includeConfigServiceLinkedRoleCheck`. Dengan menyetel parameter ini `false`, Anda dapat memilih untuk tidak memeriksa apakah AWS Config menggunakan peran terkait layanan.

Agustus 15, 2024

[Tentukan Wilayah asal tanpa Wilayah yang terhubung](#)

Anda sekarang dapat membuat agregator temuan dan membangun Wilayah rumah tanpa menghubungkan apa pun Wilayah AWS ke Wilayah asal. Ini memungkinkan Anda mengaktifkan [konfigurasi pusat](#) tanpa menentukan Wilayah yang ditautkan.

Juli 25, 2024

Pilih kontrol yang tersedia di lebih banyak Wilayah

Kontrol berikut sekarang tersedia dalam tambahan Wilayah AWS, termasuk US East (Virginia N.) dan US East (Ohio).

Juli 15, 2024

- the section called “[DataFirehose.1] Aliran pengirim n Firehose harus dienkrpsi saat istirahat”
- the section called “[DMS.10] Titik akhir DMS untuk database Neptunus harus mengaktifkan otorisasi IAM”
- the section called “[DMS.11] Titik akhir DMS untuk MongoDB harus mengaktifkan mekanisme otentikasi”
- the section called “[DMS.12] Titik akhir DMS untuk Redis OSS seharusnya mengaktifkan TLS”
- the section called “[DynamoDB.7] Cluster DynamoDB Accelerator harus dienkrpsi saat transit”
- the section called “[EFS.6] Target pemasangan EFS tidak boleh dikaitkan dengan subnet publik”
- the section called “[EKS.3] Kluster EKS harus menggunakan rahasia Kubernetes terenkrpsi”

- [the section called “\[FSx.2\] FSx untuk sistem file Lustre harus dikonfigurasi untuk menyalin tag ke cadangan”](#)
- [the section called “\[MQ.2\] Broker ActiveMQ harus mengalirkan log audit ke CloudWatch”](#)
- [the section called “\[MQ.3\] Broker Amazon MQ harus mengaktifkan peningkatan versi minor otomatis”](#)
- [the section called “\[Opensearch.11\] OpenSearch domain harus memiliki setidaknya tiga node primer khusus”](#)
- [the section called “\[Redshift.15\] Grup keamanan Redshift harus mengizinkan masuknya port cluster hanya dari asal yang dibatasi”](#)
- [the section called “\[SageMaker.4\] varian produksi SageMaker titik akhir harus memiliki jumlah instance awal yang lebih besar dari 1”](#)
- [the section called “\[ServiceCatalog.1\] Portofolio Service Catalog harus dibagikan hanya dalam suatu organisasi AWS”](#)
- [the section called “\[Transfer.2\] Server Transfer Family](#)

tidak boleh menggunakan
protokol FTP untuk koneksi
titik akhir”

Kontrol keamanan baru

Kontrol CSPM Security Hub baru berikut ini tersedia:

Juli 11, 2024

- [the section called “\[GuardDuty.5\] Pemantauan Log Audit GuardDuty EKS harus diaktifkan”](#)
- [the section called “\[GuardDuty.6\] Perlindungan GuardDuty Lambda harus diaktifkan”](#)
- [the section called “\[GuardDuty.8\] Perlindungan GuardDuty Malware untuk EC2 harus diaktifkan”](#)
- [the section called “\[GuardDuty.9\] Perlindungan GuardDuty RDS harus diaktifkan”](#)
- [the section called “\[GuardDuty.10\] Perlindungan GuardDuty S3 harus diaktifkan”](#)
- [the section called “\[Inspector.1\] Pemindaian Amazon Inspector harus diaktifkan EC2 ”](#)
- [the section called “\[Inspector.2\] Pemindaian ECR Amazon Inspector harus diaktifkan”](#)
- [the section called “\[Inspector.3\] Pemindaian kode Amazon Inspector Lambda harus diaktifkan”](#)

- [the section called “\[Inspekt or.4\] Pemindaian standar Amazon Inspector Lambda harus diaktifkan”](#)

Rilis Tolok Ukur AWS Yayasan CIS v3.0.0

Security Hub CSPM merilis [Center for Internet Security \(CIS\) AWS Foundations Benchmark v3.0.0](#). Rilis ini mencakup kontrol baru berikut, serta pemetaan ke beberapa kontrol yang ada.

13 Mei 2024

- [the section called “\[EC2.53\] grup EC2 keamanan seharusnya tidak mengizinkan masuknya dari 0.0.0.0/0 ke port administrasi server jarak jauh”](#)
- [the section called “\[EC2.54\] grup EC2 keamanan tidak boleh mengizinkan masuknya dari :/0 ke port administrasi server jarak jauh”](#)
- [the section called “\[IAM.26\] Sertifikat SSL/TLS kedaluwarsa yang dikelola di IAM harus dihapus”](#)
- [the section called “\[IAM.27\] Identitas IAM seharusnya tidak memiliki kebijakan yang dilampirkan AWSCloud ShellFullAccess ”](#)
- [the section called “\[IAM.28\] IAM Access Analyzer penganalisis akses eksternal harus diaktifkan”](#)
- [the section called “\[S3.22\] Bucket tujuan umum S3](#)

harus mencatat peristiwa
penulisan tingkat objek”

- the section called “[S3.23]
Bucket tujuan umum S3
harus mencatat peristiwa
pembacaan tingkat objek”

Kontrol keamanan baru

Kontrol CSPM Security Hub baru berikut ini tersedia:

3 Mei 2024

- [the section called “\[DataFirehose.1\] Aliran pengirim n Firehose harus dienkripsi saat istirahat”](#)
- [the section called “\[DMS.10\] Titik akhir DMS untuk database Neptune harus mengaktifkan otorisasi IAM”](#)
- [the section called “\[DMS.11\] Titik akhir DMS untuk MongoDB harus mengaktifkan mekanisme otentikasi”](#)
- [the section called “\[DMS.12\] Titik akhir DMS untuk Redis OSS seharusnya mengaktifkan TLS”](#)
- [the section called “\[DynamoDB.7\] Cluster DynamoDB Accelerator harus dienkripsi saat transit”](#)
- [the section called “\[EFS.6\] Target pemasangan EFS tidak boleh dikaitkan dengan subnet publik”](#)
- [the section called “\[EKS.3\] Kluster EKS harus menggunakan rahasia Kubernetes terenkripsi”](#)
- [the section called “\[FSx.2\] FSx untuk sistem file Lustre harus dikonfigurasi untuk menyalin tag ke cadangan”](#)

- the section called “[MQ.2] Broker ActiveMQ harus mengalirkan log audit ke CloudWatch”
- the section called “[MQ.3] Broker Amazon MQ harus mengaktifkan peningkatan versi minor otomatis”
- the section called “[Opensearch.11] OpenSearch domain harus memiliki setidaknya tiga node primer khusus”
- the section called “[Redshift.15] Grup keamanan Redshift harus mengizinkan masuknya port cluster hanya dari asal yang dibatasi”
- the section called “[SageMaker.4] varian produksi SageMaker titik akhir harus memiliki jumlah instance awal yang lebih besar dari 1”
- the section called “[Service Catalog.1] Portofolio Service Catalog harus dibagikan hanya dalam suatu organisasi AWS”
- the section called “[Transfer.2] Server Transfer Family tidak boleh menggunakan protokol FTP untuk koneksi titik akhir”

AWS Standar Penandaan Sumber Daya	Standar Penandaan AWS Sumber Daya dari Security Hub CSPM sekarang tersedia secara umum, bersama dengan kontrol baru yang berlaku untuk standar.	April 30, 2024
Memperbarui ke kebijakan terkelola yang ada	Security Hub CSPM memperbarui kebijakan AWS terkelola yang diberi nama AmazonSecurityHubFullAccess untuk mendapatkan detail harga Layanan AWS dan produk.	April 24, 2024
Konfigurasi parameter kontrol dalam konteks	Jika Anda menggunakan konfigurasi pusat, Anda sekarang dapat mengonfigurasi parameter kontrol dalam konteks , dari halaman detail kontrol pada konsol CSPM Security Hub.	Maret 29, 2024
Memperbarui ke kebijakan terkelola yang ada	Security Hub CSPM memperbarui kebijakan AWS terkelola bernama AWSSecurityHubReadOnlyAccess dengan menambahkan bidang. Sid	Februari 22, 2024
Kontrol keamanan baru	Kontrol [Macie.2] Penemuan data sensitif otomatis Macie harus diaktifkan sekarang tersedia. Untuk batasan Regional pada kontrol ini, lihat Ketersediaan kontrol menurut Wilayah .	Februari 19, 2024

[Security Hub CSPM tersedia di Kanada Barat \(Calgary\)](#)

Security Hub CSPM sekarang tersedia di Kanada Barat (Calgary). Semua fitur CSPM Security Hub sekarang tersedia di Wilayah ini, dengan pengecualian kontrol keamanan tertentu. Untuk informasi selengkapnya, lihat [Ketersediaan kontrol menurut Wilayah](#).

20 Desember 2023

Kontrol keamanan baru

Kontrol CSPM Security Hub baru berikut ini tersedia:

14 Desember 2023

- [the section called “\[Backup.1\] titik AWS Backup pemulihan harus dienkripsi saat istirahat”](#)
- [the section called “\[DynamoDB.6\] Tabel DynamoDB harus mengaktifkan perlindungan penghapusan”](#)
- [the section called “\[EC2.51\] Titik akhir EC2 Client VPN harus mengaktifkan pencatatan koneksi klien”](#)
- [the section called “\[EKS.8\] Kluster EKS harus mengaktifkan pencatatan audit”](#)
- [the section called “\[EMR.2\] Pengaturan akses publik blok EMR Amazon harus diaktifkan”](#)
- [the section called “\[FSx.1\] FSx untuk sistem file OpenZFS harus dikonfigurasi untuk menyalin tag ke cadangan dan volume”](#)
- [the section called “\[Macie.1\] Amazon Macie harus diaktifkan”](#)
- [the section called “\[MSK.2\] Kluster MSK seharusnya telah meningkatkan](#)

pemantauan yang dikonfigurasi

- the section called “[Neptunus.9] Cluster DB Neptunus harus digunakan di beberapa Availability Zone”
- the section called “[Network Firewall.1] Firewall Jaringan harus digunakan di beberapa Availability Zone”
- the section called “[Network Firewall.2] Pencatatan Firewall Jaringan harus diaktifkan”
- the section called “[Opensearch.10] OpenSearch domain harus menginstal pembaruan perangkat lunak terbaru”
- the section called “[PCA.1] otoritas sertifikat AWS Private CA root harus dinonaktifkan”
- the section called “[S3.19] Titik akses S3 harus mengaktifkan pengaturan akses publik blok”
- the section called “[S3.20] Bucket tujuan umum S3 harus mengaktifkan penghapusan MFA”

[Menemukan pengayaan](#)

Security Hub CSPM menambahkan bidang pencarian baru `AwsAccountName`, `ApplicationArn`, dan `ApplicationName` ke AWS Security Finding Format (ASFF).

27 November 2023

[Penyempurnaan dasbor Ringkasan](#)

Anda sekarang dapat mengakses lebih banyak widget dasbor di halaman Ringkasan konsol CSPM Security Hub, menyimpan set filter dasbor untuk fokus dengan cepat pada masalah keamanan tertentu, dan menyesuaikan tata letak dasbor.

27 November 2023

[Konfigurasi pusat](#)

Konfigurasi pusat sekarang tersedia. Dengan konfigurasi pusat, administrator yang didelegasikan CSPM Security Hub dapat mengonfigurasi CSPM Security Hub, standar, dan kontrol di beberapa akun organisasi, unit organisasi (OUs), dan Wilayah.

27 November 2023

Pembaruan kebijakan terkelola	Security Hub CSPM menambahkan izin baru ke kebijakan <code>AWSSecurityHubServiceRolePolicy</code> terkelola yang memungkinkan CSPM Security Hub membaca dan memperbarui properti kontrol keamanan yang dapat disesuaikan.	26 November 2023
Parameter kontrol kustom	Sekarang Anda dapat menyesuaikan nilai parameter untuk kontrol CSPM Security Hub tertentu. Ini dapat membuat temuan untuk kontrol spesifik lebih relevan dengan persyaratan bisnis dan harapan keamanan Anda.	26 November 2023
Pembaruan kebijakan terkelola	Security Hub CSPM memperbarui <code>AWSSecurityHubFullAccess</code> dan <code>AWSSecurityHubOrganizationsAccess</code> mengelola kebijakan yang memungkinkan Anda untuk menggunakan, masing-masing, fitur CSPM Security Hub dan integrasi dengan. AWS Organizations	16 November 2023

[Kontrol keamanan yang ada
ditambahkan ke Standar
yang Dikelola Layanan: AWS
Control Tower](#)

14 November 2023

Kontrol CSPM Security
Hub yang ada berikut telah
ditambahkan ke Standar
yang Dikelola Layanan: AWS
Control Tower

- ACM.2
- AppSync.5
- CloudTrail.6
- DMS.9
- DokumenDB.3
- DynamoDB.3
- EC2.23
- EKS.1
- ElastiCache.3
- ElastiCache.4
- ElastiCache.5
- ElastiCache.6
- EventBridge.3
- KMS.4
- Lambda.3
- MQ.5
- MQ.6
- MSK.1
- RDS.12
- RDS.15
- S3.17

Pembaruan kebijakan terkelola

Security Hub CSPM menambahkan izin penandaan baru ke kebijakan `AWSSecurityHubServiceRolePolicy` terkelola yang memungkinkan CSPM Security Hub membaca tag sumber daya yang terkait dengan temuan.

7 November 2023

Kontrol keamanan baru

Kontrol CSPM Security Hub baru berikut ini tersedia:

10 Oktober 2023

- [the section called “\[AppSync.5\] AWS AppSync APIs GraphQL tidak boleh diautentikasi dengan kunci API”](#)
- [the section called “\[DMS.6\] Instans replikasi DMS harus mengaktifkan peningkatan versi minor otomatis”](#)
- [the section called “\[DMS.7\] Tugas replikasi DMS untuk database target seharusnya mengaktifkan logging”](#)
- [the section called “\[DMS.8\] Tugas replikasi DMS untuk database sumber seharusnya mengaktifkan logging”](#)
- [the section called “\[DMS.9\] Titik akhir DMS harus menggunakan SSL”](#)
- [the section called “\[DocumentDB.3\] Cuplikan cluster manual Amazon DocumentDB seharusnya tidak bersifat publik”](#)
- [the section called “\[DocumentDB.4\] Cluster Amazon DocumentDB harus mempublikasikan log audit ke Log CloudWatch ”](#)
- [the section called “\[DocumentDB.5\] Cluster](#)

Amazon DocumentDB harus mengaktifkan perlindungan penghapusan”

- the section called “[ECS.9] Definisi tugas ECS harus memiliki konfigurasi logging”
- the section called “[EventBridge.3] bus acara EventBridge khusus harus memiliki kebijakan berbasis sumber daya terlampir”
- the section called “[EventBridge.4] titik akhir EventBridge global harus mengaktifkan replikasi acara”
- the section called “[MSK.1] Kluster MSK harus dienkripsi saat transit di antara node broker”
- the section called “[MQ.5] Broker ActiveMQ harus menggunakan mode penerapan aktif/siaga”
- the section called “[MQ.6] Broker RabbitMQ harus menggunakan mode penerapan cluster”
- the section called “[Network Firewall.9] Firewall Jaringan harus mengaktifkan perlindungan penghapusan”
- the section called “[RDS.34] Kluster Aurora MySQL DB

[harus menerbitkan log audit ke Log CloudWatch ”](#)

- [the section called “\[RDS.35\] Cluster RDS DB harus mengaktifkan peningkatan versi minor otomatis”](#)
- [the section called “\[Route53 .2\] Route 53 zona yang dihosting publik harus mencatat kueri DNS”](#)
- [the section called “AWS WAF Aturan \[WAF.12\] harus mengaktifkan metrik CloudWatch ”](#)

Pembaruan kebijakan terkelola

Security Hub CSPM menambahkan tindakan Organizations baru ke kebijakan AWSSecurityHubServiceRolePolicy terkelola yang memungkinkan CSPM Security Hub untuk mengambil informasi akun dan unit organisasi (OU). Kami juga menambahkan tindakan CSPM Security Hub baru yang memungkinkan CSPM Security Hub membaca dan memperbarui konfigurasi layanan, termasuk standar dan kontrol.

27 September 2023

Kontrol keamanan yang ada
ditambahkan ke Standar
yang Dikelola Layanan: AWS
Control Tower

Kontrol CSPM Security
Hub yang ada berikut telah
ditambahkan ke Standar
yang Dikelola Layanan: AWS
Control Tower

26 September 2023

- the section called “[Athena.1] Kelompok kerja Athena harus dienkripsi saat istirahat”
- the section called “[DocumentDB.1] Cluster Amazon DocumentDB harus dienkripsi saat istirahat”
- the section called “[DocumentDB.2] Cluster Amazon DocumentDB harus memiliki periode retensi cadangan yang memadai”
- the section called “[Neptunus.1] Cluster DB Neptunus harus dienkripsi saat istirahat”
- the section called “[Neptune.2] Cluster DB Neptunus harus menerbitkan log audit ke Log CloudWatch ”
- the section called “[Neptune.3] Snapshot cluster Neptunus DB seharusnya tidak publik”
- the section called “[Neptunus.4] Cluster DB Neptunus harus mengaktifkan perlindungan penghapusan”

- [the section called “\[Neptunus.5\] Cluster DB Neptunus harus mengaktifkan cadangan otomatis”](#)
- [the section called “\[Neptune .6\] Snapshot cluster Neptunus DB harus dienkripsi saat istirahat”](#)
- [the section called “\[Neptune .7\] Cluster DB Neptunus harus mengaktifkan otentikasi basis data IAM”](#)
- [the section called “\[Neptunus.8\] Cluster DB Neptunus harus dikonfigurasi untuk menyalin tag ke snapshot”](#)
- [the section called “\[RDS.27\] Cluster RDS DB harus dienkripsi saat istirahat”](#)

[Tampilan kontrol konsolidasi dan temuan kontrol konsolidasi tersedia di AWS GovCloud \(US\)](#)

Tampilan kontrol konsolidasi dan temuan kontrol terkonsolidasi sekarang tersedia di. AWS GovCloud (US) Region Halaman Kontrol konsol CSPM Security Hub menampilkan semua kontrol Anda di seluruh standar. Setiap kontrol memiliki ID kontrol yang sama di seluruh standar. Ketika Anda mengaktifkan temuan kontrol konsolidasi, Anda menerima satu temuan per pemeriksaan keamanan bahkan ketika kontrol berlaku untuk beberapa standar yang diaktifkan.

September 6, 2023

[Tampilan kontrol konsolidasi dan temuan kontrol konsolidasi tersedia di Wilayah Tiongkok](#)

Pandangan kontrol konsolidasi dan temuan kontrol konsolidasi sekarang tersedia di Wilayah Tiongkok. Halaman Kontrol konsol CSPM Security Hub menampilkan semua kontrol Anda di seluruh standar. Setiap kontrol memiliki ID kontrol yang sama di seluruh standar. Ketika Anda mengaktifkan temuan kontrol konsolidasi, Anda menerima satu temuan per pemeriksaan keamanan bahkan ketika kontrol berlaku untuk beberapa standar yang diaktifkan.

28 Agustus 2023

[Security Hub CSPM tersedia di Wilayah Israel \(Tel Aviv\)](#)

Security Hub CSPM sekarang tersedia di Israel (Tel Aviv). Semua fitur CSPM Security Hub sekarang tersedia di Wilayah ini, dengan pengecualian kontrol keamanan tertentu. Untuk informasi selengkapnya, lihat [Ketersediaan kontrol menurut Wilayah](#).

8 Agustus 2023

Kontrol keamanan baru

Kontrol CSPM Security Hub baru berikut ini tersedia:

28 Juli 2023

- [the section called “\[Athena.1\] Kelompok kerja Athena harus dienkripsi saat istirahat”](#)
- [the section called “\[DocumentDB.1\] Cluster Amazon DocumentDB harus dienkripsi saat istirahat”](#)
- [the section called “\[DocumentDB.2\] Cluster Amazon DocumentDB harus memiliki periode retensi cadangan yang memadai”](#)
- [the section called “\[Neptunu s.1\] Cluster DB Neptunus harus dienkripsi saat istirahat”](#)
- [the section called “\[Neptune .2\] Cluster DB Neptunus harus menerbitkan log audit ke Log CloudWatch ”](#)
- [the section called “\[Neptune .3\] Snapshot cluster Neptunus DB seharusnya tidak publik”](#)
- [the section called “\[Neptunu s.4\] Cluster DB Neptunus harus mengaktifkan perlindungan penghapusan”](#)
- [the section called “\[Neptunu s.5\] Cluster DB Neptunus](#)

[harus mengaktifkan cadangan otomatis”](#)

- [the section called “\[Neptune .6\] Snapshot cluster Neptune DB harus dienkripsi saat istirahat”](#)
- [the section called “\[Neptune .7\] Cluster DB Neptune harus mengaktifkan otentikasi basis data IAM”](#)
- [the section called “\[Neptunu s.8\] Cluster DB Neptune harus dikonfigurasi untuk menyalin tag ke snapshot”](#)
- [the section called “\[RDS.27\] Cluster RDS DB harus dienkripsi saat istirahat”](#)

[Operator baru untuk kriteria aturan otomatisasi](#)

Anda sekarang dapat menggunakan operator perbandingan CONTAINS dan NOT_CONTAINS untuk peta aturan otomatisasi dan kriteria string.

25 Juli 2023

[Aturan otomatisasi](#)

Security Hub CSPM sekarang menawarkan aturan otomatisasi yang secara otomatis memperbarui temuan berdasarkan kriteria yang Anda tentukan.

13 Juni 2023

[Integrasi pihak ketiga yang baru](#)

Snyk adalah integrasi pihak ketiga baru yang mengirimkan temuan ke Security Hub CSPM.

12 Juni 2023

Kontrol keamanan yang ada
ditambahkan ke Standar
yang Dikelola Layanan: AWS
Control Tower

Kontrol CSPM Security
Hub yang ada berikut telah
ditambahkan ke Standar
yang Dikelola Layanan: AWS
Control Tower

12 Juni 2023

- the section called “[Akun.1] Informasi kontak keamanan harus disediakan untuk Akun AWS”
- the section called “[APIGate way.8] Rute API Gateway harus menentukan jenis otorisasi”
- the section called “[APIGate way.9] Pencatatan akses harus dikonfigurasi untuk Tahap API Gateway V2”
- the section called “[CodeBui ld.3] Log CodeBuild S3 harus dienkripsi”
- the section called “[EC2.25] Templat EC2 peluncuran Amazon tidak boleh menetapkan publik IPs ke antarmuka jaringan”
- the section called “[ELB.1] Application Load Balancer harus dikonfigurasi untuk mengalihkan semua permintaan HTTP ke HTTPS”
- the section called “[Redshif t.10] Cluster Redshift harus dienkripsi saat istirahat”

- [the section called “\[SageMaker.2\] instance SageMaker notebook harus diluncurkan dalam VPC khusus”](#)
- [the section called “\[SageMaker.3\] Pengguna seharusnya tidak memiliki akses root ke instance SageMaker notebook”](#)
- [the section called “\[WAF.10\] AWS WAF web ACLs harus memiliki setidaknya satu aturan atau kelompok aturan”](#)

Kontrol keamanan baru

Kontrol CSPM Security Hub baru berikut ini tersedia:

6 Juni 2023

- [the section called “\[ACM.2\] Sertifikat RSA yang dikelola oleh ACM harus menggunakan panjang kunci minimal 2.048 bit”](#)
- [the section called “\[AppSync .2\] AWS AppSync harus mengaktifkan logging tingkat lapangan”](#)
- [the section called “\[CloudFront.13\] CloudFront distribusi harus menggunakan kontrol akses asal”](#)
- [the section called “\[Elastic Beanstalk.3\] Elastic Beanstalk harus mengalirkan log ke CloudWatch”](#)
- [the section called “\[S3.17\] Ember tujuan umum S3 harus dienkripsi saat istirahat AWS KMS keys”](#)
- [the section called “\[StepFunctions.1\] Mesin status Step Functions seharusnya mengaktifkan logging”](#)

[Security Hub CSPM tersedia di Asia Pasifik \(Melbourne\)](#)

Security Hub CSPM sekarang tersedia di Asia Pasifik (Melbourne). Semua fitur CSPM Security Hub sekarang tersedia di Wilayah ini, dengan pengecualian kontrol keamanan tertentu. Untuk informasi selengkapnya, lihat [Ketersediaan kontrol menurut Wilayah](#).

25 Mei 2023

[Menemukan sejarah](#)

Security Hub CSPM sekarang dapat melacak riwayat temuan selama 90 hari terakhir.

4 Mei 2023

[Kontrol keamanan baru](#)

Kontrol CSPM Security Hub baru berikut ini tersedia:

29 Maret 2023

- [the section called “\[EKS.1\] Titik akhir kluster EKS seharusnya tidak dapat diakses publik”](#)
- [the section called “\[ELB.16\] Application Load Balancers harus dikaitkan dengan ACL web AWS WAF”](#)
- [the section called “\[Redshift.10\] Cluster Redshift harus dienkripsi saat istirahat”](#)
- [the section called “\[S3.15\] Bucket tujuan umum S3 harus mengaktifkan Object Lock”](#)

Dukungan yang diperluas untuk temuan kontrol terkonsolidasi	Respon Keamanan Otomatis pada AWS v2.0.0 sekarang mendukung temuan kontrol terkonsolidasi.	24 Maret 2023
Security Hub CSPM tersedia dalam versi baru Wilayah AWS	Security Hub CSPM sekarang tersedia di Asia Pasifik (Hyderabad), Eropa (Spanyol), dan Eropa (Zurich). Ada batasan di mana kontrol tersedia di Wilayah ini.	21 Maret 2023
Memperbarui ke kebijakan terkelola	Security Hub CSPM telah memperbarui izin yang ada dalam kebijakan <code>AWSecurityHubServiceRolePolicy</code> terkelola.	Maret 17, 2023

Kontrol keamanan baru untuk standar NIST 800-53

Security Hub CSPM telah menambahkan kontrol keamanan berikut, yang berlaku untuk standar NIST 800-53:

3 Maret 2023

- the section called “[Akun.2] Akun AWS harus menjadi bagian dari organisasi AWS Organizations”
- the section called “[CloudWatch.15] CloudWatch alarm harus memiliki tindakan tertentu yang dikonfigurasi”
- the section called “[CloudWatch.16] grup CloudWatch log harus dipertahankan untuk jangka waktu tertentu”
- the section called “[CloudWatch.17] tindakan CloudWatch alarm harus diaktifkan”
- the section called “[DynamoDB.4] Tabel DynamoDB harus ada dalam rencana cadangan”
- the section called “[EC2.28] Volume EBS harus dicakup oleh rencana cadangan”
- EC2.29 — EC2 instance harus diluncurkan dalam VPC (pensiun)
- the section called “[RDS.26] Instans RDS DB harus dilindungi oleh rencana cadangan”

- [the section called “\[S3.14\] Bucket tujuan umum S3 harus mengaktifkan versi”](#)
- [the section called “\[WAF.11\] pencatatan ACL AWS WAF web harus diaktifkan”](#)

[Institut Nasional Standar dan Teknologi \(NIST\) 800-53 Wahyu 5](#)

Security Hub CSPM sekarang mendukung standar NIST 800-53 Rev. 5 dengan lebih dari 200 kontrol keamanan yang berlaku.

28 Februari 2023

[Kontrol konsolidasi melihat dan mengendalikan temuan](#)

Dengan rilis tampilan kontrol konsolidasi, halaman Kontrol konsol CSPM Security Hub menampilkan semua kontrol Anda di seluruh standar. Setiap kontrol memiliki ID kontrol yang sama di seluruh standar. Ketika Anda mengaktifkan temuan kontrol konsolidasi, Anda menerima satu temuan per pemeriksaan keamanan bahkan ketika kontrol berlaku untuk beberapa standar yang diaktifkan.

23 Februari 2023

Kontrol keamanan baru

Kontrol CSPM Security Hub baru berikut ini tersedia. Beberapa kontrol memiliki keterbatasan Regional.

16 Februari 2023

- the section called “[ElastiC ache.1] Cluster ElastiCache (Redis OSS) harus mengaktifkan pencadangan otomatis”
- the section called “[ElastiC ache.2] ElastiCache cluster harus mengaktifkan peningkatan versi minor otomatis”
- the section called “[ElastiC ache.3] grup ElastiCache replikasi harus mengaktifkan failover otomatis”
- the section called “[ElastiC ache.4] grup ElastiCache replikasi harus dienkripsi saat istirahat”
- the section called “[ElastiC ache.5] grup ElastiCache replikasi harus dienkripsi saat transit”
- the section called “[ElastiC ache.6] ElastiCache (Redis OSS) grup replikasi dari versi sebelumnya harus mengaktifkan Redis OSS AUTH”
- the section called “[ElastiC ache.7] ElastiCache cluster

[tidak boleh menggunakan grup subnet default](#)

[Bidang ASFF baru](#)

Security Hub CSPM telah ditambahkan. ProductFields ArchivalReasons:0/Deskripsi dan. ProductFields ArchivalReasons:0/ ReasonCode ke AWS Security Finding Format (ASFF).

Februari 8, 2023

[Bidang ASFF baru](#)

Security Hub CSPM telah menambahkan Kepatuhan . AssociatedStandards dan Kepatuhan. SecurityControlId ke AWS Security Finding Format (ASFF).

31 Januari 2023

[Detail kerentanan sekarang tersedia](#)

Anda sekarang dapat melihat detail kerentanan di konsol CSPM Security Hub untuk temuan yang dikirimkan Amazon Inspector ke Security Hub CSPM.

Januari 14, 2023

[Security Hub CSPM tersedia di Timur Tengah \(UEA\)](#)

Security Hub CSPM sekarang tersedia di Timur Tengah (UEA). Beberapa kontrol memiliki batas Regional.

Januari 12, 2023

[Menambahkan integrasi pihak ketiga dengan MetricStream](#)

Security Hub CSPM sekarang mendukung integrasi pihak ketiga dengan MetricStream di semua Wilayah kecuali China dan. AWS GovCloud (US)

11 Januari 2023

Peningkatan batas akun organisasi	Security Hub CSPM sekarang mendukung hingga 11.000 akun anggota untuk setiap akun administrator CSPM Security Hub per Wilayah.	Desember 27, 2022
ElasticBeanstalk.3 digulung kembali	Security Hub CSPM memutar kembali kontrol [ElasticBeanstalk.3] Elastic Beanstalk harus mengalirkan log dari standar FSBP di semua Wilayah. CloudWatch	21 Desember 2022
Security Hub CSPM menambahkan kontrol keamanan baru	Kontrol CSPM Security Hub baru tersedia untuk pelanggan yang telah mengaktifkan standar FSBP. Beberapa kontrol memiliki keterbatasan Regional .	15 Desember 2022
Panduan tentang fitur yang akan datang	Security Hub CSPM berencana untuk merilis dua fitur baru: tampilan kontrol konsolidasi dan temuan kontrol terkonsolidasi. Fitur yang akan datang ini dapat memengaruhi alur kerja yang ada yang bergantung pada bidang dan nilai pencarian kontrol.	Desember 9, 2022
Integrasi Amazon Security Lake sekarang tersedia	Security Lake sekarang terintegrasi dengan Security Hub CSPM dengan menerima temuan CSPM Security Hub.	29 November 2022

<u>Dukungan untuk Standar yang Dikelola Layanan: AWS Control Tower</u>	Security Hub CSPM mendukung standar keamanan baru yang disebut Service-Managed Standard: . AWS Control Tower AWS Control Tower mengelola standar ini.	28 November 2022
<u>CIS AWS Foundations Benchmark v1.4.0 sekarang tersedia di Wilayah Tiongkok</u>	Security Hub CSPM sekarang mendukung CIS AWS Foundations Benchmark v1.4.0 di Wilayah Tiongkok.	18 November 2022
<u>Integrasi Cloud Manajemen Layanan Jira sekarang tersedia</u>	Jira Service Management Cloud sekarang menerima temuan CSPM Security Hub di semua Wilayah yang tersedia, kecuali Wilayah Tiongkok.	17 November 2022
<u>AWS IoT Device Defender integrasi sekarang tersedia</u>	AWS IoT Device Defender sekarang mengirimkan temuan ke Security Hub CSPM di semua Wilayah yang tersedia.	17 November 2022
<u>Support untuk CIS AWS Foundations Benchmark v1.4.0</u>	Security Hub CSPM sekarang menyediakan kontrol keamanan yang mendukung CIS AWS Foundations Benchmark v1.4.0. Standar ini tersedia di semua Wilayah yang tersedia, kecuali Wilayah Tiongkok.	9 November 2022

[Dukungan untuk pengumuman CSPM Security Hub di AWS GovCloud \(US\)](#)

Anda sekarang dapat berlangganan pengumuman CSPM Security Hub dengan Amazon Simple Notification Service (Amazon SNS) AWS GovCloud di (AS-Timur) AWS GovCloud dan (AS-Barat) untuk menerima pemberitahuan tentang Security Hub CSPM.

3 Oktober 2022

[AWS Security Hub Cloud Security Posture Management \(CSPM\) menambahkan kontrol keamanan baru](#)

Kontrol CSPM Security Hub yang baru AutoScaling.9 tersedia untuk pelanggan yang telah mengaktifkan standar FSBP. Kontrol mungkin memiliki [batasan Regional](#).

September 1, 2022

[Berlangganan pengumuman CSPM Security Hub](#)

Anda sekarang dapat berlangganan pengumuman CSPM Security Hub dengan Amazon Simple Notification Service (Amazon SNS) untuk menerima pemberitahuan tentang Security Hub CSPM.

Agustus 29, 2022

[Perluasan wilayah untuk agregasi lintas wilayah](#)

Agregasi Lintas Wilayah sekarang tersedia untuk temuan, menemukan pembaruan, dan wawasan di seluruh wilayah. AWS GovCloud (US)

2 Agustus 2022

Integrasi produk pihak ketiga yang baru	Fortinet - FortiCNP adalah integrasi pihak ketiga yang menerima temuan CSPM Security Hub, dan JFrog merupakan integrasi pihak ketiga yang mengirimkan temuan ke Security Hub CSPM.	26 Juli 2022
EC2.27 sudah pensiun	Security Hub CSPM telah pensiun EC2.27 - EC2 Instans Menjalankan tidak boleh menggunakan pasangan kunci, kontrol sebelumnya dalam standar Praktik Terbaik Keamanan AWS Dasar (FSBP).	20 Juli 2022
Lambda.2 tidak lagi mendukung python3.6	Security Hub CSPM tidak lagi mendukung python3.6 sebagai parameter untuk Lambda.2 - Fungsi Lambda harus menggunakan runtime yang didukung, kontrol dalam standar Foundational Security Best Practices (FSBP). AWS	19 Juli 2022
AWS Security Hub Cloud Security Posture Management (CSPM) menambahkan kontrol keamanan baru	Kontrol CSPM Security Hub baru tersedia untuk pelanggan yang telah mengaktifkan standar FSBP. Beberapa kontrol memiliki keterbatasan Regional .	Juni 22, 2022

AWS Security Hub Cloud Security Posture Management (CSPM) mendukung Wilayah baru	Security Hub CSPM sekarang tersedia di Asia Pasifik (Jakarta). Beberapa kontrol tidak tersedia di Wilayah ini.	7 Juni 2022
Peningkatan integrasi antara AWS Security Hub Cloud Security Posture Management (CSPM) dan AWS Config	Pengguna CSPM Security Hub dapat melihat hasil evaluasi AWS Config aturan sebagai temuan di Security Hub CSPM.	6 Juni 2022
Menambahkan kemampuan untuk memilih keluar dari standar yang diaktifkan secara otomatis	Untuk pengguna yang telah terintegrasi AWS Organizations, fitur ini memungkinkan Anda untuk masuk ke akun administrator CSPM Security Hub dan memilih akun anggota baru dari standar yang diaktifkan secara otomatis.	April 25, 2022
Agregasi lintas wilayah yang diperluas	Menambahkan agregasi lintas wilayah untuk mengontrol status dan skor keamanan.	20 April 2022
CompanyName dan ProductName sekarang atribut tingkat atas	Menambahkan atribut tingkat atas baru untuk menetapkan nama perusahaan dan produk yang terkait dengan integrasi kustom	1 April 2022
Menambahkan kontrol baru ke standar Praktik Terbaik Keamanan AWS Dasar	Menambahkan 5 kontrol baru ke standar Praktik Terbaik Keamanan AWS Dasar.	31 Maret 2022
Menambahkan rincian sumber daya baru keberatan dengan ASFF	Menambahkan jenis AwsRdsDbSecurityGroup sumber daya ke ASFF.	Maret 25, 2022

Menambahkan rincian sumber daya tambahan di ASFF	Menambahkan detail tambahan ke <code>AwsAutoScalingScalingGroup</code> , <code>AwsElbLoadBalancer</code> , <code>AwsRedshiftCluster</code> , dan <code>AwsCodeBuildProject</code> .	Maret 25, 2022
Menambahkan kontrol baru ke standar Praktik Terbaik Keamanan AWS Dasar	Menambahkan 15 kontrol baru ke standar Praktik Terbaik Keamanan AWS Dasar.	16 Maret 2022
Menambahkan kontrol baru ke standar Praktik Terbaik Keamanan AWS Dasar dan Standar Keamanan Data Industri Kartu Pembayaran (PCI DSS)	Menambahkan kontrol baru untuk Amazon OpenSearch Service, Amazon RDS, Amazon EC2, Elastic Load Balancing, CloudFront dan standar Praktik AWS Terbaik Keamanan Dasar. Juga menambahkan dua kontrol baru untuk OpenSearch Layanan ke PCI DSS.	Februari 15, 2022
Menambahkan bidang baru ke ASFF	Ditambahkan bidang baru: Contoh.	26 Januari 2022
Integrasi ditambahkan dengan AWS Health	AWS Health menggunakan pesan service-to-service acara untuk mengirim temuan ke Security Hub CSPM.	Januari 19, 2022

[Integrasi ditambahkan dengan AWS Trusted Advisor](#)

Trusted Advisor mengirimkan hasil pemeriksaannya ke Security Hub CSPM sebagai temuan CSPM Security Hub. Security Hub CSPM mengirimkan hasil pemeriksaan Praktik Terbaik Keamanan AWS Dasar ke Trusted Advisor

18 Januari 2022

[Diperbarui objek rincian sumber daya di ASFF](#)

Ditambahkan `MixedInstancesPolicy` dan `AvailabilityZones` ke `AwsAutoScalingAutoScalingGroup`. Menambahkan `MetadataOptions` ke `AwsAutoScalingLaunchConfiguration`. Menambahkan `BucketVersioningConfiguration` ke `AwsS3Bucket`.

Desember 20, 2021

[Diperbarui output untuk dokumentasi ASFF](#)

Deskripsi atribut ASFF sebelumnya dalam satu topik. Setiap objek tingkat atas dan setiap objek detail sumber daya sekarang dalam topiknya sendiri. Topik sintaks ASFF berisi tautan ke topik tersebut.

Desember 20, 2021

[Menambahkan objek detail sumber daya baru ke ASFF untuk AWS Network Firewall](#)

Untuk AWS Network Firewall, menambahkan objek detail sumber daya berikut: `AwsNetworkFirewall`, `AwsNetworkFirewallPolicy`, dan `AwsNetworkFirewallRuleGroup`.

Desember 20, 2021

[Ditambahkan dukungan untuk versi baru Amazon Inspector](#)

Security Hub CSPM terintegrasi dengan versi baru Amazon Inspector serta dengan Amazon Inspector Classic. Amazon Inspector mengirimkan temuan ke Security Hub CSPM.

29 November 2021

[Mengubah tingkat keparahan EC2 .19](#)

Tingkat keparahan EC2 .19 (Grup keamanan tidak boleh mengizinkan akses tidak terbatas ke port dengan risiko tinggi) diubah dari Tinggi ke Kritis.

17 November 2021

[Integrasi baru dengan Sonrai Dig](#)

Security Hub CSPM sekarang menawarkan integrasi dengan Sonrai Dig. Sonrai Dig membantu lingkungan cloud untuk mengidentifikasi risiko keamanan. Sonrai Dig mengirimkan temuan ke Security Hub CSPM.

12 November 2021

[Pemeriksaan yang diperbarui untuk kontrol CIS 2.1 dan CloudTrail .1](#)

Selain memeriksa bahwa setidaknya satu CloudTrail jejak Multi-wilayah sudah ada, CIS 2.1 dan CloudTrail .1 sekarang juga memeriksa apakah ExcludeManagementEventSources parameter-nya kosong di setidaknya satu jalur Multi-wilayah. CloudTrail

November 9, 2021

[Menambahkan dukungan untuk titik akhir VPC](#)

Security Hub CSPM sekarang terintegrasi dengan AWS PrivateLink dan mendukung titik akhir VPC.

3 November 2021

[Menambahkan kontrol ke standar Praktik Terbaik Keamanan AWS Dasar](#)

Menambahkan kontrol baru untuk Elastic Load Balancing (ELB.2 dan ELB.8) dan (SSM.4). AWS Systems Manager

2 November 2021

[Menambahkan port ke cek untuk kontrol EC2 .19](#)

EC2.19 sekarang juga memeriksa bahwa grup keamanan tidak mengizinkan akses masuk tanpa batas ke port berikut: 3000 (kerangka kerja pengembangan web Go, Node.js, dan Ruby), 5000 (kerangka kerja pengembangan web Python), 8088 (port HTTP lama), dan 8888 (port HTTP alternatif)

27 Oktober 2021

[Menambahkan integrasi dengan Logz.io Cloud SIEM](#)

Logz.io adalah penyedia Cloud SIEM yang menyediakan korelasi lanjutan data log dan peristiwa untuk membantu tim keamanan mendeteksi, menganalisis, dan merespons ancaman keamanan secara real time. Logz.io menerima temuan dari Security Hub CSPM.

25 Oktober 2021

[Menambahkan dukungan untuk agregasi temuan lintas wilayah](#)

Agregasi Lintas Wilayah memungkinkan Anda untuk melihat semua temuan Anda tanpa harus mengubah Wilayah. Akun administrator memilih Wilayah agregasi dan Wilayah yang ditautkan. Temuan untuk akun administrator dan akun anggotanya dikumpulkan dari Wilayah yang ditautkan ke Wilayah agregasi.

20 Oktober 2021

[Diperbarui objek rincian sumber daya di ASFF](#)

Menambahkan detail sertifikat penampil ke `AwsCloudFrontDistribution` . Menambahkan detail tambahan ke `AwsCodeBuildProject` . Menambahkan atribut penyeimbang beban ke `AwsElasticLoadBalancingV2LoadBalancer` . Menambahkan pengenalan akun pemilik bucket S3 ke `AwsS3Bucket`

Oktober 8, 2021

[Menambahkan objek detail sumber daya baru ke ASFF](#)

Menambahkan objek rincian sumber daya baru berikut ke ASFF: AwsEc2Vpc, EndpointService, AwsEcrRepository, AwsEksCluster, AwsOpenSearchServiceDomain, AwsWafRateBasedRule, AwsWafRegionalRateBasedRule, AwsXrayEncryptionConfig.

Oktober 8, 2021

[Menghapus runtime usang dari kontrol Lambda.2](#)

Dalam standar Praktik Terbaik Keamanan AWS Dasar, menghapus dotnetcore2.1 runtime dari fungsi Lambda [Lambda.2] harus menggunakan runtime yang didukung.

Oktober 6, 2021

[Nama baru untuk integrasi Check Point](#)

Integrasi dengan Check Point Dome9 Arc sekarang Check Point CloudGuard Posture Management. Integrasi ARN tidak berubah.

1 Oktober 2021

[Menghapus integrasi dengan Alcide](#)

Integrasi dengan Alcide Kaudit dihentikan.

30 September 2021

[Mengubah tingkat keparahan EC2 .19](#)

Tingkat keparahan [EC2.19] Grup keamanan tidak boleh mengizinkan akses tidak terbatas ke port dengan risiko tinggi diubah dari Sedang ke Tinggi.

30 September 2021

AWS Organizations Integrasi dengan sekarang didukung di Wilayah Tiongkok	Integrasi CSPM Security Hub dengan Organizations sekarang didukung di Tiongkok (Beijing) dan China (Ningxia).	September 20, 2021
AWS Config Aturan baru untuk kontrol S3.1 dan PCI.S3.6	Baik S3.1 dan PCI.S3.6 memverifikasi bahwa pengaturan Akses Publik Blok Amazon S3 diaktifkan. AWS Config Aturan untuk kontrol ini diubah dari <code>s3-account-level-public-access-blocks</code> menjadi <code>s3-account-level-public-access-blocks-periodic</code> .	14 September 2021
Menghapus runtime usang dari kontrol Lambda.2	Dalam standar Praktik Terbaik Keamanan AWS Dasar, menghapus <code>nodejs10.x</code> dan <code>ruby2.5</code> runtime dari fungsi Lambda [Lambda.2] harus menggunakan runtime yang didukung.	13 September 2021
Mengubah tingkat keparahan kontrol CIS 2.2	Dalam standar CIS AWS Foundations Benchmark, tingkat keparahan untuk 2.2. — Pastikan validasi file CloudTrail log diaktifkan diubah dari Rendah ke Sedang.	13 September 2021

[Memperbarui ECS.1, Lambda.2, dan SSM.1 dalam standar Praktik Terbaik Keamanan Dasar AWS](#)

Dalam standar Praktik Terbaik 7 September 2021
Keamanan AWS Dasar, ECS.1 sekarang memiliki `SkipInactiveTaskDefinitions` parameter yang disetel ke `true` Ini memastikan bahwa kontrol hanya memeriksa definisi tugas aktif. Untuk Lambda.2, menambahkan Python 3.9 ke daftar runtime. SSM.1 sekarang memeriksa instance berhenti dan berjalan.

[Kontrol PCI.lambda.2 sekarang mengecualikan sumber daya Lambda @Edge](#)

Dalam standar Standar 7 September 2021
Keamanan Data Industri Kartu Pembayaran (PCI DSS), kontrol PCI.lambda.2 sekarang mengecualikan sumber daya Lambda @Edge.

[Menambahkan integrasi dengan HackerOne Vulnerability Intelligence](#)

Security Hub CSPM sekarang 7 September 2021
menawarkan integrasi dengan. HackerOne Vulnerability Intelligence Integrasi mengirimkan temuan ke Security Hub CSPM.

Diperbarui objek rincian sumber daya di ASFF	Untuk <code>AwsKmsKey</code> , ditambahkan <code>KeyRotationStatus</code> . Untuk <code>AwsS3Bucket</code> , ditambahkan <code>AccessControlList</code> , <code>BucketLoggingConfiguration</code> , <code>BucketNotificationConfiguration</code> , dan <code>BucketWebsiteConfiguration</code> .	2 September 2021
Menambahkan objek detail sumber daya baru ke ASFF	Menambahkan objek rincian sumber daya baru berikut ke ASFF: <code>AwsAutoScalingLaunchConfiguration</code> , <code>AwsEc2VpnConnection</code> , dan <code>AwsEcrContainerImage</code> .	2 September 2021
Menambahkan detail ke Vulnerabilities objek di ASFF	<code>DiCvss</code> , ditambahkan <code>Adjustments</code> dan <code>Source</code> . <code>DiVulnerablePackages</code> , menambahkan jalur file dan manajer paket.	2 September 2021
Systems Manager Explorer dan OpsCenter integrasi sekarang didukung di Wilayah Tiongkok	Integrasi Security Hub CSPM dengan SSM Explorer dan sekarang OpsCenter didukung di Tiongkok (Beijing) dan China (Ningxia).	31 Agustus 2021

[Menghentikan kontrol
Lambda.4](#)

Security Hub CSPM menghentikan kontrol [Lambda.4] Fungsi Lambda harus memiliki antrian huruf mati yang dikonfigurasi. Ketika kontrol dihentikan, kontrol tidak lagi ditampilkan di konsol, dan Security Hub CSPM tidak melakukan pemeriksaan terhadapnya.

31 Agustus 2021

[Pensiun PCI. EC2.3 kontrol](#)

Security Hub CSPM menghentikan kontrol [PCI. EC2.3] Grup EC2 keamanan yang tidak digunakan harus dihapus. Ketika kontrol dihentikan, kontrol tidak lagi ditampilkan di konsol, dan Security Hub CSPM tidak melakukan pemeriksaan terhadapnya.

Agustus 27, 2021

[Ubah cara CSPM Security
Hub mengirimkan temuan ke
tindakan kustom](#)

Saat Anda mengirim temuan ke tindakan kustom, Security Hub CSPM sekarang mengirimkan setiap temuan dalam acara terpisah Security Hub Findings - Custom Action.

Agustus 20, 2021

[Menambahkan kode alasan status kepatuhan baru untuk runtime Lambda kustom](#)

Menambahkan kode alasan status LAMBDA_CUSTOM_RUNTIME_DETAILS_NOT_AVAILABLE kepatuhan baru. Kode alasan ini menunjukkan bahwa Security Hub CSPM tidak dapat melakukan pemeriksaan terhadap runtime Lambda kustom.

Agustus 20, 2021

[AWS Firewall Manager integrasi sekarang didukung di Wilayah Tiongkok](#)

Integrasi CSPM Security Hub dengan Firewall Manager sekarang didukung di Tiongkok (Beijing) dan China (Ningxia).

19 Agustus 2021

[Integrasi baru dengan Caveonix Cloud dan Forcepoint Cloud Security Gateway](#)

Security Hub CSPM sekarang menawarkan integrasi dengan dan. Caveonix Cloud Forcepoint Cloud Security Gateway Kedua integrasi mengirimkan temuan ke Security Hub CSPM.

Agustus 10, 2021

[Ditambahkan baruCompanyName, ProductName, dan Region atribut ke ASFF](#)

Ditambahkan CompanyName, ProductName, dan Region bidang ke tingkat atas ASFF. Bidang ini diisi secara otomatis dan, kecuali untuk integrasi produk khusus, tidak dapat diperbarui menggunakan BatchImportFindings atau BatchUpdateFindings. Di konsol, menemukan filter menggunakan bidang baru ini. Di API, ProductName filter CompanyName dan menggunakan atribut yang ada di bawah ProductFields.

23 Juli 2021

[Ditambahkan dan diperbarui rincian sumber daya objek di ASFF](#)

Menambahkan jenis AwsRdsEventSubscription sumber daya baru dan detail sumber daya. Menambahkan detail sumber daya untuk jenis AwsEcsService sumber daya. Ditambahkan atribut ke objek rincian AwsElasticsearchDomain sumber daya.

23 Juli 2021

[Menambahkan kontrol ke standar Praktik Terbaik Keamanan AWS Dasar](#)

Menambahkan kontrol baru untuk Amazon API Gateway (APIGateway.5), Amazon EC2 (EC2.19), Amazon ECS EC2 (ECS.2), Elastic Load Balancing (ELB.7), Amazon OpenSearch Service (ES.5 hingga ES.8), Amazon RDS (RDS.16 hingga RDS.23), Amazon Redshift (Redshift.4), dan Amazon SQS (SQS.1).

20 Juli 2021

[Memindahkan izin dalam kebijakan terkelola peran terkait layanan](#)

Memindahkan config:PutEvaluations izin dalam kebijakan terkelolaAWSSecurityHubServiceRolePolicy , sehingga diterapkan ke semua sumber daya.

14 Juli 2021

[Menambahkan kontrol ke standar Praktik Terbaik Keamanan AWS Dasar](#)

Menambahkan kontrol baru untuk Amazon API Gateway (APIGateway.4), Amazon CloudFront (CloudFront.5 dan CloudFront .6), Amazon EC2 (EC2.17 dan EC2 .18), Amazon ECS EC2 (ECS.1), Amazon Service (ES.4), (IAM.21), OpenSearch Amazon RDS (RDS.15) AWS Identity and Access Management , dan Amazon S3 (S3.8).

8 Juli 2021

[Menambahkan kode alasan status kepatuhan baru untuk temuan kontrol](#)

INTERNAL_SERVICE_ERROR menunjukkan bahwa kesalahan yang tidak diketahui terjadi. SNS_TOPIC_CROSS_ACCOUNT menunjukkan bahwa topik SNS dimiliki oleh akun yang berbeda. SNS_TOPIC_INVALID menunjukkan bahwa topik SNS terkait tidak valid.

6 Juli 2021

[Menambahkan integrasi dengan Amazon Q Developer dalam aplikasi obrolan](#)

Menambahkan integrasi dengan Amazon Q Developer dalam aplikasi obrolan. Security Hub CSPM mengirimkan temuan ke Amazon Q Developer dalam aplikasi obrolan.

30 Juni 2021

[Menambahkan izin baru ke kebijakan terkelola peran terkait layanan](#)

Menambahkan izin baru ke kebijakan terkelola AWSSecurityHubServiceRolePolicy untuk memungkinkan peran terkait layanan memberikan hasil evaluasi. AWS Config

29 Juni 2021

[Objek detail sumber daya baru dan diperbarui di ASFF](#)

Menambahkan objek detail sumber daya baru untuk cluster ECS dan definisi tugas ECS. Diperbarui objek EC2 instance untuk daftar antarmuka jaringan terkait. Menambahkan ID sertifikat klien untuk tahap API Gateway V2. Menambahkan konfigurasi siklus hidup untuk bucket S3.

24 Juni 2021

[Memperbarui perhitungan status kontrol agregat dan skor keamanan standar](#)

Security Hub CSPM sekarang menghitung status kontrol keseluruhan dan skor keamanan standar setiap 24 jam. Untuk akun administrator, skor sekarang mencerminkan apakah setiap kontrol diaktifkan atau dinonaktifkan untuk setiap akun.

23 Juni 2021

[Informasi terbaru tentang penanganan CSPM Security Hub atas akun yang ditangguhkan](#)

Menambahkan informasi tentang cara Security Hub CSPM menangani akun yang ditangguhkan. AWS

23 Juni 2021

[Menambahkan tab untuk menampilkan kontrol yang diaktifkan dan dinonaktifkan untuk akun administrator individu](#)

Untuk akun administrator, tab utama pada halaman detail standar berisi informasi agregat di seluruh akun. Tab baru Diaktifkan untuk akun ini dan Dinonaktifkan untuk akun ini mencantumkan akun yang diaktifkan atau dinonaktifkan untuk akun administrator individu.

23 Juni 2021

Ditambahkan java8.a12 ke parameter untuk Lambda .2	Dalam standar Praktik Terbaik Keamanan AWS Dasar, ditambahkan java8.a12 ke runtime yang didukung untuk kontrol. Lambda .2	8 Juni 2021
Integrasi baru dengan MicroFocus ArcSight dan NETSCOUT Cyber Investigator	Menambahkan integrasi dengan MicroFocus ArcSight dan NETSCOUT Cyber Investigator. MicroFocus ArcSight menerima temuan dari Security Hub CSPM. NETSCOUT Cyber Investigator mengirimkan temuan ke Security Hub CSPM.	7 Juni 2021
Menambahkan rincian untuk AWSSecurityHubServiceRolePolicy	Memperbarui bagian kebijakan terkelola untuk menambahkan detail kebijakan terkelola yang adaAWSSecurityHubServiceRolePolicy , yang digunakan oleh peran terkait layanan CSPM Security Hub.	4 Juni 2021
Integrasi baru dengan Manajemen Layanan Jira	Konektor Manajemen AWS Layanan untuk Jira mengirimkan temuan ke Jira dan menggunakannya untuk membuat masalah Jira. Ketika masalah Jira diperbarui, temuan terkait di Security Hub CSPM juga diperbarui.	26 Mei 2021

<u>Memperbarui daftar kontrol yang didukung untuk Wilayah Asia Pasifik (Osaka)</u>	Memperbarui standar CIS AWS Foundations dan Payment Card Industry Data Security Standard (PCI DSS) untuk menunjukkan kontrol yang tidak didukung di Asia Pasifik (Osaka).	21 Mei 2021
<u>Integrasi baru dengan Sysdig Secure untuk cloud</u>	Menambahkan integrasi dengan Sysdig Secure untuk cloud. Integrasi mengirimkan temuan ke Security Hub CSPM.	14 Mei 2021
<u>Menambahkan kontrol ke standar Praktik Terbaik Keamanan AWS Dasar</u>	Menambahkan kontrol baru untuk Amazon API Gateway (APIGateway.2 dan APIGateway .3), (.4 dan .5), Amazon (EC2.15 dan EC2 .16), AWS CloudTrail (CloudTrailElasticBeanstalk.1 dan CloudTrail .2), (AWS Lambda Lambda.4), Amazon RDS EC2 (RDS.12 - RDS.14), Amazon Redshift AWS Elastic Beanstalk (Redshift.7 ElasticBeanstalk), (.3 dan .4), dan (WAF.7), dan (WAF.7), dan (WAF.7), dan (WAF.7) 1). AWS Secrets Manager SecretsManager AWS WAF	10 Mei 2021

Pembaruan untuk GuardDuty dan kontrol Amazon RDS	Mengubah tingkat keparahan GuardDuty.1 dan PCI.GuardDuty.1 dari Sedang ke Tinggi. Menambahkan databaseEngines parameter keRDS.8.	4 Mei 2021
Menambahkan rincian sumber daya baru ke ASFF	DiResources.Details , menambahkan objek detail sumber daya baru untuk EC2 jaringan Amazon ACLs, EC2 subnet Amazon, dan AWS Elastic Beanstalk lingkungan.	3 Mei 2021
Menambahkan bidang konsol untuk memberikan nilai filter untuk EventBridge aturan Amazon	Pola filter baru yang telah ditentukan untuk EventBridge aturan CSPM Security Hub menyediakan bidang konsol yang dapat Anda gunakan untuk menentukan nilai filter.	30 April 2021
Menambahkan integrasi dengan AWS Systems Manager Explorer dan OpsCenter	Security Hub CSPM sekarang mendukung integrasi dengan Systems Manager Explorer dan. OpsCenter Integrasi ini menerima temuan dari Security Hub CSPM dan memperbarui temuan tersebut di Security Hub CSPM.	26 April 2021
Tipe baru untuk integrasi produk	Jenis integrasi baru,UPDATE_FINDINGS_IN_SECURITY_HUB , menunjukkan bahwa integrasi produk memperbarui temuan yang diterimanya dari Security Hub CSPM.	22 April 2021

Mengubah “akun master” menjadi “akun administrator”	Istilah "akun utama" diubah menjadi "akun administrator." Istilah ini juga diubah di konsol dan API Security Hub CSPM.	22 April 2021
Diperbarui APIGateway .1 untuk mengganti HTTP dengan Websocket	Memperbarui judul, deskripsi , dan remediasi untuk APIGateway .1. Kontrol sekarang memeriksa logging eksekusi API Websocket alih-alih untuk logging eksekusi HTTP API.	9 April 2021
GuardDuty Integrasi Amazon sekarang didukung di Beijing dan Ningxia	Integrasi CSPM Security Hub dengan sekarang GuardDuty didukung di Wilayah Tiongkok (Beijing) dan China (Ningxia).	5 April 2021
Ditambahkan nodejs14.x ke runtime yang didukung untuk kontrol Lambda.2	Kontrol Lambda.2 dalam standar Praktik Terbaik Keamanan Dasar sekarang mendukung runtime. nodejs14.x	30 Maret 2021
Security Hub CSPM diluncurkan di Asia Pasifik (Osaka)	Security Hub CSPM sekarang tersedia di Wilayah Asia Pasifik (Osaka).	29 Maret 2021
Menambahkan bidang penyedia pencarian untuk menemukan detail	Pada panel rincian temuan, bagian Finding Provider Fields yang baru berisi nilai penyedia temuan untuk kepercayaan diri, kekritisannya, temuan terkait, tingkat keparahan, dan jenis.	24 Maret 2021

[Menambahkan opsi untuk menerima temuan sensitif dari Amazon Macie](#)

Integrasi dengan Macie sekarang dapat dikonfigurasi untuk mengirim temuan sensitif ke Security Hub CSPM.

23 Maret 2021

[Transisi ke manajemen AWS Organizations akun](#)

Untuk pelanggan yang memiliki akun administrator dengan akun anggota, menambahkan informasi baru tentang cara mengubah dari mengelola akun dengan undangan menjadi mengelola akun menggunakan Organizations.

22 Maret 2021

[Objek baru di ASFF untuk informasi tentang konfigurasi Blok Akses Publik Amazon S3](#)

DiResources , objek tipe dan detail AwsS3AccountPublicAccessBlock sumber daya baru memberikan informasi tentang konfigurasi Blok Akses Publik Amazon S3 untuk akun. Dalam objek detail AwsS3Bucket sumber daya, PublicAccessBlockConfiguration objek menyediakan konfigurasi Blok Akses Publik untuk bucket S3.

18 Maret 2021

[Objek baru di ASFF untuk memungkinkan penyedia pencarian memperbarui bidang tertentu](#)

FindingProviderFields Objek baru di ASFF digunakan BatchImportFindings untuk memberikan nilai untukConfidence, Criticality, RelatedFindings Severity, danTypes. Bidang asli hanya boleh diperbarui menggunakanBatchUpdateFindings.

18 Maret 2021

[DataClassification Objek baru untuk sumber daya di ASFF](#)

Resources.DataClassification Objek baru di ASFF digunakan untuk memberikan informasi tentang data sensitif yang terdeteksi pada sumber daya.

18 Maret 2021

[CONFIG_RETURNS_NOT_APPLICABLE Nilai tambah pada kode status kepatuhan yang tersedia](#)

Untuk status NOT_AVAILABLE kepatuhan, hapus kode alasan RESOURCE_NO_LONGER_EXISTS dan tambahkan kode alasanCONFIG_RETURNS_NOT_APPLICABLE.

16 Maret 2021

Kebijakan terkelola baru untuk integrasi dengan AWS Organizations	Kebijakan terkelola baru <code>AWSecurityHubOrganizationsAccess</code> , menyediakan izin <code>Organizations</code> yang diperlukan oleh akun manajemen organisasi dan akun administrator CSPM Security Hub yang didelegasikan.	15 Maret 2021
Kebijakan terkelola dan informasi peran terkait layanan dipindahkan ke bagian Keamanan	Informasi tentang kebijakan yang dikelola direvisi dan diperluas. Baik informasi kebijakan terkelola maupun informasi tentang peran terkait layanan telah dipindahkan ke bagian Keamanan.	15 Maret 2021
Integrasi baru dengan SecureCloud DB	Menambahkan SecureCloud DB ke daftar integrasi pihak ketiga. SecureCloudDB adalah alat keamanan database asli cloud yang menyediakan visibilitas komprehensif postur dan aktivitas keamanan internal dan eksternal. SecureCloudDB mengirimkan temuan ke Security Hub CSPM.	4 Maret 2021
Tingkat keparahan yang direvisi untuk kontrol CIS 1.1 dan CIS 3.1 - CIS 3.14	Tingkat keparahan kontrol CIS 1.1 dan CIS 3.1 - CIS 3.14 diubah menjadi Rendah.	3 Maret 2021
Menghapus kontrol RDS.11	Menghapus kontrol RDS.11 dari standar Praktik Terbaik Keamanan Dasar.	3 Maret 2021

Integrasi yang diperbarui untuk Turbot	Integrasi Turbot diperbarui untuk mengirim dan menerima temuan.	26 Februari 2021
Menambahkan kontrol ke standar Praktik Terbaik Keamanan Dasar	Menambahkan kontrol baru untuk Amazon API Gateway (APIGateway.1), Amazon EC2 (EC2.9 dan EC2 .10), Amazon Elastic File System (EFS.2), OpenSearch Amazon Service (ES.2 dan ES.3), Elastic Load Balancing (ELB.6), dan () (KMS.3). AWS Key Management Service AWS KMS	11 Februari 2021
Menambahkan ProductArn filter opsional ke DescribeProducts API	Operasi DescribeProducts API sekarang menyertakan ProductArn parameter opsional. ProductArn Parameter ini digunakan untuk mengidentifikasi integrasi produk tertentu untuk mengembalikan detail untuk.	3 Februari 2021
Integrasi baru dengan Antivirus untuk Amazon S3 dari Cloud Storage Security	Integrasi dengan Antivirus untuk Amazon S3 mengirimkan hasil pemindaian virus ke Security Hub CSPM sebagai temuan.	27 Januari 2021

[Memperbarui proses perhitungan skor keamanan untuk akun administrator](#)

Untuk akun administrator, Security Hub CSPM menggunakan proses terpisah untuk menghitung skor keamanan. Proses baru memastikan bahwa skor mencakup kontrol yang diaktifkan untuk akun anggota tetapi dinonaktifkan untuk akun administrator.

21 Januari 2021

[Bidang dan objek baru di ASFF](#)

Menambahkan Action objek baru untuk melacak tindakan yang terjadi terhadap sumber daya. Menambahkan bidang ke `AwsEc2NetworkInterface` objek untuk melacak nama DNS dan alamat IP. Menambahkan `AwsSsmPatchCompliance` objek baru ke detail sumber daya.

21 Januari 2021

[Menambahkan kontrol ke standar Praktik Terbaik Keamanan Dasar](#)

Menambahkan kontrol baru untuk Amazon CloudFront (CloudFront.1 hingga CloudFront.4), Amazon DynamoDB (DynamoDB.1 melalui DynamoDB.3), Elastic Load Balancing (ELB.3 hingga ELB.5), Amazon RDS (RDS.9 hingga RDS.11), Amazon Redshift (Redshift.1 melalui Redshift.3 dan Redshift.6), dan Amazon SNS (SNS.1).

15 Januari 2021

Status alur kerja diatur ulang berdasarkan status catatan atau status kepatuhan	Security Hub CSPM secara otomatis mengatur ulang status alur kerja dari NOTIFIED atau RESOLVED ke NEW jika temuan yang diarsipkan dibuat aktif, atau jika status kepatuhan temuan berubah dari PASSED salah satu,, atau. FAILED WARNING NOT_AVAILABLE Perubahan ini menunjukkan bahwa penyelidikan tambahan diperlukan.	7 Januari 2021
Menambahkan ProductFields informasi untuk temuan berbasis kontrol	Untuk temuan yang dihasilkan dari kontrol, tambahkan informasi tentang konten ProductFields objek dalam AWS Security Finding Format (ASFF).	29 Desember 2020
Pembaruan untuk wawasan terkelola	Mengubah judul wawasan 5. Menambahkan wawasan baru, 32, yang memeriksa pengguna IAM dengan aktivitas mencurigakan.	22 Desember 2020
Pembaruan untuk kontrol IAM.7 dan Lambda.1	Dalam standar Praktik Terbaik Keamanan AWS Dasar, memperbarui parameter untuk IAM.7. Memperbarui judul dan deskripsi Lambda.1.	22 Desember 2020

[Integrasi yang diperluas dengan ServiceNow ITSM](#)

Integrasi ServiceNow ITSM memungkinkan pengguna untuk secara otomatis membuat insiden atau masalah ketika temuan CSPM Security Hub diterima. Pembaruan untuk insiden atau masalah ini menghasilkan pembaruan temuan di Security Hub CSPM.

11 Desember 2020

[Integrasi baru dengan AWS Audit Manager](#)

Security Hub CSPM sekarang menawarkan integrasi dengan AWS Audit Manager. Integrasi ini memungkinkan Audit Manager untuk menerima temuan berbasis kontrol dari Security Hub CSPM.

8 Desember 2020

[Integrasi baru dengan Aqua Security Kube-Bench](#)

Security Hub CSPM menambahkan integrasi dengan Aqua Security Kube-Bench. Integrasi mengirimkan temuan ke Security Hub CSPM.

24 November 2020

[Cloud Custodian sekarang tersedia di Wilayah Tiongkok](#)

Integrasi dengan Cloud Custodian sekarang tersedia di Wilayah Tiongkok (Beijing) dan China (Ningxia).

24 November 2020

[BatchImportFindings sekarang dapat digunakan untuk memperbarui bidang tambahan](#)

Sebelumnya, Anda tidak dapat menggunakan BatchImportFindings untuk memperbarui uiConfidence ,Criticality ,RelatedFindings ,Severity, dan Types bidang. Sekarang, jika bidang ini belum diperbarui olehBatchUpdateFindings , mereka dapat diperbarui olehBatchImportFindings . Setelah diperbarui olehBatchUpdateFindings , mereka tidak dapat diperbarui olehBatchImportFindings .

24 November 2020

[Security Hub CSPM sekarang terintegrasi dengan AWS Organizations](#)

Pelanggan sekarang dapat mengelola akun anggota menggunakan konfigurasi akun Organizations mereka. Akun manajemen organisasi menunjuk akun administrator CSPM Security Hub, yang menentukan akun organisasi mana yang akan diaktifkan di CSPM Security Hub. Proses undangan manual masih dapat digunakan untuk akun yang bukan bagian dari organisasi.

23 November 2020

[Menghapus format daftar temuan terpisah untuk kontrol volume tinggi](#)

Daftar temuan untuk kontrol tidak lagi menggunakan format halaman Temuan ketika ada sejumlah besar temuan.

19 November 2020

[Integrasi pihak ketiga yang baru dan diperbarui](#)

Security Hub CSPM sekarang mendukung integrasi dengan cloudtamer.io, 3, Prowler, dan Kubernetes Security. CORESec StackRox IBM QRadar tidak lagi mengirimkan temuan. Itu hanya menerima temuan.

30 Oktober 2020

[Ditambahkan pilihan untuk men-download daftar temuan dari halaman rincian kontrol.](#)

Pada halaman detail kontrol, opsi Unduh baru memungkinkan Anda mengunduh daftar temuan ke file.csv. Daftar yang diunduh menghormati filter apa pun yang ada dalam daftar. Jika Anda memilih temuan spesifik, maka daftar yang diunduh hanya mencakup temuan tersebut.

26 Oktober 2020

[Ditambahkan pilihan untuk men-download daftar kontrol dari halaman rincian standar.](#)

Pada halaman detail standar, opsi Unduh baru memungkinkan Anda mengunduh daftar kontrol ke file.csv. Daftar yang diunduh menghormati filter apa pun yang ada dalam daftar. Jika Anda memilih kontrol tertentu, maka daftar yang diunduh hanya menyertakan kontrol itu.

26 Oktober 2020

[Integrasi mitra baru dan diperbarui](#)

Security Hub CSPM sekarang terintegrasi dengan. ThreatModeler Memperbarui integrasi mitra berikut untuk mencerminkan nama produk baru mereka. Twistlock Enterprise Edition sekarang menjadi Palo Alto Networks - Prisma Cloud Compute. Juga dari Palo Alto Networks, Demisto sekarang Cortex XSOAR dan Redlock sekarang Prisma Cloud Enterprise.

23 Oktober 2020

[Security Hub CSPM diluncurkan di Tiongkok \(Beijing\) dan China \(Ningxia\)](#)

Security Hub CSPM sekarang tersedia di Wilayah Tiongkok (Beijing) dan China (Ningxia).

21 Oktober 2020

[Format yang direvisi untuk atribut ASFF dan integrasi pihak ketiga](#)

Daftar [atribut ASFF](#) dan [integrasi mitra](#) sekarang menggunakan format berbasis daftar, bukan tabel. Sintaks ASFF, atribut, dan tipe taksonomi sekarang dalam topik terpisah.

15 Oktober 2020

[Halaman detail standar yang didesain ulang](#)

Halaman detail standar untuk standar yang diaktifkan sekarang menampilkan daftar kontrol tab. Tab memfilter daftar kontrol berdasarkan status kontrol.

7 Oktober 2020

[CloudWatch Acara yang diganti dengan EventBridge](#)

Mengganti referensi ke CloudWatch Acara Amazon dengan Amazon EventBridge.

1 Oktober 2020

[Integrasi baru dengan Blue Hexagon for AWS, Alcide KaUdit, dan Palo Alto Networks VM-series.](#)

Security Hub CSPM sekarang terintegrasi dengan Blue Hexagon for AWS, Alcide KaUdit, dan Palo Alto Networks VM-Series. Blue Hexagon for AWS dan Kaudit mengirimkan temuan ke Security Hub CSPM. Seri VM menerima temuan dari Security Hub CSPM.

30 September 2020

[Objek detail sumber daya baru dan diperbarui di ASFF](#)

Ditambahkan Resources .Details objek baru untuk AwsApiGatewayRestApi, AwsApiGatewayStage, AwsApiGatewayV2Api, AwsApiGatewayV2Stage, AwsCertificateManagerCertificate, AwsElasticLoadBalancing, AwsElasticLoadBalancingV2, AwsElasticLoadBalancingV2Listener, AwsElasticLoadBalancingV2ListenerV2, AwsElasticLoadBalancingV2TargetGroup, AwsElasticLoadBalancingV2TargetGroupV2, AwsElasticLoadBalancingV2TargetGroupV2ListenerV2, dan AwsElasticLoadBalancingV2TargetGroupV2ListenerV2. Menambahkan detail keAwsCloudFrontDistribution, AwsIamRole, dan AwsIamAccessKey objek.

30 September 2020

[ResourceRole Atribut baru untuk sumber daya di ASFF untuk melacak apakah sumber daya adalah aktor atau target.](#)

ResourceRole Atribut untuk sumber daya menunjukkan apakah sumber daya adalah target dari aktivitas pencarian atau pelaku aktivitas pencarian. Nilai yang valid adalah ACTOR dan TARGET.

30 September 2020

Menambahkan AWS Systems Manager Patch Manager ke integrasi AWS layanan yang tersedia	AWS Systems Manager Patch Manager sekarang terintegrasi dengan Security Hub CSPM. Patch Manager mengirimkan temuan ke Security Hub CSPM ketika instance dalam armada pelanggan tidak sesuai dengan standar kepatuhan patch mereka.	22 September 2020
Menambahkan kontrol baru ke standar Praktik Terbaik Keamanan AWS Dasar	Menambahkan kontrol baru untuk layanan berikut: Amazon EC2 (EC2.7 dan EC2 .8), Amazon EMR (EMR.1), IAM (IAM.8), Amazon RDS (RDS.4 hingga RDS.8), Amazon S3 (S3.6), dan (.1 dan .2). AWS Secrets Manager SecretsManager	15 September 2020
Kunci konteks baru untuk kebijakan IAM untuk mengontrol akses ke bidang BatchUpdateFindings	Kebijakan IAM sekarang dapat dikonfigurasi untuk membatasi akses ke bidang dan nilai bidang saat menggunakan BatchUpdateFindings	10 September 2020
Akses yang diperluas ke BatchUpdateFindings akun anggota	Secara default, akun anggota sekarang memiliki akses yang BatchUpdateFindings sama dengan akun administrator.	10 September 2020

Kontrol baru untuk AWS KMS Standar Praktik Terbaik Keamanan Dasar	Menambahkan dua kontrol baru (KMS.1 dan KMS.2) ke Standar Praktik Terbaik Keamanan Dasar. Kontrol baru memeriksa apakah kebijakan IAM membatasi akses ke tindakan AWS KMS dekripsi.	9 September 2020
Menghapus temuan tingkat akun untuk kontrol	Security Hub CSPM tidak lagi menghasilkan temuan tingkat akun untuk kontrol. Hanya temuan tingkat sumber daya yang dihasilkan.	1 September 2020
PatchSummaryObjek baru di ASFF	Menambahkan PatchSummary objek ke ASFF. PatchSummary Objek memberikan informasi tentang kepatuhan tambalan sumber daya relatif terhadap standar kepatuhan yang dipilih.	1 September 2020
Halaman detail kontrol yang didesain ulang	Halaman detail untuk kontrol didesain ulang. Daftar pencarian kontrol menyediakan tab untuk memungkinkan Anda memfilter daftar dengan cepat berdasarkan status kepatuhan. Anda juga dapat dengan cepat melihat temuan yang ditekan. Setiap entri menyediakan akses ke detail tambahan tentang sumber daya penemuan, AWS Config aturan, dan catatan pencarian.	28 Agustus 2020

Opsi filter baru untuk temuan	Untuk menemukan filter, Anda dapat menggunakan filter <code>is not</code> untuk menemukan temuan yang nilai bidangnya tidak sama dengan nilai filter. Anda dapat menggunakan <code>is not</code> untuk menemukan temuan yang nilai bidangnya tidak dimulai dengan nilai filter yang ditentukan.	28 Agustus 2020
Objek detail sumber daya baru di ASFF	Menambahkan Resources .Details objek baru untuk jenis sumber daya berikut: <code>AwsDynamoDbTable</code> <code>AwsEc2Eip</code> <code>AwsIamPolicy</code> <code>AwsIamUser</code> <code>AwsRdsDbCluster</code> <code>AwsRdsDbClusterSnapshot</code> <code>AwsSecretsManagerSecret</code>	18 Agustus 2020
Integrasi baru dengan RSA Archer	Security Hub CSPM sekarang terintegrasi dengan RSA Archer. RSA Archer menerima temuan dari Security Hub CSPM.	18 Agustus 2020
Bidang Deskripsi Baru untuk AwsKmsKey	Menambahkan Description bidang ke <code>AwsKmsKey</code> objek di bawah Resources .Details .	18 Agustus 2020

<u>Menambahkan bidang ke AwsRdsDbInstance</u>	Menambahkan beberapa atribut ke <code>AwsRdsDbInstance</code> objek di <code>bawahResources</code> <code>.Details</code> .	18 Agustus 2020
<u>Memperbarui cara Security Hub CSPM menentukan status keseluruhan kontrol</u>	Untuk kontrol yang tidak memiliki temuan, statusnya adalah No data, bukan Unknown. Status kontrol mencakup temuan tingkat akun dan tingkat sumber daya. Status kontrol tidak menggunakan status alur kerja temuan, kecuali untuk mengabaikan temuan yang ditekan.	13 Agustus 2020
<u>Memperbarui cara Security Hub CSPM menghitung skor keamanan untuk standar</u>	Saat menghitung skor keamanan untuk standar, Security Hub CSPM sekarang mengabaikan kontrol dengan status No Data. Skor keamanan adalah proporsi kontrol yang diteruskan ke kontrol yang diaktifkan, tidak termasuk kontrol tanpa data.	13 Agustus 2020
<u>Opsi baru untuk mengaktifkan kontrol baru secara otomatis dalam standar yang diaktifkan</u>	Menambahkan opsi <code>Pengaturan</code> untuk secara otomatis mengaktifkan kontrol baru dalam standar yang diaktifkan. Anda juga dapat menggunakan operasi <code>UpdateSecurityHubConfiguration</code> API untuk mengonfigurasi opsi ini.	31 Juli 2020

<u>Kontrol baru untuk standar Standar Keamanan Data Industri Kartu Pembayaran (PCI DSS)</u>	Menambahkan kontrol baru ke standar PCI DSS. Pengidentifikasi kontrol baru adalah PCI.DMS.1, PCI. EC2.5, PCI. EC2.6, PCI. ELBV2.1, PCI. GuardDuty.1, PCI.IAM.7, PCI.IAM.8, PCI.S3.5, PCI.S3.6, PCI. SageMaker.1, PCI.SSM.2, dan PCI.SSM.3.	29 Juli 2020
<u>Kontrol baru dan diperbarui untuk standar Praktik Terbaik Keamanan Dasar</u>	Menambahkan kontrol baru ke standar Praktik Terbaik Keamanan Dasar. Pengidentifikasi kontrol baru adalah AutoScaling .1, DMS.1, EC2 .4, .6, S3.5, dan EC2 SSM.3. Memperbarui judul ACM.1 dan mengubah nilai daysToExpiration parameter menjadi 30.	29 Juli 2020
<u>Vulnerabilities Objek baru di ASFF</u>	Menambahkan Vulnerabilities objek, yang memberikan informasi tentang kerentanan yang terkait dengan temuan.	1 Juli 2020
<u>Resource.Details Objek baru di ASFF untuk grup Auto Scaling, volume EC2, dan EC2 VPCs</u>	MenambahkanAwsAutoScalingAutoScalingGroup, AWSEc2Volume, dan AwsEc2Vpc objek keResource.Details.	1 Juli 2020
<u>NetworkPath Objek baru di ASFF</u>	Ditambahkan NetworkPath objek, yang memberikan informasi tentang jalur jaringan yang terkait dengan temuan.	1 Juli 2020

Secara otomatis menyelesaikan temuan kapan Compliance.Status PASSED	Untuk temuan dari kontrol, jika Compliance.Status ada PASSED, maka Security Hub CSPM secara otomatis disetel Workflow.Status ke. RESOLVED	24 Juni 2020
AWS Command Line Interface contoh	Ditambahkan AWS CLI sintaks dan contoh untuk beberapa tugas Security Hub CSPM. Termasuk mengaktifkan Security Hub CSPM, mengelola wawasan, mengelola standar dan kontrol, mengelola integrasi produk, dan menonaktifkan CSPM Security Hub.	24 Juni 2020
Severity.Original Atribut baru di ASFF	Menambahkan Severity.Original atribut, yang merupakan tingkat keparahan asli dari penyedia temuan. Ini menggantikan atribut usang Severity.Product .	20 Mei 2020
Compliance.StatusReasons Objek baru di ASFF untuk detail tentang status kontrol	Ditambahkan Compliance.StatusReasons objek, yang menyediakan konteks tambahan untuk status kontrol saat ini.	20 Mei 2020

[Standar Praktik Terbaik
Keamanan AWS Dasar Baru](#)

Menambahkan standar Praktik Terbaik Keamanan AWS Dasar yang baru, yang merupakan serangkaian kontrol yang mendeteksi kapan akun dan sumber daya yang Anda gunakan menyimpang dari praktik terbaik keamanan.

22 April 2020

[Opsi konsol baru untuk
memperbarui status alur kerja
untuk temuan](#)

Menambahkan informasi untuk menggunakan konsol Security Hub atau API untuk menyetel status alur kerja untuk temuan.

16 April 2020

[BatchUpdateFindings API baru untuk pembaruan
pelanggan terhadap temuan](#)

Menambahkan informasi tentang penggunaan BatchUpdateFindings untuk memperbarui informasi yang terkait dengan proses investigasi temuan. BatchUpdateFindings menggantikan UpdateFindings, yang sudah usang.

16 April 2020

[Pembaruan untuk AWS Security Finding Format \(ASFF\)](#)

Menambahkan beberapa jenis sumber daya baru. Menambahkan Label atribut baru ke Severity objek. Label dimaksudkan untuk menggantikan Normalized bidang. Menambahkan Workflow objek baru untuk melacak proses investigasi terhadap sebuah temuan. Workflow berisi Status atribut, yang menggantikan Workflowstate atribut yang ada.

12 Maret 2020

[Pembaruan ke halaman Integrasi](#)

Diperbarui untuk mencerminkan perubahan pada halaman Integrasi. Untuk setiap integrasi, halaman sekarang menunjukkan kategori integrasi dan apakah setiap integrasi mengirimkan temuan ke atau menerima temuan dari Security Hub CSPM. Ini juga menyediakan langkah-langkah spesifik yang diperlukan untuk mengaktifkan setiap integrasi.

26 Februari 2020

[Integrasi produk pihak ketiga yang baru](#)

Menambahkan integrasi produk baru berikut: Cloud Custodian, FireEye Helix, Forcepoint CASB, Forcepoint DLP, Forcepoint NGFW, Rackspace Cloud Native Security, dan Vectra.ai Cognito Detect.

Februari 21, 2020

Standar keamanan baru untuk Standar Keamanan Data Industri Kartu Pembayaran (PCI DSS)	Menambahkan standar keamanan CSPM Security Hub untuk Payment Card Industry Data Security Standard (PCI DSS). Ketika standar ini diaktifkan, Security Hub CSPM melakukan pemeriksaan otomatis terhadap kontrol yang terkait dengan persyaratan PCI DSS.	13 Februari 2020
Pembaruan untuk AWS Security Finding Format (ASFF)	Menambahkan bidang untuk persyaratan terkait untuk kontrol standar . Menambahkan jenis sumber daya baru dan detail sumber daya baru . ASFF juga sekarang memungkinkan Anda menyediakan hingga 32 sumber daya.	5 Februari 2020
Opsi baru untuk menonaktifkan kontrol standar keamanan individu	Menambahkan informasi tentang cara mengontrol apakah setiap kontrol standar keamanan individu diaktifkan.	15 Januari 2020
Pembaruan konsep CSPM Security Hub	Memperbarui beberapa deskripsi dan menambahkan istilah baru ke konsep CSPM Security Hub .	September 21, 2019
AWS Security Hub Cloud Security Posture Management (CSPM) rilis ketersediaan umum	Pembaruan konten untuk mencerminkan peningkatan yang dilakukan pada Security Hub CSPM selama periode beta.	25 Juni 2019

[Menambahkan langkah-langkah remediasi untuk pemeriksaan CIS AWS Foundations](#)

Menambahkan langkah-langkah remediasi ke [Standar Keamanan yang Didukung di AWS Security Hub Cloud Security Posture Management \(CSPM\)](#).

April 15, 2019

[rilis beta AWS Security Hub Cloud Security Posture Management \(CSPM\)](#)

Menerbitkan versi rilis beta dari Panduan Pengguna AWS Security Hub Cloud Security Posture Management (CSPM) Security Hub.

November 18, 2018

Terjemahan disediakan oleh mesin penerjemah. Jika konten terjemahan yang diberikan bertentangan dengan versi bahasa Inggris aslinya, utamakan versi bahasa Inggris.