



Respons Insiden Keamanan AWS Panduan Pengguna



Versi May 13, 2026

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Respons Insiden Keamanan AWS Panduan Pengguna:

Copyright © 2026 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 mungkin tidak terafiliasi, terkait dengan, atau disponsori oleh Amazon.

Table of Contents

Apa itu Respons Insiden Keamanan AWS?	1
Konfigurasi yang didukung	1
Ringkasan Fitur	3
Pemantauan dan investigasi	3
Merampingkan respons insiden	3
Solusi keamanan swalayan	3
Dasbor untuk visibilitas	3
Postur keamanan	3
Bantuan yang dipercepat	4
Kesiapan dan kesiapan	4
Konsep dan Terminologi	5
Memulai	8
Mendaftar untuk Akun AWS	8
Panduan orientasi	8
Bersiaplah untuk onboarding	8
Prasyarat orientasi	9
Langkah 1: Aktifkan Respons Insiden Keamanan AWS	10
Langkah 2: Konfigurasi tim respons insiden Anda	13
Langkah 3: Memahami jenis kasus dan manajemen	14
Langkah 4: Integrasikan dengan alat yang ada	18
Aktifkan Respons Insiden Keamanan menggunakan API/CLI	22
Lampiran A: Titik kontak dan informasi penting	24
Matriks RACI	25
Pilih akun keanggotaan	27
Siapkan detail keanggotaan	29
Mengaitkan akun dengan AWS Organizations	29
Siapkan respons proaktif dan alur kerja triaging peringatan	30
Memahami Pengarsipan Otomatis dengan Respon Proaktif	31
Tugas pengguna	33
Dasbor Respons Insiden Keamanan	33
Mengelola Tim Respons Insiden saya	33
Preferensi Komunikasi	34
Asosiasi akun ke AWS Organizations	36
Pemantauan dan investigasi	3
Agen Investigasi AI	42

Mengandung	46
Membasmi	50
Memulihkan	51
Laporan bulanan	51
Kasus	53
Buat kasus yang AWS didukung	53
Membuat kasus yang dikelola sendiri	57
Bekerja dengan teknisi Respons Insiden AWS Keamanan	58
Menanggapi kasus yang AWS dihasilkan	61
Mengelola Kasus	62
Mengubah status kasus	62
Mengubah resolver	63
Item Aksi	63
Edit kasus	63
Komunikasi	64
Izin	64
Lampiran	65
Tag	66
Kegiatan kasus	66
Menutup kasus	66
Bekerja dengan CloudFormation StackSets	67
CloudFormation templat	67
Batalkan Keanggotaan	81
Sumber daya penandaan Respons Insiden Keamanan AWS	83
Menggunakan AWS CloudShell	84
Memperoleh izin IAM untuk AWS CloudShell	84
Berinteraksi dengan Respons Insiden Keamanan menggunakan AWS CloudShell	85
CloudTrail log	86
Informasi Respons Insiden Keamanan di CloudTrail	86
Memahami entri file log Respons Insiden Keamanan	88
Mengelola akun dengan AWS Organizations	91
Pertimbangan dan rekomendasi	91
Akses tepercaya	92
Izin yang diperlukan untuk menunjuk akun administrator Respons Insiden Keamanan yang didelegasikan	94
Mengelola keanggotaan dengan unit organisasi (OU)	96
Menambahkan anggota ke Respons Insiden Keamanan AWS	97

Menghapus anggota dari Respons Insiden Keamanan AWS	97
.....	98
Mengelola acara menggunakan EventBridge	98
Mengirim peristiwa Respon Insiden Keamanan	99
Referensi detail acara	100
Peristiwa Kasus	102
Acara Komentar Kasus	105
Acara Keanggotaan	108
Menggunakan Respons Insiden Keamanan AWS Acara	110
Tutorial: Mengirim peringatan Amazon Simple Notification Service untuk acara Membership Updated	112
Prasyarat	112
Tutorial: Membuat dan berlangganan topik Amazon SNS	112
Tutorial: Daftarkan aturan acara	113
Tutorial: Uji aturan Anda	114
Aturan alternatif: Pembaruan Kasus Respons Insiden Keamanan	115
Pemecahan masalah	116
Masalah	116
Kesalahan	116
Dukungan	117
Keamanan	119
Perlindungan Data di Respons Insiden Keamanan AWS	119
Enkripsi data	120
Pengumpulan dan penggunaan data	121
Data residensi dan perilaku regional	123
Akses dan izin data	125
Inter-network privasi lalu lintas	126
Lalu lintas antara layanan dan aplikasi serta klien on-premise	126
Lalu lintas antara AWS sumber daya di Wilayah yang sama	127
Identity and Access Management	127
Mengautentikasi dengan identitas	128
Bagaimana Respons Insiden Keamanan AWS Bekerja dengan IAM	132
Memecahkan masalah Respons Insiden Keamanan AWS identitas dan akses	139
Menggunakan peran layanan	141
Menggunakan Peran Terkait Layanan	141
AWSServiceRoleForSecurityIncidentResponse	142
AWSServiceRoleForSecurityIncidentResponse_Triase	143

Wilayah yang didukung untuk SLR	145
AWS Kebijakan Terkelola	146
kebijakan terkelola: AWSSecurityIncidentResponseServiceRolePolicy	147
kebijakan terkelola: AWSSecurityIncidentResponseAdmin	148
kebijakan terkelola: AWSSecurityIncidentResponseReadOnlyAccess	148
kebijakan terkelola: AWSSecurityIncidentResponseCaseFullAccess	149
kebijakan terkelola: AWSSecurityIncidentResponseTriageServiceRolePolicy	150
Pembaruan untuk SLR dan kebijakan terkelola	151
Respons insiden	155
Validasi kepatuhan	156
Tanggung jawab bersama untuk kepatuhan	157
Metadata sebagai data yang diatur	157
Pencatatan dan pemantauan dalam Respons Insiden AWS Keamanan	157
Ketahanan	158
Keamanan infrastruktur	158
Konfigurasi dan analisis kerentanan	159
Cross-service pencegahan wakil bingung	159
Service Quotas	161
Respons Insiden Keamanan AWS	161
Respons Insiden Keamanan AWS Panduan Teknis	162
Abstrak	162
Apakah Anda sudah Well-Architected?	162
Pengantar	163
Sebelum Anda mulai	163
AWS ikhtisar respons insiden	164
Persiapan	171
Orang	171
Proses	175
Teknologi	183
Ringkasan item persiapan	190
Operasi	195
Deteksi	196
Analisis	200
Penahanan	205
Pemberantasan	211
Pemulihan	212
Kesimpulan	214

Aktivitas pascainsiden	215
Menetapkan kerangka kerja untuk belajar dari insiden	215
Menetapkan metrik keberhasilan	217
Menggunakan indikator penyusupan	221
Pendidikan dan pelatihan berkelanjutan	222
Kesimpulan	222
Kontributor	223
Lampiran A: Definisi kemampuan cloud	223
Pencatatan log dan peristiwa	223
Visibilitas dan peringatan	225
Otomatisasi	228
Penyimpanan aman	229
Kemampuan Keamanan Masa Depan dan Kustom	229
Lampiran B: sumber daya respons AWS insiden	230
Sumber daya playbook	230
Sumber daya forensik	230
Pemberitahuan	231
Riwayat dokumen	232
.....	ccli

Apa itu Respons Insiden Keamanan AWS?

Respons Insiden Keamanan AWS membantu Anda dengan cepat mempersiapkan, menanggapi, dan menerima panduan untuk membantu memulihkan diri dari insiden keamanan. Ini termasuk insiden seperti pengambilalihan akun, pelanggaran data, dan serangan ransomware.

Respons Insiden Keamanan AWS triase temuan ancaman, meningkatkan peristiwa keamanan, dan mengelola kasus yang membutuhkan perhatian segera Anda. Selain itu, Anda memiliki akses ke insinyur Respons Insiden Keamanan, yang akan menyelidiki sumber daya yang terkena dampak.

Note

Tidak ada jaminan sumber daya yang terkena dampak dapat dipulihkan. Kami merekomendasikan untuk membuat dan memelihara cadangan untuk sumber daya yang dapat memengaruhi kebutuhan bisnis Anda.

Respons Insiden Keamanan AWS bekerja dengan layanan [AWS Deteksi dan Respons](#) lainnya, memandu Anda melalui seluruh siklus hidup insiden — mulai dari deteksi hingga pemulihan.

Daftar Isi

- [Konfigurasi yang didukung](#)
- [Ringkasan Fitur](#)

Konfigurasi yang didukung

Respons Insiden Keamanan AWS mendukung konfigurasi bahasa dan wilayah berikut:

- Bahasa: Respons Insiden Keamanan AWS menyediakan dukungan bahasa Inggris khusus. Dukungan bahasa Jepang terbatas pada jam kerja Waktu Standar Jepang dan dilengkapi dengan batasan khusus:

Note

Dukungan bahasa Jepang diberikan dengan upaya terbaik selama jam kerja (09:00-17:00, Senin-Jumat, tidak termasuk hari libur)

- AWS Wilayah yang Didukung:

Respons Insiden Keamanan AWS tersedia dalam subset dari Wilayah AWS Di Wilayah yang didukung ini, Anda membuat keanggotaan, membuat dan melihat kasus, dan mengakses dasbor.

- AS Timur (Ohio)
- AS Barat (Oregon)
- AS Timur (Virginia)
- Eropa (Frankfurt)
- Eropa (Irlandia)
- Eropa (London)
- Eropa (Milan)
- Eropa (Paris)
- Eropa (Spanyol)
- Eropa (Stockholm)
- Europe (Zurich)
- Asia Pasifik (Hong Kong)
- Asia Pasifik (Hyderabad)
- Asia Pasifik (Jakarta)
- Asia Pasifik (Melbourne)
- Asia Pasifik (Mumbai)
- Asia Pasifik (Seoul)
- Asia Pasifik (Singapura)
- Asia Pasifik (Sydney)
- Asia Pasifik (Tokyo)
- (Canada (Central)
- Timur Tengah (Bahrain)
- Timur Tengah (UEA)
- Amerika Selatan (Sao Paulo)
- Africa (Cape Town)

Saat Anda mengaktifkan fitur pemantauan dan investigasi, Respons Insiden Keamanan AWS pantau GuardDuty temuan Amazon dari semua iklan aktif Wilayah AWS. Sebagai praktik

aktivitas yang tidak sah atau tidak biasa, bahkan di Wilayah AWS tempat Anda tidak secara aktif menyebarkan sumber daya. Dengan demikian, Anda meningkatkan postur keamanan Anda secara keseluruhan dan mempertahankan cakupan deteksi ancaman yang komprehensif di seluruh AWS lingkungan Anda.

Note

Amazon GuardDuty melaporkan temuan untuk wilayah yang dikonfigurasi. Jika Anda memilih untuk tidak mengaktifkan layanan di wilayah tertentu, maka peringatan tidak akan tersedia.

Ringkasan Fitur

Pemantauan dan investigasi

Respons Insiden Keamanan AWS dengan cepat meninjau peringatan ancaman keamanan dari Amazon GuardDuty dan integrasi pihak ketiga dengan AWS Security Hub CSPM, mengurangi jumlah yang perlu dianalisis tim Anda. Ini mengonfigurasi aturan penekanan berdasarkan lingkungan Anda untuk mengurangi peringatan ancaman yang perlu Anda lakukan triase dan selidiki.

Merampingkan respons insiden

Skala dan jalankan respons insiden dalam hitungan menit dengan pemangku kepentingan, layanan pihak ketiga, dan alat yang relevan.

Solusi keamanan swalayan

Respons Insiden Keamanan AWS menyediakan APIs untuk mengintegrasikan dan memungkinkan Anda membangun solusi keamanan khusus Anda sendiri.

Dasbor untuk visibilitas

Pantau dan ukur kesiapan respons insiden.

Postur keamanan

Akses praktik AWS terbaik dan alat yang diperiksa untuk penilaian keamanan dan investigasi respons insiden cepat.

Bantuan yang dipercepat

Connect dengan teknisi Security Incident Response untuk menyelidiki, memuat, dan menerima panduan tentang cara memulihkan diri dari peristiwa keamanan.

Kesiapan dan kesiapan

Terapkan pemberitahuan yang disederhanakan dengan menyiapkan tim Respons Insiden Anda yang memicu peringatan ke individu atau grup yang ditunjuk, dengan kebijakan izin yang telah ditentukan sebelumnya.

Konsep dan Terminologi

Istilah dan konsep berikut ini penting untuk memahami Respons Insiden Keamanan AWS layanan dan cara kerjanya.

Lingkup: Respons Insiden Keamanan AWS sejalan dengan National Institute of Standards and Technology (NIST) 800-61 Computer Security Incident Handling Guide, memberikan pendekatan yang konsisten untuk manajemen acara keamanan yang terkait dengan praktik terbaik industri.

Analisis: Investigasi terperinci dan pemeriksaan peristiwa keamanan untuk memahami ruang lingkup, dampak, dan akar penyebabnya.

Respons Insiden Keamanan AWS portal layanan: Portal swalayan bagi Anda untuk memulai dan mengelola kasus peristiwa keamanan. Komunikasi dan pelaporan yang sedang berlangsung difasilitasi melalui sistem tiket, pemberitahuan otomatis, dan keterlibatan langsung dengan tim layanan.

Komunikasi: Dialog yang sedang berlangsung dan berbagi informasi antara tim AWS Security Incident Response dan pelanggan selama proses respons insiden.

Penahanan, Pemberantasan, dan Pemulihan: Pencegahan aktivitas tambahan yang tidak sah (penahanan), ditambah dengan penghapusan sumber daya yang tidak sah dan kerentanan asli (pemberantasan), dan memulihkan sumber daya untuk kembali ke bisnis seperti biasa.

Continuous Improvement: Respons Insiden Keamanan AWS menggabungkan umpan balik dan pelajaran dari keterlibatan sebelumnya untuk meningkatkan kemampuan deteksi, proses investigasi, dan tindakan remediasi. Respons Insiden Keamanan AWS juga tetap up-to-date dengan ancaman keamanan terbaru dan praktik terbaik untuk mengatasi tantangan keamanan yang berkembang.

Peristiwa Keamanan Siber: Tindakan yang menggunakan sistem informasi atau jaringan untuk menghasilkan efek buruk pada sistem, jaringan, atau informasi yang dikandungnya.

Insiden Keamanan Siber: Pelanggaran atau ancaman pelanggaran kebijakan keamanan komputer, kebijakan penggunaan yang dapat diterima, atau praktik keamanan standar.

Insinyur Respons Insiden Keamanan: Sekelompok individu yang memberikan dukungan selama acara keamanan aktif. Untuk kasus AWS yang didukung, ini adalah insinyur Respons Insiden Keamanan.

Alur Kerja Respons Insiden: Urutan langkah dan aktivitas yang ditentukan yang terlibat dalam end-to-end pengelolaan peristiwa keamanan, selaras dengan standar NIST 800-61.

Investigative Tooling: Respons Insiden Keamanan AWS alat dan peran terkait layanan yang digunakan untuk meninjau kesehatan operasional akun dan sumber daya Anda.

Pelajaran yang Dipelajari: Tinjauan dan dokumentasi respons peristiwa keamanan untuk mengidentifikasi area untuk perbaikan dan menginformasikan perencanaan respons insiden di masa depan.

Pemantauan dan Investigasi: Respons Insiden Keamanan AWS dengan cepat meninjau peringatan keamanan dari Amazon GuardDuty, membawa ke garis depan peringatan paling penting yang perlu dianalisis tim Anda. Ini mengonfigurasi aturan penekanan berdasarkan spesifikasi lingkungan Anda untuk mencegah peringatan yang tidak perlu.

Persiapan: Kegiatan yang dilakukan untuk membuat organisasi siap merespons dan mengelola peristiwa keamanan secara efektif, seperti mengembangkan rencana respons insiden dan prosedur pengujian.

Pelaporan dan Komunikasi: Proses yang digunakan untuk memberi Anda informasi selama proses respons insiden, termasuk pemberitahuan otomatis, jembatan panggilan, dan pengiriman artefak investigasi. Respons Insiden Keamanan AWS menyediakan satu dasbor terpusat Konsol Manajemen AWS untuk mengelola semua Respons Insiden Keamanan AWS upaya Anda.

Responder Generated Intelligence: indikator kompromi; taktik, teknik, dan prosedur; dan pola terkait yang diamati oleh AWS investigasi.

Keahlian Acara Keamanan: Pengetahuan dan keterampilan khusus yang diperlukan untuk merespons dan mengelola peristiwa keamanan secara efektif, terutama dalam konteks AWS cloud.

Model Tanggung Jawab Bersama: Pembagian tanggung jawab keamanan antara AWS dan pelanggan, di mana AWS bertanggung jawab atas keamanan cloud, dan pelanggan bertanggung jawab atas keamanan di cloud.

Ancaman Intelijen: Umpan data internal dan eksternal yang berisi rincian aktivitas yang tidak sah untuk membantu mengidentifikasi dan menanggapi ancaman keamanan yang berkembang.

Sistem Tiket: Platform manajemen kasus khusus yang memungkinkan Anda melakukan onboard dan mengelola kasus peristiwa keamanan, menambahkan lampiran, dan melacak siklus hidup respons insiden.

Triase: Penilaian awal dan prioritas peristiwa keamanan untuk menentukan respons yang tepat dan langkah selanjutnya.

Alur Kerja: Urutan yang ditentukan dari langkah-langkah dan kegiatan yang terlibat dalam end-to-end pengelolaan peristiwa keamanan.

Memulai

[Memulai dengan Respons Insiden Keamanan AWS](#)

Daftar Isi

- [Mendaftar untuk Akun AWS](#)
- [Panduan orientasiing](#)
- [Matriks RACI](#)
- [Pilih akun keanggotaan](#)
- [Menyiapkan rincian keanggotaan](#)
- [Mengaitkan akun dengan AWS Organizations](#)
- [Siapkan respons proaktif dan alur kerja triaging peringatan](#)

Mendaftar untuk Akun AWS

Untuk memulai AWS, Anda membutuhkan Akun AWS. Untuk informasi tentang membuat Akun AWS, lihat [Memulai dengan Akun AWS](#) di Panduan AWS Account Management Referensi.

Panduan orientasiing

Respons Insiden Keamanan AWS membantu Anda mempersiapkan, menanggapi, dan memulihkan dari peristiwa keamanan seperti pengambilalihan akun, pelanggaran data, dan serangan ransomware. Layanan melakukan triase temuan dari Amazon GuardDuty dan AWS Security Hub CSPM, meningkatkan peristiwa keamanan, dan mengelola kasus yang memerlukan perhatian Anda. Anda juga memiliki akses ke tim Security Incident Response Engineering, yang menyelidiki sumber daya yang terkena dampak dan memberikan panduan sepanjang siklus hidup insiden.

Untuk ikhtisar lengkap tentang layanan ini, lihat [Apa itu Respons Insiden Keamanan AWS?](#)

Bersiaplah untuk onboarding

Sebaiknya gunakan pendekatan proof-of-concept (POC) saat mengimplementasikan. Respons Insiden Keamanan AWS Sebelum penerapan, selesaikan langkah-langkah persiapan berikut dengan tim internal dan tim AWS akun Anda.

- Identifikasi pemangku kepentingan utama: Petakan pembuat keputusan respons insiden di organisasi Anda. Keterlibatan mereka dalam pembaruan kebijakan dan perubahan proses sangat penting untuk peluncuran yang sukses.
- Validasi sumber pencarian: Konfirmasikan bahwa semua sumber pencarian keamanan dikonfigurasi dan digunakan dengan benar. GuardDuty dan Security Hub CSPM adalah input penting untuk teknologi auto-triage layanan.
- Tentukan cakupan akun: Putuskan apakah Respons Insiden Keamanan AWS akan mencakup seluruh AWS organisasi Anda atau unit organisasi tertentu (OU). Mendefinisikan cakupan ini lebih awal membuat implementasi dan penskalaan lebih mudah.
- Tetapkan protokol eskalasi: Perbarui prosedur eskalasi yang ada untuk disertakan. Respons Insiden Keamanan AWS Komunikasikan protokol yang diperbarui kepada semua pemangku kepentingan dan personel respons.
- Kumpulkan titik kontak dan informasi penting: Mengumpulkan metadata pelanggan lebih awal memastikan pengalaman orientasi yang lancar dan memungkinkan penjangkauan tepat waktu dari tim AWS Security Incident Response Engineering saat diperlukan. Lihat [Lampiran A: Titik kontak dan informasi penting](#) untuk informasi yang diperlukan.

Prasyarat orientasi

Satu-satunya prasyarat yang diperlukan adalah mengaktifkan [AWS Organizations](#) dengan Semua Fitur diaktifkan. Penagihan konsolidasi saja tidak cukup.

Meskipun tidak diperlukan, kami sangat menyarankan untuk mengaktifkan [Amazon GuardDuty](#) dan [AWS Security Hub CSPM](#) di semua akun dan aktif Wilayah AWS untuk mendapatkan nilai maksimal.

Respons Insiden Keamanan AWS

- [GuardDuty dan Respons Insiden Keamanan AWS](#)
- [GuardDuty praktik terbaik](#)

Third-party Integrasi EDR

Security Hub CSPM dapat menyerap temuan dari vendor deteksi dan respons titik akhir (EDR) pihak ketiga. Ketika dicerna, temuan ini diprioritaskan secara otomatis Respons Insiden Keamanan AWS untuk pembuatan kasus proaktif. Untuk menyiapkan integrasi EDR pihak ketiga, ikuti langkah-langkah dalam dokumentasi integrasi [CSPM Security Hub](#).

Note

Anda tidak perlu mengaktifkan standar atau kontrol CSPM Security Hub. Hanya integrasi vendor yang diperlukan untuk Respons Insiden Keamanan AWS mencerna temuan pihak ketiga.

Harga: Temuan CSPM 10.000 Security Hub pertama gratis. Setelah itu, biayanya adalah \$0,00003 per temuan. Untuk informasi selengkapnya, lihat harga [CSPM Security Hub](#).

Langkah 1: Aktifkan Respons Insiden Keamanan AWS

Proses orientasi memakan waktu sekitar 10 hingga 15 menit per AWS organisasi. Untuk penelusurannya, lihat [video Memulai](#) di dokumentasi layanan.

Note

Petunjuk di bagian ini menguraikan cara mengaktifkan Security Incident Response dan mengatur tim Anda menggunakan Respons Insiden Keamanan AWS konsol (Langkah 1 dan Langkah 2). Anda juga dapat melakukan langkah-langkah ini menggunakan API/CLI. Untuk petunjuk tentang penggunaan API/CLI, lihat [Aktifkan Respons Insiden Keamanan dan konfigurasi tim respons insiden Anda menggunakan API/CLI](#).

Aktifkan Respons Insiden Keamanan AWS menggunakan Respons Insiden Keamanan AWS konsol

1. Masuk ke Konsol AWS Manajemen menggunakan akun manajemen Anda.
2. Buka Respons Insiden Keamanan AWS konsol dan pilih Daftar.

The screenshot shows the AWS Security Incident Response console landing page. The main heading is "AWS Security Incident Response" with the subtitle "Security incident response and recovery for your accounts and workloads". Below this, a brief description states: "AWS Security Incident Response helps your central security teams quickly prepare for, respond to, and recover from security events." On the right side, there is a "Get started with AWS Security Incident Response" section with a bulleted list of features: "Automatic monitoring and triaging of alerts", "Streamline security incident response", and "Get 24/7 AWS security support and tools". A "Sign up" button is located below this list. Further down, there is a "Pricing (USD)" section with a "Learn more" link. The "How it works" section is divided into four columns: "Automated monitoring and triaging of security findings" (describing automatic detection and escalation), "24/7 Incident response support" (describing 24/7 access to engineers), "Streamline incident response" (describing self-managed response with exclusive tools), and "Monitor, track, and improve" (describing a dashboard for tracking metrics). On the right side of the "How it works" section, there are two more sections: "Getting started" with a link to "What is AWS Security Incident Response?" and "Getting started with AWS Security Incident Response", and "More resources" with a link to "Documentation".

3. Siapkan akun keanggotaan pusat Anda. Untuk panduan, lihat [Arsitektur Referensi Keamanan](#) dalam Panduan AWS Preskriptif dan [Pertimbangan dan rekomendasi](#) tentang cara akun administrator Respons Insiden Keamanan yang didelegasikan beroperasi.

✔ Successfully set delegated administrator account
✕

Step 1

Set up central membership account

Step 2

Define membership details

Step 3


Review service permissions

Step 4


Review and sign up

Set up central membership account Info

▼ What is the purpose of the central membership account?



Centralized account location
Create, manage, and access active and resolved security cases.



Manage membership
Modify and change membership configurations including permissions, contacts, and more.

Central membership account

It is recommended that you align your AWS Security Incident Response central account to the same administrator account you have enabled for services such as Amazon GuardDuty and AWS Security Hub.

Use delegated administrator account - Recommended

Delegated administrator account can manage membership and cases.

Use this account

Use this account to manage membership and cases.

Delegated administrator

<p><small>Account ID</small></p> <p>111122223333</p> <p style="text-align: center;">Remove</p>	<p><small>AWS Organizations ID</small></p> <p>0-00000000</p>
--	--

Proactive response permissions

A service-linked role for proactive response will be created in this management account to enable monitoring and triaging.

[View permission details](#)

Cancel
Next

4. Masuk ke akun administrator yang didelegasikan.
5. Masukkan detail keanggotaan Anda dan kaitkan akun yang relevan.
6. Untuk cakupan Akun, pilih untuk mengaktifkan Respons Insiden Keamanan AWS untuk seluruh AWS organisasi Anda atau untuk OU tertentu. Anda dapat memilih cakupan di tingkat OU, tetapi tidak pada tingkat akun individu.
7. Respons proaktif aktif secara default dan menciptakan peran terkait layanan yang memungkinkan Security Incident Response Engineering untuk menelan GuardDuty temuan dan membuka kasus investigasi proaktif ketika ancaman terdeteksi. Untuk informasi selengkapnya, lihat [Respons proaktif](#).

Respons Insiden Keamanan AWS secara otomatis membuat peran `AWSServiceRoleForSecurityIncidentResponse_Triage` terkait layanan di akun AWS Organizations manajemen Anda dan di semua akun yang berada dalam cakupan.

8. (Opsional) Pilih untuk melakukan pra-otorisasi Security Incident Response Engineering untuk melakukan tindakan penahanan atas nama Anda selama insiden aktif. Tindakan penahanan yang didukung termasuk runbook untuk bucket S3 yang dikompromikan, instans EC2, dan prinsip IAM. Jika Anda melewati langkah ini, Security Incident Response Engineering akan memberikan panduan manual selama investigasi. Untuk informasi selengkapnya, lihat [Tindakan penahanan](#).

9. Tinjau izin layanan dan konfigurasi orientasi, lalu pilih Daftar.

Langkah 2: Konfigurasi tim respons insiden Anda

Setelah Anda menyelesaikan penerapan, konfigurasi tim respons insiden Anda untuk memastikan pemberitahuan dan eskalasi yang tepat selama peristiwa keamanan.

Konfigurasi tim respons insiden Anda menggunakan Respons Insiden Keamanan AWS konsol

1. Buka Respons Insiden Keamanan AWS konsol.
2. Di panel navigasi kiri, pilih Tim Respons Insiden.

3. Tambahkan hingga 10 anggota tim. Untuk setiap anggota, berikan nama, judul, dan alamat email mereka.

The screenshot shows the 'Incident Response Team' configuration page in the AWS Security Incident Response console. The page has a sidebar on the left with navigation options like 'Dashboard', 'Cases', 'Configure notifications and permissions', 'Manage membership', 'Documentation', 'Amazon GuardDuty', and 'AWS Security Hub'. The main content area is titled 'Incident Response Team' and includes a 'Set up your Incident Response Team' button. Below this, there is a section for 'Teammates (10/10)' with a note: 'You can specify up to 10 members in your Incident Response Team. Additional members can be added for individual cases.' A table lists the team members:

<input type="checkbox"/>	Name	Job title	Email
<input type="checkbox"/>	Brian Boyd	Network Analyst Lead	brianb@anycompany.com
<input type="checkbox"/>	Chris Beck	Blue Team Lead	chrisb@anycompany.com
<input type="checkbox"/>	David Buckendorf	Incident Response Manager	davidb@anycompany.com
<input type="checkbox"/>	John Bheuler	SOC Commander	johnb@anycompany.com
<input type="checkbox"/>	Jordan Schroff	SOC Operations Manager	jordans@anycompany.com
<input type="checkbox"/>	Kyle Prime	Detection Lead	wearekyle@anycompany.com

Tim Anda dapat mencakup kepemimpinan organisasi, penasihat hukum, mitra deteksi dan respons terkelola (MDR), insinyur cloud, dan pemangku kepentingan lainnya yang perlu diberi tahu selama acara keamanan.

Langkah 3: Memahami jenis kasus dan manajemen

Respons Insiden Keamanan AWS menyediakan dua jenis kasus untuk mengelola peristiwa keamanan: kasus proaktif yang dibuat secara otomatis saat ancaman terdeteksi, dan kasus reaktif yang Anda buat saat Anda membutuhkan bantuan dari Security Incident Response Engineering. Anda juga dapat memberikan visibilitas kasus kepada pihak eksternal seperti mitra, tim hukum, atau ahli materi pelajaran.

Topik-topik berikut dibahas di bagian ini:

- [Kasus proaktif](#)
- [Kasus reaktif](#)
- [Pengamat](#)

Kasus proaktif

Fitur auto-triage terus meninjau peringatan volume tinggi untuk menyaring kebisingan dan fokus pada ancaman kritis dan berdampak tinggi. Ketika ancaman potensial terdeteksi, sistem meningkatkan temuan ke responden Security Incident Response Engineering untuk penyelidikan. Jika temuan dikonfirmasi sebagai ancaman asli, kasus proaktif dibuat di portal manajemen kasus dan semua pemangku kepentingan yang dikonfigurasi diberitahu secara otomatis.

Tidak diperlukan konfigurasi manual untuk kasus proaktif selain mengaktifkan GuardDuty dan mengintegrasikan solusi keamanan pihak ketiga dengan Security Hub CSPM. Layanan ini juga terintegrasi dengan agen investigasi AI yang menghubungkan data dari berbagai sumber untuk mempercepat penyelidikan. Kemampuan ini saat ini tersedia untuk kasus reaktif yang AWS didukung.

Kasus reaktif

Respons Insiden Keamanan AWS menyediakan portal manajemen kasus berbasis langganan tempat organisasi Anda bekerja secara langsung dengan Security Incident Response Engineering. Security Incident Response Engineering membantu investigasi keamanan dan insiden aktif dengan tujuan tingkat layanan 15 menit (SLO). Tidak ada batasan jumlah kasus reaktif yang dapat Anda buka.

Untuk membuat kasus

1. Buka Respons Insiden Keamanan AWS konsol.
2. Pilih Kasus, lalu pilih Buat kasus.
3. Pilih jenis casing:
 - AWS-didukung: Ditingkatkan langsung ke Security Incident Response Engineering untuk investigasi dan bimbingan (15 menit SLO).
 - Self-managed: Tetap internal organisasi Anda untuk melacak dan mendokumentasikan.
4. Lengkapi semua bidang yang relevan. Sertakan sedetail mungkin untuk mendukung penyelidikan yang efisien.

Kedua tipe kasus menggunakan bidang data yang sama. Anda dapat meningkatkan kasus yang dikelola sendiri ke Security Incident Response Engineering kapan saja dengan memilih Dapatkan bantuan dari AWS sudut kanan atas kasus.

☰ [AWS Security Incident Response](#) > Create case

Create case

Resolver Info

Select resolver

AWS-supported: Resolve case with AWS
24/7 dedicated AWS security professionals from the AWS Customer Incident Response Team (CRT).

Self-managed: Resolve case with my own Incident Response Team
Respond and recover internally and/or with 3rd party security providers.

Case type Info

Select type of request

Active security incident

Investigation


Case overview

Title Info

Active Incident [2025-9-17]

Generate title

Start date estimate Info
Identify the earliest date you observed activity in the impacted account(s).

2025/09/17 

Date must be less than 5 years in the past.

Untuk petunjuk mendetail, lihat [Membuat kasing](#).

Pengamat

Anda dapat memberikan visibilitas kasus kepada pihak eksternal menggunakan kebijakan Watchers atau IAM. Opsi ini memungkinkan Anda menyertakan mitra, tim risiko dan kepatuhan, penasihat hukum, atau pakar materi pelajaran dalam penyelidikan Anda. Pengamat menerima pemberitahuan untuk semua pembaruan untuk kasus tertentu. Kebijakan IAM menyediakan akses konsol langsung dengan izin hak istimewa paling sedikit.

Untuk menambahkan pengamat ke kasing

1. Buka Respons Insiden Keamanan AWS konsol dan pilih Kasus.
2. Buka kasing yang ingin Anda bagikan.
3. Pilih tab Izin, lalu pilih Tambah.

The screenshot shows the AWS Security Incident Response console for case ID 0928191969. The interface includes a left-hand navigation menu with options like Dashboard, Cases, Configure notifications and permissions, and Manage membership. The main content area displays an overview of the case, including the resolver (Self), name (CIRT - Proactive Case - Customer Servers Compromised), type (Security Incident), start date estimate (2025-07-15), and status (Detection & Analysis). Below the overview, there are tabs for Details, Communications, Permissions, Attachments, Tags, and Case activities. The 'Permissions' tab is active, showing a 'Watchers (3/30)' section with a search bar and a table of users. The table lists Jon 'Application' Doe (Lead Application Architect), Legal Team (Corporate Lawyer), and Our MSSP Vendor (MSSP Vendor). There is also a section for the 'Incident response team (10)'.

4. Salin kebijakan IAM yang telah diisi sebelumnya dan terapkan pada peran atau pengguna IAM yang sesuai.

The screenshot shows the AWS IAM console 'Permissions' tab for the same case. It displays the 'Watchers (3/30)' table and the 'Incident response team (10)' section. Below this, there is a 'Template case permission policy' section. It includes a 'Go to IAM' button and a 'Copy to clipboard' button. A code block shows the JSON policy template:

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "SecurityIncidentResponseCaseReadAccess",
      "Effect": "Allow",
      "Action": [
        "security-ir:GetCase",
        "security-ir:GetCaseAttachmentDownloadUrl",
        "security-ir:ListComments",
        "security-ir:ListCaseEdits",
        "security-ir:ListTagsForResource"
      ]
    }
  ]
}
    
```

Note

Setiap kasus mencakup kebijakan IAM yang telah diisi sebelumnya yang mencakup kasus tertentu tersebut. Ini mempertahankan akses hak istimewa paling sedikit untuk mitra MDR pihak ketiga dan tim investigasi.

Langkah 4: Integrasikan dengan alat yang ada

Respons Insiden Keamanan AWS terintegrasi dengan alat keamanan dan alur kerja Anda yang ada untuk merampingkan operasi respons insiden. Anda dapat mengonfigurasi konsumsi pencarian otomatis dari GuardDuty, mengatur alur kerja berbasis peristiwa, terhubung ke platform ITSM seperti Jira dan EventBridge ServiceNow, dan berkolaborasi dengan penyedia SIEM dan MDR Anda.

Topik-topik berikut dibahas di bagian ini:

- [GuardDuty temuan dan aturan penindasan](#)
- [Amazon EventBridge](#)
- [Jira, Slack, dan integrasi ServiceNow](#)
- [SIEM dan perangkat eksternal](#)

GuardDuty temuan dan aturan penindasan

Respons Insiden Keamanan AWS secara otomatis mencerna, melakukan triase, dan menanggapi GuardDuty temuan dan temuan CSPM Security Hub dari integrasi pihak ketiga. Teknologi auto-triage menangani analisis sebagai lapisan deteksi dan analisis tambahan. Layanan ini dapat membuat aturan arsip otomatis GuardDuty setelah meningkatkan temuan positif palsu. Responden akan selalu mendiskusikan hal ini dengan Anda sebelum menerapkan aturan.


Untuk meninjau aturan GuardDuty penindasan

1. Buka GuardDuty konsol.

The screenshot shows the AWS GuardDuty console interface. On the left, there is a navigation sidebar with sections like 'Summary', 'Findings', 'Protection plans', 'Accounts', and 'Settings'. The main area displays 'Findings (198)' with a search bar and filters for 'Status' (Current) and 'Threat type' (All findings). Below this, there is a table of findings with columns for Severity, Finding type, Resource, and Count. The table lists various findings such as 'Execution:Runtime/MaliciousFileExecuted', 'Execution:Runtime/SuspiciousTool', and 'Discovery:IAMUser/AnomalousBehavior'. A 'Suppression rules' section is also visible, listing rules like 'CIRT-Create-Suppression-Rule-DEMO1' and 'CIRT-Create-Suppression-Rule-DEMO2'.

Severity	Finding type	Resource	Count
High	Execution:Runtime/MaliciousFileExecuted	EC2 Instance: i-0e25811f91da2a88e	103
Medium	Execution:Runtime/SuspiciousTool	EC2 Instance: i-0e25811f91da2a88e	87
Low	Discovery:IAMUser/AnomalousBehavior	Access Key: ASIA4OAMZF4IQA4HJB2EB	90
High	Execution:EC2/MaliciousFile	EC2 Instance: i-0e25811f91da2a88e	1
Low	Policy:S3/BucketBlockPublicAccessDisabled	Access Key: ASIAKNC6ZRO4EUTFTET	94
Low	Policy:S3/BucketBlockPublicAccessDisabled	Access Key: ASIAZQJHLGGVA3X646WJ	95
Low	Discovery:IAMUser/AnomalousBehavior	Access Key: ASIA4OAMZF4IQA4HJB2EB	693
High	Execution:EC2/MaliciousFile	EC2 Instance: i-0e25811f91da2a88e	1
High	Execution:EC2/MaliciousFile	EC2 Instance: i-0e25811f91da2a88e	1
Low	Discovery:IAMUser/AnomalousBehavior	Access Key: ASIAKNC6ZRO4EUTFTET	150

2. Pilih Temuan.
3. Di panel navigasi, pilih Aturan penindasan. Halaman Aturan Supresi menampilkan daftar semua aturan penekanan untuk akun Anda.
4. Untuk meninjau atau mengubah pengaturan aturan, pilih aturan, lalu pilih Perbarui aturan penekanan dari menu Tindakan.

 Note

Organizations menggunakan teknologi SIEM akan melihat penurunan volume GuardDuty temuan dari waktu ke waktu, yang meningkatkan Respons Insiden Keamanan AWS efisiensi dan kinerja SIEM.

Amazon EventBridge

[Amazon EventBridge](#) memungkinkan alur kerja berbasis peristiwa untuk. Respons Insiden Keamanan AWS Anda dapat mengonfigurasi aktivitas kasus untuk memicu AWS layanan hilir (Amazon Simple Notification Service AWS Lambda, Amazon Simple Queue Service, AWS Step Functions) atau alat eksternal seperti Jira,, Slack ServiceNow, dan. PagerDuty

Untuk mengkonfigurasi EventBridge aturan untuk Respons Insiden Keamanan AWS

1. Masuk ke akun administrator yang didelegasikan untuk Respons Insiden Keamanan AWS.
2. Buka EventBridge konsol.
3. Di panel navigasi, di bawah Bus, pilih Aturan.
4. Pilih Buat aturan, lengkapi detail aturan, lalu pilih Berikutnya.
5. Di bawah AWS layanan, pilih Respons Insiden Keamanan AWS dari dropdown.
6. Untuk jenis Event, pilih event atau API call yang ingin Anda cocokkan. Anda dapat mengedit pola secara manual untuk menyertakan beberapa peristiwa.
7. Pilih Berikutnya.

Event pattern [Info](#)

Creation method

Use schema
Use an Amazon EventBridge schema to generate the event pattern.

Use pattern form
Use a template provided by EventBridge to create an event pattern.

Custom pattern (JSON editor)
Write an event pattern in JSON.

Event source
AWS service or EventBridge partner as source

AWS services

AWS service
The name of the AWS service as the event source

AWS Security Incident Response

Event type
The type of events as the source of the matching pattern

Case Created

Event pattern
Event pattern, or filter to match the events

```

1 {
2   "source": ["aws.security-ir"],
3   "detail-type": ["Case Created"]
4 }
    
```

Copy Test pattern Edit pattern

Cancel Previous Next

- Pilih satu atau beberapa target untuk acara Anda, seperti Amazon SNS, dokumen SSM AWS Lambda, atau Step Functions. Konfigurasi target lintas akun jika diperlukan.

Target 1

Target types
Select an EventBridge event bus, EventBridge API destination (SaaS partner), or another AWS service as a target.

EventBridge event bus

EventBridge API destination

AWS service

Select a target [Info](#)
Select target(s) to invoke when an event matches your event pattern or when schedule is triggered (limit of 5 targets per rule)

SNS topic

Target location

Target in this account Target in another AWS account

Topic

SIR-Demo-SNS-from-EventBridge

Permissions

Use execution role (recommended)

Execution role
EventBridge needs permission to send events to the target specified above. By continuing, you are allowing us to do so. [EventBridge and AWS Identity and Access Management](#)

Create a new role for this specific resource Use existing role

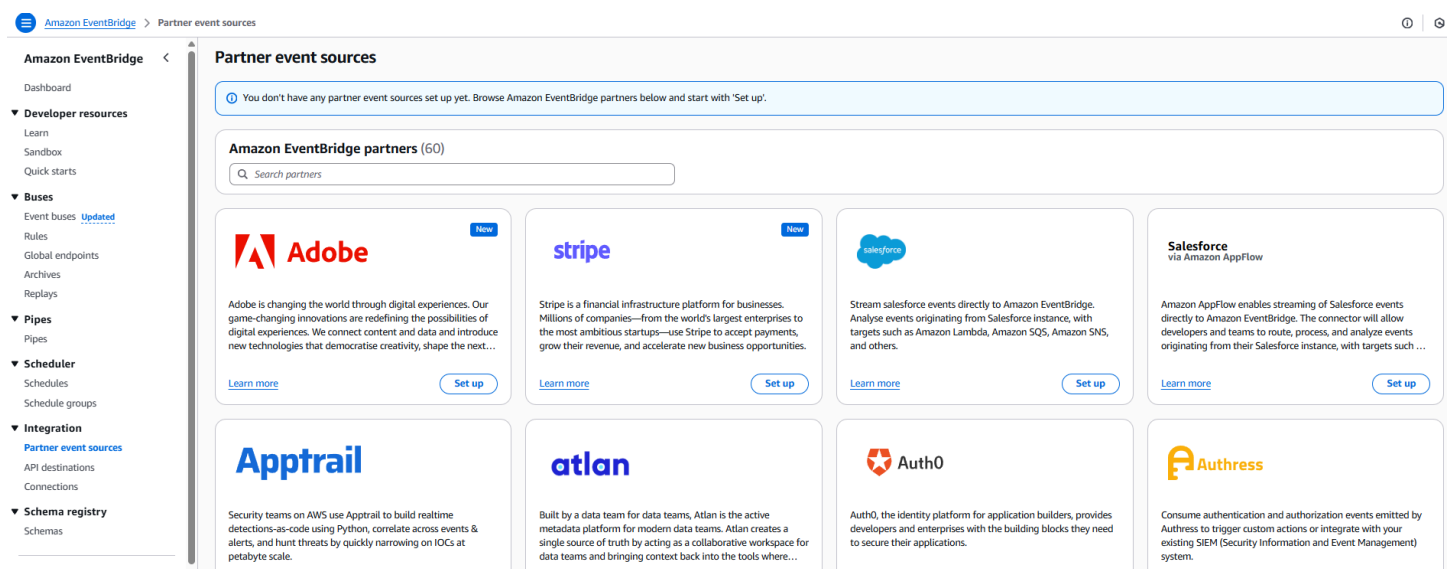
Role name

Amazon_EventBridge_Invoke_Sns_727705831

► Additional settings

- Tinjau dan buat aturan.

Untuk menggunakan integrasi mitra yang sudah dibuat sebelumnya, periksa Sumber Acara Mitra di konsol. EventBridge Mitra yang tersedia termasuk Atlassian (Jira), Datadog, New Relic, Symantec, dan Zendesk. PagerDuty



Jira, Slack, dan integrasi ServiceNow

AWS menyediakan solusi yang dikembangkan sepenuhnya untuk integrasi dua arah dengan Jira, Slack, dan ServiceNow. Integrasi ini membuat Respons Insiden Keamanan AWS kasus dan ITSM atau ChatOps platform Anda tetap sinkron — pembaruan dalam satu sistem secara otomatis tercermin di sistem lainnya.

Manfaat Integrasi

Mengintegrasikan Respons Insiden Keamanan AWS dengan platform ITSM Anda yang ada merampingkan operasi keamanan Anda dengan memusatkan alur kerja pelacakan insiden dan respons. Solusi pra-bangun ini menghilangkan kebutuhan akan pengembangan khusus, memungkinkan tim keamanan Anda mempertahankan visibilitas di seluruh sistem manajemen AWS insiden asli dan perusahaan. Dengan memanfaatkan EventBridge otomatisasi berbasis peristiwa, pembaruan mengalir dengan mulus antar platform secara real-time, membantu memastikan bahwa insiden keamanan dilacak secara konsisten terlepas dari mana asalnya. Pendekatan terpadu ini mengurangi peralihan konteks untuk analisis keamanan, meningkatkan waktu respons, dan menyediakan jejak audit komprehensif di seluruh siklus hidup respons insiden Anda.

Untuk petunjuk penerapan, lihat [AWS contoh solusi untuk Jira, Slack, dan ServiceNow](#)

SIEM dan perangkat eksternal

Respons Insiden Keamanan AWS tidak secara langsung menelan temuan dari SIEM Anda. Namun, ketika Anda membuka kasus yang AWS didukung, responden Security Incident Response Engineering menganalisis dan menyelidiki temuan SIEM secara paralel dengan tim Anda. Security

Incident Response Engineering membantu mengidentifikasi korelasi di seluruh lingkungan hybrid dan multi-cloud dan membantu pelingkupan aktivitas aktor ancaman di seluruh penyedia.

Security Incident Response Engineering juga berkolaborasi langsung dengan penyedia MDR Anda dan tim investigasi pihak ketiga untuk membantu membangun proses koordinasi yang efektif sebelum insiden terjadi.

Aktifkan Respons Insiden Keamanan dan konfigurasi tim respons insiden Anda menggunakan API/CLI

Bagian ini menyediakan langkah-langkah untuk mengaktifkan Respons Insiden Keamanan AWS, menunjuk administrator yang didelegasikan Respons Insiden Keamanan AWS, dan mengonfigurasi tim respons insiden Anda menggunakan API/CLI

Sebagai manajer Organizations, pastikan Anda membaca [Pertimbangan dan rekomendasi](#) tentang cara akun administrator Security Incident Response yang didelegasikan beroperasi. Sebelum melanjutkan, pastikan Anda memilikinya [izin yang diperlukan untuk menunjuk akun administrator Respons Insiden Keamanan yang didelegasikan](#).

Onboard with a delegated administrator using the API/CLI (recommended)

1. Buat peran `AWSServiceRoleForSecurityIncidentResponse_Triage` terkait layanan di akun AWS Organizations manajemen Anda:

```
aws iam create-service-linked-role --aws-service-name "triage.security-ir.amazonaws.com"
```

2. (Opsional) Untuk memverifikasi bahwa peran telah dibuat, jalankan perintah berikut:

```
aws iam get-role --role-name AWSServiceRoleForSecurityIncidentResponse_Triage
```

3. Dari akun AWS Organizations manajemen Anda, daftarkan akun administrator yang didelegasikan untuk Respons Insiden Keamanan AWS:

```
aws organizations register-delegated-administrator \  
--account-id delegated-admin-account-id \  
--service-principal security-ir.amazonaws.com
```

4. Aktifkan akses Respons Insiden Keamanan AWS layanan untuk organisasi Anda:

```
aws organizations enable-aws-service-access \  
--service-name security-ir
```

```
--service-principal security-ir.amazonaws.com
```

5. Masuk ke akun administrator yang didelegasikan untuk membuat keanggotaan dan menunjuk tim respons insiden Anda. Anda harus mencantumkan setidaknya dua anggota tim respons insiden.

```
aws security-ir create-membership \
  --membership-name "membership-name" \
  --incident-response-team '[
    {
      "name": "name",
      "jobTitle": "job-title",
      "email": "email@example.com",
      "communicationPreferences": ["email"]
    }
    {
      "name": "name",
      "jobTitle": "job-title",
      "email": "email@example.com",
      "communicationPreferences": ["email"]
    }
  ]'
```

6. (Opsional) Verifikasi bahwa keanggotaan telah dibuat:

```
aws security-ir list-memberships
```

7. (Opsional) Dapatkan rincian keanggotaan:

```
aws security-ir get-membership \
  --membership-id membership-id
```

Onboard with a management account using the API/CLI

1. Aktifkan akses Respons Insiden Keamanan AWS layanan untuk organisasi Anda:

```
aws organizations enable-aws-service-access \
  --service-principal security-ir.amazonaws.com
```

2. Masuk ke akun manajemen untuk membuat keanggotaan dan menunjuk tim respons insiden Anda. Anda harus mencantumkan setidaknya dua anggota tim respons insiden.

```
aws security-ir create-membership \  
  --membership-name "membership-name" \  
  --incident-response-team '[  
    {  
      "name": "name",  
      "jobTitle": "job-title",  
      "email": "email@example.com",  
      "communicationPreferences": ["email"]  
    }  
    {  
      "name": "name",  
      "jobTitle": "job-title",  
      "email": "email@example.com",  
      "communicationPreferences": ["email"]  
    }  
  ]'
```

3. (Opsional) Verifikasi bahwa keanggotaan telah dibuat:

```
aws security-ir list-memberships
```

4. (Opsional) Dapatkan rincian keanggotaan:

```
aws security-ir get-membership \  
  --membership-id membership-id
```

Lampiran A: Titik kontak dan informasi penting

Lengkapi tabel berikut dan berikan ke tim AWS akun Anda sebelum penerapan. Informasi ini memungkinkan Security Incident Response Engineering untuk menjangkau orang yang tepat dengan cepat selama acara keamanan.

Informasi Kontak Personil IR dan SOC

Ent	IR Personil SOC: Peran, Nama, Email	Kontak: Eskalasi Prime Sekur	Rentang CIDR yang Diket	Ekstensi, Kisaran CIDR yang Diken	Penyediaan Layanan Cloud Tamb	Bekerja Wilayah AWS	IP Server DNS (jika selain Amaz Route 53 Resol	VPN Solusi Akses Jarak Jauh dan IP	Nama Aplikasi Kritis Nomor Akun	Pelab yang Tidak Biasa Digun	EDR AV Alat Manajemen Kerentanan Digunak	IDP Lokasi
1	Komand SOC, John Smith, jsmith@ample.c	Prime	10.0.0.0/16	5.5.60.0/20 (Azur	Biru langit	us-east-1, us-east-2	N/A	Direct Connect Public VIF 116.32.87	Server Web Nginx (Contoh Kritis) 12345670	8080	CrowdStrike Falcon	Entra, Azure

Untuk mengirimkan informasi ini, selesaikan langkah-langkah berikut:

- Lengkapi tabel metadata sebelumnya dengan informasi lingkungan Anda.
- Buat [AWS Dukungan kasing](#) dengan detail berikut:
 - Jenis kasus: Teknis
 - Layanan: Respon Insiden Keamanan
 - Kategori: Lain-lain
- Lampirkan tabel metadata yang sudah selesai ke kasing.

Matriks RACI

Matriks RACI berikut mendefinisikan peran dan tanggung jawab di seluruh proses implementasi Security Incident Response. RACI adalah singkatan dari Responsible (R), Accountable (A), Consulted (C), dan Informed (I).

Aktifitas	Pelanggan	AWS Tim Akun	Tim SIR
Pre-Onboarding			
Identifikasi Pemangku Kepentingan Utama	R		I
Validasi Menemukan Sumber	R	C	I
[Integrasi EDR Pihak Ketiga] Security Hub CSPM	R	C	I
GuardDuty Validation/Health Memeriksa	C	R	I
Tentukan Lingkup Akun	R		
Menetapkan Protokol Eskalasi	R	I	C
Aktifkan AWS Organizations	R	C	
Mengaitkan akun dengan AWS Organizations	R	I	
Pilih Administrator Delegasi/Akun Perangkat Keamanan	R	I	
Orientasi			
Menyiapkan rincian keanggotaan	R	I	
Walkthrough (Menyiapkan respons proaktif dan alur kerja triaging peringatan; Menyebarkan peran terkait layanan ke akun manajemen; Otorisasi tindakan penahanan)	R	C	I
Post-Deployment Konfigurasi			

Aktifitas	Pelanggan	AWS Tim Akun	Tim SIR
Tinjau kemampuan integrasi operasional	R	C	I
Kirim Kasus Reaktif Respon Insiden Keamanan	R		
Konfigurasi EventBridge integrasi Amazon	R	C	C
Connect perangkat pihak ketiga (Jira,, ServiceNow, Teams PagerDuty, dll.)	R	I	C
Layanan deep dive dan demo	A	R	C

Definisi RACI:

- Bertanggung jawab (R) - Pihak yang melakukan pekerjaan untuk menyelesaikan tugas
- Akuntabel (A) - Pihak pada akhirnya bertanggung jawab atas penyelesaian tugas yang benar
- Konsultasikan (C) - Pihak yang pendapatnya dicari dan dengan siapa ada komunikasi dua arah
- Informed (I) - Pihak yang selalu up-to-date tentang kemajuan dan dengan siapa ada komunikasi satu arah

Pilih akun keanggotaan

Akun keanggotaan adalah AWS akun yang digunakan untuk mengonfigurasi detail akun, menambah dan menghapus detail untuk tim respons insiden Anda, dan tempat semua peristiwa keamanan aktif dan historis dapat dibuat dan dikelola. Disarankan agar Anda menyelaraskan akun Respons Insiden Keamanan AWS keanggotaan Anda ke akun yang sama yang telah Anda aktifkan untuk layanan seperti Amazon GuardDuty dan AWS Security Hub CSPM.

Anda memiliki dua opsi untuk memilih akun Respons Insiden Keamanan AWS keanggotaan Anda menggunakan AWS Organizations. Anda dapat membuat keanggotaan di akun manajemen Organisasi atau di akun administrator yang didelegasikan Organizations.

Gunakan akun administrator yang didelegasikan: tugas Respons Insiden Keamanan AWS administratif dan manajemen kasus terletak di akun administrator yang didelegasikan. Sebaiknya

gunakan administrator terdelegasi yang sama dengan yang Anda tetapkan untuk layanan AWS keamanan dan kepatuhan lainnya. Berikan 12 digit ID akun administrator yang didelegasikan dan kemudian masuk ke akun itu untuk melanjutkan.

Respons Insiden Keamanan AWS secara otomatis membuat peran `AWSServiceRoleForSecurityIncidentResponse_Triage` terkait layanan di akun AWS Organizations manajemen Anda dan di semua akun yang berada dalam cakupan saat melakukan orientasi melalui konsol. Respons Insiden Keamanan AWS Untuk petunjuk tentang mengaktifkan Respons Insiden Keamanan AWS dan menunjuk akun administrator yang didelegasikan menggunakan, lihat. API/CLI [Aktifkan Respons Insiden Keamanan dan konfigurasi tim respons insiden Anda menggunakan API/CLI](#)

Gunakan akun yang saat ini masuk: Memilih akun ini berarti akun saat ini akan ditetapkan sebagai akun keanggotaan pusat untuk Respons Insiden Keamanan AWS keanggotaan Anda. Individu dalam organisasi Anda perlu mengakses layanan melalui akun ini untuk membuat, mengakses, dan mengelola kasus yang aktif dan diselesaikan.

Pastikan Anda memiliki izin yang cukup untuk dikelola Respons Insiden Keamanan AWS.

Lihat [Menambahkan dan menghapus izin identitas IAM untuk langkah-langkah spesifik untuk menambahkan izin](#).

Lihat [kebijakan Respons Insiden Keamanan AWS terkelola](#).

Untuk memverifikasi izin IAM, Anda dapat mengikuti langkah-langkah berikut:

- Periksa Kebijakan IAM: Tinjau kebijakan IAM yang dilampirkan pada pengguna, grup, atau peran Anda untuk memastikannya memberikan izin yang diperlukan. Anda dapat melakukan ini dengan menavigasi ke, pilih Users opsi <https://console.aws.amazon.com/iam/>, pilih pengguna tertentu, dan kemudian pada halaman ringkasan mereka, buka Permissions tab di mana Anda dapat melihat daftar semua kebijakan terlampir; Anda dapat memperluas setiap baris kebijakan untuk melihat detailnya.
- Uji Izin: Cobalah untuk melakukan tindakan yang Anda perlukan untuk memverifikasi izin. Misalnya, jika Anda perlu mengakses kasing, cobalah `ListCases`. Jika Anda tidak memiliki izin yang diperlukan, Anda akan menerima pesan kesalahan.
- Gunakan AWS CLI atau SDK: Anda dapat menggunakan AWS Command Line Interface atau AWS SDK dalam bahasa pemrograman pilihan Anda untuk menguji izin. Misalnya, dengan AWS Command Line Interface, Anda dapat menjalankan `aws sts get-caller-identity` perintah untuk memverifikasi izin pengguna Anda saat ini.

- Periksa AWS CloudTrail log: [Tinjau CloudTrail log](#) untuk melihat apakah tindakan yang Anda coba lakukan sedang dicatat. Ini dapat membantu Anda mengidentifikasi masalah izin apa pun.
- Gunakan simulator kebijakan IAM: Simulator [kebijakan IAM](#) adalah alat yang memungkinkan Anda menguji kebijakan IAM dan melihat efeknya terhadap izin Anda.

Note

Langkah-langkah spesifik dapat bervariasi tergantung pada AWS layanan dan tindakan yang Anda coba lakukan.

Menyiapkan rincian keanggotaan

- Pilih Wilayah AWS tempat keanggotaan dan kasus Anda akan disimpan.

Warning

Anda tidak dapat mengubah default Wilayah AWS setelah pendaftaran keanggotaan awal.

- Pilih apakah Anda ingin memberikan cakupan keanggotaan penuh atas seluruh AWS Organizations atau sebagian dari Anda AWS Organizations melalui unit organisasi (OU).
- Anda dapat memilih nama untuk keanggotaan ini secara opsional.
- Kontak primer dan sekunder harus diberikan sebagai bagian dari alur kerja buat keanggotaan. Kontak ini secara otomatis disertakan sebagai bagian dari tim respons insiden Anda. Setidaknya dua kontak harus ada untuk satu keanggotaan yang juga memastikan minimal dua kontak dimasukkan dalam tim respons insiden.
- Tentukan tag opsional untuk keanggotaan Anda. Tag membantu Anda melacak AWS biaya dan mencari sumber daya.

Mengaitkan akun dengan AWS Organizations

Jika Anda memilih untuk mengaitkan keseluruhan AWS Organizations selama penyiapan, keanggotaan Anda berhak mendapatkan cakupan pada semua akun anggota di organisasi. Akun terkait akan diperbarui secara otomatis saat akun ditambahkan atau dihapus dari organisasi Anda.

Jika Anda memilih untuk mengaitkan bagian dari pengaturan Anda AWS Organizations selama pengaturan dan telah membatasi keanggotaan Anda ke unit organisasi tertentu (OU), keanggotaan Anda memberikan hak cakupan atas semua akun di bawah OU yang dipilih. Ini termasuk akun di bawah sub-OU dari OU yang dipilih. Akun terkait diperbarui secara otomatis saat akun ditambahkan atau dihapus dari OU tersebut.

Untuk mempelajari lebih lanjut tentang praktik terbaik yang melibatkan unit organisasi, silakan lihat [Mengatur AWS lingkungan Anda Menggunakan beberapa akun](#).

Siapkan respons proaktif dan alur kerja triaging peringatan

Respons Insiden Keamanan AWS memantau dan menyelidiki peringatan ancaman yang dihasilkan dari Amazon GuardDuty dan alat deteksi ancaman pihak ketiga menggunakan integrasi CSPM Security Hub. Respons Insiden Keamanan AWS Secara otomatis melakukan triase semua peringatan yang didukung sehingga tim Anda dapat fokus pada masalah yang paling kritis.

Important

Respons Insiden Keamanan AWS tidak mengharuskan Anda untuk mengaktifkan Amazon GuardDuty. Namun, fitur respons proaktif bergantung pada penerimaan temuan ancaman dari layanan deteksi. Jika Anda tidak memiliki Amazon GuardDuty atau Security Hub CSPM yang dikonfigurasi untuk menyerap temuan, tidak Respons Insiden Keamanan AWS akan ada peringatan untuk dipantau dan diselidiki, yang membatasi nilai fitur ini.

Respons Insiden Keamanan AWS memantau dan menyelidiki temuan di semua akun yang tercakup dan aktif didukung Wilayah AWS di organisasi Anda. Untuk memfasilitasi fungsi ini, Respons Insiden Keamanan AWS secara otomatis membuat peran terkait layanan di semua akun anggota yang tercakup dalam akun Anda. AWS Organizations Namun, untuk akun manajemen, Anda harus membuat peran terkait layanan secara manual untuk mengaktifkan pemantauan.

Jika Anda melakukan [Respons Insiden Keamanan AWS onboard](#) Konsol Manajemen AWS, Security Incident Response secara otomatis membuat peran `AWSServiceRoleForSecurityIncidentResponse_Triage` terkait layanan di akun AWS Organizations manajemen Anda dan di semua akun yang berada dalam cakupan. Jika Anda melakukan onboarding menggunakan API/CLI, maka Anda harus membuat peran secara manual. Untuk informasi selengkapnya, lihat [Aktifkan Respons Insiden Keamanan dan konfigurasi tim respons insiden Anda menggunakan API/CLI](#).

Jika Anda mengalami masalah orientasi atau memerlukan bantuan untuk mengaktifkan Amazon GuardDuty atau Security Hub CSPM, [buat](#) kasus untuk bantuan. AWS Dukungan

Note

Jika Anda memiliki pertanyaan tentang aturan GuardDuty penindasan Amazon, konfigurasi triaging peringatan, atau alur kerja respons proaktif, Anda dapat membuat kasus yang AWS didukung dengan jenis kasus Investigasi dan Pertanyaan untuk berkonsultasi dengan tim. Respons Insiden Keamanan AWS Untuk informasi selengkapnya, lihat [Buat sebuah AWS kasus yang didukung](#).

Memahami Pengarsipan Otomatis dengan Respon Proaktif

Saat Anda mengaktifkan respons proaktif dan triaging peringatan, Respons Insiden Keamanan AWS secara otomatis memantau dan mem-triase temuan keamanan dari Amazon dan Security GuardDuty Hub CSPM. Sebagai bagian dari alur kerja triase otomatis ini, temuan secara otomatis diarsipkan berdasarkan kriteria berikut:

Perilaku pengarsipan otomatis:

- **Temuan jinak:** Ketika proses auto-triase menentukan bahwa temuan itu jinak (bukan ancaman keamanan sejati), Respons Insiden Keamanan AWS secara otomatis mengarsipkan temuan di Amazon GuardDuty dan membuat aturan penindasan untuk mencegah temuan serupa menghasilkan peringatan di masa depan.
- **Aturan penindasan:** Layanan ini membuat aturan penekanan dan pengarsipan otomatis di Amazon dan Security GuardDuty Hub CSPM untuk temuan yang sesuai dengan pola lingkungan Anda yang diketahui baik, seperti alamat IP yang diharapkan, entitas IAM, dan perilaku operasional normal.
- **Mengurangi volume peringatan:** Organizations menggunakan teknologi SIEM melihat volume GuardDuty pencarian Amazon berkurang secara signifikan dari waktu ke waktu karena layanan mempelajari lingkungan Anda dan secara otomatis mengarsipkan temuan jinak. Ini meningkatkan efisiensi untuk Respons Insiden Keamanan AWS layanan dan SIEM Anda.

Melihat temuan yang diarsipkan:

Anda dapat meninjau temuan yang diarsipkan secara otomatis dan aturan penekanan yang dibuat oleh: Respons Insiden Keamanan AWS

1. Arahkan ke GuardDuty konsol Amazon
2. Pilih Temuan
3. Pilih Diarsipkan dari filter temuan
4. Tinjau aturan penindasan dengan memilih panah bawah di samping setiap aturan

Pertimbangan penting:

- Temuan yang diarsipkan disimpan di Amazon GuardDuty selama 90 hari dan dapat dilihat kapan saja selama periode tersebut
- Anda dapat mengubah atau menghapus aturan penindasan kapan saja melalui konsol Amazon GuardDuty
- Proses auto-triase terus beradaptasi dengan lingkungan Anda, meningkatkan akurasi dari waktu ke waktu dan mengurangi positif palsu

Penahanan: Jika terjadi insiden keamanan, Respons Insiden Keamanan AWS dapat melakukan tindakan penahanan untuk mengurangi dampak dengan cepat, seperti mengisolasi host yang dikompromikan atau memutar kredensial. Respons Insiden Keamanan tidak mengaktifkan kemampuan pembatasan secara default. Untuk menjalankan tindakan penahanan ini, Anda harus terlebih dahulu memberikan izin yang diperlukan untuk layanan. Ini dapat dilakukan dengan menerapkan [AWS CloudFormation StackSet](#), yang menciptakan peran yang diperlukan.

Tugas pengguna

Daftar Isi

- [Dasbor Respons Insiden Keamanan](#)
- [Mengelola Tim Respons Insiden saya](#)
- [Kasus](#)
- [Mengelola Kasus](#)
- [Bekerja dengan CloudFormation StackSets](#)
- [Batalkan Keanggotaan](#)

Dasbor Respons Insiden Keamanan

Di Respons Insiden Keamanan AWS konsol, dasbor memberi Anda gambaran umum tentang tim respons insiden Anda, status respons proaktif Anda, dan hitungan kasus bergulir empat minggu.

Tim Respon Insiden

Pilih Lihat tim respons insiden untuk mengakses detail rekan tim respons insiden Anda.

Kasus Saya

Bagian Kasus Saya di dasbor menunjukkan jumlah kasus yang AWS didukung terbuka dan tertutup, bersama dengan kasus yang dikelola sendiri yang ditetapkan kepada Anda dalam periode yang ditentukan. Ini juga menunjukkan waktu rata-rata yang dibutuhkan untuk menyelesaikan kasus yang ditutup dalam beberapa jam.

Mengelola Tim Respons Insiden saya

Tim respons insiden Anda berisi pemangku kepentingan untuk proses respons insiden. Anda dapat mengonfigurasi hingga sepuluh pemangku kepentingan sebagai bagian dari keanggotaan Anda.

Contoh untuk pemangku kepentingan internal termasuk anggota tim respons insiden Anda, analis keamanan, pemilik aplikasi, dan tim kepemimpinan keamanan Anda.

Contoh untuk pemangku kepentingan eksternal termasuk individu dari vendor perangkat lunak independen (ISV) dan penyedia layanan terkelola (MSP) yang ingin Anda sertakan dalam proses respons insiden.

Note

Menyiapkan tim respons insiden Anda tidak secara otomatis memberi rekan tim akses ke sumber daya layanan seperti keanggotaan dan kasus. Anda dapat menggunakan kebijakan AWS terkelola Respons Insiden Keamanan AWS untuk memberikan akses baca dan tulis ke sumber daya. [Klik di sini untuk mempelajari lebih lanjut.](#)

Rekan tim respons insiden Anda yang ditentukan pada tingkat keanggotaan akan ditambahkan secara otomatis ke kasus apa pun. Anda dapat menambah atau menghapus rekan satu tim kapan saja setelah kasus dibuat.

Tim respons insiden akan menerima pemberitahuan email tentang peristiwa yang tercantum dalam [preferensi komunikasi](#).

Preferensi komunikasi

Konfigurasi preferensi komunikasi Anda untuk mengontrol cara Anda menerima notifikasi dan berinteraksi dengan sistem respons insiden selama insiden keamanan.

Kelola Preferensi Komunikasi Tim

Anda dapat mengonfigurasi preferensi komunikasi untuk individu dalam tim respons insiden Anda dari halaman dasbor.

Ikuti langkah-langkah berikut untuk mengelola pengaturan komunikasi anggota tim:

1. Arahkan ke halaman tim respons insiden dari dasbor Anda
2. Lakukan salah satu tindakan berikut:
 - Untuk memperbarui anggota tim yang ada: Pilih rekan tim yang preferensi komunikasinya ingin Anda ubah, lalu pilih Edit
 - Untuk menambahkan anggota tim baru: Pilih Tambah
3. Di bagian bawah formulir Anda akan melihat Komunikasi
 - a. Pilih kotak centang untuk komunikasi yang ingin Anda terima
 - b. Kosongkan kotak centang untuk komunikasi yang tidak ingin Anda terima

Communications

Select communication type

- Case acknowledged
- Case assignee updated
- Case attachment scan failed
- Case attachment scan succeeded
- Case attachment uploaded
- Case attachment URL uploaded
- Case break glass
- Case closed
- Case comment added
- Case comment updated
- Case created
- Case entitlement updated
- Case owner updated
- Case pending customer action reminder
- Case updated
Notifications about cases, such as new case creations, new case updates, and case closure.
- Case updated to service managed
- Case update case status
- Deregister delegated administrator
- Disable AWS service access
- Membership cancelled
- Membership created
- Membership updated
Notifications about changes to membership, such as membership account updates and cancellations.
- Register delegated administrator

4. Simpan perubahan Anda

Incident Response Team

Set up your Incident Response Team

Add members and grant permissions
Configure your team by adding key stakeholders from within and outside your organization. This can include stakeholders such as legal, application leads, product managers, or 3rd party security services.

Receive email notifications by default
Team members automatically added to any case that is being created by default. These members can be removed before creating the case. Team members are automatically notified for any updates to service membership.

Teammates (2/10)
You can specify up to 10 members in your Incident Response Team. Additional members can be added for individual cases.

Name	Job title	Email	Communications
<input type="checkbox"/> John	Security Engineer	john@security-engineer.com	<ul style="list-style-type: none"> • Case updated • Case acknowledged • Case status updated • Case comment added Show more (+1)
<input type="checkbox"/> Sarah	Security Manager	sarah@security-manager.com	<ul style="list-style-type: none"> • Case created • Case updated • Case acknowledged • Case status updated Show more (+2)

Pengaturan Komunikasi Default

Secara default, anggota tim respons insiden akan mengaktifkan semua komunikasi. Anda dapat mengubah pengaturan ini kapan saja menggunakan langkah-langkah di atas.

Opsi Komunikasi

Preferensi komunikasi Anda mengontrol cara Anda berinteraksi dengan sistem respons insiden dan bagaimana pemberitahuan dikirimkan kepada Anda selama insiden keamanan.

Note

Preferensi ini berlaku untuk semua komunikasi future dalam sistem Security Incident Response. Anda dapat mengubah pengaturan ini kapan saja dengan mengulangi langkah-langkah di atas.

Asosiasi akun ke AWS Organizations

Ketika Anda mengaktifkan Respons Insiden Keamanan AWS, Anda akan diberikan opsi untuk memilih seluruh organisasi atau unit organisasi tertentu (OU) Anda. Jika OU tertentu dipilih, keanggotaan Anda hanya akan mencakup akun yang termasuk dalam OU yang dipilih tersebut. Jika seluruh organisasi dipilih, maka keanggotaan Anda akan mencakup semua akun dalam organisasi Anda.

Untuk detail lebih lanjut, silakan lihat [Mengelola Respons Insiden Keamanan AWS akun dengan AWS Organizations](#).

Mengelola Cakupan Keanggotaan Anda

Anda dapat mengubah opsi cakupan keanggotaan kapan saja, termasuk beralih dari cakupan seluruh organisasi ke OU tertentu.

Memperbarui Asosiasi OU

Untuk mengelola cakupan keanggotaan Anda:

1. Arahkan ke halaman Setelan asosiasi akun
2. Pilih Tambahkan OU untuk memilih OU yang ingin Anda kaitkan dengan keanggotaan Anda
3. Pilih OU yang ingin Anda kaitkan dengan keanggotaan Anda
4. Klik Perbarui Asosiasi untuk menyimpan asosiasi OU pada keanggotaan Anda

Setelah memperbarui asosiasi Anda, Anda dapat kembali ke halaman yang sama dan menghapus OU yang ingin Anda pisahkan dari keanggotaan Anda. Fleksibilitas ini berlaku bahkan jika Anda

awalnya memilih seluruh organisasi Anda—nantinya Anda dapat memperbarui keanggotaan Anda untuk hanya mencakup OU tertentu tanpa membatalkan dan mengaktifkan kembali layanan.

Untuk informasi lebih lanjut, silakan lihat [Mengelola keanggotaan dengan unit organisasi \(OU\)](#).

Pertimbangan Penting

Akun langsung di bawah root: Saat memilih OU tertentu untuk keanggotaan Anda, akun yang berada langsung di bawah akar organisasi (bukan bagian dari OU mana pun) tidak akan dikaitkan dengan keanggotaan Anda. Untuk memasukkan akun ini dalam cakupan keanggotaan Anda, Anda harus terlebih dahulu menambahkannya ke OU, lalu mengaitkan OU tersebut dengan keanggotaan Anda.

Note

Kami terus meningkatkan pengalaman pengguna asosiasi OU untuk membuat proses lebih intuitif dan jelas.

Pemantauan dan investigasi

Respons Insiden Keamanan AWS ulasan dan triase peringatan keamanan dari Amazon GuardDuty dan AWS Security Hub CSPM, kemudian mengonfigurasi aturan penekanan berdasarkan lingkungan Anda untuk mencegah peringatan yang tidak perlu. Tim Security Incident Response Engineering menyelidiki temuan dan dengan cepat meningkatkan dan memandu tim Anda untuk mengatasi masalah potensial dengan cepat. Jika diinginkan, Anda dapat memberikan Respons Insiden Keamanan AWS izin untuk menerapkan tindakan penahanan atas nama Anda.

Respons Insiden Keamanan AWS sejajar dengan Panduan Penanganan [peristiwa Keamanan Komputer NIST 800-61r2 untuk Respons peristiwa Keamanan](#). Dengan menyelaraskan standar industri ini, Respons Insiden Keamanan AWS memberikan pendekatan yang konsisten untuk manajemen acara keamanan dan mematuhi praktik terbaik dalam mengamankan dan menanggapi peristiwa keamanan di lingkungan Anda. AWS

Saat Respons Insiden Keamanan AWS mengidentifikasi peringatan keamanan atau Anda meminta bantuan keamanan, Security Incident Response Engineering menyelidiki. Tim mengumpulkan peristiwa log dan data layanan seperti GuardDuty peringatan, triase dan analisis data tersebut, melakukan aktivitas remediasi dan penahanan, dan menyediakan pelaporan pasca-insiden.

Daftar Isi

- [Persiapkan](#)

- [Mendeteksi dan Menganalisis](#)

Persiapkan

Respons Insiden Keamanan AWS Tim menyelidiki dan bermitra dengan Anda selama siklus hidup respons peristiwa keamanan. Disarankan agar Anda mengatur tim ini dan menetapkan izin yang diperlukan sebelum peristiwa keamanan terjadi.

Mendeteksi dan Menganalisis

Melaporkan Acara

Anda dapat meningkatkan acara keamanan melalui Respons Insiden Keamanan AWS portal. Penting untuk tidak menunggu selama acara keamanan. Respons Insiden Keamanan AWS menggunakan teknik otomatis dan manual untuk menyelidiki peristiwa keamanan, menganalisis log, dan mencari pola anomali. Kemitraan dan pemahaman Anda tentang lingkungan Anda mempercepat analisis ini.

Mengaktifkan sumber deteksi yang didukung

Note

Respons Insiden Keamanan AWS Biaya layanan tidak termasuk penggunaan dan biaya dan biaya lain yang terkait dengan sumber deteksi atau penggunaan AWS layanan lain yang didukung. Silakan merujuk ke fitur individual atau halaman layanan untuk detail biaya.

Amazon GuardDuty

Untuk mengaktifkan GuardDuty di seluruh organisasi Anda, silakan lihat [Setting up GuardDuty](#) bagian [Panduan GuardDuty Pengguna Amazon](#).

Kami sangat menyarankan agar Anda mengaktifkan GuardDuty semua yang didukung Wilayah AWS. Ini memungkinkan GuardDuty untuk menghasilkan temuan tentang aktivitas yang tidak sah atau tidak biasa bahkan di wilayah yang tidak Anda gunakan secara aktif. Untuk informasi selengkapnya, rujuk [GuardDuty Wilayah Amazon dan titik akhir](#)

Mengaktifkan GuardDuty menyediakan Respons Insiden Keamanan AWS akses ke data deteksi ancaman kritis, meningkatkan kemampuannya untuk mengidentifikasi dan menanggapi potensi masalah keamanan di lingkungan Anda AWS .

AWS Security Hub CSPM

AWS Security Hub CSPM dapat menyerap temuan keamanan dari beberapa AWS layanan dan mendukung solusi keamanan pihak ketiga. Integrasi ini dapat membantu Respons Insiden Keamanan AWS memantau dan menyelidiki temuan yang berasal dari alat deteksi lainnya.

Untuk mengaktifkan Security Hub CSPM dengan integrasi Organizations, silakan lihat [AWS Security Hub CSPM Panduan Pengguna](#).

Ada beberapa cara untuk mengaktifkan integrasi pada Security Hub CSPM. 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. Pelajari lebih lanjut tentang [cara mengaktifkan AWS Security Hub CSPM integrasi](#).

Respons Insiden Keamanan AWS dapat memantau dan menyelidiki temuan dari alat-alat berikut ketika mereka terintegrasi dengan AWS Security Hub CSPM:

- [CrowdStrike — CrowdStrike Elang](#)
- [Lacework — Lacework](#)
- [Trend Micro - Cloud One](#)

Dengan mengaktifkan integrasi ini, Anda dapat secara signifikan meningkatkan ruang lingkup dan efektivitas Respons Insiden Keamanan AWS kemampuan pemantauan dan investigasi.

Deteksi

Dengan [Proactive Response](#) Respons Insiden Keamanan AWS, Anda dapat menyerap temuan dari AWS Security Hub CSPM Amazon GuardDuty dan melalui EventBridge aturan Amazon yang diterapkan ke akun Anda selama orientasi.

Respons Insiden Keamanan AWS secara otomatis mengarsipkan GuardDuty temuan Amazon yang ditentukan selama triase otomatis menjadi jinak atau terkait dengan aktivitas yang diharapkan. Anda dapat melihat temuan yang diarsipkan di GuardDuty konsol Amazon dengan memilih Diarsipkan dari filter Status temuan. Untuk informasi selengkapnya, lihat [Melihat temuan yang dihasilkan di GuardDuty konsol](#) di Panduan GuardDuty Pengguna Amazon.

Respons Insiden Keamanan AWS secara otomatis mengarsipkan GuardDuty temuan Amazon yang ditentukan selama triase otomatis menjadi jinak atau terkait dengan aktivitas yang diharapkan. Pengarsipan ini hanya terjadi untuk temuan yang telah diprioritaskan dan memiliki hasil yang ditetapkan sebagai “arsip”. Temuan yang sedang diselidiki aktif tetap terlihat di GuardDuty konsol Amazon bahkan setelah penyelidikan selesai. Anda dapat melihat temuan yang diarsipkan

di GuardDuty konsol Amazon dengan memilih Diarsipkan dari filter temuan. Untuk informasi selengkapnya tentang bekerja dengan temuan yang diarsipkan, lihat [Bekerja dengan temuan](#) di Panduan GuardDuty Pengguna Amazon.

Ketika AWS Security Hub CSPM menelan temuan keamanan, sistem memperbarui setiap temuan dengan catatan yang menunjukkan bahwa triase otomatis telah dimulai. Status alur kerja berubah dari BARU ke NOTIFIED, yang menghapus temuan dari tampilan AWS Security Hub CSPM temuan default. Jika triase menentukan bahwa temuan itu jinak atau terkait dengan aktivitas yang diharapkan, sistem menambahkan catatan ke temuan dan memperbarui status alur kerja ke SUPPRESSED.

Analisis: Triase Otomatis

Respons Insiden Keamanan AWS secara otomatis melakukan triase temuan keamanan. Proses triase menentukan apakah aktivitas yang terdeteksi mewakili perilaku yang diharapkan, dengan menganalisis data dari berbagai sumber termasuk muatan temuan, metadata AWS layanan, data AWS pencatatan dan pemantauan (seperti dan Log Aliran AWS CloudTrail VPC), intelijen AWS ancaman, dan konteks yang diundang untuk Anda berikan tentang lingkungan Anda dan lokal. AWS

Jika triase otomatis menentukan bahwa aktivitas yang terdeteksi diharapkan, sistem tidak mengambil tindakan investigasi lebih lanjut.

Analisis: Investigasi Keamanan Respon Insiden

Respons Insiden Keamanan AWS Engineering adalah tim profesional keamanan global yang selalu tersedia dengan keahlian AWS dan respons insiden keamanan. Jika triase otomatis tidak dapat menentukan bahwa aktivitas tersebut diharapkan, Respons Insiden Keamanan AWS Engineering dilibatkan untuk melakukan penyelidikan keamanan. Jika acara itu tertelan dari Security Hub, sebuah catatan diposting ke temuan terkait yang menyatakan bahwa penyelidikan Respons Insiden Keamanan AWS Engineering sedang berlangsung.

Respons Insiden Keamanan AWS Rekayasa melakukan penyelidikan keamanan langsung dengan menganalisis metadata layanan tambahan dan intelijen ancaman, meninjau wawasan dari temuan dan investigasi masa lalu di lingkungan Anda, dan menerapkan keahlian respons insiden. Bergantung pada preferensi Penahanan Anda (lihat Mengandung) Rekayasa Respons Insiden AWS Keamanan dapat melibatkan tim Respons Insiden organisasi Anda melalui kasus Respons Insiden Keamanan di Respons Insiden Keamanan AWS konsol untuk memverifikasi apakah aktivitas yang terdeteksi diharapkan dan diizinkan [Menanggapi kasus yang AWS dihasilkan](#).

Sebagai bagian dari investigasi keamanan, Respons Insiden Keamanan AWS Anda juga dapat mengumpulkan informasi investigasi dari instans Amazon Elastic Compute Cloud menggunakan EC2

Triage. Saat diaktifkan, kemampuan ini memungkinkan Respons Insiden Keamanan AWS responden AWS Systems Manager menjalankan Run Command di instans Amazon EC2 untuk mengumpulkan data investigasi, memeriksa proses yang sedang berjalan, dan menganalisis status sistem — tanpa memerlukan akses langsung ke instans.

EC2 Triage mendukung sistem operasi berikut:

Linux

- Amazon Linux 2, Amazon Linux 2023
- Ubuntu 18.04, 20.04, 22.04, 24.04
- Red Hat Enterprise Linux (RHEL) 7.x, 8.x, 9.x
- CentOS 7.x, 8.x
- Server Perusahaan SUSE Linux (SLES) 12.x, 15.x
- Debian 10, 11, 12

Windows

- Windows Server 2012 R2
- Server Windows 2016, 2019, 2022

Untuk menggunakan Triage EC2, Anda harus menerapkan template Containment with EC2 CloudFormation Triage ke akun Anda. Untuk informasi selengkapnya, lihat [Bekerja dengan CloudFormation StackSets](#). Instans Amazon EC2 target harus memiliki [Agen SSM](#) yang diinstal dan dijalankan, dan harus online dan dikelola oleh AWS Systems Manager Untuk informasi penyiapan, lihat [Menyiapkan Systems Manager untuk instans Amazon EC2](#).

Berkomunikasi

Respons Insiden Keamanan AWS membuat Anda mendapat informasi selama investigasi keamanan dengan terlibat dengan tim Respons Insiden Anda melalui kasus Respons Insiden Keamanan. Beberapa anggota Respons Insiden Keamanan AWS Teknik dapat mendukung penyelidikan. Komunikasi dapat mencakup: pengakuan atau pemberitahuan tentang pembuatan investigasi keamanan; membangun jembatan panggilan; analisis artefak seperti file log; permintaan konfirmasi aktivitas yang diharapkan; dan berbagi hasil investigasi.

Ketika Respons Insiden Keamanan AWS secara proaktif melibatkan tim Respons Insiden Anda, sebuah kasus dibuat di akun Respons Insiden Keamanan AWS Keanggotaan Anda, yang memusatkan komunikasi untuk semua akun Organisasi di satu tempat. Kasus-kasus ini berisi awalan “[Kasus proaktif]” dalam judulnya, yang mengidentifikasi mereka sebagai diprakarsai oleh Respons

Insiden Keamanan AWS Dengan secara aktif terlibat dan memberikan tanggapan tepat waktu terhadap komunikasi ini, tim Respons Insiden Anda dapat membantu Respons Insiden Keamanan AWS melakukan hal berikut:

- Pastikan respons cepat terhadap insiden keamanan asli.
- Pahami lingkungan Anda dan perilaku yang diharapkan.
- Kurangi deteksi positif palsu dari waktu ke waktu.

Efektivitas Respons Insiden Keamanan AWS meningkatkan dengan kolaborasi Anda dan menghasilkan AWS lingkungan yang lebih efektif dipantau dan aman.

Memperbarui Temuan

Respons Insiden Keamanan AWS mengelola temuan secara berbeda tergantung pada sumber dan hasil triasenya.

Layanan Tuning

[Jika kuota layanan akun Anda mengizinkan, cobalah Respons Insiden Keamanan AWS menerapkan aturan GuardDuty penindasan Amazon atau aturan otomatisasi.AWS Security Hub CSPM](#) Aturan ini menekan temuan future yang cocok dengan jenis dan sumber aktivitas resmi yang diketahui (misalnya, alamat IP sumber, ASN, prinsipal identitas, atau sumber daya). AWS Security Hub CSPM aturan diterapkan dengan prioritas 10, yang memungkinkan Anda untuk mengganti otomatisasi ini dengan aturan yang ditentukan sendiri jika diperlukan.

Dengan cara ini, Respons Insiden Keamanan AWS menyetel sumber deteksi berdasarkan perilaku yang diharapkan di AWS lingkungan Anda. Tim Respons Insiden Anda diberi tahu tentang modifikasi pada set aturan ini, dan perubahan akan dibatalkan berdasarkan permintaan.

Agen Investigasi AI

Ikhtisar

Agan AI-powered investigasi bekerja bersama pelanggan dan Respons Insiden Keamanan AWS insinyur untuk mempercepat penyelidikan keamanan. Ketika pelanggan membuat kasus yang AWS didukung, agen secara otomatis mengaktifkan secara paralel dengan keterlibatan insinyur Security Incident Response, mengurangi waktu resolusi dari hari ke jam.

Selama eskalasi pelanggan, kasus Respons Insiden Keamanan mungkin dibuat oleh Anda atau secara proaktif oleh. Respons Insiden Keamanan AWS Ketika kasus baru yang AWS didukung

dibuat, agen investigasi secara otomatis terpicu. Anda dapat mengelola semua kasus melalui EventBridge integrasi konsol, API, atau Amazon.

Manfaat utama

- Investigasi paralel — Agen bekerja secara bersamaan dengan responden — menyediakan AI-powered otomatisasi dan keahlian manusia.
- Pengumpulan bukti otomatis — Menghilangkan analisis log manual dengan melakukan kueri secara otomatis AWS CloudTrail, IAM, Amazon EC2, dan Cost Explorer.
- Antarmuka bahasa alami — Jelaskan masalah keamanan dalam bahasa sederhana tanpa memerlukan keahlian dalam format AWS log.
- Respon lebih cepat — Ringkasan investigasi tersedia dalam beberapa menit di tab Investigasi.
- Auditabilitas penuh — Semua tindakan agen masuk di AWS CloudTrail bawah `AWSServiceRoleForSupport` peran.

Important

Fitur ini hanya tersedia untuk kasus AWS yang didukung. Self-managed Kasus tidak termasuk kemampuan investigasi AI.


Cara kerjanya

Agan investigasi AI mengikuti alur kerja terstruktur saat menganalisis kasus keamanan yang AWS didukung:

Alur kerja investigasi

1. Pembuatan kasus — Pelanggan membuat kasus yang AWS didukung di konsol Security Incident Response yang menjelaskan masalah keamanan.
2. Aktivasi paralel
 - Insinyur Security Incident Response terlibat dengan kasus ini.
 - Bersamaan dengan itu, agen AI memulai alur kerja penyelidikannya.
3. Pertanyaan kontekstual (opsional) — Agen dapat mengajukan pertanyaan klarifikasi untuk mengumpulkan detail spesifik:
 - ID AWS akun yang terpengaruh

- Prinsipal IAM yang terlibat (pengguna, peran, kunci akses)
 - Pengidentifikasi sumber daya khusus (bucket S3, instans EC2, ARN)
 - Jangka waktu aktivitas mencurigakan
4. Pengumpulan bukti — Agen secara otomatis menanyakan sumber AWS data:
 - AWS CloudTrail— Panggilan API dan aktivitas yang terkait dengan insiden tersebut
 - IAM — Izin pengguna dan peran, perubahan kebijakan, dan pembuatan identitas baru
 - API Instans Amazon EC2 — Informasi tentang sumber daya komputasi jika terlibat
 - Cost Explorer — Metrik biaya dan penggunaan untuk konsumsi sumber daya yang tidak biasa
 5. Analisis dan korelasi — Agen menghubungkan bukti di seluruh layanan, mengidentifikasi pola, dan membangun garis waktu peristiwa.
 6. Pembuatan ringkasan — Dalam beberapa menit, agen menyajikan ringkasan investigasi komprehensif di tab Investigasi.

 Note

Semua bidang bersifat opsional. Jika tidak ada jawaban yang diberikan dalam 10 menit, penyelidikan dimulai secara otomatis. Dalam beberapa kasus, jika informasi yang cukup sudah tersedia, agen dapat melewati pertanyaan opsional sepenuhnya.

Mengakses hasil investigasi

Untuk melihat analisis AI:

1. Arahkan ke kasus Anda di konsol Security Incident Response.
2. Pilih tab Investigasi.
3. Tinjau ringkasan investigasi dengan temuan, garis waktu, dan konteks.

Ringkasan agen investigasi AI secara otomatis diposting sebagai komentar di bagian Komunikasi kasus, sehingga mudah untuk ditinjau bersama pembaruan kasus lainnya.

Akses dan izin data

Agen investigasi AI menggunakan `AWSServiceRoleForSupport` Service-Linked Peran untuk mengakses AWS sumber daya. Peran ini memberikan izin hanya-baca yang diperlukan untuk pengumpulan bukti.

Semua tindakan yang dilakukan oleh agen masuk AWS CloudTrail, memungkinkan pelanggan untuk mengaudit dengan tepat data apa yang diakses selama penyelidikan. Dalam AWS CloudTrail log, tindakan ini dikaitkan dengan `AWSServiceRoleForSupport`.

Prasyarat

Sebelum menggunakan kemampuan AI-powered investigasi, pastikan hal-hal berikut:

Pengaturan yang diperlukan

- Respons Insiden Keamanan AWS diaktifkan — Layanan harus diaktifkan melalui akun AWS Organizations manajemen.
- AWS jenis kasus yang didukung - Investigasi AI hanya tersedia untuk kasus yang AWS didukung (bukan kasus yang dikelola sendiri).
- `AWSServiceRoleForSupport`— Peran terkait layanan ini dibuat secara otomatis dan memberikan izin yang diperlukan untuk agen investigasi.

Izin yang diperlukan

Untuk membuat kasus yang AWS didukung dan mengakses hasil investigasi, prinsipal IAM memerlukan izin berikut:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "security-ir:CreateCase",
        "security-ir:GetCase",
        "security-ir:ListCases",
        "security-ir:UpdateCase"
      ],
      "Resource": "*"
    }
  ]
}
```

Menggunakan agen investigasi

Agan investigasi AI aktif secara otomatis saat membuat kasus yang AWS didukung.

Untuk memantau kemajuan investigasi AI

1. Buka kasing Anda di Respons Insiden Keamanan AWS konsol.
2. Pilih tab Investigasi.
3. Lihat status investigasi (Sedang Berlangsung atau Selesai).
4. Setelah selesai, tinjau ringkasan investigasi komprehensif dengan temuan, garis waktu, dan rekomendasi.

Pengungkapan AI yang bertanggung jawab

Ringkasan investigasi dihasilkan menggunakan kemampuan AWS Generative AI. Anda bertanggung jawab untuk mengevaluasi AI-generated rekomendasi dalam konteks spesifik Anda, menerapkan mekanisme pengawasan yang tepat, memverifikasi temuan secara independen, dan menjaga pengawasan manusia terhadap semua keputusan keamanan.

Penggunaan data pelanggan

Agen Investigasi AI tidak menggunakan data pelanggan untuk pelatihan model, dan tidak membagikan data pelanggan dengan pihak ketiga.

Mengandung

AWS Security Incident Response bermitra dengan Anda untuk memuat peristiwa. Anda dapat mengonfigurasi layanan untuk mengambil tindakan penahanan proaktif di akun Anda sebagai tanggapan terhadap temuan keamanan. Anda juga dapat melakukan penahanan sendiri atau dalam kemitraan dengan hubungan pihak ketiga Anda dengan menggunakan [dokumen SSM](#) yang dijelaskan dalam Tindakan [Penahanan yang Didukung](#).

Important

AWS Security Incident Response tidak mengaktifkan kemampuan penahanan secara default. Dua langkah diperlukan untuk mengaktifkan kemampuan penahanan proaktif:

1. Berikan izin yang diperlukan untuk layanan menggunakan peran IAM. Anda dapat membuat peran ini secara individual per akun atau di seluruh organisasi Anda dengan bekerja dengan AWS CloudFormation stacksets, yang membuat peran yang diperlukan.
2. Tentukan preferensi penahanan Anda per akun atau di seluruh organisasi Anda untuk mengotorisasi tindakan penahanan proaktif. Account-level preferensi menggantikan

preferensi tingkat organisasi. Hal ini dapat dilakukan dengan membuat AWS Support Case (Technical: Security Incident Response Service/Other). Preferensi penahanan yang tersedia adalah:

- **Persetujuan Diperlukan (default):** Jangan melakukan penahanan proaktif sumber daya apa pun tanpa otorisasi eksplisit berdasarkan kasus per kasus.
- **Berisi Konfirmasi:** Lakukan penahanan proaktif dari sumber daya yang dikonfirmasi untuk dikompromikan.
- **Mengandung Tersangka:** Lakukan penahanan proaktif sumber daya dengan kemungkinan besar telah dikompromikan, berdasarkan analisis yang dilakukan oleh AWS Security Incident Response Engineering.

Penahanan Decision-Making

Bagian penting dari penahanan adalah pengambilan keputusan, seperti apakah akan mematikan sistem, mengisolasi sumber daya dari jaringan, mematikan akses, atau mengakhiri sesi. Keputusan ini dibuat lebih mudah ketika ada strategi dan prosedur yang telah ditentukan untuk menahan acara tersebut. AWS Security Incident Response menyediakan strategi penahanan, memberi tahu Anda tentang dampak potensial, dan memandu Anda untuk menerapkan solusi hanya setelah Anda mempertimbangkan dan menyetujui risiko yang terlibat.

Tindakan Penahanan yang Didukung

Respons Insiden Keamanan AWS mengeksekusi tindakan penahanan yang didukung atas nama Anda untuk mempercepat respons dan mengurangi waktu yang dimiliki pelaku ancaman untuk berpotensi menyebabkan kerusakan di lingkungan Anda. Kemampuan ini memungkinkan mitigasi ancaman yang teridentifikasi dengan lebih cepat, meminimalkan potensi dampak dan meningkatkan postur keamanan Anda secara keseluruhan. Ada opsi penahanan yang berbeda tergantung pada sumber daya yang dianalisis. Tindakan penahanan yang didukung dijelaskan dalam sub-bagian di bawah ini.

Penahanan EC2

Otomatisasi `AWSSupport-ContainEC2Instance` penahanan melakukan penahanan jaringan reversibel dari instans EC2, membiarkan instance utuh dan berjalan, tetapi mengisolasinya dari aktivitas jaringan baru dan mencegahnya berkomunikasi dengan sumber daya di dalam dan di luar VPC Anda.

⚠ Important

Penting untuk dicatat bahwa koneksi yang dilacak yang ada tidak akan dimatikan sebagai akibat dari perubahan kelompok keamanan - hanya lalu lintas future yang akan diblokir secara efektif oleh grup keamanan baru dan dokumen SSM ini. Informasi lebih lanjut tersedia di bagian [penahanan sumber](#) dari panduan teknis layanan.

Penahanan IAM

Otomatisasi `AWSSupport-ContainIAMPrincipal` penahanan melakukan penahanan jaringan reversibel dari pengguna atau peran IAM, meninggalkan pengguna atau peran dalam IAM, tetapi mengisolasinya dari berkomunikasi dengan sumber daya dalam akun Anda.

Penahanan S3

Otomatisasi `AWSSupport-ContainS3Resource` penahanan melakukan penahanan reversibel bucket S3, meninggalkan objek di bucket, dan mengisolasi bucket atau objek Amazon S3 dengan memodifikasi kebijakan aksesnya.

Mengembangkan Strategi Penahanan

Respons Insiden Keamanan AWS mendorong Anda untuk mempertimbangkan strategi penahanan untuk setiap jenis acara besar yang sesuai dengan selera risiko Anda. Dokumentasikan kriteria yang jelas untuk membantu pengambilan keputusan selama suatu acara. Kriteria yang perlu dipertimbangkan meliputi:

- Potensi kerusakan sumber daya
- Pelestarian bukti dan persyaratan peraturan
- Ketidakterediaan layanan (misalnya, konektivitas jaringan, layanan yang diberikan kepada pihak eksternal)
- Waktu dan sumber daya yang dibutuhkan untuk mengimplementasikan strategi
- Efektivitas strategi (misalnya, penahanan sebagian vs penuh)
- Permanen solusi (misalnya, reversibel vs. ireversibel)
- Durasi solusi (misalnya, solusi darurat, solusi sementara, solusi permanen)

Terapkan kontrol keamanan yang dapat menurunkan risiko dan memberikan waktu untuk menentukan dan menerapkan strategi penahanan yang lebih efektif.

Pendekatan Penahanan Bertahap

Respons Insiden Keamanan AWS menyarankan pendekatan bertahap untuk mencapai penahanan yang efisien dan efektif, yang melibatkan strategi jangka pendek dan jangka panjang berdasarkan jenis sumber daya.

Strategi Penahanan

Dapat Respons Insiden Keamanan AWS mengidentifikasi ruang lingkup acara keamanan?

- Jika ya, identifikasi semua sumber daya (pengguna, sistem, sumber daya).
- Jika tidak, selidiki secara paralel dengan mengeksekusi langkah berikutnya pada sumber daya yang diidentifikasi.

Bisakah sumber daya diisolasi?

- Jika ya, maka lanjutkan untuk mengisolasi sumber daya yang terpengaruh.
- Jika tidak, maka bekerja dengan pemilik dan manajer sistem untuk menentukan tindakan lebih lanjut yang diperlukan untuk mengatasi masalah.

Apakah semua sumber daya yang terpengaruh terisolasi dari sumber daya yang tidak terpengaruh?

- Jika ya, lanjutkan ke langkah berikutnya.
- Jika tidak, maka teruskan mengisolasi sumber daya yang terkena dampak untuk menyelesaikan penahanan jangka pendek dan mencegah peristiwa meningkat lebih lanjut.

Sistem Backup

Apakah salinan cadangan dari sistem yang terpengaruh dibuat untuk analisis lebih lanjut?

Apakah salinan forensik dienkripsi dan disimpan di lokasi yang aman?

- Jika ya, lanjutkan ke langkah berikutnya.
- Jika tidak, enkripsi gambar forensik, lalu simpan di lokasi yang aman untuk mencegah penggunaan, kerusakan, dan gangguan yang tidak disengaja.

Kirim preferensi penahanan

Untuk mengonfigurasi preferensi penahanan untuk akun atau organisasi Anda, buat [AWS Dukungan kasus](#).

Dalam kasus dukungan Anda, tentukan informasi berikut:

- AWS Organizations ID Anda atau ID akun tertentu di mana tindakan penahanan harus diotorisasi.
- Opsi penahanan pilihan Anda.

Saat dikonfigurasi, Respons Insiden Keamanan AWS jalankan tindakan penahanan resmi selama insiden keamanan aktif untuk membantu melindungi lingkungan Anda.

Note

Respons Insiden Keamanan AWS mengeksekusi tindakan penahanan hanya ketika dikonfigurasi dengan preferensi yang sesuai dan setelah AWS CloudFormation StackSet diperlukan digunakan untuk memberikan izin yang diperlukan.

Membasmi

Selama fase pemberantasan, penting untuk mengidentifikasi dan menangani semua akun, sumber daya, dan contoh yang terpengaruh - seperti dengan menghapus malware, menghapus akun pengguna yang disusupi, dan mengurangi kerentanan yang ditemukan - untuk menerapkan remediasi seragam di seluruh lingkungan.

Ini adalah praktik terbaik untuk menggunakan pendekatan bertahap untuk pemberantasan dan pemulihan, dan untuk memprioritaskan langkah-langkah remediasi. Tujuan dari fase awal adalah untuk meningkatkan keamanan secara keseluruhan dengan cepat (hari ke minggu) dengan perubahan bernilai tinggi untuk mencegah kejadian di masa depan. Fase selanjutnya dapat berfokus pada perubahan jangka panjang (misalnya, perubahan infrastruktur), dan pekerjaan berkelanjutan untuk menjaga perusahaan seaman mungkin. Setiap kasus unik dan insinyur Respons Insiden AWS Keamanan akan bekerja sama dengan Anda untuk menilai tindakan yang diperlukan.

Pertimbangkan hal berikut:

- Bisakah Anda mencitrakan ulang sistem dan mengeraskannya dengan tambalan atau tindakan pencegahan lainnya untuk mencegah atau mengurangi risiko serangan?

- Bisakah Anda mengganti sistem yang terinfeksi dengan instance atau sumber daya baru, mengaktifkan garis dasar yang bersih saat menghentikan item yang terinfeksi?
- Sudahkah Anda menghapus semua malware dan artefak lain yang ditinggalkan oleh penggunaan yang tidak sah, dan mengeraskan sistem yang terpengaruh terhadap serangan lebih lanjut?
- Apakah ada persyaratan untuk forensik pada sumber daya yang terkena dampak?

Memulihkan

Respons Insiden Keamanan AWS memberi Anda panduan untuk membantu memulihkan sistem ke operasi normal, mengonfirmasi bahwa sistem berfungsi dengan baik, dan memulihkan kerentanan apa pun untuk mencegah kejadian serupa di masa mendatang. Respons Insiden Keamanan AWS tidak secara langsung membantu pemulihan sistem. Pertimbangan utama meliputi:

- Apakah sistem yang terkena dampak ditambah dan dikeraskan terhadap serangan baru-baru ini?
- Apa garis waktu yang layak untuk mengembalikan sistem ke produksi?
- Alat apa yang akan Anda gunakan untuk menguji, memantau, dan memverifikasi sistem yang dipulihkan?

Laporan bulanan

Respons Insiden Keamanan AWS mengirim email laporan bulanan ke semua kontak di tim Respons Insiden Anda. Untuk memperbarui siapa yang menerima laporan ini, ubah daftar kontak di Respons Insiden Keamanan AWS konsol. Laporan dikirimkan dalam format PDF dan menyertakan metrik yang dijelaskan dalam [Metrik kasus](#). Anda dapat mengharapkan pengiriman dalam satu hingga dua minggu setelah bulan berakhir. Baris subjek email adalah: Respons Insiden Keamanan AWS Monthly Report - (*Month Year*). Anda menerima satu laporan per organisasi yang ditentukan dalam AWS Organizations.

Metrik kasus

- Kasus dibuat
 - Nama dimensi: Jenis
 - Nilai dimensi: AWS didukung, didukung sendiri
 - Unit: Jumlah
 - Deskripsi: Jumlah kasus yang dibuat.

- Kasus ditutup
 - Nama dimensi: Jenis
 - Nilai dimensi: AWS didukung, dikelola sendiri
 - Unit: Jumlah
 - Deskripsi: Ukuran jumlah total kasus yang ditutup.
- Kasus terbuka
 - Nama dimensi: Jenis
 - Nilai dimensi: AWS didukung, didukung sendiri
 - Unit: Jumlah
 - Keterangan: Jumlah kasus terbuka.

Metrik triaging

- Temuan diterima
 - Unit: Jumlah
 - Keterangan: Jumlah temuan yang dikirim ke triaging.
- Temuan diarsipkan
 - Unit: Jumlah
 - Keterangan: Jumlah temuan yang diarsipkan setelah diproses tanpa investigasi manual.
- Temuan Diselidiki secara manual
 - Unit: Jumlah
 - Keterangan: Jumlah temuan dengan investigasi manual yang dilakukan.
- Investigasi diarsipkan
 - Unit: Jumlah
 - Keterangan: Jumlah investigasi manual yang menghasilkan false positive dan dikirim untuk pengarsipan
- Investigasi meningkat
 - Unit: Jumlah
 - Deskripsi: Jumlah investigasi manual yang mengakibatkan insiden keamanan

Kasus

Respons Insiden Keamanan AWS memungkinkan Anda membuat dua jenis kasus - kasus yang AWS didukung atau dikelola sendiri.

Buat sebuah AWS kasus yang didukung

Anda dapat membuat kasus yang AWS didukung Respons Insiden Keamanan AWS melalui Konsol, API, atau AWS Command Line Interface. AWS kasus yang didukung memungkinkan Anda menerima dukungan dari teknisi Security Incident Response.

Important

Demo/simulation-cases ditutup setelah jangka waktu 90 hari.

Note

AWS Insinyur Respons Insiden Keamanan akan menanggapi kasus Anda dalam waktu 15 menit. Waktu respons adalah untuk respons pertama dari insinyur Respons Insiden AWS Keamanan. Kami akan melakukan segala upaya yang wajar untuk menanggapi permintaan awal Anda dalam jangka waktu ini. Waktu respons ini tidak berlaku untuk tanggapan selanjutnya.

Note

Anda dapat membuat kasus yang AWS didukung tidak hanya untuk insiden dan investigasi keamanan aktif, tetapi juga untuk pertanyaan tentang kemampuan Respons Insiden AWS Keamanan. Ini termasuk pertanyaan tentang aturan GuardDuty penekanan, konfigurasi triaging peringatan, alur kerja respons proaktif, dan panduan umum tentang postur keamanan. Pilih jenis kasus Investigasi dan Pertanyaan untuk tujuan ini.

Kapan harus menghubungi Respons Insiden Keamanan AWS

Anda dapat menghubungi AWS Security Incident Response untuk berbagai keperluan tergantung kebutuhan Anda. Tabel berikut menjelaskan skenario yang berbeda dan metode kontak yang sesuai untuk masing-masing.

Skenario	Kapan Harus Digunakan	Waktu Respons	Jenis Kasus
Insiden Keamanan Aktif	Anda mengalami insiden keamanan mendesak yang membutuhkan dukungan dan layanan respons insiden segera	15 menit (respons pertama)	Insiden Keamanan Aktif
Investigasi	Anda memiliki insiden keamanan yang dirasakan dan membutuhkan dukungan dengan analisis log dan konfirmasi sekunder dari investigasi respons insiden	15 menit (respons pertama)	Investigasi dan Pertanyaan
Pertanyaan dan Bimbingan	Anda memiliki pertanyaan tentang GuardDuty temuan Amazon, aturan penekanan, konfigurasi triaging peringatan, alur kerja respons proaktif, atau postur keamanan umum yang terkait dengan kemampuan Respons Insiden Keamanan AWS	15 menit (respons pertama)	Investigasi dan Pertanyaan
Masalah Orientasi	Anda mengalami masalah teknis selama proses orientasi untuk AWS Security Incident Response	Bervariasi berdasarkan rencana dukungan	AWS Dukungan kasus

Untuk semua kasus yang AWS didukung (Insiden Keamanan Aktif dan Investigasi dan Pertanyaan), teknisi AWS Security Incident Response akan merespons dalam waktu 15 menit untuk tanggapan pertama. Waktu respons ini hanya berlaku untuk kontak awal dan tidak berlaku untuk tanggapan selanjutnya.

Contoh berikut mencakup penggunaan konsol.

1. Masuk Respons Insiden Keamanan AWS melalui Konsol Manajemen AWS.
2. Pilih Buat Kasus
3. Pilih Selesaikan kasus dengan AWS
4. Pilih jenis permintaan
 - a. Insiden Keamanan Aktif: Jenis ini untuk dukungan dan layanan respons insiden mendesak.
 - b. Investigasi dan Pertanyaan: Gunakan jenis ini untuk insiden keamanan yang dirasakan di mana insinyur Respons Insiden AWS Keamanan dapat mendukung analisis log dan konfirmasi sekunder dari investigasi respons insiden. Anda juga dapat menggunakan jenis ini untuk pertanyaan tentang GuardDuty temuan, aturan penekanan, konfigurasi triaging peringatan, alur kerja respons proaktif, dan pertanyaan postur keamanan umum yang terkait dengan kemampuan Respons Insiden Keamanan. AWS
5. Tetapkan perkiraan tanggal mulai ke tanggal indikator awal insiden Anda. Misalnya, ketika Anda mengalami perilaku abnormal untuk pertama kalinya atau ketika Anda menerima peringatan keamanan terkait pertama.
6. Tentukan judul untuk kasus ini
7. Berikan deskripsi rinci tentang kasus ini. Pertimbangkan aspek-aspek berikut yang dapat membantu responden insiden dengan penyelesaian kasus:
 - a. Apa yang terjadi?
 - b. Siapa yang menemukan dan melaporkan kejadian itu?
 - c. Siapa yang terpengaruh oleh kasus ini?
 - d. Apa dampak yang diketahui?
 - e. Apa urgensi untuk kasus ini?
 - f. Tambahkan satu atau beberapa Akun AWS ID yang berada dalam lingkup kasus ini.
8. Tambahkan detail kasus opsional:
 - a. Pilih layanan utama yang terkena dampak dari daftar drop-down.
 - b. Pilih wilayah utama yang terkena dampak dari daftar drop-down.
 - c. Tambahkan satu atau banyak alamat IP aktor ancaman yang Anda identifikasi sebagai bagian dari kasus ini.
9. Tambahkan responden insiden tambahan opsional ke kasus yang akan menerima pemberitahuan. Untuk menambahkan individu, lakukan hal berikut:
 - a. Tambahkan alamat email.
 - b. Tambahkan nama depan dan belakang opsional.

- c. Pilih Tambahkan baru untuk menambahkan individu lain.
- d. Untuk menghapus individu, pilih opsi Hapus untuk individu.
- e. Pilih Tambahkan untuk menambahkan semua individu yang terdaftar ke kasing.
 - i. Anda dapat memilih beberapa individu dan memilih Hapus untuk menghapusnya dari daftar.

10. Tambahkan tag opsional ke kasing.

- a. Untuk menambahkan tanda, lakukan hal berikut:
- b. Pilih Tambahkan tag baru.
- c. Untuk Kunci, masukkan nama tag.
- d. Untuk Nilai, masukkan nilai tag.
- e. Untuk menghapus tag, pilih opsi Hapus untuk tag itu.

Setelah kasus yang AWS didukung dibuat, teknisi Respons Insiden AWS Keamanan dan tim respons insiden Anda segera diberitahu.

Untuk membuat kasus yang AWS didukung dengan investigasi AI

1. Buka Respons Insiden Keamanan AWS konsol di console.aws.amazon.com/.
2. Pilih Kasus dari panel navigasi.
3. Pilih Buat kasus.
4. Untuk tipe Kasus, pilih AWS-supported case.
5. Berikan rincian kasus termasuk judul, tanggal mulai insiden, dan ID AWS akun yang terpengaruh.
6. Di bagian Jelaskan peristiwa keamanan, berikan deskripsi menyeluruh tentang insiden tersebut.
7. Memberikan informasi tambahan tentang AWS layanan, wilayah, dan detail relevan lainnya yang terpengaruh.
8. Pilih Buat kasus.

Setelah pembuatan kasus, baik insinyur Security Incident Response dan agen AI mulai bekerja secara bersamaan.

Untuk menanggapi pertanyaan klarifikasi AI (opsional)

1. Arahkan ke tab Investigasi dalam kasus Anda.
2. Tinjau setiap pertanyaan klarifikasi yang disajikan oleh agen AI.

3. Tanggapi pertanyaan atau pilih Lewati jika Anda memilih untuk tidak menjawab.
4. Pilih Kirim untuk melanjutkan. Semua bidang bersifat opsional.

Pengungkapan AI yang bertanggung jawab

Ringkasan investigasi dihasilkan menggunakan kemampuan AWS Generative AI. Anda bertanggung jawab untuk mengevaluasi AI-generated rekomendasi dalam konteks spesifik Anda, menerapkan mekanisme pengawasan yang tepat, memverifikasi temuan secara independen, dan menjaga pengawasan manusia terhadap semua keputusan keamanan.

Membuat kasus yang dikelola sendiri

Anda dapat membuat untuk yang dikelola sendiri Respons Insiden Keamanan AWS melalui Konsol, API, atau AWS Command Line Interface. Jenis kasus ini TIDAK melibatkan insinyur Respons Insiden AWS Keamanan. Contoh berikut mencakup penggunaan konsol.

1. Masuk Respons Insiden Keamanan AWS melalui Konsol Manajemen AWS at <https://console.aws.amazon.com/security-ir/>.
2. Pilih Buat Kasus.
3. Pilih Selesaikan kasus dengan tim respons insiden saya sendiri.
4. Tetapkan perkiraan tanggal mulai ke tanggal indikator awal insiden Anda. Misalnya, ketika Anda mengalami perilaku abnormal untuk pertama kalinya atau ketika Anda menerima peringatan keamanan terkait pertama.
5. Tentukan judul untuk kasus ini. Disarankan untuk memasukkan data ke dalam judul kasus seperti yang disarankan saat memilih opsi Hasilkan Judul.
6. Masukkan Akun AWS ID yang merupakan bagian dari kasing. Untuk menambahkan ID akun, lakukan hal berikut:
 - a. Masukkan ID akun 12 digit dan pilih Tambah akun.
 - b. Untuk menghapus akun, pilih Hapus di samping akun yang ingin Anda hapus dari kasing.
7. Berikan deskripsi rinci tentang kasus ini.
 - a. Pertimbangkan aspek-aspek berikut yang dapat membantu responden insiden dengan penyelesaian kasus:
 - i. Apa yang terjadi?
 - ii. Siapa yang menemukan dan melaporkan kejadian itu?
 - iii. Siapa yang terpengaruh oleh kasus ini?

- iv. Apa dampak yang diketahui?
 - v. Apa urgensi untuk kasus ini?
8. Tambahkan detail kasus opsional:
 - a. Pilih layanan utama yang terkena dampak dari daftar drop-down.
 - b. Pilih wilayah utama yang terkena dampak dari daftar drop-down.
 - c. Tambahkan satu atau banyak alamat IP aktor ancaman yang Anda identifikasi sebagai bagian dari kasus ini.
 9. Tambahkan responden insiden tambahan opsional ke kasus yang akan menerima pemberitahuan. Untuk menambahkan individu, lakukan hal berikut:
 - a. Tambahkan alamat email.
 - b. Tambahkan nama depan dan belakang opsional.
 - c. Pilih Tambahkan baru untuk menambahkan individu lain.
 - d. Untuk menghapus individu, pilih opsi Hapus untuk individu.
 - e. Pilih Tambahkan untuk menambahkan semua individu yang terdaftar ke kasing. Anda dapat memilih beberapa individu dan memilih Hapus untuk menghapusnya dari daftar.
 10. Tambahkan tag opsional ke kasing. Untuk menambahkan tanda, lakukan hal berikut:
 - a. Pilih Tambahkan tag baru.
 - b. Untuk Kunci, masukkan nama tag.
 - c. Untuk Nilai, masukkan nilai tag.
 - d. Untuk menghapus tag, pilih opsi Hapus untuk tag itu.

Tim respons insiden akan diberitahu melalui email setelah kasus dibuat.

Bekerja dengan AWS Insinyur Respons Insiden Keamanan

Setelah Anda membuka kasus insiden keamanan, insinyur AWS Security Incident Response mulai mengerjakan insiden Anda. Bagian ini menjelaskan apa yang diharapkan selama penyelidikan dan bagaimana berkolaborasi secara efektif dengan tim kami.

Apa yang diharapkan dari AWS Insinyur Respons Insiden Keamanan

Saat Anda membuka kasus yang AWS didukung, insinyur Respons Insiden Keamanan ditugaskan untuk insiden Anda. Responden Anda yang ditugaskan akan:

- Tinjau informasi awal yang Anda berikan dalam kasus ini

- Menganalisis log AWS layanan yang relevan dan temuan keamanan
- Identifikasi ruang lingkup dan dampak insiden keamanan
- Kembangkan rencana investigasi dan respons yang disesuaikan dengan situasi Anda

Garis waktu respons: Tujuan tingkat layanan (SLO) untuk pengakuan kasus baru oleh para Respons Insiden Keamanan AWS insinyur adalah dalam waktu 15 menit. Garis waktu penilaian awal dapat bervariasi berdasarkan tingkat keparahan dan kompleksitas kasus. Jika Respons Insiden Keamanan AWS insinyur tidak menerima tanggapan atau informasi penting dari Anda dalam waktu 5 hari kerja, kasing ditutup.

Alur kerja investigasi

AWS Insinyur Security Incident Response mengikuti proses respons insiden terstruktur yang selaras dengan kerangka kerja NIST 800-61r2. Selama penyelidikan Anda, Anda dapat mengharapkan tahapan berikut:

1. Triase awal - Insinyur Respons Insiden Keamanan meninjau detail kasus Anda dan mengkonfirmasi ruang lingkup insiden
2. Investigasi - Insinyur Security Incident Response menganalisis log, mengidentifikasi indikator kompromi, dan menentukan akar penyebab
3. Penahanan - Insinyur Respons Insiden Keamanan merekomendasikan tindakan untuk membatasi dampak insiden
4. Pemberantasan dan pemulihan - Insinyur Respons Insiden Keamanan membantu Anda menghilangkan ancaman dan memulihkan operasi normal
5. Post-incident review - Security Incident Response engineer memberikan temuan dan rekomendasi untuk mencegah insiden future

Selama fase ini, teknisi Respons Insiden Keamanan Anda memberi Anda informasi melalui pembaruan kasus dan dapat meminta informasi atau tindakan tambahan dari Anda.

Insinyur Respons Insiden Keamanan Informasi dapat meminta

Untuk menyelidiki insiden Anda secara efektif, teknisi AWS Security Incident Response dapat meminta Anda untuk memberikan:

- Detail garis waktu - Ketika Anda pertama kali mendeteksi insiden dan peristiwa relevan yang mengarah ke sana

- Sumber daya yang terpengaruh - ID AWS akun, layanan, wilayah, dan ARN sumber daya tertentu yang terlibat
- Informasi akses - Detail tentang siapa yang memiliki akses ke sumber daya yang terpengaruh dan perubahan akses terbaru
- Konteks bisnis - Bagaimana sumber daya yang terpengaruh digunakan dan potensi dampak bisnis
- Log dan bukti - Log tambahan, tangkapan layar, atau artefak yang dapat membantu penyelidikan
- Otorisasi - Persetujuan untuk melakukan tindakan penahanan atau remediasi tertentu atas nama Anda

Insinyur Respons Insiden Keamanan Anda akan menjelaskan mengapa setiap informasi diperlukan dan bagaimana hal itu membantu penyelidikan.

Praktik terbaik komunikasi

Komunikasi yang efektif mempercepat resolusi insiden. Ikuti praktik berikut saat bekerja dengan teknisi AWS Security Incident Response:

- Segera tanggap permintaan informasi dari teknisi Security Incident Response Anda
- Berikan informasi lengkap bahkan jika Anda tidak yakin tentang relevansinya
- Ajukan pertanyaan jika Anda tidak memahami rekomendasi atau perlu klarifikasi
- Perbarui kasus dengan perkembangan atau perubahan baru pada insiden tersebut
- Tentukan kontak utama dari tim Anda untuk berkoordinasi dengan teknisi Security Incident Response

Important

Jika Respons Insiden Keamanan AWS teknisi tidak menerima tanggapan atas permintaan informasi penting dalam waktu 5 hari kerja, kami bekerja menuju penutupan kasus. Anda dapat membuka kembali kasus jika informasi baru tersedia.

Peran Anda selama investigasi

Sementara Respons Insiden Keamanan AWS insinyur memimpin penyelidikan, partisipasi Anda sangat penting. Anda bertanggung jawab atas tindakan berikut:

- Memberikan tanggapan tepat waktu terhadap permintaan informasi
- Menerapkan tindakan penahanan dan remediasi yang direkomendasikan di lingkungan Anda AWS
- Mengotorisasi teknisi Respons Insiden Keamanan untuk mengambil tindakan atas nama Anda (jika Anda mengaktifkan respons proaktif)
- Berkoordinasi dengan tim internal Anda (keamanan, hukum, kepatuhan) sesuai kebutuhan
- Membuat keputusan bisnis tentang prioritas respons insiden dan trade-off

Respons Insiden Keamanan AWS insinyur memberikan keahlian dan rekomendasi, tetapi Anda mempertahankan kendali atas AWS sumber daya Anda dan membuat keputusan akhir tentang tindakan respons.

Penutupan kasus

Respons Insiden Keamanan AWS insinyur menutup kasus Anda ketika:

- Insiden tersebut telah diatasi dan diperbaiki
- Semua temuan investigasi telah dibagikan dengan Anda
- Tidak diperlukan bantuan insinyur Respons Insiden Keamanan lebih lanjut
- Anda meminta penutupan kasus

Sebelum menutup kasus, teknisi Security Incident Response Anda memberikan ringkasan temuan, tindakan yang diambil, dan rekomendasi untuk meningkatkan postur keamanan Anda.

Jika Anda memerlukan bantuan tambahan setelah penutupan kasus, Anda dapat membuka kasus atau kontak baru AWS Dukungan.

Menanggapi sebuah AWS kasus yang dihasilkan

Respons Insiden Keamanan AWS dapat membuat notifikasi atau kasus keluar ketika Anda perlu menindaklanjuti atau mengetahui sesuatu yang berpotensi memengaruhi akun atau sumber daya Anda. Ini hanya terjadi jika Anda mengaktifkan respons proaktif dan alur kerja triaging peringatan sebagai bagian dari langganan Anda.

Pemberitahuan ini muncul sebagai kasus Respons Insiden Keamanan dengan awalan “[Kasus proaktif]” di Respons Insiden Keamanan AWS konsol. Untuk melihat dan mengelola kasus ini, selesaikan langkah-langkah berikut:

- Buka konsol Security Incident Response di <https://console.aws.amazon.com/security-ir/>

- Pilih Kasus.
- Anda melihat semua kasus, termasuk yang memiliki awalan “[Kasus proaktif]”.

Anda dapat memperbarui, menyelesaikan, dan membuka kembali kasus ini sesuai kebutuhan. Anda dapat berkomunikasi langsung dengan Respons Insiden Keamanan AWS tim melalui kasus-kasus ini, memastikan penanganan yang efisien dari potensi masalah keamanan.

Mengelola Kasus

Daftar Isi

- [Mengubah status kasus](#)
- [Mengubah resolver](#)
- [Item Aksi](#)
- [Edit kasus](#)
- [Komunikasi](#)
- [Izin](#)
- [Lampiran](#)
- [Tag](#)
- [Kegiatan kasus](#)
- [Menutup kasus](#)

Mengubah status kasus

Sebuah kasus berada di salah satu negara bagian berikut:

- Dikirim: Ini adalah status awal suatu kasus. Kasus dalam status ini telah diajukan oleh yang diminta, tetapi belum dikerjakan.
- Deteksi dan Analisis: Status ini menunjukkan responden insiden telah mulai mengerjakan kasus ini. Fase ini mencakup pengumpulan data, triaging acara, dan melakukan analisis untuk membuat kesimpulan berbasis data.
- Penahanan, Pemberantasan dan Pemulihan: Dalam status ini responden insiden telah mengidentifikasi aktivitas mencurigakan yang membutuhkan upaya tambahan untuk menghapusnya. Responden insiden akan memberikan rekomendasi kepada Anda untuk analisis risiko bisnis dan tindakan tambahan. Jika Anda telah mengaktifkan fitur opt-in untuk layanan, maka

AWS responden insiden akan meminta persetujuan Anda untuk melakukan tindakan penahanan dengan dokumen SSM di akun yang terkena dampak.

- **Post-incident aktivitas:** Dalam status ini peristiwa keamanan utama telah terkandung. Fokusnya sekarang adalah memulihkan dan mengembalikan operasi bisnis ke normal. Ringkasan dan analisis akar penyebab disediakan jika resolver untuk kasus ini didukung AWS.
- **Ditutup:** Ini adalah status akhir dari alur kerja. Kasus dalam status tertutup menunjukkan pekerjaan telah selesai. Kasus tertutup tidak dapat dibuka kembali, jadi pastikan semua tindakan selesai sebelum beralih ke status ini.

Pilih Action/Update Status untuk mengubah status kasus untuk kasus yang dikelola sendiri. Untuk kasus yang AWS didukung, status ditetapkan oleh teknisi AWS Security Incident Response.

Mengubah resolver

Untuk kasus yang dikelola sendiri, tim respons insiden Anda dapat meminta bantuan AWS. Pilih Dapatkan bantuan dari AWS untuk mengubah resolver untuk kasus ini menjadi. AWS Setelah kasus diperbarui ke AWS didukung, status diubah menjadi Kirim. Riwayat kasus yang ada akan tersedia untuk insinyur AWS Security Incident Response. Setelah Anda meminta bantuan dari AWS Anda tidak akan dapat mengubahnya kembali ke yang dikelola sendiri.

Item Aksi

Insinyur Respons Insiden AWS Keamanan yang bekerja pada kasus ini dapat meminta tindakan dari tim internal Anda.

Item tindakan yang muncul setelah kasus dibuat meliputi:

- Permintaan untuk memberikan izin bagi responden insiden untuk mengakses kasus
- Permintaan untuk memberikan informasi lebih lanjut tentang kasus ini

Item tindakan saat kasing siap ditutup:

- Permintaan untuk meninjau laporan kasus
- Permintaan untuk menutup kasus

Edit kasus

Pilih Edit untuk mengubah detail kasus.

Untuk kasus AWS yang didukung dan dikelola sendiri:

Anda dapat mengubah detail kasus berikut setelah kasus dibuat:

- judul
- Deskripsi

Hanya untuk kasus yang AWS didukung:

Anda dapat mengubah bidang tambahan:

- Tipe permintaan:
 - Insiden Keamanan Aktif: Jenis ini untuk dukungan dan layanan respons insiden mendesak.
 - Investigasi: Investigasi memungkinkan Anda untuk mendapatkan dukungan untuk insiden keamanan yang dirasakan di mana insinyur Respons Insiden AWS Keamanan dapat mendukung dalam penyelaman log dan konfirmasi sekunder dari peristiwa keamanan.
- Estimasi tanggal mulai: Ubah bidang ini jika Anda menerima indikator untuk kasus ini yang mendahului tanggal mulai awal yang disediakan. Pertimbangkan untuk memberikan rincian tambahan sehubungan dengan indikator yang baru terdeteksi di bidang deskripsi atau menambahkan komentar di tab komunikasi.

Komunikasi

AWS Insinyur Security Incident Response dapat menambahkan komentar untuk mendokumentasikan aktivitas mereka saat mengerjakan sebuah kasus. Insinyur Respons Insiden AWS Keamanan yang berbeda dapat mengerjakan kasing pada saat yang bersamaan. Mereka direpresentasikan sebagai AWS Responder dalam log komunikasi.

Izin

Tab izin mencantumkan semua individu yang akan diberi tahu untuk setiap perubahan pada kasus ini. Anda dapat menambah dan menghapus individu dari daftar sampai kasing ditutup.

Note

Kasus individual memungkinkan Anda untuk memasukkan hingga 30 pemangku kepentingan total. Konfigurasi izin tambahan diperlukan untuk memberikan akses tingkat kasus ke pemangku kepentingan ini.

Berikan akses ke kasing di konsol

Untuk memberikan akses ke kasus di Konsol Manajemen AWS, Anda dapat menyalin templat kebijakan izin IAM dan menambahkan izin ini ke pengguna atau peran.

Menambahkan kebijakan IAM ke pengguna atau peran:

1. Salin kebijakan izin IAM.
2. Buka IAM di via <https://console.aws.amazon.com/iam/>.
3. Di panel navigasi, pilih Pengguna atau Peran.
4. Pilih pengguna atau peran untuk membuka halaman detail.
5. Di tab izin, pilih Tambahkan izin.
6. Pilih Lampirkan kebijakan.
7. Pilih [kebijakan Respons Insiden Keamanan AWS terkelola](#) yang sesuai.
8. Pilih Tambahkan kebijakan.

Lampiran

Responden insiden Anda dapat menambahkan lampiran pada kasus yang membantu responden insiden lainnya dengan penyelidikan mereka untuk kasus yang dikelola sendiri.

Note

Jika Anda memilih kasus yang AWS didukung, AWS tidak dapat melihat lampiran. Semua detail untuk kasus yang AWS didukung harus dibagikan melalui komentar kasus atau melalui Anda menyediakan screenshare menggunakan teknologi komunikasi pilihan Anda.

Pilih Unggah untuk memilih file dari komputer Anda untuk ditambahkan ke kasing.

Note

Lampiran apa pun yang diunggah akan dihapus tujuh hari setelah kasus terjadi. Closed

Tag

Tag adalah label opsional yang dapat Anda tetapkan ke kasus Anda untuk menyimpan metadata tentang sumber daya tersebut. Setiap tag adalah label yang terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tag untuk mencari, mengalokasikan biaya, dan mengautentikasi izin untuk sumber daya.

Untuk menambahkan tanda, lakukan hal berikut:

1. Pilih Tambahkan tag baru.
2. Untuk Kunci, masukkan nama tag.
3. Untuk Nilai, masukkan nilai tag.

Untuk menghapus tag, pilih opsi Hapus untuk tag itu.

Kegiatan kasus

Jejak audit memberikan catatan kronologis terperinci dari semua kegiatan kasus. Mereka memberikan informasi penting dalam kegiatan pasca-acara dan membantu mengidentifikasi potensi perbaikan. Waktu, pengguna, tindakan, dan detail dari setiap perubahan kasus dicatat dalam jejak audit kasus.

Menutup kasus

Untuk kasus yang AWS didukung, pilih Tutup Kasus pada halaman detail kasus untuk menutup kasus secara permanen pada status apa pun. Kasus biasanya mencapai status Siap Tutup sebelum ditutup secara permanen. Jika Anda menutup kasing sebelum waktunya pada status lain selain Siap Tutup, Anda meminta agar teknisi Respons Insiden AWS Keamanan berhenti mengerjakan kasus yang didukung ini AWS .

Jika tim respons insiden Anda adalah responden, pilih Action/Close Kasus pada halaman detail kasus.

Note

Status “Siap Tutup” menandakan bahwa suatu kasus dapat ditutup secara permanen dan tidak ada pekerjaan tambahan yang harus dilakukan pada suatu kasus.

Kasus tidak dapat dibuka kembali setelah ditutup secara permanen. Semua informasi akan tersedia hanya-baca. Untuk mencegah penutupan yang tidak disengaja, Anda akan diminta untuk mengonfirmasi bahwa Anda ingin menutup kasus ini.

Bekerja dengan CloudFormation StackSets

Untuk petunjuk khusus tentang cara membuat izin yang dikelola layanan StackSet dengan layanan, lihat [Membuat CloudFormation StackSets dengan izin yang dikelola layanan](#) di Panduan Pengguna.AWS CloudFormation

Respons Insiden Keamanan AWS menyediakan dua CloudFormation template. Kedua template membuat dua AWS Identity and Access Management peran yang sama, `AWSecurityIncidentResponseContainment` dan `AWSecurityIncidentResponseContainmentExecution`. Template `Containment with EC2 Triage` menambahkan `AWSecurityIncidentResponseInvestigationPolicy` ke `AWSecurityIncidentResponseContainment` peran, yang memberikan izin tambahan untuk EC2 Triage. Pilih template yang sesuai dengan persyaratan keamanan Anda:

- [Hanya penahanan](#): Membuat izin minimum yang diperlukan untuk tindakan penahanan.
- [Penahanan dengan Triase EC2](#): Termasuk semua izin penahanan ditambah izin tambahan untuk Triase EC2. Template ini memungkinkan Respons Insiden Keamanan AWS untuk AWS Systems Manager menjalankan Run Command pada instans Amazon Elastic Compute Cloud selama penyelidikan keamanan.

Untuk informasi lebih lanjut tentang EC2 Triage, lihat. [Mendeteksi dan Menganalisis](#)

CloudFormation templat

Template berikut membuat peran IAM yang diperlukan untuk tindakan Respons Insiden Keamanan AWS penahanan. Pilih template yang paling sesuai dengan persyaratan keamanan Anda.

Daftar Isi

- [Hanya penahanan](#)
- [Penahanan dengan Triase EC2](#)

Hanya penahanan

Template ini membuat peran minimum yang diperlukan untuk tindakan penahanan. Gunakan template ini jika Anda tidak memerlukan fungsionalitas EC2 Triage.

```

AWSTemplateFormatVersion: '2010-09-09'
Description: 'Template for production SIR containment roles'

Resources:
  AWSSecurityIncidentResponseContainment:
    Type: 'AWS::IAM::Role'
    Properties:
      RoleName: AWSSecurityIncidentResponseContainment
      AssumeRolePolicyDocument:
        {
          'Version': '2012-10-17',
          'Statement':
            [
              {
                'Effect': 'Allow',
                'Principal': { 'Service': 'containment.security-ir.amazonaws.com' },
                'Action': 'sts:AssumeRole',
                'Condition': { 'StringEquals': { 'sts:ExternalId': !Sub
'${AWS::AccountId}' } } },
              {
                'Effect': 'Allow',
                'Principal': { 'Service': 'containment.security-ir.amazonaws.com' },
                'Action': 'sts:TagSession',
              },
            ],
        }
    Policies:
      - PolicyName: AWSSecurityIncidentResponseContainmentPolicy
        PolicyDocument:
          {
            'Version': '2012-10-17',
            'Statement':
              [
                {
                  'Effect': 'Allow',
                  'Action': ['ssm:StartAutomationExecution'],
                  'Resource':
                    [

```

```

        !Sub 'arn:${AWS::Partition}:ssm:*::document/AWSSupport-
ContainEC2Instance',
        !Sub 'arn:${AWS::Partition}:ssm:*::document/AWSSupport-
ContainS3Resource',
        !Sub 'arn:${AWS::Partition}:ssm:*::document/AWSSupport-
ContainIAMPrincipal',
        !Sub 'arn:${AWS::Partition}:ssm:*:${AWS::AccountId}:automation-
execution/*',
    ],
  },
  {
    'Effect': 'Allow',
    'Action':
      ['ssm:DescribeInstanceInformation', 'ssm:GetAutomationExecution',
'ssm:ListCommandInvocations'],
    'Resource': '*',
  },
  {
    'Effect': 'Allow',
    'Action': ['iam:PassRole'],
    'Resource': !GetAtt
AWSSecurityIncidentResponseContainmentExecution.Arn,
    'Condition': { 'StringEquals': { 'iam:PassedToService':
'ssm.amazonaws.com' } } },
  },
],
}

AWSSecurityIncidentResponseContainmentExecution:
  Type: 'AWS::IAM::Role'
  Properties:
    RoleName: AWSSecurityIncidentResponseContainmentExecution
    AssumeRolePolicyDocument:
      {
        'Version': '2012-10-17',
        'Statement':
          [{ 'Effect': 'Allow', 'Principal': { 'Service': 'ssm.amazonaws.com' } },
'Action': 'sts:AssumeRole' ]],
      }
    ManagedPolicyArns:
      - !Sub arn:${AWS::Partition}:iam::aws:policy/SecurityAudit
    Policies:
      - PolicyName: AWSSecurityIncidentResponseContainmentExecutionPolicy
        PolicyDocument:
          {

```

```
'Version': '2012-10-17',
'Statement':
[
  {
    'Sid': 'AllowIAMContainment',
    'Effect': 'Allow',
    'Action':
      [
        'iam:AttachRolePolicy',
        'iam:AttachUserPolicy',
        'iam:DeactivateMFADevice',
        'iam>DeleteLoginProfile',
        'iam>DeleteRolePolicy',
        'iam>DeleteUserPolicy',
        'iam:GetLoginProfile',
        'iam:GetPolicy',
        'iam:GetRole',
        'iam:GetRolePolicy',
        'iam:GetUser',
        'iam:GetUserPolicy',
        'iam:ListAccessKeys',
        'iam:ListAttachedRolePolicies',
        'iam:ListAttachedUserPolicies',
        'iam:ListMfaDevices',
        'iam:ListPolicies',
        'iam:ListRolePolicies',
        'iam:ListUserPolicies',
        'iam:ListVirtualMFADevices',
        'iam:PutRolePolicy',
        'iam:PutUserPolicy',
        'iam:TagMFADevice',
        'iam:TagPolicy',
        'iam:TagRole',
        'iam:TagUser',
        'iam:UntagMFADevice',
        'iam:UntagPolicy',
        'iam:UntagRole',
        'iam:UntagUser',
        'iam:UpdateAccessKey',
        'identitystore:CreateGroupMembership',
        'identitystore>DeleteGroupMembership',
        'identitystore:IsMemberInGroups',
        'identitystore:ListUsers',
        'identitystore:ListGroups',
```

```
        'identitystore:ListGroupMemberships',
      ],
      'Resource': '*',
    },
    {
      'Sid': 'AllowOrgListAccounts',
      'Effect': 'Allow',
      'Action': 'organizations:ListAccounts',
      'Resource': '*',
    },
    {
      'Sid': 'AllowSSOContainment',
      'Effect': 'Allow',
      'Action':
        [
          'sso:CreateAccountAssignment',
          'sso:DeleteAccountAssignment',
          'sso:DeleteInlinePolicyFromPermissionSet',
          'sso:GetInlinePolicyForPermissionSet',
          'sso:ListAccountAssignments',
          'sso:ListInstances',
          'sso:ListPermissionSets',
          'sso:ListPermissionSetsProvisionedToAccount',
          'sso:PutInlinePolicyToPermissionSet',
          'sso:TagResource',
          'sso:UntagResource',
        ],
      'Resource': '*',
    },
    {
      'Sid': 'AllowSSORead',
      'Effect': 'Allow',
      'Action': ['sso-directory:SearchUsers', 'sso-
directory:DescribeUser'],
      'Resource': '*',
    },
    {
      'Sid': 'AllowS3Read',
      'Effect': 'Allow',
      'Action':
        [
          's3:GetAccountPublicAccessBlock',
          's3:GetBucketAcl',
          's3:GetBucketLocation',
```

```
        's3:GetBucketOwnershipControls',
        's3:GetBucketPolicy',
        's3:GetBucketPolicyStatus',
        's3:GetBucketPublicAccessBlock',
        's3:GetBucketTagging',
        's3:GetEncryptionConfiguration',
        's3:GetObject',
        's3:GetObjectAcl',
        's3:GetObjectTagging',
        's3:GetReplicationConfiguration',
        's3:ListBucket',
        's3express:GetBucketPolicy',
    ],
    'Resource': '*',
},
{
    'Sid': 'AllowS3Write',
    'Effect': 'Allow',
    'Action':
    [
        's3:CreateBucket',
        's3>DeleteBucketPolicy',
        's3>DeleteObjectTagging',
        's3:PutAccountPublicAccessBlock',
        's3:PutBucketACL',
        's3:PutBucketOwnershipControls',
        's3:PutBucketPolicy',
        's3:PutBucketPublicAccessBlock',
        's3:PutBucketTagging',
        's3:PutBucketVersioning',
        's3:PutObject',
        's3:PutObjectAcl',
        's3express:CreateSession',
        's3express>DeleteBucketPolicy',
        's3express:PutBucketPolicy',
    ],
    'Resource': '*',
},
{
    'Sid': 'AllowAutoScalingWrite',
    'Effect': 'Allow',
    'Action':
    [
        'autoscaling:CreateOrUpdateTags',
```

```
        'autoscaling:DeleteTags',
        'autoscaling:DescribeAutoScalingGroups',
        'autoscaling:DescribeAutoScalingInstances',
        'autoscaling:DescribeTags',
        'autoscaling:EnterStandby',
        'autoscaling:ExitStandby',
        'autoscaling:UpdateAutoScalingGroup',
    ],
    'Resource': '*',
},
{
    'Sid': 'AllowEC2Containment',
    'Effect': 'Allow',
    'Action':
    [
        'ec2:AuthorizeSecurityGroupEgress',
        'ec2:AuthorizeSecurityGroupIngress',
        'ec2:CopyImage',
        'ec2:CreateImage',
        'ec2:CreateSecurityGroup',
        'ec2:CreateSnapshot',
        'ec2:CreateTags',
        'ec2>DeleteSecurityGroup',
        'ec2>DeleteTags',
        'ec2:DescribeImages',
        'ec2:DescribeInstances',
        'ec2:DescribeSecurityGroups',
        'ec2:DescribeSnapshots',
        'ec2:DescribeTags',
        'ec2:ModifyNetworkInterfaceAttribute',
        'ec2:RevokeSecurityGroupEgress',
    ],
    'Resource': '*',
},
{
    'Sid': 'AllowKMSActions',
    'Effect': 'Allow',
    'Action':
    [
        'kms:CreateGrant',
        'kms:DescribeKey',
        'kms:GenerateDataKeyWithoutPlaintext',
        'kms:ReEncryptFrom',
        'kms:ReEncryptTo',
```

```

        ],
        'Resource': '*',
    },
    {
        'Sid': 'AllowSSMActions',
        'Effect': 'Allow',
        'Action': ['ssm:DescribeAutomationExecutions'],
        'Resource': '*',
    },
],
}

```

Penahanan dengan Triase EC2

Template ini membuat peran penahanan dengan izin tambahan untuk fungsionalitas EC2 Triage. Gunakan template ini jika Anda Respons Insiden Keamanan AWS perlu menjalankan Systems Manager Run Command di instans Amazon EC2 selama penyelidikan keamanan.

```

AWSTemplateFormatVersion: '2010-09-09'
Description: 'Template for AWS Security Incident Response containment roles'

Resources:
  AWSSecurityIncidentResponseContainment:
    Type: 'AWS::IAM::Role'
    Properties:
      RoleName: AWSSecurityIncidentResponseContainment
      AssumeRolePolicyDocument:
        {
          'Version': '2012-10-17',
          'Statement':
            [
              {
                'Effect': 'Allow',
                'Principal': { 'Service': 'containment.security-ir.amazonaws.com' },
                'Action': 'sts:AssumeRole',
                'Condition': { 'StringEquals': { 'sts:ExternalId': !Sub
'${AWS::AccountId}' } } },
            ],
          {
            'Effect': 'Allow',
            'Principal': { 'Service': 'containment.security-ir.amazonaws.com' },
            'Action': 'sts:TagSession',

```

```

    },
  ],
}
Policies:
- PolicyName: AWSSecurityIncidentResponseContainmentPolicy
  PolicyDocument:
  {
    'Version': '2012-10-17',
    'Statement':
    [
      {
        'Effect': 'Allow',
        'Action': ['ssm:StartAutomationExecution'],
        'Resource':
        [
          !Sub 'arn:${AWS::Partition}:ssm:*::document/AWSSupport-
ContainEC2Instance',
          !Sub 'arn:${AWS::Partition}:ssm:*::document/AWSSupport-
ContainS3Resource',
          !Sub 'arn:${AWS::Partition}:ssm:*::document/AWSSupport-
ContainIAMPrincipal',
          !Sub 'arn:${AWS::Partition}:ssm:*:${AWS::AccountId}:automation-
execution/*',
        ],
      },
      {
        'Effect': 'Allow',
        'Action':
        ['ssm:DescribeInstanceInformation', 'ssm:GetAutomationExecution',
'ssm:ListCommandInvocations'],
        'Resource': '*',
      },
      {
        'Effect': 'Allow',
        'Action': ['iam:PassRole'],
        'Resource': !GetAtt
AWSSecurityIncidentResponseContainmentExecution.Arn,
        'Condition': { 'StringEquals': { 'iam:PassedToService':
'ssm.amazonaws.com' } } },
    ],
  }
- PolicyName: AWSSecurityIncidentResponseInvestigationPolicy
  PolicyDocument:

```

```

    {
      'Version': '2012-10-17',
      'Statement':
        [
          {
            'Effect': 'Allow',
            'Action': [
              'ec2:DescribeInstanceStatus',
              'ec2:DescribeInstances',
              'ec2:DescribeRouteTables',
              'ec2:DescribeSecurityGroupRules',
              'iam:GetInstanceProfile',
              'ssm:DescribeInstanceInformation',
              'ssm:GetCommandInvocation'
            ],
            'Resource': '*'
          },
          {
            'Effect': 'Allow',
            'Action': [
              'ssm:SendCommand'
            ],
            'Resource': '*'
          }
        ]
    }

```

AWSecurityIncidentResponseContainmentExecution:

Type: 'AWS::IAM::Role'

Properties:

RoleName: AWSecurityIncidentResponseContainmentExecution

AssumeRolePolicyDocument:

```

{
  'Version': '2012-10-17',
  'Statement':
    [{ 'Effect': 'Allow', 'Principal': { 'Service': 'ssm.amazonaws.com' } },
  'Action': 'sts:AssumeRole' ]],
}

```

ManagedPolicyArns:

- !Sub arn:\${AWS::Partition}:iam::aws:policy/SecurityAudit

Policies:

- PolicyName: AWSecurityIncidentResponseContainmentExecutionPolicy

PolicyDocument:

```

{
  'Version': '2012-10-17',

```

```
'Statement':  
  [  
    {  
      'Sid': 'AllowIAMContainment',  
      'Effect': 'Allow',  
      'Action':  
        [  
          'iam:AttachRolePolicy',  
          'iam:AttachUserPolicy',  
          'iam:DeactivateMFADevice',  
          'iam>DeleteLoginProfile',  
          'iam>DeleteRolePolicy',  
          'iam>DeleteUserPolicy',  
          'iam:GetLoginProfile',  
          'iam:GetPolicy',  
          'iam:GetRole',  
          'iam:GetRolePolicy',  
          'iam:GetUser',  
          'iam:GetUserPolicy',  
          'iam>ListAccessKeys',  
          'iam>ListAttachedRolePolicies',  
          'iam>ListAttachedUserPolicies',  
          'iam>ListMfaDevices',  
          'iam>ListPolicies',  
          'iam>ListRolePolicies',  
          'iam>ListUserPolicies',  
          'iam>ListVirtualMFADevices',  
          'iam:PutRolePolicy',  
          'iam:PutUserPolicy',  
          'iam:TagMFADevice',  
          'iam:TagPolicy',  
          'iam:TagRole',  
          'iam:TagUser',  
          'iam:UntagMFADevice',  
          'iam:UntagPolicy',  
          'iam:UntagRole',  
          'iam:UntagUser',  
          'iam:UpdateAccessKey',  
          'identitystore>CreateGroupMembership',  
          'identitystore>DeleteGroupMembership',  
          'identitystore:IsMemberInGroups',  
          'identitystore>ListUsers',  
          'identitystore>ListGroups',  
          'identitystore>ListGroupMemberships',
```

```
    ],
    'Resource': '*',
  },
  {
    'Sid': 'AllowOrgListAccounts',
    'Effect': 'Allow',
    'Action': 'organizations:ListAccounts',
    'Resource': '*',
  },
  {
    'Sid': 'AllowSSOContainment',
    'Effect': 'Allow',
    'Action':
      [
        'sso:CreateAccountAssignment',
        'sso:DeleteAccountAssignment',
        'sso:DeleteInlinePolicyFromPermissionSet',
        'sso:GetInlinePolicyForPermissionSet',
        'sso:ListAccountAssignments',
        'sso:ListInstances',
        'sso:ListPermissionSets',
        'sso:ListPermissionSetsProvisionedToAccount',
        'sso:PutInlinePolicyToPermissionSet',
        'sso:TagResource',
        'sso:UntagResource',
      ],
    'Resource': '*',
  },
  {
    'Sid': 'AllowSSORead',
    'Effect': 'Allow',
    'Action': ['sso-directory:SearchUsers', 'sso-
directory:DescribeUser'],
    'Resource': '*',
  },
  {
    'Sid': 'AllowS3Read',
    'Effect': 'Allow',
    'Action':
      [
        's3:GetAccountPublicAccessBlock',
        's3:GetBucketAcl',
        's3:GetBucketLocation',
        's3:GetBucketOwnershipControls',
```

```
        's3:GetBucketPolicy',
        's3:GetBucketPolicyStatus',
        's3:GetBucketPublicAccessBlock',
        's3:GetBucketTagging',
        's3:GetEncryptionConfiguration',
        's3:GetObject',
        's3:GetObjectAcl',
        's3:GetObjectTagging',
        's3:GetReplicationConfiguration',
        's3:ListBucket',
        's3express:GetBucketPolicy',
    ],
    'Resource': '*',
},
{
    'Sid': 'AllowS3Write',
    'Effect': 'Allow',
    'Action':
        [
            's3:CreateBucket',
            's3>DeleteBucketPolicy',
            's3>DeleteObjectTagging',
            's3:PutAccountPublicAccessBlock',
            's3:PutBucketACL',
            's3:PutBucketOwnershipControls',
            's3:PutBucketPolicy',
            's3:PutBucketPublicAccessBlock',
            's3:PutBucketTagging',
            's3:PutBucketVersioning',
            's3:PutObject',
            's3:PutObjectAcl',
            's3express:CreateSession',
            's3express>DeleteBucketPolicy',
            's3express:PutBucketPolicy',
        ],
    'Resource': '*',
},
{
    'Sid': 'AllowAutoScalingWrite',
    'Effect': 'Allow',
    'Action':
        [
            'autoscaling:CreateOrUpdateTags',
            'autoscaling>DeleteTags',
```

```
        'autoscaling:DescribeAutoScalingGroups',
        'autoscaling:DescribeAutoScalingInstances',
        'autoscaling:DescribeTags',
        'autoscaling:EnterStandby',
        'autoscaling:ExitStandby',
        'autoscaling:UpdateAutoScalingGroup',
    ],
    'Resource': '*',
},
{
    'Sid': 'AllowEC2Containment',
    'Effect': 'Allow',
    'Action':
    [
        'ec2:AuthorizeSecurityGroupEgress',
        'ec2:AuthorizeSecurityGroupIngress',
        'ec2:CopyImage',
        'ec2:CreateImage',
        'ec2:CreateSecurityGroup',
        'ec2:CreateSnapshot',
        'ec2:CreateTags',
        'ec2>DeleteSecurityGroup',
        'ec2>DeleteTags',
        'ec2:DescribeImages',
        'ec2:DescribeInstances',
        'ec2:DescribeSecurityGroups',
        'ec2:DescribeSnapshots',
        'ec2:DescribeTags',
        'ec2:ModifyNetworkInterfaceAttribute',
        'ec2:RevokeSecurityGroupEgress',
    ],
    'Resource': '*',
},
{
    'Sid': 'AllowKMSActions',
    'Effect': 'Allow',
    'Action':
    [
        'kms:CreateGrant',
        'kms:DescribeKey',
        'kms:GenerateDataKeyWithoutPlaintext',
        'kms:ReEncryptFrom',
        'kms:ReEncryptTo',
    ],
}
```

```
        'Resource': '*',
    },
    {
        'Sid': 'AllowSSMActions',
        'Effect': 'Allow',
        'Action': ['ssm:DescribeAutomationExecutions'],
        'Resource': '*',
    },
],
}
```

Batalkan Keanggotaan

Peran yang memiliki CancelMembership izin Respons Insiden Keamanan AWS dapat membatalkan keanggotaan dari konsol, API, atau AWS Command Line Interface.

Important

Setelah membatalkan keanggotaan, Anda tidak dapat melihat data kasus historis. Ketika Anda membatalkan keanggotaan, keanggotaan Anda segera dihapus dan Anda tidak akan memiliki akses lebih lanjut ke kasus pada keanggotaan. Sumber daya atau investigasi apa pun yang ready to close sedang Active atau dihentikan setelah pembatalan keanggotaan.


Saat Anda membatalkan keanggotaan:

Keanggotaan Anda dihapus dan Anda tidak akan mengakses lebih lanjut ke kasus pada keanggotaan.

Important

Jika Anda berlangganan kembali ke layanan, keanggotaan baru dibuat dan sumber daya kasus yang hidup di bawah keanggotaan sebelumnya hanya dapat diakses jika Anda mengunduhnya sebelum pembatalan.

Setelah keanggotaan dibatalkan, semua orang di tim respons insiden keanggotaan diberitahu melalui email.

 **Important**

Jika Anda membuat keanggotaan menggunakan akun administrator yang didelegasikan dan Anda menggunakan AWS Organizations API untuk menghapus penunjukan administrator yang didelegasikan dari akun, keanggotaan akan segera dihentikan.

Sumber daya penandaan Respons Insiden Keamanan AWS

Tag adalah label metadata yang Anda tetapkan atau yang ditetapkan ke sumber AWS daya. AWS Setiap tanda terdiri dari kunci dan nilai. Untuk tanda yang Anda tetapkan, Anda menentukan kunci dan nilai. Misalnya, Anda dapat menentukan kunci sebagai stage dan nilai untuk satu sumber daya sebagai test.

Tanda membantu Anda melakukan hal berikut:

- Identifikasi dan atur AWS sumber daya Anda. Banyak penandaan Layanan AWS dukungan, sehingga Anda dapat menetapkan tag yang sama ke sumber daya dari layanan yang berbeda untuk menunjukkan bahwa sumber daya terkait.
- Lacak AWS biaya Anda. Anda mengaktifkan tag ini di AWS Billing dasbor. AWS menggunakan tag untuk mengkategorikan biaya Anda dan mengirimkan laporan alokasi biaya bulanan kepada Anda. Untuk informasi selengkapnya, lihat [Menggunakan tag alokasi biaya](#) di [Panduan Pengguna AWS Penagihan](#).
- Kontrol akses ke AWS sumber daya Anda. Untuk informasi selengkapnya, lihat [Mengontrol akses menggunakan tag](#) di [Panduan Pengguna IAM](#).

Lihat [referensi Respons Insiden Keamanan AWS API untuk penandaan](#).

Menggunakan AWS CloudShell untuk bekerja dengan AWS Security Incident Response

AWS CloudShell adalah shell pra-otentikasi berbasis browser yang dapat Anda luncurkan langsung dari file. Konsol Manajemen AWS Anda dapat menjalankan AWS CLI perintah terhadap AWS layanan (termasuk AWS Security Incident Response) menggunakan shell pilihan Anda (Bash, PowerShell atau Z shell). Anda juga dapat melakukan ini tanpa perlu mengunduh atau menginstal alat baris perintah.

Anda [meluncurkan AWS CloudShell dari Konsol Manajemen AWS](#), dan AWS kredensial yang Anda gunakan untuk masuk ke konsol secara otomatis tersedia di sesi shell baru. Pra-otentikasi AWS CloudShell pengguna ini memungkinkan Anda untuk melewati konfigurasi kredensial saat berinteraksi dengan AWS layanan seperti Security Incident Response menggunakan AWS CLI versi 2 (pra-instal pada lingkungan komputasi shell).

Daftar Isi

- [Memperoleh izin IAM untuk AWS CloudShell](#)
- [Berinteraksi dengan Respons Insiden Keamanan menggunakan AWS CloudShell](#)

Memperoleh izin IAM untuk AWS CloudShell


Dengan menggunakan sumber daya manajemen akses yang disediakan oleh AWS Identity and Access Management, administrator dapat memberikan izin kepada pengguna IAM sehingga mereka dapat mengakses AWS CloudShell dan menggunakan fitur lingkungan.

Cara tercepat bagi administrator untuk memberikan akses ke pengguna adalah melalui kebijakan AWS terkelola. [Kebijakan AWS terkelola](#) adalah kebijakan mandiri yang dibuat dan dikelola oleh AWS. Kebijakan AWS terkelola berikut ini CloudShell dapat dilampirkan ke identitas IAM:

- `AWSCloudShellFullAccess`: Memberikan izin untuk menggunakan AWS CloudShell dengan akses penuh ke semua fitur.

Jika ingin membatasi cakupan tindakan yang dapat dilakukan oleh pengguna IAM AWS CloudShell, Anda dapat membuat kebijakan kustom yang menggunakan kebijakan `AWSCloudShellFullAccess` terkelola sebagai templat. Untuk informasi selengkapnya tentang


membatasi tindakan yang tersedia bagi pengguna CloudShell, lihat [Mengelola AWS CloudShell akses dan penggunaan dengan kebijakan IAM](#) di Panduan AWS CloudShell Pengguna.

 Note

Identitas IAM Anda juga memerlukan kebijakan yang memberikan izin untuk melakukan panggilan ke Security Incident Response.

Berinteraksi dengan Respons Insiden Keamanan menggunakan AWS CloudShell

Setelah Anda meluncurkan AWS CloudShell dari Konsol Manajemen AWS, Anda dapat segera mulai berinteraksi dengan Security Incident Response menggunakan antarmuka baris perintah.

 Note

Saat menggunakan AWS Command Line Interface in AWS CloudShell, Anda tidak perlu mengunduh atau menginstal sumber daya tambahan apa pun. Selain itu, karena Anda sudah diautentikasi di dalam shell, Anda tidak perlu mengonfigurasi kredensial sebelum melakukan panggilan.

Bekerja dengan AWS CloudShell dan Respon Insiden Keamanan

1. Dari Konsol Manajemen AWS, luncurkan CloudShell dengan memilih opsi berikut yang tersedia di bilah navigasi:
 - Pilih CloudShell ikonnya.
 - Mulai mengetik “cloudshell” di kotak Pencarian dan kemudian pilih opsi. CloudShell
2. Gunakan standar AWS Command Line Interface untuk berinteraksi dengan AWS Security Incident Response. Untuk referensi lengkap dari perintah CLI yang tersedia, lihat [Referensi Perintah untuk AWS CLI Respons Insiden AWS Keamanan](#).

Pencatatan panggilan API Respons Insiden AWS Keamanan menggunakan AWS CloudTrail

AWS Security Incident Response terintegrasi dengan AWS CloudTrail, layanan yang menyediakan catatan tindakan yang diambil oleh pengguna, peran, atau AWS layanan dalam Security Incident Response. CloudTrail menangkap semua panggilan API untuk Security Incident Response sebagai peristiwa. Panggilan yang diambil termasuk panggilan dari konsol Security Incident Response dan panggilan kode ke operasi Security Incident Response API. Jika Anda membuat jejak, Anda dapat mengaktifkan pengiriman CloudTrail peristiwa secara terus menerus ke bucket Amazon S3, termasuk peristiwa untuk Respons Insiden Keamanan. Jika Anda tidak mengonfigurasi jejak, Anda masih dapat melihat peristiwa terbaru di CloudTrail konsol dalam Riwayat acara. Dengan menggunakan informasi yang dikumpulkan oleh CloudTrail, Anda dapat menentukan permintaan yang dibuat untuk Respons Insiden Keamanan, alamat IP dari mana permintaan dibuat, siapa yang membuat permintaan, kapan dibuat, dan detail tambahan.

Untuk mempelajari selengkapnya CloudTrail, lihat [Panduan AWS CloudTrail Pengguna](#).

Informasi Respons Insiden Keamanan di CloudTrail

CloudTrail diaktifkan pada Akun AWS saat Anda membuat akun. Ketika aktivitas terjadi di Security Incident Response, aktivitas tersebut dicatat dalam suatu CloudTrail peristiwa bersama dengan peristiwa AWS layanan lainnya dalam riwayat Peristiwa. Anda dapat melihat, mencari, dan mengunduh acara terbaru di situs Anda Akun AWS. Untuk informasi selengkapnya, lihat [Melihat peristiwa dengan Riwayat CloudTrail acara](#).

Untuk catatan acara yang sedang berlangsung dalam 90 hari Akun AWS terakhir Anda, buat jejak atau penyimpanan data acara [CloudTrailDanau](#).

CloudTrail jalan setapak

Jejak memungkinkan CloudTrail untuk mengirimkan file log ke bucket Amazon S3. Semua jalur yang dibuat menggunakan Konsol Manajemen AWS Multi-region. Anda dapat membuat jalur Single-region atau Multi-region dengan menggunakan `aws`. AWS CLI Membuat jejak Multi-wilayah disarankan karena Anda menangkap aktivitas Wilayah AWS di semua akun Anda. Jika Anda membuat jejak wilayah Tunggal, Anda hanya dapat melihat peristiwa yang dicatat di jejak.

Wilayah AWS Untuk informasi selengkapnya tentang jejak, lihat [Membuat jejak untuk Anda Akun AWS](#) dan [Membuat jejak untuk organisasi](#) di Panduan AWS CloudTrail Pengguna.

Anda dapat mengirimkan satu salinan acara manajemen yang sedang berlangsung ke bucket Amazon S3 Anda tanpa biaya CloudTrail dengan membuat jejak, namun, ada biaya penyimpanan Amazon S3. Untuk informasi selengkapnya tentang CloudTrail harga, lihat [AWS CloudTrail Harga](#). Untuk informasi tentang harga Amazon S3, lihat [Harga Amazon S3](#).

CloudTrail Menyimpan data acara danau

CloudTrail Lake memungkinkan Anda menjalankan kueri berbasis SQL pada acara Anda. CloudTrail [Lake mengonversi peristiwa yang ada dalam format JSON berbasis baris ke format Apache ORC](#). ORC adalah format penyimpanan kolomar yang dioptimalkan untuk pengambilan data dengan cepat. Peristiwa digabungkan ke dalam penyimpanan data peristiwa, yang merupakan kumpulan peristiwa yang tidak dapat diubah berdasarkan kriteria yang Anda pilih dengan menerapkan pemilih acara [tingkat lanjut](#). Penyeleksi yang Anda terapkan ke penyimpanan data acara mengontrol peristiwa mana yang bertahan dan tersedia untuk Anda kueri. Untuk informasi lebih lanjut tentang CloudTrail Danau, lihat [Bekerja dengan AWS CloudTrail Danau](#) di Panduan AWS CloudTrail Pengguna.

CloudTrail Penyimpanan data acara danau dan kueri menimbulkan biaya. Saat Anda membuat penyimpanan data acara, Anda memilih [opsi harga](#) yang ingin Anda gunakan untuk penyimpanan data acara. Opsi penetapan harga menentukan biaya untuk menelan dan menyimpan peristiwa, dan periode retensi default dan maksimum untuk penyimpanan data acara. Untuk informasi selengkapnya tentang CloudTrail harga, lihat [AWS CloudTrail Harga](#).

Semua tindakan Respons Insiden Keamanan dicatat oleh CloudTrail dan didokumentasikan dalam [Referensi API Respons Insiden AWS Keamanan](#). Misalnya, panggilan keCreateMembership, CreateCase dan UpdateCase tindakan menghasilkan entri dalam file CloudTrail log.

Setiap entri peristiwa atau log berisi informasi tentang entitas yang membuat permintaan tersebut. Informasi identitas membantu Anda menentukan hal berikut ini:

- Apakah permintaan itu dibuat dengan kredensial pengguna root atau AWS Identity and Access Management (IAM).
- Apakah permintaan tersebut dibuat dengan kredensial keamanan sementara untuk satu peran atau pengguna gabungan.
- Apakah permintaan itu dibuat oleh AWS layanan lain.

Untuk informasi selengkapnya, lihat [Elemen userIdentity CloudTrail](#) .

Memahami entri file log Respons Insiden Keamanan

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, sehingga file tersebut tidak muncul dalam urutan tertentu.

Contoh berikut menunjukkan entri CloudTrail log yang menunjukkan CreateCase tindakan.

```
{
  "eventVersion": "1.09",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROAA000000000000000000000000:user",
    "arn": "arn:aws:sts::123412341234:assumed-role/Admin/user",
    "accountId": "123412341234",
    "accessKeyId": "*****",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROAA000000000000000000000000",
        "arn": "arn:aws:iam::123412341234:role/Admin",
        "accountId": "123412341234",
        "userName": "Admin"
      },
      "attributes": {
        "creationDate": "2024-10-13T06:32:53Z",
        "mfaAuthenticated": "false"
      }
    }
  },
  "eventTime": "2024-10-13T06:40:45Z",
  "eventSource": "security-ir.amazonaws.com",
  "eventName": "CreateCase",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "1.2.3.4",
  "userAgent": "aws-cli/2.17.23 md/awscrt#0.20.11 ua/2.0 os/macos#23.6.0 md/arch#x86_64 lang/python#3.11.9 md/pyimpl#CPython cfg/retry-mode#standard md/installer#exe md/prompt#off md/command#security-ir.create-case",
  "requestParameters": {
    "impactedServices": [
```

```

        "Amazon GuardDuty"
    ],
    "impactedAccounts": [],
    "clientToken": "testToken112345679",
    "resolverType": "Self",
    "description": "****",
    "engagementType": "Investigation",
    "watchers": [
        {
            "email": "****",
            "name": "****",
            "jobTitle": "****"
        }
    ],
    "membershipId": "m-r1abcdabcd",
    "title": "****",
    "impactedAwsRegions": [
        {
            "region": "ap-southeast-1"
        }
    ],
    "reportedIncidentStartDate": 1711553521,
    "threatActorIpAddresses": [
        {
            "ipAddress": "****",
            "userAgent": "browser"
        }
    ]
},
"responseElements": {
    "caseId": "0000000001"
},
"requestID": "2db4b08d-94a9-457a-9474-5892e6c8191f",
"eventID": "b3fa3990-db82-43be-b120-c81262cc2f19",
"readOnly": false,
"resources": [
    {
        "accountId": "123412341234",
        "type": "AWS::SecurityResponder::Case",
        "ARN": "arn:aws:security-ir:us-east-1:123412341234:case/*"
    }
],
"eventType": "AwsApiCall",
"managementEvent": true,

```

```
"recipientAccountId": "123412341234",  
"eventCategory": "Management"  
}
```

Mengelola Respons Insiden Keamanan AWS akun dengan AWS Organizations

Respons Insiden Keamanan AWS terintegrasi dengan AWS Organizations. Akun AWS Organizations manajemen untuk organisasi dapat menunjuk akun sebagai administrator yang didelegasikan untuk. Respons Insiden Keamanan AWS Tindakan ini memungkinkan Respons Insiden Keamanan AWS sebagai layanan terpercaya di AWS Organizations. Untuk informasi tentang cara izin ini diberikan, lihat [Menggunakan AWS Organizations dengan AWS layanan lain](#).

Bagian berikut akan memandu Anda melalui berbagai tugas yang dapat Anda lakukan sebagai akun administrator Respons Insiden Keamanan yang didelegasikan.

Daftar Isi

- [Pertimbangan dan rekomendasi untuk menggunakan Respons Insiden Keamanan AWS dengan AWS Organizations](#)
- [Mengaktifkan akses terpercaya untuk AWS Account Management](#)
- [Izin yang diperlukan untuk menunjuk akun administrator Respons Insiden Keamanan yang didelegasikan](#)
- [Mengelola keanggotaan dengan unit organisasi \(OU\) untuk Respons Insiden Keamanan AWS](#)
- [Menambahkan anggota ke Respons Insiden Keamanan AWS](#)
- [Menghapus anggota dari Respons Insiden Keamanan AWS](#)

Pertimbangan dan rekomendasi untuk menggunakan Respons Insiden Keamanan AWS dengan AWS Organizations

Pertimbangan dan rekomendasi berikut dapat membantu Anda memahami cara akun administrator Respons Insiden Keamanan yang didelegasikan beroperasi di: Respons Insiden Keamanan AWS

Akun administrator yang didelegasikan untuk Respons Insiden Keamanan AWS.

Anda dapat menetapkan satu akun anggota sebagai akun administrator Respons Insiden Keamanan yang didelegasikan. Misalnya, jika Anda menunjuk akun **111122223333** anggota **Europe (Ireland)**, Anda tidak dapat menunjuk akun **555555555555** anggota lain. **Canada (Central)** Anda harus menggunakan akun yang sama dengan akun administrator Respons Insiden Keamanan yang didelegasikan di semua Wilayah lainnya.

Anda menyiapkan akun administrator Respons Insiden Keamanan yang didelegasikan secara spesifik Wilayah AWS.

Anda menetapkan akun administrator Security Incident Response yang didelegasikan dalam satu akun Wilayah AWS selama penyiapan awal. Meskipun pengaturannya bersifat regional, Respons Insiden Keamanan AWS menyediakan cakupan seluruh organisasi di semua yang didukung. Wilayah AWS Temuan keamanan dari Amazon GuardDuty dan AWS Security Hub CSPM dicerna dari semua yang didukung Wilayah AWS, dan kasus dikelola secara terpusat di Wilayah tempat Anda mengaktifkan langganan. Akun administrator Security Incident Response dan akun anggota yang didelegasikan harus ditambahkan. AWS Organizations

Tidak disarankan untuk menetapkan akun manajemen organisasi Anda sebagai akun administrator Respons Insiden Keamanan yang didelegasikan.

Akun manajemen organisasi Anda dapat berupa akun administrator Respons Insiden Keamanan yang didelegasikan. Namun, praktik terbaik AWS keamanan mengikuti prinsip hak istimewa paling sedikit dan tidak merekomendasikan konfigurasi ini.

Menghapus akun administrator Respons Insiden Keamanan yang didelegasikan dari langganan langsung akan segera membatalkan langganan.

Jika Anda menghapus akun administrator Respons Insiden Keamanan yang didelegasikan, Respons Insiden Keamanan AWS hapus semua akun anggota yang terkait dengan akun administrator Respons Insiden Keamanan yang didelegasikan ini. Respons Insiden Keamanan AWS tidak akan lagi diaktifkan untuk semua akun anggota.

Mengaktifkan akses tepercaya untuk AWS Account Management

Mengaktifkan akses tepercaya untuk Respons Insiden Keamanan AWS memungkinkan administrator yang didelegasikan dari akun manajemen untuk memodifikasi informasi dan metadata (misalnya, detail kontak primer atau alternatif) khusus untuk setiap akun anggota di. AWS Organizations

Gunakan prosedur berikut untuk mengaktifkan akses tepercaya Respons Insiden Keamanan AWS di organisasi Anda.

Izin minimum

Untuk melakukan tugas-tugas ini, Anda harus memenuhi persyaratan berikut:

- Anda dapat melakukan ini hanya dari akun manajemen organisasi.

- Organisasi Anda harus [mengaktifkan semua fitur](#).

Console

Untuk mengaktifkan akses terpercaya untuk Respons Insiden Keamanan AWS

1. Masuklah ke [konsol AWS Organizations](#). Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna root (tidak direkomendasikan) di akun pengelolaan organisasi.
2. Pilih Layanan di panel navigasi.
3. Pilih Respons Insiden Keamanan AWS dalam daftar layanan.
4. Pilih Aktifkan akses terpercaya.
5. Di kotak Respons Insiden Keamanan AWS dialog Aktifkan akses terpercaya untuk, ketik aktifkan untuk mengonfirmasinya, lalu pilih Aktifkan akses terpercaya.

API/CLI

Untuk mengaktifkan akses terpercaya untuk AWS Account Management

Setelah menjalankan perintah berikut, Anda dapat menggunakan kredensial dari akun manajemen organisasi untuk memanggil operasi API Manajemen Akun yang menggunakan `--accountId` parameter untuk mereferensikan akun anggota dalam organisasi.

- AWS CLI: [mengaktifkan akses layanan aws](#)

Contoh berikut memungkinkan akses terpercaya untuk Respons Insiden Keamanan AWS di organisasi akun panggilan.

```
$ aws organizations enable-aws-service-access \
                                --service-principal security-
ir.amazonaws.com
```

Perintah ini tidak menghasilkan output jika berhasil.

Izin yang diperlukan untuk menunjuk akun administrator Respons Insiden Keamanan yang didelegasikan

Anda dapat memilih untuk mengatur Respons Insiden Keamanan AWS keanggotaan Anda menggunakan administrator yang didelegasikan untuk AWS Organizations. Untuk informasi tentang cara izin ini diberikan, lihat [Menggunakan AWS Organizations dengan AWS layanan lain](#).

Note

Respons Insiden Keamanan AWS secara otomatis mengaktifkan hubungan AWS Organizations tepercaya saat menggunakan konsol untuk pengaturan dan manajemen. Jika Anda menggunakan CLI/SDK maka Anda harus mengaktifkan ini secara manual dengan menggunakan [EnableAWSServiceAccess API](#) untuk `mempercayaisecurity-ir.amazonaws.com`.

Sebagai AWS Organizations manajer, sebelum Anda menetapkan akun administrator Respons Insiden Keamanan yang didelegasikan untuk organisasi Anda, verifikasi bahwa Anda dapat melakukan Respons Insiden Keamanan AWS tindakan berikut: `security-ir:CreateMembership` dan `security-ir:UpdateMembership`. Tindakan ini memungkinkan Anda untuk menunjuk akun administrator Respons Insiden Keamanan yang didelegasikan untuk organisasi Anda dengan menggunakan Respons Insiden Keamanan AWS. Anda juga harus memastikan bahwa Anda diizinkan untuk melakukan AWS Organizations tindakan yang membantu Anda mengambil informasi tentang organisasi Anda.

Untuk memberikan izin ini, sertakan pernyataan berikut dalam kebijakan AWS Identity and Access Management (IAM) untuk akun Anda:

```
{
  "Sid": "PermissionsForSIRAdmin",
  "Effect": "Allow",
  "Action": [
    "security-ir:CreateMembership",
    "security-ir:UpdateMembership",
    "organizations:EnableAWSServiceAccess",
    "organizations:RegisterDelegatedAdministrator",
    "organizations:ListDelegatedAdministrators",
    "organizations:ListAWSServiceAccessForOrganization",
```

```

        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "iam:CreateServiceLinkedRole",
        "iam:GetPolicy"
    ],
    "Resource": "*"
}

```

Jika Anda ingin menetapkan akun AWS Organizations manajemen Anda sebagai akun administrator Respons Insiden Keamanan yang didelegasikan, akun Anda juga akan memerlukan tindakan IAM: `CreateServiceLinkedRole`. Tinjau [Pertimbangan dan rekomendasi untuk menggunakan Respons Insiden Keamanan AWS dengan AWS Organizations](#) sebelum Anda melanjutkan untuk menambahkan izin.

Untuk melanjutkan penunjukan akun AWS Organizations manajemen Anda sebagai akun administrator Respons Insiden Keamanan yang didelegasikan, tambahkan pernyataan berikut ke kebijakan IAM dan ganti `111122223333` dengan Akun AWS ID akun manajemen Anda AWS Organizations :

```

{
  "Sid": "PermissionsToEnableSecurityIncidentResponse"
  "Effect": "Allow",
  "Action": [
    "iam:CreateServiceLinkedRole"
  ],
  "Resource": "arn:aws:iam::111122223333:role/aws-service-role/security-ir.amazonaws.com/AWSServiceRoleForSecurityIncidentResponse",
  "Condition": {
    "StringLike": {
      "iam:AWSServiceName": "security-ir.amazonaws.com"
    }
  }
}

```

Mengelola keanggotaan dengan unit organisasi (OU) untuk Respons Insiden Keamanan AWS

Respons Insiden Keamanan AWS mendukung cakupan keanggotaan untuk unit organisasi individu (OU). Anda dapat memperbarui keanggotaan Anda untuk mencakup OU tertentu kapan saja. Semua akun dalam OU yang dipilih, termasuk akun di bawah OU anak, akan ditanggung oleh keanggotaan Anda.

Saat memperbarui asosiasi keanggotaan Anda, pembaruan dapat diterapkan hingga 5 OU sekaligus. Jika Anda ingin membuat perubahan ke lebih dari 5 OU, selesaikan perubahan asosiasi dalam batch 5 OU hingga semua pembaruan selesai.

Console

1. Buka konsol Security Incident Response di <https://console.aws.amazon.com/security-ir/>

Untuk masuk, gunakan kredensi manajemen untuk organisasi Anda AWS Organizations .

2. Arahkan ke Kelola keanggotaan > Akun
3. Klik Perbarui asosiasi
4. Pilih Pilih unit organisasi (OU)
5. Pilih Tambahkan OU atau Hapus OU
6. Pilih hingga 5 OU yang ingin Anda perbarui. Anda tidak dapat menambahkan dan menghapus OU secara bersamaan.

Note

Semua akun dan OU anak di bawah OU yang dipilih akan dikaitkan.

7. Klik Perbarui asosiasi

8.

Note

Jika Anda ingin membuat perubahan ke lebih dari 5 OU, ulangi langkah 5 dan 6 sampai semua OU telah dikaitkan.

Untuk mempelajari lebih lanjut tentang membuat perubahan OU dalam AWS organisasi Anda, silakan lihat [Mengelola unit organisasi \(OU\) dengan AWS Organizations](#).

Menambahkan anggota ke Respons Insiden Keamanan AWS

Ada hubungan satu lawan satu dengan AWS Organizations dan Respons Insiden Keamanan AWS keanggotaan Anda. Karena akun ditambahkan (atau dihapus) dari Organizations atau unit organisasi (OU) Anda, perubahan ini akan tercermin dalam akun yang tercakup untuk Respons Insiden Keamanan AWS keanggotaan Anda.

Untuk menambahkan akun ke keanggotaan Anda, ikuti salah satu opsi untuk [Mengelola akun di organisasi dengan AWS Organizations](#).

Anda juga dapat menambahkan OU tambahan ke keanggotaan Anda kapan saja — lihat [Mengelola keanggotaan dengan unit organisasi \(OU\)](#).

Menghapus anggota dari Respons Insiden Keamanan AWS

Untuk menghapus akun dari keanggotaan Anda, Anda dapat menghapus akun anggota dari organisasi Anda, memindahkan akun dari OU pilihan Anda, atau menghapus OU dari keanggotaan Anda.

Untuk menghapus akun dari keanggotaan Anda, ikuti prosedur untuk [menghapus akun anggota dari organisasi](#).

Untuk memindahkan akun dari OU Anda, ikuti prosedur untuk [Memindahkan akun ke unit organisasi \(OU\) atau antara root dan OU dengan AWS Organizations](#).

Untuk menghapus OU dari keanggotaan Anda, ikuti prosedur untuk [Mengelola keanggotaan dengan unit organisasi \(OU\)](#).

Amazon EventBridge

Menggunakan Amazon EventBridge, Anda dapat bereaksi, memantau, dan mengatur peristiwa yang terkait dengan Respons Insiden Keamanan AWS kasus dan keanggotaan. Anda dapat merutekan peristiwa ini melalui Aturan (untuk skenario fan-out ke satu atau beberapa target) atau melalui Pipes (untuk point-to-point integrasi dengan kemampuan penyaringan, pengayaan, dan transformasi yang ditingkatkan).

Anda dapat membuat integrasi antara Security Incident Response dan tooling pihak ketiga atau data agregat untuk dianalisis menggunakan AI generatif dan perangkat lainnya. AWS Misalnya, ketika Security Incident Response secara proaktif membuat kasus, Anda dapat menggunakan EventBridge otomatisasi untuk memicu sistem untuk memberi tahu pemangku kepentingan. Selain itu, jika Anda mengelola beberapa AWS lingkungan, Anda dapat menggunakan EventBridge integrasi Amazon untuk memantau Respons Insiden Keamanan AWS keanggotaan guna memastikan semua lingkungan mempertahankan postur keamanan yang kuat.

Untuk informasi lebih lanjut, Anda dapat meninjau [Apa itu Amazon EventBridge?](#)

Note

Untuk pembaruan terbaru tentang EventBridge integrasi Amazon dengan Respons Insiden Keamanan AWS, termasuk integrasi ITSM, lihat [AWS Security Incident Response sekarang mendukung integrasi ITSM](#) di halaman AWS Apa yang Baru.

Daftar Isi

- [Mengelola peristiwa Respons Insiden Keamanan menggunakan Amazon EventBridge](#)
- [Menggunakan Respons Insiden Keamanan AWS Acara](#)
- [Tutorial: Mengirim peringatan Amazon Simple Notification Service untuk acara Membership Updated](#)

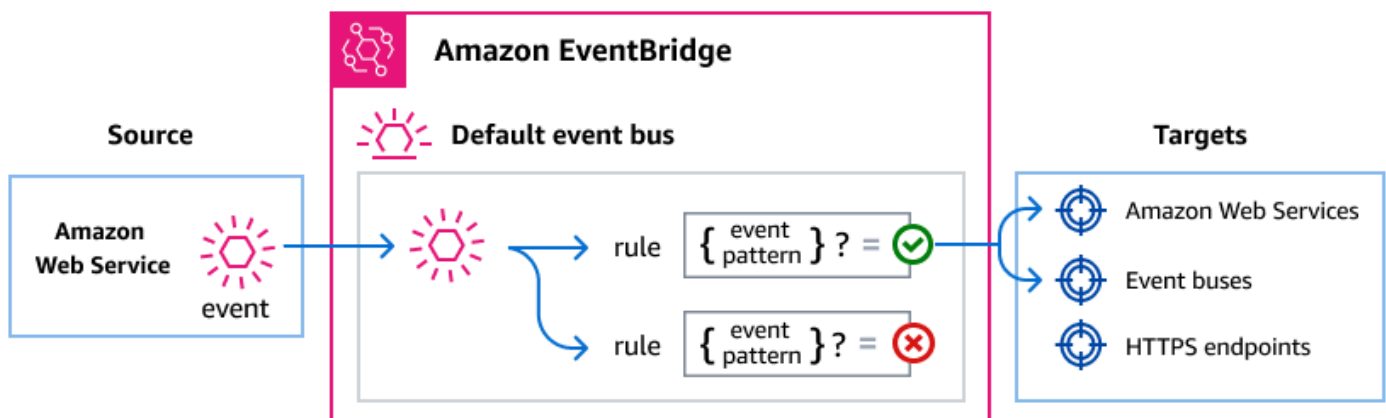
Mengelola peristiwa Respons Insiden Keamanan menggunakan Amazon EventBridge

Amazon EventBridge adalah layanan tanpa server yang menggunakan peristiwa untuk menghubungkan komponen aplikasi bersama-sama, sehingga memudahkan Anda untuk

membangun aplikasi berbasis peristiwa yang dapat diskalakan. Arsitektur berbasis peristiwa adalah gaya membangun sistem perangkat lunak yang digabungkan secara longgar yang bekerja sama dengan memancarkan dan menanggapi peristiwa. Peristiwa mewakili perubahan dalam sumber daya atau lingkungan.

Begini cara kerjanya:

Seperti banyak AWS layanan, Security Incident Response menghasilkan dan mengirim acara ke bus acara EventBridge default. (Bus acara default secara otomatis disediakan di AWS akun Anda.) Bus acara adalah router yang menerima acara dan mengirimkannya ke nol atau lebih tujuan, atau target. Aturan yang Anda tentukan untuk bus acara mengevaluasi peristiwa saat mereka tiba. Setiap aturan memeriksa apakah suatu peristiwa cocok dengan pola acara aturan. Jika acara tidak cocok, bus acara mengirimkan acara ke target yang ditentukan.



Menyampaikan peristiwa Respons Insiden Keamanan menggunakan EventBridge aturan

Agar bus acara EventBridge default mengirim peristiwa Respons Insiden Keamanan ke target, Anda harus membuat aturan. Setiap aturan berisi pola acara, yang EventBridge cocok dengan setiap acara yang diterima di bus acara. Jika data peristiwa cocok dengan pola peristiwa yang ditentukan, EventBridge mengirimkan peristiwa itu ke target aturan.

Untuk petunjuk komprehensif tentang cara membuat aturan bus acara, lihat [Membuat aturan yang bereaksi terhadap peristiwa](#) di Panduan EventBridge Pengguna Amazon.

Membuat pola acara yang cocok dengan peristiwa Security Incident Response

Setiap pola acara adalah objek JSON yang berisi:

- `source` Atribut yang mengidentifikasi layanan yang mengirim acara. Untuk peristiwa Respons Insiden Keamanan, sumbernya adalah `"aws.security-ir"`.
- (Opsional): `detail-type` Atribut yang berisi array jenis acara yang cocok.
- (Opsional): `detail` Atribut yang berisi data acara lain yang cocok.

Misalnya, pola acara berikut cocok dengan semua Case Updated by Respons Insiden Keamanan AWS Service peristiwa untuk yang ditentukan Akun AWS:

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Case Updated",
  "source": "aws.security-ir",
  "account": "111122223333",
  "time": "2023-05-12T03:45:00Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
  ],
  "detail": {
    "caseId": "1234567890",
    "updatedBy": "security-ir.amazonaws.com"
  }
}
```

Untuk informasi selengkapnya tentang penulisan pola acara, lihat [Pola acara](#) di Panduan EventBridge Pengguna.

Referensi detail peristiwa Respon Insiden Keamanan

Semua peristiwa dari AWS layanan memiliki seperangkat bidang umum yang berisi metadata tentang acara tersebut, seperti AWS layanan yang merupakan sumber acara, waktu acara dibuat, akun dan wilayah tempat acara berlangsung, dan lainnya. Untuk definisi bidang umum ini, lihat [Referensi struktur acara](#) di Panduan EventBridge Pengguna Amazon.

Selain itu, setiap acara memiliki `detail` bidang yang berisi data khusus untuk peristiwa tertentu. Referensi di bawah ini mendefinisikan bidang detail untuk berbagai peristiwa Security Incident Response.

Saat menggunakan EventBridge untuk memilih dan mengelola peristiwa Security Incident Response, penting untuk mengingat hal berikut:

- `source` Bidang untuk semua peristiwa dari Security Incident Response diatur ke `"aws.security-ir"`.
- `detail-type` Bidang menentukan jenis acara.

Misalnya, `"Case Updated"`.

- `detail` Bidang berisi data yang spesifik untuk peristiwa tertentu.

Untuk informasi tentang membuat pola peristiwa yang memungkinkan aturan agar sesuai dengan peristiwa Respons Insiden Keamanan, lihat [Pola peristiwa](#) di Panduan EventBridge Pengguna Amazon.

Untuk informasi selengkapnya tentang peristiwa dan cara EventBridge memprosesnya, lihat [EventBridge peristiwa](#) di Panduan EventBridge Pengguna Amazon.

Bidang Umum: Semua Respons Insiden Keamanan AWS acara menyertakan EventBridge bidang Amazon standar ini

- `versi`: versi format EventBridge acara
- `id`: Pengidentifikasi unik untuk acara tersebut
- `detail-type`: Deskripsi yang dapat dibaca manusia dari jenis acara
- `sumber`: Selalu `"aws.security-ir"` untuk acara Respons Insiden Keamanan
- `akun`: ID AWS akun tempat kejadian terjadi
- `waktu`: Stempel waktu ISO 8601 saat peristiwa terjadi
- `wilayah`: Wilayah AWS di mana sumber daya ada
- `sumber daya`: Array yang berisi ARN dari sumber daya yang terpengaruh

Bidang Detail: `detail` Objek berisi informasi spesifik Respons Insiden Keamanan

- `caseId`: Pengidentifikasi unik untuk kasus ini (hanya peristiwa kasus)
- `MembershipId`: Pengidentifikasi unik untuk keanggotaan (hanya acara keanggotaan)
- `UpdatedBy`: Siapa yang melakukan pembaruan (acara pembaruan kasus dan komentar saja)
- `CreatedBy`: Siapa yang membuat entitas (hanya acara pembuatan kasus dan komentar)

Nilai Aktor: `createdBy` Bidang `updatedBy` dan dapat berisi

- AWS Responder: Tindakan yang dilakukan oleh responden AWS keamanan
- `security-ir.amazonaws.com`: Tindakan dilakukan secara otomatis oleh layanan
- ID Akun: Tindakan yang dilakukan oleh pelanggan (mis., "111122223333")

Nilai ARN sumber daya: Respons Insiden Keamanan AWS sumber daya menggunakan format ARN ini

- Kasus: `arn:aws:security-ir:{region}:{account-id}:case/{case-id}`
- Keanggotaan: `arn:aws:security-ir:{region}:{account-id}:membership/{membership-id}`

Peristiwa Kasus

Kasus Dibuat oleh AWS Responder

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Case Created",
  "source": "aws.security-ir",
  "account": "111122223333",
  "time": "2023-05-12T00:00:00Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
  ],
  "detail": {
    "caseId": "1234567890",
    "createdBy": "AWS Responder"
  }
}
```

Kasus Dibuat oleh Layanan

```
{
```

```
"version": "0",
"id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
"detail-type": "Case Created",
"source": "aws.security-ir",
"account": "111122223333",
"time": "2023-05-12T00:00:00Z",
"region": "us-west-2",
"resources": [
  "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
],
"detail": {
  "caseId": "1234567890",
  "createdBy": "security-ir.amazonaws.com"
}
}
```

Kasus yang Dibuat oleh Pelanggan

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Case Created",
  "source": "aws.security-ir",
  "account": "111122223333",
  "time": "2023-05-12T00:00:00Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
  ],
  "detail": {
    "caseId": "1234567890",
    "createdBy": "111122223333"
  }
}
```

Kasus Diperbarui oleh AWS Responder

```
{
  "version": "0",
```

```

    "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "detail-type": "Case Updated",
    "source": "aws.security-ir",
    "account": "111122223333",
    "time": "2023-05-12T01:30:00Z",
    "region": "us-west-2",
    "resources": [
      "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
    ],
    "detail": {
      "caseId": "1234567890",
      "updatedBy": "AWS Responder"
    }
  }
}

```

Kasus Diperbarui oleh AWS Pelanggan

```

{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Case Updated",
  "source": "aws.security-ir",
  "account": "111122223333",
  "time": "2023-05-12T02:15:00Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
  ],
  "detail": {
    "caseId": "1234567890",
    "updatedBy": "111122223333"
  }
}

```

Kasus Diperbarui oleh Respons Insiden Keamanan AWS Layanan

```

{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",

```

```
"detail-type": "Case Updated",
"source": "aws.security-ir",
"account": "111122223333",
"time": "2023-05-12T03:45:00Z",
"region": "us-west-2",
"resources": [
  "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
],
"detail": {
  "caseId": "1234567890",
  "updatedBy": "security-ir.amazonaws.com"
}
}
```

Kasus Tertutup

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Case Closed",
  "source": "aws.security-ir",
  "account": "111122223333",
  "time": "2023-05-15T14:22:00Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
  ],
  "detail": {
    "caseId": "1234567890"
  }
}
```

Acara Komentar Kasus

Komentar Kasus Dibuat oleh AWS Responder

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
```

```

    "detail-type": "Case Comment Created",
    "source": "aws.security-ir",
    "account": "111122223333",
    "time": "2023-05-12T04:30:00Z",
    "region": "us-west-2",
    "resources": [
      "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
    ],
    "detail": {
      "caseId": "1234567890",
      "createdBy": "AWS Responder"
    }
  }
}

```

Komentar Kasus Dibuat oleh Pelanggan

```

{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Case Comment Created",
  "source": "aws.security-ir",
  "account": "111122223333",
  "time": "2023-05-12T02:15:00Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
  ],
  "detail": {
    "caseId": "1234567890",
    "createdBy": "111122223333"
  }
}

```

Komentar Kasus Dibuat oleh Respons Insiden Keamanan AWS Layanan

```

{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Case Comment Created",

```

```

    "source": "aws.security-ir",
    "account": "111122223333",
    "time": "2023-05-12T02:15:00Z",
    "region": "us-west-2",
    "resources": [
      "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
    ],
    "detail": {
      "caseId": "1234567890",
      "createdBy": "security-ir.amazonaws.com"
    }
  }
}

```

Komentar Kasus Diperbarui oleh Pelanggan

```

{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Case Comment Updated",
  "source": "aws.security-ir",
  "account": "111122223333",
  "time": "2023-05-12T02:45:00Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
  ],
  "detail": {
    "caseId": "1234567890",
    "updatedBy": "111122223333"
  }
}

```

Komentar Kasus Diperbarui oleh Respons Insiden Keamanan AWS Layanan

```

{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Case Comment Updated",
  "source": "aws.security-ir",

```

```
"account": "111122223333",
"time": "2023-05-12T02:45:00Z",
"region": "us-west-2",
"resources": [
  "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
],
"detail": {
  "caseId": "1234567890",
  "updatedBy": "security-ir.amazonaws.com"
}
}
```

Komentar Kasus Dibuat oleh AWS Responder

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Case Comment Updated",
  "source": "aws.security-ir",
  "account": "111122223333",
  "time": "2023-05-12T02:45:00Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
  ],
  "detail": {
    "caseId": "1234567890",
    "updatedBy": "AWS Responder"
  }
}
```

Acara Keanggotaan

Keanggotaan Dibuat

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Membership Created",
```

```
    "source": "aws.security-ir",
    "account": "111122223333",
    "time": "2023-04-01T10:00:00Z",
    "region": "us-west-2",
    "resources": [
      "arn:aws:security-ir:us-west-2:111122223333:membership/
m-1234567890abcdef0"
    ],
    "detail": {
      "membershipId": "m-1234567890abcdef0"
    }
  }
}
```

Keanggotaan Diperbarui

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Membership Updated",
  "source": "aws.security-ir",
  "account": "111122223333",
  "time": "2023-04-15T16:30:00Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:security-ir:us-west-2:111122223333:membership/
m-1234567890abcdef0"
  ],
  "detail": {
    "membershipId": "m-1234567890abcdef0"
  }
}
```

Keanggotaan Dibatalkan

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Membership Closed",
  "source": "aws.security-ir",
```

```

    "account": "111122223333",
    "time": "2023-06-30T23:59:59Z",
    "region": "us-west-2",
    "resources": [
      "arn:aws:security-ir:us-west-2:111122223333:membership/
m-1234567890abcdef0"
    ],
    "detail": {
      "membershipId": "m-1234567890abcdef0"
    }
  }
}

```

Keanggotaan Diakhiri

```

{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Membership Terminated",
  "source": "aws.security-ir",
  "account": "111122223333",
  "time": "2023-07-01T00:00:00Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:security-ir:us-west-2:111122223333:membership/
m-123456s7890abcdef0"
  ],
  "detail": {
    "membershipId": "m-1234567890abcdef0"
  }
}

```

Menggunakan Respons Insiden Keamanan AWS Acara

Anda dapat membuat EventBridge aturan untuk mencocokkan peristiwa ini dan memicu tindakan otomatis. Berikut adalah beberapa contoh kasus penggunaan:

Cocokkan semua Respons Insiden Keamanan AWS acara:

```
{
  "source": ["aws.security-ir"]
}
```

Cocokkan acara kasus saja:

```
{
  "source": ["aws.security-ir"],
  "detail-type": [
    "Case Created",
    "Case Updated",
    "Case Closed",
    "Case Comment Added",
    "Case Comment Updated"
  ]
}
```

Kasus kecocokan diperbarui oleh AWS Responder:

```
{
  "source": ["aws.security-ir"],
  "detail-type": ["Case Updated"],
  "detail": {
    "updatedBy": ["AWS Responder"]
  }
}
```

Pertandingan acara untuk kasus tertentu:

```
{
  "source": ["aws.security-ir"],
  "detail": {
    "caseId": ["1234567890"]
  }
}
```

Tutorial: Mengirim peringatan Amazon Simple Notification Service untuk acara **Membership Updated**

Dalam tutorial ini, Anda mengonfigurasi aturan EventBridge acara Amazon yang hanya menangkap peristiwa di mana langganan Anda memasuki Membership Updated status.

Prasyarat

Tutorial ini mengasumsikan bahwa Anda memiliki langganan yang berfungsi dan AWS akun aktif dalam keanggotaan Anda.

Topik

- [Tutorial: Membuat dan berlangganan topik Amazon SNS](#)
- [Tutorial: Daftarkan aturan acara](#)
- [Tutorial: Uji aturan Anda](#)
- [Aturan alternatif: Pembaruan Kasus Respons Insiden Keamanan](#)

Tutorial: Membuat dan berlangganan topik Amazon SNS

Untuk tutorial ini, Anda mengonfigurasi topik Amazon SNS yang berfungsi sebagai target peristiwa untuk aturan peristiwa baru Anda.

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. Pilih Topics (Topik), Create topic (Buat topik).
3. Untuk Tipe, pilih Standar.
4. Untuk Nama, masukkan **MembershipUpdated** dan pilih Buat topik.
5. Di MembershipUpdatedlayar, pilih Buat langganan.
6. Untuk Protokol, pilih Email.
7. Untuk Titik akhir, masukkan alamat email yang Anda dapat mengaksesnya dan pilih Buat langganan.
8. Periksa akun email Anda dan tunggu sampai Anda menerima pesan email konfirmasi langganan. Saat Anda menerimanya, pilih Konfirmasi langganan.

Tutorial: Daftarkan aturan acara

Selanjutnya, daftarkan aturan acara yang hanya menangkap Membership Updated peristiwa.

Untuk mendaftarkan EventBridge aturan Anda

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 untuk aturan.

Note

Aturan tidak boleh memiliki nama yang sama dengan aturan lain di Wilayah yang sama dan di bus kejadian yang sama.

5. Untuk bus acara, pilih bus acara yang ingin Anda kaitkan dengan aturan ini. Jika Anda ingin aturan ini cocok dengan acara yang berasal dari akun Anda, pilih bus acara AWS default. Ketika AWS layanan di akun Anda memancarkan suatu acara, itu selalu masuk ke bus acara default akun Anda.

Note

Ini harus diatur di akun administrator Anda AWS Organizations atau yang didelegasikan tempat Anda membuat Respons Insiden Keamanan AWS keanggotaan.

6. Untuk Tipe aturan, pilih Aturan dengan pola peristiwa.
7. Pilih Selanjutnya.
8. Untuk sumber acara, pilih Lainnya.
9. Untuk pola Acara, pilih Pola kustom (editor JSON).
10. Tempel pola peristiwa berikut ke area teks.

```
{
  "source": ["aws.security-ir"],
  "detail-type": ["Membership Updated"]
}
```

Kode ini mendefinisikan EventBridge aturan yang cocok dengan acara apa pun di mana keanggotaan layanan Anda diperbarui atau dimodifikasi. Untuk informasi selengkapnya tentang pola peristiwa, lihat [Peristiwa dan Pola Peristiwa](#) di Panduan EventBridge Pengguna Amazon.

11. Pilih Berikutnya.
12. Untuk Jenis target, pilih Layanan AWS .
13. Untuk Pilih target, pilih topik SNS, dan untuk Topik, pilih MembershipUpdated.
14. (Opsional) Untuk pengaturan tambahan, lakukan hal berikut:
 - a. Untuk Masa peristiwa maksimal, masukkan nilai antara satu menit (00:01) dan 24 jam (24:00).
 - b. Untuk Upaya coba lagi, masukkan angka antara 0 dan 185.
 - c. Untuk antrian Dead-letter, pilih apakah akan menggunakan antrian Amazon SQS standar sebagai antrian huruf mati. EventBridge mengirimkan peristiwa yang cocok dengan aturan ini ke antrian huruf mati jika tidak berhasil dikirim ke target. Lakukan salah satu tindakan berikut:
 - Pilih Tidak ada untuk tidak menggunakan antrian surat mati.
 - Pilih Pilih antrian Amazon SQS di AWS akun saat ini untuk digunakan sebagai antrian huruf mati dan kemudian pilih antrian yang akan digunakan dari tarik-turun.
 - Pilih Pilih antrian Amazon SQS di AWS akun lain sebagai antrian huruf mati dan kemudian masukkan ARN antrian yang akan digunakan. Anda harus melampirkan kebijakan berbasis sumber daya ke antrian yang memberikan EventBridge izin untuk mengirim pesan ke antrian tersebut. Untuk informasi selengkapnya, lihat [Memberikan izin untuk antrian huruf mati di Panduan Pengguna](#) Amazon. EventBridge
15. Pilih Berikutnya.
16. (Opsional) Masukkan satu atau lebih tanda untuk aturan. Untuk informasi selengkapnya, lihat [EventBridge tag Amazon](#) di Panduan EventBridge Pengguna Amazon.
17. Pilih Berikutnya.
18. Tinjau detail aturan dan pilih Buat aturan.

Tutorial: Uji aturan Anda

Untuk menguji aturan Anda, kirimkan pembaruan Respons Insiden Keamanan AWS keanggotaan Anda. Jika aturan Anda dikonfigurasi dengan benar, Anda akan menerima pesan email dalam beberapa menit dengan teks acara.

Aturan alternatif: Pembaruan Kasus Respons Insiden Keamanan

Untuk membuat aturan acara yang memantau semua pembaruan kasus, ulangi tutorial ini dengan perubahan berikut:

1. Di [Tutorial: Membuat dan berlangganan topik Amazon SNS](#), gunakan *CaseUpdates* sebagai nama topik.
2. Dalam [Tutorial: Daftarkan aturan acara](#), gunakan pola berikut di editor JSON:

```
{
  "source": ["aws.security-ir"],
  "detail-type": [
    "Case Created",
    "Case Updated",
    "Case Closed",
    "Case Comment Created",
    "Case Comment Updated"
  ]
}
```

Pemecahan Masalah

Ketika Anda mengalami masalah yang terkait dengan melakukan tindakan khusus Respons Insiden Keamanan AWS, lihat topik di bagian ini.

ERROR adalah status operasi yang menunjukkan kesalahan dalam beberapa atau semua operasi. Atau, Anda menerima peringatan ketika masalah terjadi tetapi tugas masih selesai.

Daftar Isi

- [Masalah](#)
- [Kesalahan](#)
- [Dukungan](#)

Masalah

Tidak mengirim permintaan dari konteks yang benar.

Semua panggilan ke Respons Insiden Keamanan AWS APIs harus berasal dari kepala IAM di administrator atau akun keanggotaan yang didelegasikan layanan. Pastikan bahwa Anda beroperasi dari kepala IAM yang benar di akun administrator atau keanggotaan Akun AWS yang Respons Insiden Keamanan AWS didelegasikan organisasi Anda.

Kesalahan

`AccessDeniedException`

Anda tidak memiliki akses yang memadai untuk melakukan tindakan ini.

Silakan bekerja sama dengan AWS administrator Anda untuk memastikan bahwa Anda memiliki izin untuk mengambil Peran IAM di administrator atau akun keanggotaan Respons Insiden Keamanan AWS yang didelegasikan. Juga periksa peran memiliki kebijakan IAM yang mengizinkan tindakan yang diminta. Untuk informasi lebih lanjut lihat [Respons Insiden Keamanan AWS IAM](#).

`ConflictException`

Permintaan menyebabkan keadaan tidak konsisten.

Harap periksa apakah nama file lampiran kasus atau anggota tim respons default yang telah Anda tentukan adalah unik. Periksa juga apakah keanggotaan Respons Insiden Keamanan

AWS layanan Anda belum dikonfigurasi. Buka konsol Security Incident Response di <https://console.aws.amazon.com/security-ir/> dan navigasikan ke **Membership Details**.

InternalServerErrorException

Kesalahan tak terduga terjadi selama pemrosesan permintaan. Silakan coba lagi dalam beberapa menit. Jika masalah berlanjut, [angkat kasus dengan Dukungan](#).

ResourceNotFoundException

Permintaan referensi sumber daya yang tidak ada.

Satu atau lebih sumber daya yang ditentukan dalam permintaan Anda tidak ada. Harap periksa apakah semua sumber daya IDs yang diberikan ARNs atau benar. Ini berlaku untuk AWS Organizations IDs, akun IDs, peran IAM, keanggotaan, kasus, anggota tim respons, kasus, responden kasus, lampiran kasus, dan komentar kasus.

ThrottlingException

Permintaan ditolak karena throttling permintaan.

Terlalu banyak permintaan telah dibuat oleh prinsipal IAM Anda ke fungsi API tersebut dalam periode tertentu. Tunggu sebentar dan coba lagi. Jika masalah berlanjut, harap pertimbangkan untuk menerapkan backoff eksponensial dan algoritma coba lagi.

ValidationException

Input gagal memenuhi kendala yang ditentukan oleh file. Layanan AWS

Satu atau beberapa bidang data dalam permintaan Anda tidak memenuhi persyaratan kombinasi and/or logis validasi. Harap periksa apakah semua sumber daya ARNs lengkap, dan bahwa nilai teks memenuhi batasan ukuran dan format dari Panduan Referensi [Respons Insiden Keamanan AWS API](#). Periksa juga apakah pembaruan nilai apa pun diizinkan. Misalnya, mengubah kasus dari AWS didukung menjadi dikelola sendiri tidak dimungkinkan.

Dukungan

Jika Anda memerlukan bantuan tambahan, hubungi [Dukungan Pusat](#) untuk tujuan pemecahan masalah. Harap memiliki informasi berikut yang tersedia:

- Wilayah AWS Yang Anda gunakan

- Akun AWS ID keanggotaan
- Konten sumber Anda, jika berlaku dan tersedia
- Detail lain tentang masalah yang mungkin membantu pemecahan masalah

Keamanan

Topik

- [Perlindungan Data di Respons Insiden Keamanan AWS](#)
- [Inter-network privasi lalu lintas](#)
- [Identity and Access Management](#)
- [Pemecahan masalah Respons Insiden Keamanan AWS identitas dan akses](#)
- [Menggunakan peran layanan](#)
- [Menggunakan Peran Terkait Layanan](#)
- [AWS Kebijakan Terkelola](#)
- [Respons insiden](#)
- [Validasi kepatuhan](#)
- [Penebangan dan pemantauan di AWS Respon Insiden Keamanan](#)
- [Ketahanan](#)
- [Keamanan infrastruktur](#)
- [Konfigurasi dan analisis kerentanan](#)
- [Cross-service pencegahan wakil bingung](#)

Perlindungan Data di Respons Insiden Keamanan AWS

[Model tanggung jawab AWS bersama](#) berlaku untuk perlindungan data untuk layanan Respons Insiden AWS Keamanan. Seperti yang dijelaskan dalam model AWS ini, bertanggung jawab untuk melindungi infrastruktur yang menjalankan layanan yang ditawarkan di AWS Cloud. Anda bertanggung jawab untuk mempertahankan kendali atas konten yang di-host pada infrastruktur ini. Anda juga bertanggung jawab atas konfigurasi keamanan dan tugas manajemen untuk AWS layanan yang Anda gunakan. Untuk informasi selengkapnya tentang privasi data, silakan lihat [Pertanyaan Umum Privasi Data](#). Untuk informasi tentang perlindungan data di Eropa, lihat [AWS postingan blog Model Tanggung Jawab Bersama dan GDPR AWS](#) di Blog Keamanan .

Untuk tujuan perlindungan data, praktik terbaik AWS keamanan menyatakan bahwa Anda harus melindungi kredensial AWS akun dan menyiapkan pengguna individu dengan AWS IAM Identity Center atau AWS Identity and Access Management (IAM). Dengan cara ini, setiap pengguna hanya

diberikan izin yang diperlukan untuk memenuhi tugas pekerjaan mereka. 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 AWS sumber daya. Kami mensyaratkan TLS 1.2 dan menganjurkan TLS 1.3.
- Siapkan API dan logging aktivitas pengguna dengan AWS CloudTrail.
- Gunakan solusi AWS enkripsi, bersama dengan semua kontrol keamanan default dalam AWS layanan.
- FIPS 140-3 saat ini tidak didukung oleh layanan.

Jangan pernah memasukkan informasi rahasia atau sensitif, seperti alamat email Anda, ke dalam tag atau bidang teks bentuk bebas seperti bidang Nama. Ini termasuk saat Anda bekerja dengan AWS Dukungan atau AWS layanan lain menggunakan konsol, API AWS Command Line Interface, atau AWS SDK. Data apa pun yang Anda masukkan tag atau bidang teks bentuk bebas yang digunakan untuk nama dapat digunakan untuk penagihan atau log diagnostik. Jika Anda memberikan URL ke server eksternal, kami sangat menyarankan agar Anda tidak menyertakan informasi kredensial dalam URL untuk memvalidasi permintaan Anda ke server tersebut.

Topik

- [Enkripsi data](#)
- [Pengumpulan dan penggunaan data](#)
- [Data residensi dan perilaku regional](#)
- [Akses dan izin data](#)

Enkripsi data

Respons Insiden Keamanan AWS melindungi data Anda menggunakan enkripsi saat istirahat dan dalam perjalanan. Semua data dienkripsi menggunakan protokol enkripsi standar industri untuk membantu Anda memenuhi persyaratan keamanan dan kepatuhan.

Topik

- [Enkripsi saat diam](#)
- [Enkripsi saat bergerak](#)
- [Manajemen kunci](#)

Enkripsi saat diam

Data dienkripsi saat istirahat menggunakan enkripsi sisi server transparan. Hal ini membantu mengurangi beban operasional dan kompleksitas yang terlibat dalam melindungi data sensitif. Dengan enkripsi saat istirahat, Anda dapat membangun aplikasi yang sensitif terhadap keamanan yang memenuhi persyaratan kepatuhan enkripsi dan peraturan.

Enkripsi saat bergerak

Data yang dikumpulkan dan diakses oleh Respons Insiden Keamanan AWS secara eksklusif melalui saluran yang dilindungi Transport Layer Security (TLS).

Manajemen kunci

Respons Insiden Keamanan AWS mengimplementasikan integrasi dengan AWS KMS untuk menyediakan enkripsi saat istirahat untuk data kasus dan lampiran.

Respons Insiden Keamanan AWS tidak mendukung kunci yang dikelola pelanggan.

Pengumpulan dan penggunaan data

Respons Insiden Keamanan AWS bekerja dengan tiga kategori data yang berbeda, masing-masing dengan metode pengumpulan, pola penyimpanan, dan perilaku regional yang berbeda. Memahami kategori ini sangat penting untuk mengevaluasi bagaimana Respons Insiden Keamanan sesuai dengan persyaratan kepatuhan Anda.

Topik

- [Data investigasi kasus](#)
- [Data temuan keamanan](#)
- [Pemrosesan agen investigasi](#)
- [Memahami sensitivitas metadata](#)

Data investigasi kasus

Saat Anda membuka kasus insiden keamanan, Security Incident Response mengumpulkan log dan metadata dari AWS lingkungan Anda untuk mendukung penyelidikan. Data khusus kasus ini mencakup log API, Log Aliran VPC, kueri DNS Amazon Route 53, peristiwa akses Amazon S3,

metadata sumber daya (nama, tag, dan detail konfigurasi), dan informasi kasus seperti komentar dan catatan investigasi.

Important

Security Incident Response mengumpulkan informasi tentang pola aktivitas dan konfigurasi sumber daya lingkungan Anda. Itu tidak mengumpulkan konten sebenarnya dari bucket Amazon S3 Anda, catatan database, atau data aplikasi. Security Incident Response mengumpulkan “siapa yang melakukan apa dan kapan” daripada data yang mendasarinya sendiri.

Data investigasi kasus ini dikumpulkan sesuai permintaan untuk insiden tertentu dan tetap terkait dengan kasus Anda. Security Incident Response menyimpan data ini selama 90 hari secara default untuk memungkinkan Anda meninjau riwayat investigasi, mendukung investigasi yang sedang berlangsung atau tindak lanjut, serta memenuhi persyaratan dokumentasi audit dan kepatuhan. Jika Anda memerlukan penghapusan data sebelum periode 90 hari berakhir, hubungi AWS Dukungan untuk meminta penghapusan lebih awal.

Data temuan keamanan

Security Incident Response terus menerus menyerap metadata temuan keamanan dari Amazon GuardDuty dan AWS Security Hub CSPM di semua yang didukung di Wilayah AWS mana Anda telah mengaktifkan layanan ini. Data temuan ini mencakup pengidentifikasi sumber daya, jenis temuan, tingkat keparahan, sumber daya yang terpengaruh, dan stempel waktu deteksi. Tidak seperti data investigasi kasus, data temuan dicerna secara otomatis dan terus menerus untuk memungkinkan Respons Insiden Keamanan untuk mengkorelasikan ancaman di seluruh AWS lingkungan Anda.

Data temuan tidak termasuk log rinci atau data mentah yang menghasilkan temuan—hanya metadata tentang apa yang terdeteksi, di mana terdeteksi, dan tingkat keparahan deteksi. Metadata ini memungkinkan Security Incident Response untuk mengidentifikasi pola, menghubungkan peristiwa keamanan terkait di seluruh Wilayah, dan memberikan analisis ancaman yang komprehensif.

Pemrosesan agen investigasi

Agen investigasi Security Incident Response, yang didukung oleh Amazon Bedrock, memproses metadata dari data investigasi kasus dan data temuan Anda untuk menghasilkan wawasan, mengidentifikasi pola, dan merekomendasikan tindakan respons. Pemrosesan ini terjadi di wilayah global Amazon Bedrock sebagai bagian dari alur kerja analisis agen.

⚠ Important

Agen investigasi memproses metadata secara sementara dan tidak menyimpan data ini secara terus-menerus di Wilayah global Amazon Bedrock. Metadata hanya digunakan untuk menghasilkan wawasan investigasi dan tidak dipertahankan setelah pemrosesan selesai.

Memahami sensitivitas metadata

Meskipun Security Incident Response tidak mengumpulkan data aplikasi Anda, metadata yang dikumpulkannya di ketiga kategori dapat mengungkapkan informasi sensitif tentang lingkungan Anda dan berpotensi pengguna Anda. Pertimbangkan contoh berikut:

- Nama sumber daya seperti `patient-database-prod` atau `financial-records-2026` menunjukkan tujuan dan sensitivitas sumber daya.
- Kueri DNS seperti `user12345.internal.app.com` mungkin berisi pengenalan pengguna atau informasi sistem internal.
- Pola panggilan API dapat mengungkapkan proses bisnis dan alur kerja operasional.

Organizations dalam industri yang diatur harus mengevaluasi apakah metadata ini termasuk dalam persyaratan kepatuhan mereka, meskipun itu bukan data yang diatur itu sendiri.

Data residensi dan perilaku regional

Tiga kategori data dalam Security Incident Response memiliki lokasi penyimpanan dan pola pergerakan regional yang berbeda. Memahami pola-pola ini sangat penting untuk organisasi dengan persyaratan residensi data.

Topik

- [Penyimpanan dan pergerakan data investigasi kasus](#)
- [Temuan keamanan penyimpanan dan pergerakan data](#)
- [Lokasi pemrosesan agen investigasi](#)
- [Ketersediaan wilayah](#)

Penyimpanan dan pergerakan data investigasi kasus

Data investigasi kasus tetap berada di Wilayah AWS tempat Anda membuka kasus insiden keamanan. Saat Anda membuat kasus di Wilayah tertentu, semua log, metadata, dan informasi kasus yang dikumpulkan untuk penyelidikan tersebut disimpan di Wilayah tersebut. Data ini tidak berpindah ke Wilayah lain.

Untuk standar Wilayah AWS (Wilayah tersedia secara default), data investigasi kasus tetap berada di Wilayah tempat kasus dibuat selama siklus hidup investigasi dan periode retensi 90 hari.

Untuk wilayah AWS opt-in (seperti Timur Tengah (Bahrain), Afrika (Cape Town), atau Asia Pasifik (Hong Kong)), data investigasi kasus juga tetap berada di Wilayah tempat kasus ini dibuat. Namun, jika Anda mengaktifkan Respons Insiden Keamanan di Wilayah keikutsertaan, semua data kasus dari Wilayah tersebut secara otomatis bereplikasi ke Wilayah AS Timur (Virginia N.) (us-east-1) untuk manajemen dan analisis kasus terpusat.

Important

Jika Anda beroperasi di Wilayah keikutsertaan, data investigasi kasus Anda secara otomatis mengalir ke us-east-1. Organizations dengan persyaratan residensi data yang ketat harus mengevaluasi apakah replikasi lintas wilayah ini kompatibel dengan kewajiban kepatuhan mereka. Data tidak pernah mengalir di antara Wilayah keikutsertaan yang berbeda, dan data dari Wilayah non-keikutsertaan tidak pernah bereplikasi ke Wilayah keikutsertaan.

Temuan keamanan penyimpanan dan pergerakan data

Metadata temuan keamanan melintasi Wilayah terlepas dari mana temuan itu berasal. Respons Insiden Keamanan menyerap temuan dari Amazon GuardDuty dan AWS Security Hub CSPM di semua Wilayah tempat Anda mengaktifkan layanan ini dan menghubungkan metadata ini di seluruh Wilayah untuk mengidentifikasi ancaman terdistribusi dan pola serangan.

Untuk standar Wilayah AWS, metadata temuan dari semua Wilayah dapat diakses untuk korelasi dan analisis. Gerakan lintas wilayah ini memungkinkan Security Incident Response untuk mendeteksi ancaman yang menjangkau beberapa Wilayah, seperti penyerang yang bergerak secara lateral di seluruh infrastruktur Anda.

Untuk Wilayah AWS keikutsertaan, metadata temuan mengikuti pola replikasi yang sama dengan data investigasi kasus. Temuan dari Wilayah keikutsertaan mereplikasi ke komersial Wilayah

AWS (Wilayah selain AWS GovCloud (US) Wilayah dan Wilayah Tiongkok) untuk analisis terpusat bersama temuan dari Wilayah lain.

Metadata temuan hanya mencakup pengidentifikasi sumber daya, jenis temuan, dan informasi tingkat keparahan—bukan log terperinci atau data mentah yang menghasilkan temuan. Metadata ini memungkinkan korelasi ancaman sekaligus meminimalkan volume data yang melintasi batas Wilayah.

Lokasi pemrosesan agen investigasi

Agen investigasi Security Incident Response memproses metadata di wilayah global Amazon Bedrock, terlepas dari Wilayah mana kasus atau data temuan Anda berasal. Pemrosesan ini bersifat sementara — agen menganalisis metadata untuk menghasilkan wawasan dan rekomendasi tetapi tidak menyimpan metadata secara terus-menerus di infrastruktur Amazon Bedrock.

Ketika agen menyelesaikan analisisnya, wawasan dan rekomendasi yang dihasilkan disimpan bersama data investigasi kasus Anda di Wilayah tempat kasus dibuat. Metadata yang digunakan untuk pemrosesan tidak disimpan di Amazon Bedrock Global Region setelah analisis selesai.

Ketersediaan wilayah

Untuk informasi tentang Wilayah mana yang mendukung Respons Insiden Keamanan, lihat [Layanan AWS Regional](#).

Akses dan izin data

Dua grup dapat mengakses Respons Insiden Keamanan AWS data Anda:

- Pengguna resmi Anda — pengguna IAM dan peran yang Anda berikan izin Respons Insiden Keamanan.
- AWS responden insiden — AWS karyawan dan kontraktor yang diperiksa yang menyelidiki kasus Anda.

Topik

- [AWS akses responden insiden](#)
- [Akses logging dan auditabilitas](#)
- [Mengendalikan akses dengan IAM](#)

AWS akses responden insiden

AWS Mengoperasikan Security Incident Response sebagai layanan “ikuti matahari”, menyediakan 24/7 cakupan melalui responden insiden yang berlokasi di Amerika, Eropa, dan Asia-Pacific. Ketika Anda membuka kasus insiden keamanan, responden yang ditugaskan untuk kasus Anda mungkin berlokasi di salah satu wilayah ini. Semua responden AWS insiden menjalani pemeriksaan latar belakang dan menyelesaikan pelatihan keamanan sebelum mendapatkan akses ke data pelanggan.

Important

Lokasi geografis responden insiden yang menangani kasus Anda dapat bervariasi berdasarkan kapan Anda membuka kasus dan ketersediaan responden. Organisasi dengan persyaratan tentang siapa yang dapat mengakses data mereka harus mengevaluasi apakah model akses global ini kompatibel dengan kebijakan mereka.

Akses logging dan auditabilitas

Setiap akses ke data Respons Insiden Keamanan Anda dicatat. Anda dapat mengaudit siapa yang mengakses data Anda, data apa yang diakses, dan kapan akses terjadi. Log audit ini mendukung kepatuhan dan persyaratan pemantauan keamanan Anda.

Mengendalikan akses dengan IAM

Anda mengontrol pengguna dan peran mana yang Akun AWS dapat mengakses Respons Insiden Keamanan melalui kebijakan IAM. Untuk informasi tentang mengonfigurasi izin IAM untuk Respons Insiden Keamanan, lihat [Identity and Access Management](#)

Inter-network privasi lalu lintas

Lalu lintas antara layanan dan aplikasi serta klien on-premise

Anda memiliki dua opsi konektivitas antara jaringan pribadi Anda dan AWS:

- AWS Site-to-Site VPN Koneksi. Untuk informasi selengkapnya, lihat [Apa itu AWS Site-to-Site VPN?](#) dalam Panduan Pengguna AWS Site-to-Site VPN .
- Direct Connect Koneksi. Untuk informasi selengkapnya, lihat [Apa itu Direct Connect?](#) dalam Panduan Pengguna Direct Connect .

Akses ke Respons Insiden Keamanan AWS melalui jaringan adalah melalui API yang AWS dipublikasikan. Klien harus mendukung Keamanan Lapisan Pengangkutan (TLS) 1.2. Kami merekomendasikan TLS 1.3. Klien juga harus mendukung cipher suite dengan Perfect Forward Secrecy (PFS), seperti Ephemeral (DHE) atau Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). Diffie-Hellman Sebagian besar sistem modern seperti Java 7 dan versi lebih baru mendukung mode-mode ini. Selain itu, Anda harus menandatangani permintaan menggunakan kunci akses ID dan kunci akses rahasia yang terkait dengan IAM pengguna utama, atau Anda dapat menggunakan [AWS Security Token Service \(STS\)](#) untuk membuat kredensial keamanan sementara guna menandatangani permintaan.

Lalu lintas antara AWS sumber daya di Wilayah yang sama

Titik akhir Amazon Virtual Private Cloud (Amazon VPC) untuk Respons Insiden Keamanan AWS adalah entitas logis dalam VPC yang memungkinkan konektivitas hanya untuk. Respons Insiden Keamanan AWS Rutekan VPC Amazon meminta Respons Insiden Keamanan AWS dan merutekan respons kembali ke VPC. Untuk informasi selengkapnya, lihat [Titik akhir VPC](#) di Panduan Pengguna Amazon VPC. Misalnya, kebijakan yang dapat Anda gunakan untuk mengontrol akses dari titik akhir VPC, lihat [Menggunakan Kebijakan IAM untuk mengontrol akses ke DynamoDB](#).

Note

Titik akhir Amazon VPC tidak dapat diakses melalui atau. AWS Site-to-Site VPN Direct Connect

Identity and Access Management

AWS Identity and Access Management (IAM) adalah AWS layanan yang membantu administrator mengontrol akses ke sumber daya. AWS Administrator IAM mengontrol prinsip yang diautentikasi (masuk) dan resmi (memiliki izin) untuk menggunakan sumber daya. Respons Insiden Keamanan AWS IAM adalah AWS layanan yang dapat Anda gunakan tanpa biaya tambahan.

Topik

- [Mengautentikasi dengan identitas](#)
- [Bagaimana Respons Insiden Keamanan AWS Bekerja dengan IAM](#)

Audiens

Cara Anda menggunakan AWS Identity and Access Management (IAM) berbeda, tergantung pada pekerjaan yang Anda lakukan. Respons Insiden Keamanan AWS

Administrator Keamanan

Pengguna ini disarankan untuk menggunakan kebijakan [AWS Security Incident Response Full Access](#) terkelola untuk memastikan mereka memiliki akses baca dan tulis ke sumber daya keanggotaan dan kasus.

Pengamat Kasus

Orang-orang ini tidak memiliki akses otoritatif ke semua kasus tetapi kasus individual yang Anda berikan izin eksplisit.

Anggota Tim Respons Insiden

Anggota tim dapat diberikan keanggotaan penuh dan akses kasus. Disarankan bahwa tidak semua individu memiliki tindakan otoritatif pada keanggotaan layanan tetapi harus memiliki akses ke setiap dan semua kasus yang dibuat dan dikelola melalui layanan. Untuk informasi selengkapnya, lihat [kebijakan Respons Insiden Keamanan AWS terkelola](#).

Mengautentikasi dengan identitas

Otentikasi adalah cara Anda masuk AWS menggunakan kredensi identitas Anda. Anda harus diautentikasi (masuk ke AWS) sebagai pengguna root AWS akun, sebagai pengguna IAM, atau dengan mengambil peran IAM.

Anda dapat masuk AWS sebagai identitas federasi dengan menggunakan kredensial yang disediakan melalui sumber identitas. AWS Pengguna IAM Identity Center (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 Konsol AWS Manajemen atau portal AWS akses. Untuk informasi selengkapnya tentang masuk AWS, lihat [Cara masuk ke AWS akun Anda](#) di Panduan AWS Sign-In Pengguna.

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. Untuk informasi selengkapnya tentang penggunaan metode yang disarankan untuk menandatangani permintaan sendiri, lihat [Menandatangani permintaan API AWS](#) dalam Panduan Pengguna IAM.

Terlepas dari metode otentikasi yang Anda gunakan, Anda mungkin diminta untuk memberikan informasi keamanan tambahan. Misalnya, AWS merekomendasikan agar Anda menggunakan otentikasi multi-faktor (MFA) untuk meningkatkan keamanan akun Anda. Untuk mempelajari lebih lanjut, lihat [Multi-factor otentikasi](#) di Panduan Pengguna Pusat AWS Identitas IAM dan [Menggunakan otentikasi multi-faktor \(MFA\) AWS](#) di Panduan Pengguna IAM.

AWS pengguna root akun

Saat Anda membuat AWS akun, Anda mulai dengan satu identitas masuk yang memiliki akses lengkap ke semua AWS layanan dan sumber daya di akun. Identitas ini disebut pengguna root AWS akun dan diakses dengan masuk dengan alamat email dan kata sandi yang Anda gunakan untuk membuat akun. Jangan pernah menggunakan pengguna root untuk tugas sehari-hari Anda dan mengambil langkah-langkah untuk melindungi kredensial pengguna root Anda. Gunakan hanya untuk melakukan tugas yang hanya dapat dilakukan oleh 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 federasi

Ini adalah praktik terbaik untuk meminta pengguna manusia, termasuk mereka yang membutuhkan akses administrator, untuk menggunakan federasi dengan penyedia identitas untuk mengakses AWS layanan dengan menggunakan kredensi sementara.

Identitas federasi adalah pengguna dari direktori pengguna perusahaan Anda, penyedia identitas web, AWS Directory Service, direktori Pusat Identitas, atau pengguna mana pun yang mengakses AWS layanan dengan menggunakan kredensi yang disediakan melalui sumber identitas. Ketika identitas federasi mengakses AWS akun, mereka mengambil peran, dan peran tersebut 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 AWS akun dan aplikasi Anda. Untuk informasi tentang Pusat Identitas IAM, lihat [Apa itu Pusat Identitas IAM?](#) di Panduan Pengguna Pusat AWS Identitas IAM.

Pengguna dan grup IAM

[Pengguna IAM](#) adalah identitas dalam AWS akun Anda yang memiliki izin khusus untuk satu orang atau aplikasi. Sebaiknya mengandalkan kredensi sementara daripada membuat pengguna IAM yang memiliki kredensi jangka panjang seperti kata sandi dan kunci akses. Jika Anda memiliki kasus penggunaan khusus yang memerlukan kredensial jangka panjang dengan pengguna IAM, kami sarankan Anda memutar 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 kumpulan 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 memiliki grup yang bernama IAMAdmins dan memberikan izin ke 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 [Kapan harus membuat pengguna IAM \(bukan peran\)](#) dalam Panduan Pengguna IAM.

Peran IAM

[Peran IAM](#) adalah identitas dalam AWS akun Anda yang memiliki izin khusus. Peran ini mirip dengan pengguna IAM, tetapi tidak terkait dengan orang tertentu. Anda dapat mengambil peran IAM untuk sementara waktu di Konsol AWS Manajemen dengan [beralih peran](#). Anda dapat mengambil peran dengan memanggil operasi AWS CLI atau AWS API atau dengan menggunakan URL khusus. Untuk informasi selengkapnya tentang cara menggunakan peran, lihat [Menggunakan peran IAM](#) 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 [Membuat 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](#) di Panduan Pengguna Pusat AWS Identitas IAM.

- Izin pengguna IAM sementara – Pengguna atau peran IAM dapat mengambil peran IAM guna mendapatkan berbagai izin secara sementara untuk tugas tertentu.
- Cross-account akses — Anda dapat menggunakan peran IAM untuk memungkinkan 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 AWS layanan, Anda dapat melampirkan kebijakan 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.
- Cross-service akses — Beberapa AWS layanan menggunakan fitur di AWS layanan lain. Sebagai contoh, ketika Anda memanggil suatu layanan, biasanya layanan tersebut menjalankan aplikasi di Amazon EC2 atau menyimpan objek di Amazon S3. Sebuah layanan mungkin melakukannya menggunakan izin principal yang memanggil, menggunakan peran layanan, atau peran terkait layanan.
 - 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 [Membuat peran untuk mendelegasikan izin ke layanan AWS](#) dalam Panduan Pengguna IAM.
 - Service-linked peran — Peran terkait layanan adalah jenis peran layanan yang ditautkan ke layanan. AWS Layanan dapat mengambil peran untuk melakukan tindakan atas nama Anda. Service-linked peran muncul di AWS akun Anda 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 kredensial sementara untuk aplikasi yang berjalan pada instans EC2 dan membuat AWS permintaan CLI atau API. AWS Cara ini lebih dianjurkan daripada menyimpan kunci akses dalam instans EC2. Untuk menetapkan AWS peran ke instans EC2 dan membuatnya tersedia untuk aplikasinya, Anda membuat profil instans yang dilampirkan ke instance. Profil instans berisi peran dan memungkinkan program yang berjalan di instans EC2 mendapatkan kredensial sementara. Untuk informasi selengkapnya, lihat [Menggunakan peran IAM untuk memberikan izin ke aplikasi yang berjalan dalam instans Amazon EC2](#) dalam Panduan Pengguna IAM.

Untuk mempelajari apakah kita harus menggunakan peran IAM atau pengguna IAM, lihat [Kapan harus membuat peran IAM \(bukan pengguna\)](#) dalam Panduan Pengguna IAM.

Bagaimana Respons Insiden Keamanan AWS Bekerja dengan IAM

AWS Identity and Access Management (IAM) adalah AWS layanan 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. Respons Insiden Keamanan AWS IAM adalah AWS layanan yang dapat Anda gunakan tanpa biaya tambahan.

Fitur IAM yang dapat Anda gunakan Respons Insiden Keamanan AWS	
<u>Fitur IAM</u>	<u>Penyelarasan layanan</u>
Identity-based kebijakan	Ya
Resource-based kebijakan	Tidak
Tindakan kebijakan	Ya
Sumber daya kebijakan	Ya
Kunci kondisi kebijakan	Ya (global)
ACL	Tidak
ABAC (tanda dalam kebijakan)	Ya
Kredensial sementara	Ya
Sesi akses teruskan (FAS)	Ya
Peran layanan	Tidak
Service-linked peran	Ya

Topik

- [Identity-based kebijakan untuk Respons Insiden Keamanan AWS](#)
- [Kunci kondisi kebijakan untuk Respons Insiden Keamanan AWS](#)
- [Daftar kontrol akses \(ACL\) di Respons Insiden Keamanan AWS](#)

Identity-based kebijakan untuk Respons Insiden Keamanan AWS

Identity-based kebijakan adalah dokumen kebijakan izin JSON yang dapat Anda lampirkan ke identitas, seperti pengguna IAM, grup pengguna, atau peran. 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 [Membuat kebijakan IAM](#) 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.

Topik

- [Identity-based contoh kebijakan](#)
- [Praktik terbaik kebijakan](#)
- [Menggunakan Respons Insiden Keamanan AWS konsol](#)
- [Mengizinkan pengguna melihat izin mereka sendiri](#)
- [Resource-Based Kebijakan](#)
- [Tindakan Kebijakan](#)

Identity-based contoh kebijakan

Secara default, pengguna dan peran tidak memiliki izin untuk membuat atau memodifikasi Respons Insiden Keamanan AWS sumber daya. Mereka juga tidak dapat melakukan tugas dengan menggunakan AWS Management Console, AWS Command Line Interface (AWS CLI), atau AWS API. Administrator IAM dapat membuat kebijakan IAM untuk memberikan izin kepada pengguna untuk melakukan tindakan pada sumber daya yang mereka butuhkan. Administrator kemudian akan dapat menambahkan kebijakan IAM ke peran, dan pengguna dapat mengambil peran.

Untuk mempelajari cara membuat kebijakan berbasis identitas IAM menggunakan contoh dokumen kebijakan JSON ini, lihat [Membuat kebijakan IAM](#) dalam Panduan Pengguna IAM.

Untuk detail tentang tindakan dan jenis sumber daya yang ditentukan oleh Respons Insiden AWS Keamanan, termasuk format ARN untuk setiap jenis sumber daya, lihat Kunci tindakan, sumber daya, dan kondisi Respons Insiden Keamanan AWS di Referensi Otorisasi Layanan.

Praktik terbaik kebijakan

Identity-based kebijakan menentukan apakah seseorang dapat membuat, mengakses, atau menghapus Respons Insiden Keamanan AWS sumber daya di akun Anda. Tindakan ini dapat menimbulkan biaya untuk AWS akun Anda. 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 AWS akun Anda. 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 AWS layanan tertentu, 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 IAM Access Analyzer](#) dalam Panduan Pengguna IAM.

Memerlukan otentikasi multi-faktor (MFA) - Jika Anda memiliki skenario yang mengharuskan pengguna IAM atau pengguna root di akun Anda AWS , aktifkan MFA untuk keamanan tambahan.

Untuk meminta MFA ketika operasi API dipanggil, tambahkan kondisi MFA pada kebijakan Anda. Untuk informasi selengkapnya, lihat [Mengonfigurasi akses MFA-protected API](#) di Panduan Pengguna IAM.

Untuk informasi selengkapnya tentang praktik terbaik dalam IAM, lihat [Praktik terbaik keamanan di IAM](#) dalam Panduan Pengguna IAM.

Menggunakan Respons Insiden Keamanan AWS konsol

Untuk mengakses <https://console.aws.amazon.com/security-ir/>, Anda harus memiliki set izin minimum. Izin ini harus memungkinkan Anda untuk membuat daftar dan melihat detail tentang Respons Insiden Keamanan AWS sumber daya di AWS akun Anda. 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.

Lampirkan kebijakan Respons Insiden Keamanan AWS Akses atau ReadOnly AWS terkelola untuk memastikan bahwa pengguna dan peran dapat menggunakan konsol layanan. Untuk informasi selengkapnya, lihat [Menambah izin untuk pengguna](#) dalam Panduan Pengguna IAM.

Mengizinkan pengguna 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 CLI AWS atau API secara terprogram. AWS

Resource-Based Kebijakan

[Resource-based kebijakan dalam Respons Insiden AWS Keamanan](#)

Mendukung kebijakan berbasis sumber daya: Tidak

Resource-based kebijakan 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 principal tertentu pada sumber daya tersebut dan dalam kondisi apa. Anda harus [menentukan principal](#) dalam kebijakan berbasis sumber daya. Principal dapat meliputi akun, pengguna, peran, pengguna gabungan, atau layanan AWS .

Untuk informasi selengkapnya, lihat [Akses sumber daya lintas akun di IAM](#) di Panduan Pengguna IAM.

Tindakan Kebijakan

Tindakan kebijakan untuk Respons Insiden Keamanan AWS

Tindakan kebijakan Support: Ya

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Yaitu, principal dapat melakukan tindakan pada suatu sumber daya, dan dalam suatu syarat.

Elemen Tindakan kebijakan JSON menjelaskan tindakan yang dapat Anda gunakan untuk mengizinkan atau menolak akses dalam 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.

Untuk melihat daftar Respons Insiden Keamanan AWS tindakan, lihat Tindakan yang ditentukan oleh Respons Insiden Keamanan AWS dalam Referensi Otorisasi Layanan.

Tindakan kebijakan Respons Insiden Keamanan AWS menggunakan awalan berikut sebelum tindakan:

Respons Insiden Keamanan AWS -identitas

Untuk menetapkan secara spesifik beberapa tindakan dalam satu pernyataan, pisahkan tindakan tersebut dengan koma.

“Action”: [“Respons Insiden Keamanan AWS -identity:action1”, “-identity:action2”]Respons Insiden Keamanan AWS

Sumber daya kebijakan untuk Respons Insiden AWS Keamanan Amazon

Mendukung sumber daya kebijakan: Ya Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Yaitu, principal dapat melakukan tindakan pada suatu sumber daya, dan dalam suatu syarat.

Elemen kebijakan Resource JSON menentukan objek atau objek yang tindakan tersebut berlaku. Pernyataan harus menyertakan Sumber Daya atau NotResource elemen. 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.

“Sumber Daya”: “**”

Kunci kondisi kebijakan untuk Respons Insiden Keamanan AWS

Mendukung kunci kondisi kebijakan khusus layanan: Tidak

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Yaitu, principal dapat melakukan tindakan pada suatu sumber daya, dan dalam suatu syarat.

Elemen Kondisi (atau blok Kondisi) memungkinkan Anda menentukan kondisi di mana pernyataan berlaku. Elemen Syarat 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 Kondisi dalam pernyataan, atau beberapa kunci dalam satu elemen Kondisi, AWS mengevaluasi mereka menggunakan operasi AND logis. Jika Anda menentukan beberapa nilai untuk satu kunci kondisi, AWS mengevaluasi kondisi menggunakan operasi OR 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.

Daftar kontrol akses (ACL) di Respons Insiden Keamanan AWS

Mendukung ACL: Tidak

Daftar kontrol akses (ACL) mengendalikan principal mana (anggota akun, pengguna, atau peran) yang memiliki izin untuk mengakses sumber daya. ACL serupa dengan kebijakan berbasis sumber daya, meskipun kebijakan tersebut tidak menggunakan format dokumen kebijakan JSON.

Attribute-based kontrol akses (ABAC) dengan AWS Security Incident Response

Mendukung ABAC (tanda dalam kebijakan): Ya

Attribute-based Access Control (ABAC) adalah strategi otorisasi yang mendefinisikan izin berdasarkan atribut. Dalam AWS, atribut ini disebut tag. Anda dapat melampirkan tanda ke entitas IAM (pengguna atau peran) dan ke banyak sumber daya AWS. Penandaan ke entitas dan sumber daya adalah langkah pertama dari ABAC. Kemudian rancanglah kebijakan ABAC untuk mengizinkan operasi ketika tanda milik principal 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 [Apa itu ABAC?](#) dalam Panduan Pengguna IAM. Untuk melihat tutorial dengan langkah-langkah untuk menyiapkan ABAC, lihat [Menggunakan kontrol akses berbasis atribut \(ABAC\)](#) di Panduan Pengguna AWS Identity and Access Management

Kredensi sementara dengan Respons Insiden Keamanan AWS

Mendukung kredensial sementara: Ya

AWS layanan tidak berfungsi saat Anda masuk menggunakan kredensial sementara. Untuk informasi tambahan, termasuk AWS layanan mana yang bekerja dengan kredensi sementara, lihat [AWS layanan yang bekerja dengan IAM di Panduan Pengguna AWS Identity and Access Management](#). Anda menggunakan kredensi sementara jika masuk ke Konsol AWS Manajemen 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 [Peralihan peran \(konsol\)](#) dalam Panduan Pengguna IAM.

Anda dapat membuat kredensial sementara secara manual menggunakan AWS CLI atau API. AWS Anda kemudian dapat menggunakan kredensial sementara tersebut untuk mengakses. AWS merekomendasikan agar Anda secara dinamis menghasilkan kredensial sementara alih-alih menggunakan kunci akses jangka panjang. Untuk informasi selengkapnya, lihat [Kredensial keamanan sementara di IAM](#).

Teruskan sesi akses untuk Respons Insiden Keamanan AWS

Mendukung sesi akses terusan (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 prinsipal yang memanggil AWS layanan, dikombinasikan dengan layanan yang meminta untuk membuat permintaan ke AWS layanan hilir. Permintaan FAS hanya dibuat ketika layanan menerima permintaan yang memerlukan interaksi dengan AWS layanan atau sumber daya lain untuk diselesaikan. Dalam hal ini, Anda harus memiliki izin untuk melakukan kedua tindakan tersebut. Untuk detail kebijakan ketika mengajukan permintaan FAS, lihat [Sesi akses terusan](#).

Pemecahan masalah Respons Insiden Keamanan AWS identitas dan akses

Gunakan informasi berikut untuk membantu Anda mendiagnosis dan memperbaiki masalah umum yang mungkin Anda temui saat bekerja dengan AWS Security Incident Response dan IAM.

Topik

- Saya tidak berwenang untuk melakukan suatu tindakan
- Saya tidak berwenang untuk melakukan iam: PassRole
- Saya ingin mengizinkan orang di luar AWS akun saya untuk mengakses Respons Insiden Keamanan AWS sumber daya saya

Saya tidak berwenang untuk melakukan suatu tindakan

Jika Anda menerima pesan kesalahan bahwa Anda tidak memiliki otorisasi untuk melakukan tindakan, kebijakan Anda harus diperbarui agar Anda dapat melakukan tindakan tersebut.

Contoh kesalahan berikut terjadi ketika pengguna IAM `mateojackson` mencoba menggunakan konsol untuk melihat detail tentang sumber daya `my-example-widget` fiksi tetapi tidak memiliki izin Security Incident Response: fiksi. `AWS GetWidget`

User: `arn ::iam: :123456789012 AWS: user/mateojackson` tidak berwenang untuk melakukan:: on resource: `my -example-widget` Respons Insiden Keamanan AWS `GetWidget`

Dalam hal ini, kebijakan untuk pengguna `mateojackson` harus diperbarui untuk mengizinkan akses ke sumber daya `my-example-widget` dengan menggunakan tindakan:. Respons Insiden Keamanan AWS `GetWidget`

Jika Anda memerlukan bantuan, hubungi AWS administrator Anda. Administrator Anda adalah orang yang memberi Anda kredensial masuk.

Saya tidak berwenang untuk melakukan **iam:PassRole** Jika Anda menerima kesalahan bahwa Anda tidak berwenang untuk melakukan `iam:PassRole` tindakan, kebijakan Anda harus diperbarui agar Anda dapat meneruskan peran Respons Insiden Keamanan AWS .

Beberapa AWS layanan 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 AWS Security Incident Response. Namun, tindakan tersebut memerlukan layanan untuk mendapatkan izin yang diberikan oleh peran layanan. Mary tidak memiliki izin untuk meneruskan peran tersebut pada layanan.

Pengguna: `arn ::iam:AWS:123456789012: tidak berwenang untuk melakukan: user/marymajor 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 mengizinkan orang di luar AWS akun saya untuk mengakses Respons Insiden Keamanan AWS sumber daya 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 mempelajari selengkapnya, periksa referensi berikut:

- Untuk mengetahui apakah Amazon Respons Insiden Keamanan AWS mendukung fitur ini, lihat [Cara Respons Insiden AWS Keamanan bekerja dengan IAM](#).
- Untuk mempelajari cara menyediakan akses ke sumber daya Anda di seluruh AWS akun yang Anda miliki, lihat [Menyediakan akses ke pengguna IAM di AWS akun lain yang Anda miliki](#) di Panduan Pengguna IAM.
- Untuk mempelajari cara menyediakan akses ke sumber daya Anda ke AWS akun pihak ketiga, lihat [Menyediakan akses ke AWS akun yang dimiliki oleh pihak ketiga](#) di 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](#).

Menggunakan peran layanan

Mendukung peran layanan: Tidak

Peran layanan adalah [peran IAM](#) yang diambil oleh sebuah layanan untuk melakukan tindakan atas nama Anda. Administrator IAM dapat membuat, mengubah, dan menghapus peran layanan dari dalam IAM. Untuk informasi selengkapnya, lihat [Membuat peran untuk mendelegasikan izin ke AWS layanan di Panduan](#) Pengguna IAM.

Menggunakan Peran Terkait Layanan

Service-linked peran untuk Respons Insiden Keamanan AWS

Topik

- [AWS SLR: AWSServiceRoleForSecurityIncidentResponse](#)
- [AWS SLR: _Triase AWSServiceRoleForSecurityIncidentResponse](#)
- [Wilayah yang didukung untuk Respons Insiden Keamanan AWS peran terkait layanan](#)

Mendukung peran terkait layanan: Ya

Peran terkait layanan adalah jenis peran layanan yang ditautkan ke layanan. AWS Layanan dapat mengambil peran untuk melakukan tindakan atas nama Anda. Service-linked peran muncul di AWS akun Anda dan dimiliki oleh layanan. AWS Identity and Access Management Administrator dapat melihat, tetapi tidak mengedit izin untuk peran terkait layanan.

Peran terkait layanan membuat pengaturan Respons Insiden Keamanan AWS lebih mudah karena Anda tidak perlu menambahkan izin yang diperlukan secara manual. Respons Insiden Keamanan AWS mendefinisikan izin peran terkait layanan, dan kecuali ditentukan lain, hanya Respons Insiden Keamanan AWS dapat mengambil perannya. Izin yang ditentukan mencakup kebijakan kepercayaan dan kebijakan izin, serta bahwa kebijakan izin tidak dapat dilampirkan ke entitas IAM lainnya.

Untuk informasi tentang layanan lain yang mendukung peran terkait layanan, lihat [AWS layanan yang bekerja dengan IAM](#) dan cari layanan yang memiliki Ya di kolom peran. Service-linked Pilih Ya dengan sebuah tautan untuk melihat dokumentasi peran terkait layanan untuk layanan tersebut.

AWS SLR: AWSServiceRoleForSecurityIncidentResponse

Respons Insiden Keamanan AWS menggunakan Respons Insiden Keamanan AWS kebijakan peran terkait layanan (SLR) bernama AWSServiceRoleForSecurityIncidentResponse — untuk mengidentifikasi akun yang dilanggan, membuat kasus, dan menandai sumber daya terkait.

Izin

Peran AWSServiceRoleForSecurityIncidentResponse terkait layanan mempercayai layanan berikut untuk mengambil peran:

- `security-ir.amazonaws.com`

Terlampir pada peran ini adalah kebijakan AWS terkelola bernama [AWSSecurityIncidentResponseServiceRolePolicy](#). Layanan menggunakan peran untuk melakukan tindakan pada sumber daya berikut:

- **AWS Organizations:** Memungkinkan layanan untuk mencari akun keanggotaan untuk digunakan dengan layanan.
- **CreateCase:** Memungkinkan layanan membuat kasus layanan atas nama akun keanggotaan.
- **ListCases:** Memungkinkan agen AI layanan untuk melihat kasus untuk tujuan penyelidikan keamanan.
- **UpdateCase:** Memungkinkan agen AI layanan untuk memperbarui metadata kasus.
- **CreateCaseComment:** Memungkinkan agen AI layanan untuk memposting hasilnya sebagai komentar kasus.
- **ListComments:** Memungkinkan agen AI layanan untuk melihat komentar kasus yang diperlukan untuk melakukan penyelidikan otomatis.

- **TagResource:** Memungkinkan sumber daya tag layanan yang dikonfigurasi sebagai bagian dari layanan.

Mengelola peran

Anda tidak perlu membuat peran terkait layanan secara manual. Saat Anda melakukan onboard ke Respons Insiden Keamanan AWS dalam Konsol Manajemen AWS, the AWS CLI, atau AWS API, layanan akan membuat peran terkait layanan untuk Anda.

Jika Anda menghapus peran terkait layanan ini, dan ingin membuatnya lagi, Anda dapat mengulangi proses yang sama untuk membuat kembali peran tersebut di akun Anda. Ketika Anda onboard ke layanan, itu menciptakan peran terkait layanan untuk Anda lagi.

Anda harus mengonfigurasi izin agar entitas IAM (seperti pengguna, grup, atau peran) dapat membuat, mengedit, atau menghapus peran terkait layanan. Untuk informasi selengkapnya, lihat [izin Service-linked peran](#) di Panduan Pengguna IAM.

AWS SLR: `_Triase AWSServiceRoleForSecurityIncidentResponse`

Respons Insiden Keamanan AWS menggunakan peran terkait layanan (SLR) bernama `AWSServiceRoleForSecurityIncidentResponse _Triage` — Respons Insiden Keamanan AWS kebijakan untuk terus memantau lingkungan Anda dari ancaman keamanan, menyesuaikan layanan keamanan untuk mengurangi kebisingan peringatan, dan mengumpulkan informasi untuk menyelidiki potensi insiden.

Izin

Peran terkait layanan `AWSServiceRoleForSecurityIncidentResponse _Triage` mempercayai layanan berikut untuk mengambil peran:

- `trriage.security-ir.amazonaws.com`

Terlampir pada peran ini adalah kebijakan yang AWS dikelola [AWSSecurityIncidentResponseTriageServiceRolePolicy](#). Layanan menggunakan peran untuk melakukan tindakan pada sumber daya berikut:

- **Acara:** Memungkinkan layanan untuk membuat aturan Amazon EventBridge terkelola. Aturan ini adalah infrastruktur yang diperlukan di AWS akun Anda untuk mengirimkan acara dari

akun Anda ke layanan. Tindakan ini dilakukan pada AWS sumber daya apa pun yang dikelola oleh `trriage.security-ir.amazonaws.com`.

- Amazon GuardDuty: Memungkinkan layanan untuk menyetel layanan keamanan untuk mengurangi kebisingan peringatan, mengumpulkan informasi untuk menyelidiki potensi insiden, dan memulai pemindaian GuardDuty malware.
- AWS Security Hub CSPM: Memungkinkan layanan untuk daftar standar yang diaktifkan dan integrasi produk, daftar anggota organisasi dan akun admin, dan menyetel layanan keamanan untuk mengurangi kebisingan peringatan dan mengumpulkan informasi untuk menyelidiki potensi insiden.
- AWS Identity and Access Management: Memungkinkan layanan untuk mengambil informasi peran untuk peran `AWSRoleForAmazonGuardDutyMalwareProtection` terkait layanan untuk memverifikasi apakah GuardDuty MalwareProtection dikonfigurasi.
- Respons Insiden Keamanan AWS: Memungkinkan layanan untuk membuat dan memperbarui kasus dan menandai sumber daya, terbatas pada sumber daya yang ditandai dengan `SecurityIncidentResponseManaged=true`. Memungkinkan layanan membaca informasi keanggotaan (`GetMembership`, `ListMemberships`).

Mengelola peran

Jika Anda melakukan [Respons Insiden Keamanan AWS onboard](#) Konsol Manajemen AWS, Security Incident Response secara otomatis membuat peran `AWSRoleForSecurityIncidentResponse_Triage` terkait layanan di akun AWS Organizations manajemen Anda dan di semua akun yang berada dalam cakupan. Jika Anda melakukan onboarding menggunakan API/CLI, maka Anda harus membuat peran secara manual. Untuk informasi selengkapnya, lihat [Aktifkan Respons Insiden Keamanan dan konfigurasi tim respons insiden Anda menggunakan API/CLI](#).

Jika Anda menghapus peran terkait layanan ini, dan kemudian perlu membuatnya lagi, Anda dapat menggunakannya API/CLI untuk membuat ulang peran di akun Anda.

Anda harus mengonfigurasi izin agar entitas IAM (seperti pengguna, grup, atau peran) dapat membuat, mengedit, atau menghapus peran terkait layanan. Untuk informasi selengkapnya, lihat [izin Service-linked peran](#) di Panduan Pengguna IAM.

Wilayah yang didukung untuk Respons Insiden Keamanan AWS peran terkait layanan

Respons Insiden Keamanan AWS mendukung penggunaan peran terkait layanan di semua wilayah tempat layanan tersedia.

- AS Timur (Ohio)
- AS Barat (Oregon)
- AS Timur (Virginia)
- Eropa (Frankfurt)
- Eropa (Irlandia)
- Eropa (London)
- Eropa (Milan)
- Eropa (Paris)
- Eropa (Spanyol)
- Eropa (Stockholm)
- Europe (Zurich)
- Asia Pasifik (Hong Kong)
- Asia Pasifik (Hyderabad)
- Asia Pasifik (Jakarta)
- Asia Pasifik (Melbourne)
- Asia Pasifik (Mumbai)
- Asia Pasifik (Seoul)
- Asia Pasifik (Singapura)
- Asia Pasifik (Sydney)
- Asia Pasifik (Tokyo)
- (Canada (Central))
- Timur Tengah (Bahrain)
- Timur Tengah (UEA)
- Amerika Selatan (Sao Paulo)

- [Africa \(Cape Town\)](#)

AWS Kebijakan Terkelola

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.

Untuk menambahkan izin ke pengguna, grup, dan peran, lebih mudah menggunakan kebijakan AWS terkelola daripada menulis kebijakan sendiri. Dibutuhkan waktu dan keahlian untuk [membuat kebijakan yang dikelola pelanggan IAM](#) yang hanya memberi tim Anda izin yang mereka butuhkan. Untuk memulai dengan cepat, Anda dapat menggunakan kebijakan AWS terkelola kami. Kebijakan ini mencakup kasus penggunaan umum dan tersedia di AWS akun Anda. Untuk informasi selengkapnya tentang kebijakan AWS [AWS terkelola, lihat kebijakan terkelola](#) di Panduan Pengguna IAM.

AWS layanan memelihara dan memperbarui kebijakan AWS terkelola terkait. Anda tidak dapat mengubah izin dalam kebijakan AWS terkelola. Layanan terkadang menambahkan izin tambahan ke kebijakan yang dikelola AWS untuk mendukung fitur-fitur baru. Jenis pembaruan ini akan memengaruhi semua identitas (pengguna, grup, dan peran) di mana kebijakan tersebut dilampirkan. Layanan kemungkinan besar akan memperbarui kebijakan yang dikelola AWS saat ada fitur baru yang diluncurkan atau saat ada operasi baru yang tersedia. Layanan tidak menghapus izin dari kebijakan AWS terkelola, sehingga pembaruan kebijakan tidak akan merusak izin yang ada.

Selain itu, AWS mendukung kebijakan terkelola untuk fungsi pekerjaan yang mencakup beberapa layanan. Misalnya, kebijakan ReadOnlyAccess AWS terkelola menyediakan akses hanya-baca ke semua AWS layanan dan sumber daya. Saat layanan meluncurkan fitur baru, AWS tambahkan izin hanya-baca untuk operasi dan sumber daya baru. Untuk melihat daftar dan deskripsi dari kebijakan fungsi tugas, lihat [kebijakan yang dikelola AWS untuk fungsi tugas](#) di Panduan Pengguna IAM.

Topik

- [AWS kebijakan terkelola: AWSSecurityIncidentResponseServiceRolePolicy](#)
- [AWS kebijakan terkelola: AWSSecurityIncidentResponseFullAccess](#)
- [AWS kebijakan terkelola: AWSSecurityIncidentResponseReadOnlyAccess](#)
- [AWS kebijakan terkelola: AWSSecurityIncidentResponseCaseFullAccess](#)
- [AWS kebijakan terkelola: AWSSecurityIncidentResponseTriageServiceRolePolicy](#)
- [Respons Insiden Keamanan AWS pembaruan ke SLR dan kebijakan terkelola](#)

AWS kebijakan terkelola: [AWSSecurityIncidentResponseServiceRolePolicy](#)

Respons Insiden Keamanan AWS menggunakan kebijakan [AWSSecurityIncidentResponseServiceRolePolicy](#) AWS terkelola. Kebijakan AWS terkelola ini dilampirkan pada peran [AWSServiceRoleForSecurityIncidentResponse](#) terkait layanan. Kebijakan ini menyediakan akses Respons Insiden Keamanan AWS untuk mengidentifikasi akun yang dilangan, membuat kasus, memperbarui kasus, membuat komentar kasus, daftar kasus, daftar komentar kasus, dan menandai sumber daya terkait.

Important

Jangan menyimpan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Respons Insiden Keamanan AWS menggunakan tag untuk memberi Anda layanan administrasi. Tag tidak dimaksudkan untuk digunakan untuk data pribadi atau sensitif

Rincian izin

Layanan menggunakan kebijakan ini untuk melakukan tindakan pada sumber daya berikut:

- **AWS Organizations:** Memungkinkan layanan untuk mencari akun keanggotaan untuk digunakan dengan layanan.
- **CreateCase:** Memungkinkan layanan membuat kasus layanan atas nama akun keanggotaan.
- **ListCases:** Memungkinkan agen AI layanan untuk melihat kasus untuk tujuan penyelidikan keamanan.
- **UpdateCase:** Memungkinkan agen AI layanan untuk memperbarui metadata kasus.
- **CreateCaseComment:** Memungkinkan agen AI layanan untuk memposting hasilnya sebagai komentar kasus.
- **ListComments:** Memungkinkan agen AI layanan untuk melihat komentar kasus yang diperlukan untuk melakukan penyelidikan otomatis.
- **TagResource:** Memungkinkan sumber daya tag layanan yang dikonfigurasi sebagai bagian dari layanan.

Anda dapat melihat izin yang terkait dengan kebijakan ini dalam kebijakan AWS terkelola untuk [AWSSecurityIncidentResponseServiceRolePolicy](#).

AWS kebijakan terkelola: AWSSecurityIncidentResponseFullAccess

Respons Insiden Keamanan AWS menggunakan kebijakan AWSSecurityIncidentResponseAdmin AWS terkelola. Kebijakan ini memberikan akses penuh ke sumber daya layanan dan akses ke yang terkait Layanan AWS. Anda dapat menggunakan kebijakan ini dengan prinsipal IAM Anda untuk menambahkan izin dengan cepat. Respons Insiden Keamanan AWS

Important

Jangan menyimpan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Respons Insiden Keamanan AWS menggunakan tag untuk memberi Anda layanan administrasi. Tag tidak dimaksudkan untuk digunakan untuk data pribadi atau sensitif

Rincian izin

Layanan menggunakan kebijakan ini untuk melakukan tindakan pada sumber daya berikut:

- Akses read-only utama IAM: Memberi pengguna layanan kemampuan untuk melakukan tindakan hanya-baca terhadap sumber daya yang ada. Respons Insiden Keamanan AWS
- Akses tulis utama IAM: Memberikan pengguna layanan kemampuan untuk memperbarui, memodifikasi, menghapus, dan membuat Respons Insiden Keamanan AWS sumber daya.

Anda dapat melihat izin yang terkait dengan kebijakan ini dalam kebijakan AWS terkelola untuk [AWSSecurityIncidentResponseFullAccess](#).

AWS kebijakan terkelola: AWSSecurityIncidentResponseReadOnlyAccess

Respons Insiden Keamanan AWS menggunakan kebijakan AWSSecurityIncidentResponseReadOnlyAccess AWS terkelola. Kebijakan ini memberikan akses hanya-baca ke sumber daya kasus layanan. Anda dapat menggunakan kebijakan ini dengan prinsipal IAM Anda untuk menambahkan izin dengan cepat. Respons Insiden Keamanan AWS

Important

Jangan menyimpan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Respons Insiden Keamanan AWS menggunakan tag untuk memberi Anda layanan administrasi. Tag tidak dimaksudkan untuk digunakan untuk data pribadi atau sensitif

Rincian izin

Layanan menggunakan kebijakan ini untuk melakukan tindakan pada sumber daya berikut:

- Akses read-only utama IAM: Memberi pengguna layanan kemampuan untuk melakukan tindakan hanya-baca terhadap sumber daya yang ada. Respons Insiden Keamanan AWS

Anda dapat melihat izin yang terkait dengan kebijakan ini dalam kebijakan AWS terkelola untuk [AWSSecurityIncidentResponseReadOnlyAccess](#).

AWS kebijakan terkelola: AWSSecurityIncidentResponseCaseFullAccess

Respons Insiden Keamanan AWS menggunakan kebijakan AWSSecurityIncidentResponseCaseFullAccess AWS terkelola. Kebijakan ini memberikan akses penuh ke sumber daya kasus layanan. Anda dapat menggunakan kebijakan ini dengan prinsipal IAM Anda untuk menambahkan izin dengan cepat. Respons Insiden Keamanan AWS

Important

Jangan menyimpan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Respons Insiden Keamanan AWS menggunakan tag untuk memberi Anda layanan administrasi. Tag tidak dimaksudkan untuk digunakan untuk data pribadi atau sensitif

Rincian izin

Layanan menggunakan kebijakan ini untuk melakukan tindakan pada sumber daya berikut:

- Akses hanya-baca kasus utama IAM: Memberi pengguna layanan kemampuan untuk melakukan tindakan hanya-baca terhadap kasus yang ada. Respons Insiden Keamanan AWS
- Akses tulis kasus utama IAM: Memberikan pengguna layanan kemampuan untuk memperbarui, memodifikasi, menghapus, dan membuat Respons Insiden Keamanan AWS kasus.

Anda dapat melihat izin yang terkait dengan kebijakan ini dalam kebijakan AWS terkelola untuk [AWSSecurityIncidentResponseCaseFullAccess](#).

AWS kebijakan terkelola:

AWSSecurityIncidentResponseTriageServiceRolePolicy

Respons Insiden Keamanan AWS menggunakan kebijakan AWSSecurityIncidentResponseTriageServiceRolePolicy AWS terkelola. Kebijakan AWS terkelola ini dilampirkan ke peran terkait layanan [AWSServiceRoleForSecurityIncidentResponse_Triage](#).

Kebijakan ini menyediakan akses Respons Insiden Keamanan AWS untuk terus memantau lingkungan Anda untuk ancaman keamanan, menyesuaikan layanan keamanan untuk mengurangi kebisingan peringatan, dan mengumpulkan informasi untuk menyelidiki potensi insiden. Anda tidak dapat melampirkan kebijakan ini ke entitas IAM Anda.

Important

Jangan menyimpan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Respons Insiden Keamanan AWS menggunakan tag untuk memberi Anda layanan administrasi. Tag tidak dimaksudkan untuk digunakan untuk data pribadi atau sensitif

Rincian izin

Layanan menggunakan kebijakan ini untuk melakukan tindakan pada sumber daya berikut:

- **Acara:** Memungkinkan layanan untuk membuat aturan EventBridge terkelola Amazon. Aturan ini adalah infrastruktur yang diperlukan di AWS akun Anda untuk mengirimkan acara dari akun Anda ke layanan. Tindakan ini dilakukan pada AWS sumber daya apa pun yang dikelola oleh `trriage.security-ir.amazonaws.com`.
- **Amazon GuardDuty:** Memungkinkan layanan untuk menyetel layanan keamanan untuk mengurangi kebisingan peringatan, mengumpulkan informasi untuk menyelidiki potensi insiden, dan memulai pemindaian GuardDuty malware.
- **AWS Security Hub CSPM:** Memungkinkan layanan untuk daftar standar yang diaktifkan dan integrasi produk, daftar anggota organisasi dan akun admin, dan menyetel layanan keamanan untuk mengurangi kebisingan peringatan dan mengumpulkan informasi untuk menyelidiki potensi insiden.
- **AWS Identity and Access Management:** Memungkinkan layanan untuk mengambil informasi peran untuk peran `AWSServiceRoleForAmazonGuardDutyMalwareProtection` terkait layanan untuk memverifikasi apakah GuardDuty MalwareProtection dikonfigurasi.

- Respons Insiden Keamanan AWS: Memungkinkan layanan untuk membuat dan memperbarui kasus dan menandai sumber daya, terbatas pada sumber daya yang ditandai dengan `SecurityIncidentResponseManaged=true`. Memungkinkan layanan membaca informasi keanggotaan (`GetMembership`, `ListMemberships`).

Anda dapat melihat izin yang terkait dengan kebijakan ini dalam kebijakan AWS terkelola untuk [AWSSecurityIncidentResponseTriageServiceRolePolicy](#).

Respons Insiden Keamanan AWS pembaruan ke SLR dan kebijakan terkelola

Lihat detail tentang pembaruan Respons Insiden Keamanan AWS SLR dan peran kebijakan terkelola sejak layanan ini mulai melacak perubahan ini.

Ubah	Deskripsi	Date
Diperbarui - AWSSecurityIncidentResponseReadOnlyAccess	Kebijakan sekarang termasuk <code>security-ir:ListInvestigations</code> tindakan.	April 22, 2026
Diperbarui - AWSSecurityIncidentResponseFullAccess	Kebijakan ini sekarang menggunakan <code>security-ir:*</code> alih-alih mencantumkan <code>security-ir</code> tindakan eksplisit. Delapan AWS Organizations izin baru ditambahkan (<code>organizations:ListAWSServiceAccessForOrganization</code> , <code>organizations:ListRoots</code> , <code>organizations:ListOrganizationalUnitsForParent</code> , <code>organizations:ListAccountsForParent</code> , <code>organizations:ListChildren</code> , <code>organizations:DescribeOrganizationalUnit</code> , <code>organizations:ListAccounts</code> , dan <code>organizations:DescribeAccount</code>) untuk mendukung pemilih akun konsol saat memperbarui asosiasi. Kondisi MFA telah dihapus.	April 22, 2026

Ubah	Deskripsi	Date
Diperbarui - AWS Security Incident Response Case Full Access	Kebijakan tersebut sekarang mencakup dua tindakan baru: <code>security-ir:ListInvestigations</code> dan <code>security-ir:SendFeedback</code> . Kondisi MFA telah dihapus.	April 22, 2026
Diperbarui - AWS Security Incident Response Triage Service Role Policy	Kebijakan ini sekarang memungkinkan layanan untuk memodifikasi GuardDuty filter yang ditandai dengan <code>SecurityIncidentResponseManaged=true</code> , untuk memperbarui konfigurasi detektor, dan untuk memulai GuardDuty pemindaian malware. Ini memungkinkan layanan untuk membuat dan mengelola aturan yang secara otomatis bertindak atas temuan CSPM Security Hub, dan untuk memahami struktur organisasi.	Maret 27, 2026
Diperbarui - AWS Security Incident Response Service Role Policy	Kebijakan sekarang melakukan tindakan pada sumber daya berikut: <p>ListCases: Memungkinkan agen AI layanan untuk melihat kasus untuk tujuan investigasi keamanan</p> <p>UpdateCase: Memungkinkan agen AI layanan untuk memperbarui metadata kasus.</p> <p>CreateCaseComment: Memungkinkan agen AI layanan untuk memposting hasilnya sebagai komentar kasus</p> <p>ListComments: Memungkinkan agen AI layanan untuk melihat komentar kasus yang diperlukan untuk melakukan investigasi otomatis</p>	November 2025

Ubah	Deskripsi	Date
<p>Diperbarui - AWS Security Incident Response Service Role Policy</p>	<p>Kebijakan tersebut sekarang mencakup dua tindakan baru untuk "organizations:DescribeAccount" , "organizations:ListDelegatedAdministrators" dan kondisi baru:</p> <pre data-bbox="402 424 1218 823"> "Condition": { "StringEquals": { "aws:ResourceAccount": "\${aws:PrincipalAccount}" } }</pre>	<p>November 2025</p>
<p>Pembaruan untuk SLR menambahkan izin untuk mendukung hak layanan.</p>	<p>AWS Security Incident Response Triage Service Role Policy telah diperbarui untuk menambahkan security-ir:GetMembership, security-ir:, security-ir:ListMemberships, guardduty:, guardduty:, guardduty:UpdateCase, dan guardduty: ListFilters izin. guardduty: UpdateFilter ditambahkan untuk memfasilitasi pengelolaan filter di DeleteFilter akun yang didelegasikan. GetAdministratorAccount GetAdministratorAccount GuardDuty Auto-Archival</p>	<p>02 Juni 2025</p>

Ubah	Deskripsi	Date
<p>SLR baru — AWSServiceRoleForSecurityIncidentResponse</p> <p>Kebijakan terkelola baru — AWSSecurityIncidentResponseServiceRolePolicy.</p>	<p>Peran terkait layanan baru dan kebijakan terlampir yang memungkinkan akses layanan ke AWS Organizations akun Anda untuk mengidentifikasi keanggotaan.</p>	<p>Desember 1, 2024</p>
<p>SLR Baru - _TriageAWSServiceRoleForSecurityIncidentResponse</p> <p>Kebijakan terkelola baru - AWSSecurityIncidentResponseTriageServiceRolePolicy</p>	<p>Peran terkait layanan baru dan kebijakan terlampir yang memungkinkan akses layanan ke AWS Organizations akun Anda untuk melakukan triase peristiwa keamanan.</p>	<p>Desember 1, 2024</p>
<p>Kebijakan terkelola baru - AWSSecurityIncidentResponseFullAccess</p>	<p>Respons Insiden Keamanan AWS tambahkan SLR baru untuk dilampirkan ke prinsipal IAM untuk tindakan baca dan tulis untuk layanan.</p>	<p>Desember 1, 2024</p>

Ubah	Deskripsi	Date
Peran kebijakan terkelola baru - AWSSecurityIncidentResponseReadOnlyAccess	Respons Insiden Keamanan AWS tambahkan SLR baru untuk dilampirkan ke prinsip IAM untuk tindakan baca	Desember 1, 2024
Peran kebijakan terkelola baru - AWSSecurityIncidentResponseCaseFullAccess	Respons Insiden Keamanan AWS tambahkan SLR baru untuk dilampirkan ke prinsip IAM untuk tindakan baca dan tulis untuk kasus layanan.	Desember 1, 2024
Mulai melacak perubahan.	Mulai melacak perubahan untuk Respons Insiden Keamanan AWS SLR dan kebijakan terkelola	Desember 1, 2024

Respons insiden

Keamanan dan Kepatuhan adalah tanggung jawab bersama antara AWS dan pelanggan. Model bersama ini dapat membantu meringankan beban operasional pelanggan saat AWS mengoperasikan, mengelola, dan mengontrol komponen dari sistem operasi host dan lapisan virtualisasi hingga keamanan fisik fasilitas tempat layanan beroperasi. Pelanggan memikul tanggung jawab dan pengelolaan sistem operasi tamu (termasuk pembaruan dan patch keamanan), perangkat lunak aplikasi terkait lainnya serta konfigurasi firewall grup keamanan yang AWS disediakan. Untuk informasi tambahan lihat [model tanggung jawab AWS bersama](#).

Dengan menetapkan garis dasar keamanan yang memenuhi tujuan aplikasi Anda yang berjalan di cloud, Anda dapat mendeteksi penyimpangan yang dapat Anda tanggapi. Karena respons insiden keamanan dapat menjadi topik yang kompleks, kami mendorong Anda untuk meninjau sumber daya berikut sehingga Anda lebih dapat memahami dampak respons insiden dan pilihan Anda terhadap tujuan perusahaan Anda: whitepaper [Praktik Terbaik AWS Keamanan](#), dan white paper [Perspektif Keamanan AWS Cloud Adoption Framework](#) (CAF).

Validasi kepatuhan

Third-party auditor menilai keamanan dan kepatuhan AWS layanan sebagai bagian dari beberapa program AWS kepatuhan. Program ini mencakup SOC, PCI, FedRAMP, HIPAA, dan lainnya.

Untuk daftar AWS layanan dalam lingkup program kepatuhan tertentu, lihat [AWS layanan dalam lingkup oleh program kepatuhan](#). Untuk informasi umum, lihat program AWS kepatuhan.

Anda dapat mengunduh laporan audit pihak ketiga menggunakan AWS Artifact. Untuk informasi selengkapnya, lihat [Mengunduh laporan di AWS Artifak](#).

Tanggung jawab kepatuhan Anda saat menggunakan AWS layanan ditentukan oleh sensitivitas data Anda, tujuan kepatuhan perusahaan Anda, dan hukum dan peraturan yang berlaku. AWS menyediakan sumber daya berikut untuk membantu kepatuhan:

- [Panduan memulai cepat keamanan dan kepatuhan — Panduan](#) penerapan ini membahas pertimbangan arsitektur dan memberikan langkah-langkah untuk menerapkan lingkungan dasar yang berfokus pada keamanan dan kepatuhan. AWS
- [Arsitektur untuk whitepaper keamanan dan kepatuhan HIPAA — Whitepaper](#) ini menjelaskan bagaimana perusahaan dapat menggunakan untuk membuat aplikasi. AWS HIPAA-compliant
- [AWS sumber daya kepatuhan](#) - Kumpulan buku kerja dan panduan yang berlaku berdasarkan and/or lokasi industri.
- [Mengevaluasi sumber daya dengan Aturan AWS Config](#) dalam Panduan Pengembang AWS Config — AWS Config; menilai seberapa baik konfigurasi sumber daya Anda mematuhi praktik internal, pedoman industri, dan peraturan.
- [AWS Security Hub](#) — AWS Layanan ini memberikan pandangan komprehensif tentang status keamanan Anda di dalamnya AWS. Security Hub menggunakan kontrol keamanan untuk mengevaluasi AWS sumber daya Anda dan 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](#) — AWS Layanan ini mendeteksi potensi ancaman terhadap AWS akun, beban kerja, 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](#) — AWS Layanan ini membantu Anda terus mengaudit AWS penggunaan Anda untuk menyederhanakan cara Anda mengelola risiko dan kepatuhan terhadap peraturan dan standar industri.

Tanggung jawab bersama untuk kepatuhan

Tanggung jawab kepatuhan Anda saat menggunakan Respons Insiden Keamanan AWS tergantung pada sensitivitas data Anda, tujuan kepatuhan perusahaan Anda, dan hukum dan peraturan yang berlaku. AWS menyediakan Security Incident Response sebagai alat untuk membantu Anda menyelidiki dan menanggapi insiden keamanan. Anda tetap bertanggung jawab untuk hal-hal berikut:

- Menentukan apakah Respons Insiden Keamanan sesuai dengan persyaratan kepatuhan Anda.
- Mengkonfigurasi Respons Insiden Keamanan sesuai dengan kebijakan Anda.
- Memastikan penggunaan Security Incident Response Anda mematuhi peraturan yang berlaku.

Metadata sebagai data yang diatur

Meskipun Security Incident Response tidak mengumpulkan data aplikasi Anda, metadata yang dikumpulkannya mungkin termasuk dalam persyaratan kepatuhan Anda. Organizations harus mengevaluasi hal-hal berikut:

- Apakah nama sumber daya dan pengidentifikasi merupakan data yang diatur.
- Apakah log kueri DNS berisi informasi pribadi.
- Apakah pola panggilan API mengungkapkan informasi bisnis yang dilindungi.

Konsultasikan dengan tim hukum dan kepatuhan Anda untuk menentukan bagaimana metadata Respons Insiden Keamanan harus diklasifikasikan berdasarkan peraturan yang berlaku.

Penebangan dan pemantauan di AWS Respon Insiden Keamanan

Pemantauan adalah bagian penting dari menjaga keandalan, ketersediaan, dan kinerja Respons Insiden Keamanan AWS dan AWS solusi Anda yang lain. Respons Insiden Keamanan AWS saat ini mendukung AWS layanan berikut untuk memantau organisasi Anda dan aktivitas yang terjadi di dalamnya.

AWS CloudTrail — Dengan CloudTrail Anda dapat menangkap panggilan API dari konsol AWS Security Incident Response. Misalnya, ketika pengguna mengautentikasi, CloudTrail dapat merekam detail seperti alamat IP dalam permintaan, siapa yang membuat permintaan, dan kapan itu dibuat.

Amazon CloudWatch Metrics — Dengan CloudWatch metrik, Anda dapat memantau, melaporkan, dan mengambil tindakan otomatis jika terjadi peristiwa dalam waktu dekat. Misalnya, Anda dapat membuat CloudWatch dasbor pada metrik yang disediakan untuk memantau Respons Insiden Keamanan AWS penggunaan Anda, atau Anda dapat membuat CloudWatch alarm pada metrik yang disediakan untuk memberi tahu Anda tentang pelanggaran ambang batas yang ditetapkan.

Namespace untuk layanan ini adalah `AWS/`. `Usage/ServiceName` Nama metrik yang tersedia adalah `ActiveManagedCases` dan `SelfManagedCases`.

Sesuai dengan [Ketentuan AWS Layanan](#), tim Respons Insiden Keamanan AWS responden akan memiliki akses ke riwayat, data log VPC CloudTrail, DNS, dan S3 Anda. Data ini dapat digunakan selama insiden keamanan aktif ketika kasus terbuka di portal layanan AWS Security Incident Response.

Ketahanan

Infrastruktur AWS global dibangun di sekitar AWS Wilayah dan Zona Ketersediaan. 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 AWS Wilayah dan Availability Zone, lihat [infrastruktur AWS global](#).

Keamanan infrastruktur

Respons Insiden Keamanan AWS 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 Respons Insiden Keamanan AWS melalui jaringan. Klien harus mendukung hal-hal berikut:

- Keamanan Lapisan Pengangkutan (TLS). Kami mensyaratkan TLS 1.2 dan menganjurkan TLS 1.3.
- Cipher suite dengan perfect forward secrecy (PFS) seperti DHE (Ephemeral) atau ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). 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 principal IAM. Atau Anda dapat menggunakan [AWS Security Token Service](#) (AWS STS) untuk menghasilkan kredensial keamanan sementara untuk menandatangani permintaan.

Konfigurasi dan analisis kerentanan

Anda bertanggung jawab untuk mengelola peran penahanan layanan dan kumpulan CloudFormation tumpukan terkait.

AWS menangani tugas-tugas keamanan dasar, seperti sistem operasi tamu (OS) dan patch database, konfigurasi firewall, dan pemulihan bencana. Prosedur ini telah ditinjau dan disertifikasi oleh pihak ketiga yang sesuai. Untuk detail selengkapnya, lihat AWS sumber daya berikut:

- [Model tanggung jawab bersama](#)
- [Praktik terbaik untuk keamanan, identitas, & kepatuhan](#)

Cross-service pencegahan wakil bingung

Masalah "confused deputy" adalah masalah keamanan di mana entitas yang tidak memiliki izin untuk melakukan tindakan dapat memengaruhi entitas yang memiliki hak akses lebih tinggi untuk melakukan tindakan. Pada tahun AWS, peniruan lintas layanan dapat mengakibatkan masalah wakil yang membingungkan. Cross-service peniruan identitas dapat terjadi ketika satu layanan (layanan panggilan) memanggil layanan lain (layanan yang disebut). Layanan pemanggilan dapat dimanipulasi menggunakan izinnya untuk bertindak pada sumber daya pelanggan lain dengan cara yang seharusnya tidak dilakukannya kecuali bila memiliki izin untuk mengakses. Untuk mencegah hal ini, AWS sediakan alat yang membantu Anda melindungi data Anda untuk semua layanan dengan prinsip layanan yang telah diberikan akses ke sumber daya di akun Anda.

Sebaiknya gunakan kunci konteks kondisi SourceAccount global [AWSAWS: SourceArn dan:](#) dalam kebijakan sumber daya untuk membatasi izin yang diberikan Amazon Connect kepada layanan

lain ke sumber daya. Jika Anda menggunakan kedua kunci konteks kondisi global, SourceAccount nilai AWS: dan akun dalam SourceArn nilai AWS: harus menggunakan ID akun yang sama saat digunakan dalam pernyataan kebijakan yang sama.

Cara paling efektif untuk melindungi dari masalah wakil yang membingungkan adalah dengan menggunakan Nama Sumber Daya Amazon (ARN) yang tepat dari sumber daya yang ingin Anda izinkan. Jika Anda tidak mengetahui ARN lengkap sumber daya atau jika Anda menentukan beberapa sumber daya, gunakan kunci kondisi konteks SourceArn global AWS: dengan wildcard (*) untuk bagian ARN yang tidak diketahui. Misalnya, arn ::servicename: :region-name AWS: :your account ID: *. AWS

Untuk contoh kebijakan peran asumsi yang menunjukkan bagaimana Anda dapat mencegah masalah wakil yang membingungkan, lihat [Kebijakan pencegahan wakil yang bingung](#).

Service Quotas

Respons Insiden Keamanan AWS

Panduan Referensi AWS Umum mencakup [Respons Insiden Keamanan AWS titik akhir dan kuota terbaru](#).

Respons Insiden Keamanan AWS Panduan Teknis

Daftar Isi

- [Abstrak](#)
- [Apakah Anda sudah Well-Architected?](#)
- [Pengantar](#)
- [Persiapan](#)
- [Operasi](#)
- [Aktivitas pascainsiden](#)
- [Kesimpulan](#)
- [Kontributor](#)
- [Lampiran A: Definisi kemampuan cloud](#)
- [Lampiran B: sumber daya respons AWS insiden](#)
- [Pemberitahuan](#)

Abstrak

Panduan ini menyajikan ikhtisar dasar-dasar menanggapi insiden keamanan dalam lingkungan Amazon Web Services (AWS) Cloud pelanggan. Panduan ini memberikan ikhtisar tentang keamanan cloud dan konsep respons insiden serta mengidentifikasi kemampuan, layanan, dan mekanisme cloud yang tersedia bagi pelanggan yang merespons masalah keamanan.

Panduan ini ditujukan bagi mereka yang memiliki peran teknis dan mengasumsikan bahwa Anda terbiasa dengan prinsip-prinsip umum keamanan informasi, memiliki pemahaman dasar tentang respons insiden keamanan di lingkungan lokal Anda saat ini, dan memiliki keakraban dengan layanan cloud.

Apakah Anda sudah Well-Architected?

[Kerangka Kerja AWS Well-Architected](#) membantu Anda memahami pro dan kontra dari keputusan yang Anda buat saat membangun sistem di cloud. Enam pilar dari Kerangka Kerja ini memungkinkan Anda mempelajari praktik terbaik arsitektural untuk merancang dan mengoperasikan sistem yang

andal, aman, efisien, hemat biaya, dan berkelanjutan. Menggunakan [AWS Well-Architected Tool](#), tersedia tanpa biaya di [AWS Well-Architected Tool konsol](#), Anda dapat meninjau beban kerja Anda terhadap praktik terbaik ini dengan menjawab serangkaian pertanyaan untuk setiap pilar.

Untuk panduan lebih lanjut dari para ahli dan praktik terbaik untuk arsitektur cloud Anda—referensi penerapan arsitektur, diagram, dan laporan resmi—lihat [Pusat Arsitektur AWS](#).

Pengantar

Keamanan adalah prioritas utama di AWS. AWS pelanggan mendapat manfaat dari pusat data dan arsitektur jaringan yang dibangun untuk membantu mendukung kebutuhan organisasi yang paling sensitif terhadap keamanan. AWS memiliki model tanggung jawab bersama: AWS mengelola keamanan cloud, dan pelanggan bertanggung jawab atas keamanan di cloud. Artinya, Anda memiliki kendali penuh atas implementasi keamanan Anda, termasuk akses ke beberapa alat dan layanan untuk membantu memenuhi tujuan keamanan Anda. Berbagai kemampuan ini membantu Anda menetapkan garis dasar keamanan untuk aplikasi yang berjalan di AWS Cloud.

Ketika terjadi penyimpangan dari garis dasar, misalnya karena kesalahan konfigurasi atau perubahan faktor eksternal, Anda perlu merespons dan menyelidikinya. Agar bisa melakukannya dengan baik, Anda perlu memahami konsep dasar respons insiden keamanan di lingkungan AWS Anda dan persyaratan untuk mempersiapkan, mendedukasi, dan melatih tim cloud sebelum masalah keamanan terjadi. Penting untuk mengetahui kontrol dan kemampuan mana yang dapat Anda gunakan, meninjau contoh topikal untuk mengatasi masalah potensial, dan mengidentifikasi metode remediasi yang menggunakan otomatisasi untuk meningkatkan kecepatan dan konsistensi respons. Selain itu, Anda harus memahami persyaratan kepatuhan dan peraturan karena hal ini berkaitan dengan pembuatan program respons insiden keamanan untuk memenuhi persyaratan tersebut.

Respons insiden keamanan bisa menjadi hal yang kompleks, jadi kami mendorong Anda untuk menerapkan pendekatan iteratif: mulai dengan layanan keamanan inti, bangun kemampuan deteksi dan respons dasar, kemudian kembangkan playbook untuk membuat pustaka awal mekanisme respons insiden yang dapat diiterasi dan ditingkatkan.

Sebelum Anda mulai

Sebelum Anda mulai belajar tentang respons insiden untuk peristiwa keamanan di AWS, biasakan diri Anda dengan standar dan kerangka kerja yang relevan untuk AWS keamanan dan respons insiden. Fondasi ini akan membantu Anda memahami konsep dan praktik terbaik yang disajikan dalam panduan ini.

AWS standar keamanan dan kerangka kerja

Untuk memulai, kami mendorong Anda untuk meninjau [Praktik Terbaik untuk Keamanan, Identitas, dan Kepatuhan, Pilar Keamanan - Kerangka Kerja AWS Well-Architected](#) dan [Perspektif Keamanan dari whitepaper Ikhtisar Cloud Adoption Framework AWS \(CAF\)](#). AWS

AWS CAF menyediakan panduan yang mendukung koordinasi antara berbagai bagian organisasi yang bergerak ke cloud. Panduan AWS CAF dibagi menjadi beberapa area fokus, yang disebut sebagai perspektif, yang relevan untuk membangun sistem TI berbasis cloud. Perspektif keamanan menjelaskan cara menerapkan program keamanan di seluruh alur kerja, salah satunya adalah respons insiden. Dokumen ini merupakan produk dari pengalaman kami bekerja dengan pelanggan untuk membantu mereka membangun kemampuan serta program respons insiden keamanan yang efektif dan efisien.

Standar dan kerangka kerja respons insiden industri

Whitepaper ini mengikuti standar respons insiden dan praktik terbaik dari [Computer Security Incident Handling Guide SP 800-61 r3](#), yang dibuat oleh National Institute of Standards and Technology (NIST). Membaca dan memahami konsep yang diperkenalkan oleh NIST adalah prasyarat yang bermanfaat. Konsep dan praktik terbaik dari panduan NIST ini akan diterapkan pada AWS teknologi dalam paper ini. Namun, skenario insiden on-premise tidak tercakup dalam panduan ini.

AWS ikhtisar respons insiden

Sebagai awal, penting untuk memahami bagaimana operasi keamanan dan respons insiden merupakan hal yang berbeda di cloud. Untuk membangun kemampuan respons yang efektif AWS, Anda perlu memahami penyimpangan dari respons lokal tradisional dan dampaknya terhadap program respons insiden Anda. Masing-masing perbedaan ini, serta prinsip desain respons AWS insiden inti, dirinci dalam bagian ini.

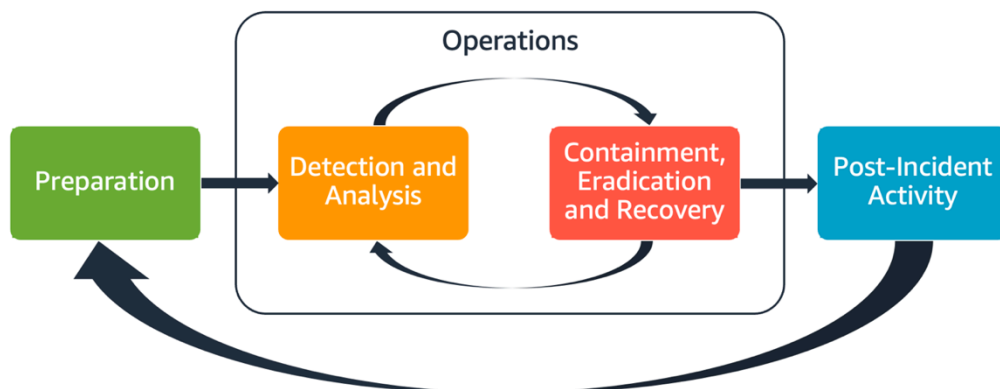
Aspek respon AWS insiden

Semua AWS pengguna dalam suatu organisasi harus memiliki pemahaman dasar tentang proses respons insiden keamanan, dan staf keamanan harus memahami bagaimana menanggapi masalah keamanan. Pendidikan, pelatihan, dan pengalaman sangat penting agar program respons insiden cloud berjalan dengan baik, dan idealnya diimplementasikan dengan baik sebelum harus menangani kemungkinan insiden keamanan. Fondasi program respons insiden yang baik di cloud adalah Persiapan, Operasi, dan Aktivitas Pascainsiden.

Untuk memahami setiap aspek ini, lihat deskripsi berikut:

- **Persiapan** — Siapkan tim respons insiden Anda untuk mendeteksi dan menanggapi insiden di dalamnya AWS dengan mengaktifkan kontrol detektif dan memverifikasi akses yang tepat ke alat dan layanan cloud yang diperlukan. Selain itu, siapkan playbook yang diperlukan, baik manual maupun otomatis, untuk memverifikasi respons yang andal dan konsisten.
- **Operasi** – Beroperasi pada peristiwa keamanan dan insiden potensial dengan mengikuti fase respons insiden NIST: mendeteksi, menganalisis, menahan, memberantas, dan memulihkan.
- **Aktivitas pascainsiden** – Lakukan iterasi pada hasil simulasi dan peristiwa keamanan Anda untuk meningkatkan efektivitas respons Anda, sehingga respons dan investigasi yang dilakukan bisa lebih bernilai, dan mengurangi risiko lebih lanjut. Anda harus belajar dari insiden dan memiliki sikap kepemilikan yang kuat terhadap aktivitas perbaikan.

Setiap aspek ini dikupas dan dibahas secara mendetail dalam panduan ini. Diagram berikut menunjukkan alur aspek-aspek ini, selaras dengan siklus hidup respons insiden NIST yang disebutkan sebelumnya, tetapi dengan operasi yang mencakup deteksi dan analisis dengan penahanan, pemberantasan, dan pemulihan.



Aspek respon AWS insiden

AWS prinsip respons insiden dan tujuan desain

Meskipun proses umum dan mekanisme respons insiden sebagaimana didefinisikan oleh [NIST SP 800-61 Computer Security Incident Handling Guide](#) sudah baik, kami mendorong Anda untuk juga mempertimbangkan tujuan desain spesifik ini, yang relevan untuk merespons insiden keamanan di lingkungan cloud:

- **Menetapkan tujuan respons** – Bekerja sama dengan pemangku kepentingan, penasihat hukum, dan kepemimpinan organisasi untuk menentukan tujuan dalam merespons suatu insiden. Beberapa tujuan umum termasuk menahan dan memitigasi masalah, memulihkan sumber daya

yang terkena dampak, menyimpan data untuk forensik, kembali ke operasi aman yang diketahui, dan belajar dari insiden.

- Merespons menggunakan cloud – Menerapkan pola respons di dalam cloud, tempat peristiwa dan data terjadi.
- Ketahui apa yang Anda miliki dan apa yang Anda butuhkan – Simpan log, sumber daya, snapshot, dan bukti lainnya dengan menyalin dan menyimpannya di akun cloud terpusat khusus untuk respons. Gunakan tag, metadata, dan mekanisme yang menerapkan kebijakan retensi. Anda harus memahami layanan apa yang Anda gunakan dan kemudian mengidentifikasi persyaratan untuk menyelidiki layanan tersebut. Untuk membantu Anda memahami lingkungan Anda, Anda juga dapat menggunakan tag, yang akan dibahas nanti dalam dokumen ini di bagian [the section called “Mengembangkan dan menerapkan strategi pemberian tag”](#).
- Gunakan mekanisme deployment ulang – Jika anomali keamanan dapat dikaitkan dengan kesalahan konfigurasi, remediasinya mungkin cukup dengan menghapus perbedaan konfigurasi ini dengan deployment ulang sumber daya menggunakan konfigurasi yang tepat. Jika teridentifikasi adanya kemungkinan penyusupan, verifikasi bahwa deployment ulang Anda mencakup mitigasi akar penyebab yang berhasil dan terverifikasi.
- Otomatiskan jika memungkinkan – Ketika masalah muncul atau insiden berulang, bangun mekanisme untuk melakukan triase secara terprogram dan merespons peristiwa umum. Gunakan respons manusia untuk insiden unik, kompleks, atau sensitif yang tidak cukup dengan otomatisasi.
- Pilih solusi yang dapat diskalakan – Berusahalah untuk mengimbangi skalabilitas pendekatan organisasi Anda terhadap komputasi cloud. Terapkan mekanisme deteksi dan respons yang dapat diskalakan di seluruh lingkungan Anda agar dapat memangkas waktu antara deteksi dan respons secara efektif.
- Pelajari dan tingkatkan proses Anda – Bersikaplah proaktif ketika mengidentifikasi kesenjangan dalam proses, alat, atau orang Anda, dan terapkan rencana untuk memperbaikinya. Simulasi adalah metode yang aman untuk menemukan kesenjangan dan memperbaiki proses. Lihat bagian [the section called “Aktivitas pascainsiden”](#) di dokumen ini untuk detail tentang cara melakukan iterasi proses Anda.

Sasaran desain ini merupakan pengingat untuk meninjau implementasi arsitektur Anda agar dapat melakukan respons insiden dan deteksi ancaman. Saat Anda merencanakan implementasi cloud Anda, pikirkan tentang menanggapi suatu insiden, idealnya dengan metodologi respons yang baik secara forensik. Dalam beberapa kasus, ini berarti Anda mungkin memiliki beberapa organisasi, akun, dan alat yang secara khusus disiapkan untuk tugas respons ini. Alat dan fungsi ini harus

tersedia bagi responden insiden melalui alur deployment. Alat dan fungsi tersebut tidak boleh statis karena dapat menyebabkan risiko yang lebih besar.

Domain insiden keamanan cloud

Untuk secara efektif mempersiapkan dan menanggapi peristiwa keamanan di AWS lingkungan Anda, Anda perlu memahami jenis insiden keamanan cloud bersama. Ada tiga domain dalam tanggung jawab pelanggan tempat insiden keamanan dapat terjadi: layanan, infrastruktur, dan aplikasi. Domain yang berbeda membutuhkan pengetahuan, alat, dan proses respons yang berbeda. Pertimbangkan domain berikut:

- Domain layanan — Insiden dalam domain layanan dapat memengaruhi izin [AWS Identity and Access Management](#) (IAM) Akun AWS, metadata sumber daya, penagihan, atau area lainnya. Peristiwa domain layanan adalah peristiwa yang Anda tanggapi secara eksklusif dengan mekanisme AWS API, atau di mana Anda memiliki akar penyebab yang terkait dengan konfigurasi atau izin sumber daya, dan mungkin memiliki logging berorientasi layanan terkait.
- Domain infrastruktur – Insiden dalam domain infrastruktur mencakup data atau aktivitas terkait jaringan, seperti proses dan data pada instans [Amazon Elastic Compute Cloud](#) (Amazon EC2), lalu lintas ke instans Amazon EC2 Anda dalam cloud privat virtual (VPC), dan area lainnya, seperti kontainer atau layanan lain ke depannya. Respons Anda terhadap peristiwa domain infrastruktur sering kali melibatkan perolehan data terkait insiden untuk analisis forensik. Ini mungkin mencakup interaksi dengan sistem operasi sebuah instance, dan, dalam berbagai kasus, mungkin juga melibatkan mekanisme AWS API. Di domain infrastruktur, Anda dapat menggunakan kombinasi alat AWS API dan forensics/incident respons digital (DFIR) dalam sistem operasi tamu, seperti instans Amazon EC2 yang didedikasikan untuk melakukan analisis dan investigasi forensik. Insiden domain infrastruktur mungkin melibatkan analisis tangkapan paket jaringan, blok disk pada volume [Amazon Elastic Block Store](#) (Amazon EBS), atau memori volatil yang diperoleh dari sebuah instans.
- Domain aplikasi – Insiden dalam domain aplikasi terjadi dalam kode aplikasi atau dalam perangkat lunak yang di-deploy untuk layanan atau infrastruktur. Domain ini harus disertakan dalam playbook deteksi dan respons ancaman cloud Anda, dan dapat menyertakan respons serupa dengan yang ada di domain infrastruktur. Dengan arsitektur aplikasi yang tepat dan bijaksana, Anda dapat mengelola domain ini dengan alat cloud dengan menggunakan akuisisi, pemulihan, dan penerapan otomatis.

Dalam domain ini, pertimbangkan aktor yang mungkin bertindak melawan AWS akun, sumber daya, atau data. Baik internal maupun eksternal, gunakan kerangka risiko untuk menentukan

risiko spesifik bagi organisasi dan melakukan persiapan sebagaimana mestinya. Selain itu, Anda harus mengembangkan model ancaman, yang dapat membantu perencanaan respons insiden dan pembangunan arsitektur yang cermat.

Perbedaan utama dari respons insiden di AWS

Respons insiden merupakan bagian integral dari strategi keamanan siber, baik on-premise maupun di cloud. Prinsip-prinsip keamanan seperti hak istimewa terkecil dan pertahanan secara mendalam dimaksudkan untuk melindungi kerahasiaan, integritas, dan ketersediaan data baik di tempat maupun di cloud. Beberapa pola respons insiden yang mendukung prinsip-prinsip keamanan ini mengikuti, termasuk retensi log, pemilihan peringatan yang berasal dari pemodelan ancaman, pengembangan playbook, serta integrasi informasi keamanan dan manajemen peristiwa (SIEM). Perbedaannya dimulai ketika pelanggan mulai merancang dan merekayasa pola-pola ini di cloud. Berikut ini adalah perbedaan utama dari respons insiden di AWS.

Perbedaan #1: Keamanan sebagai tanggung jawab bersama

Tanggung jawab untuk keamanan dan kepatuhan dibagi antara AWS dan pelanggannya. Model tanggung jawab bersama ini meringankan beberapa beban operasional pelanggan karena AWS mengoperasikan, mengelola, dan mengendalikan komponen dari sistem operasi host dan lapisan virtualisasi hingga keamanan fisik fasilitas di mana layanan beroperasi. Untuk detail lebih lanjut tentang model tanggung jawab bersama, lihat dokumentasi [Model Tanggung Jawab Bersama](#).

Saat tanggung jawab bersama Anda di cloud berubah, opsi Anda untuk respons insiden juga berubah. Merencanakan dan memahami timbal balik ini serta mencocokkannya dengan kebutuhan tata kelola Anda adalah langkah penting dalam respons insiden.

Selain hubungan langsung yang Anda miliki dengan AWS, mungkin ada entitas lain yang memiliki tanggung jawab dalam model tanggung jawab khusus Anda. Misalnya, Anda mungkin memiliki unit organisasi internal yang bertanggung jawab atas beberapa aspek operasi Anda. Anda mungkin juga memiliki hubungan dengan pihak lain yang mengembangkan, mengelola, atau mengoperasikan beberapa teknologi cloud Anda.

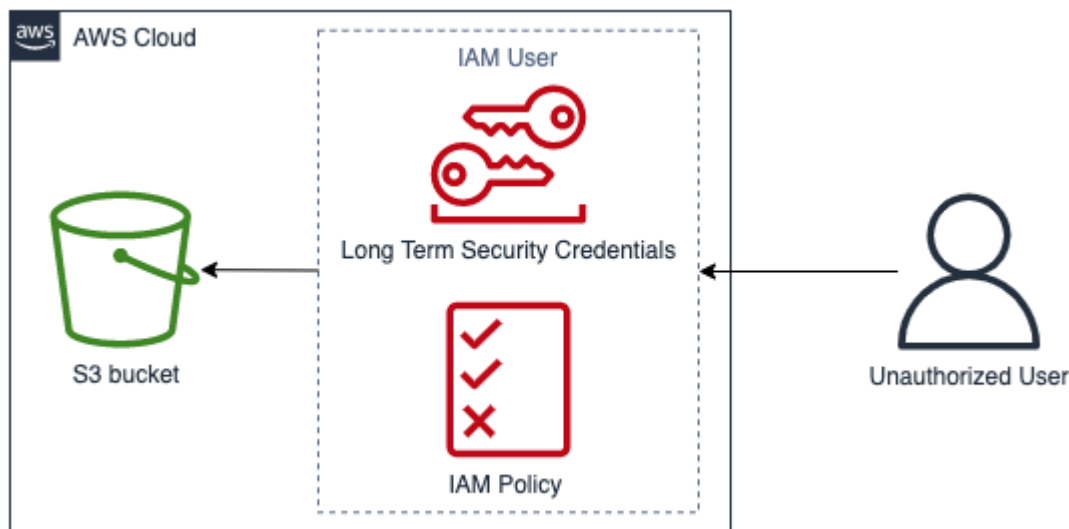
Membuat dan menguji rencana respons insiden yang sesuai dan playbook yang sesuai dengan model operasi Anda sangatlah penting.

Perbedaan #2: Domain layanan cloud

Karena perbedaan tanggung jawab keamanan yang ada di layanan cloud, diperkenalkanlah domain baru untuk insiden keamanan: domain layanan, yang dijelaskan sebelumnya di bagian [Domain](#)

[insiden](#). Domain layanan mencakup AWS akun pelanggan, izin IAM, metadata sumber daya, penagihan, dan area lainnya. Domain ini berbeda untuk respons insiden karena cara meresponsnya. Respons dalam domain layanan biasanya dilakukan dengan meninjau dan mengeluarkan panggilan API, bukan respons berbasis host dan berbasis jaringan tradisional. Dalam domain layanan, Anda tidak akan berinteraksi dengan sistem operasi sumber daya yang terpengaruh.

Diagram berikut menunjukkan contoh peristiwa keamanan dalam domain layanan berdasarkan anti-pola arsitektur. Dalam peristiwa ini, pengguna yang tidak sah mendapatkan kredensial keamanan jangka panjang dari pengguna IAM. Pengguna IAM memiliki kebijakan IAM yang memungkinkan mereka mengambil objek dari bucket [Amazon Simple Storage Service](#) (Amazon S3). Untuk menanggapi peristiwa keamanan ini, Anda akan menggunakan AWS APIs untuk menganalisis AWS log seperti [AWS CloudTrail](#) dan log akses Amazon S3. Anda juga akan menggunakan AWS APIs untuk menahan dan memulihkan dari insiden tersebut.



Contoh domain layanan

Perbedaan #3: APIs untuk penyediaan infrastruktur

Perbedaan lain berasal dari [Karakteristik cloud layanan mandiri on-demand](#). Pelanggan fasilitas utama berinteraksi dengan menggunakan RESTful API melalui titik akhir publik dan pribadi yang tersedia di banyak lokasi geografis di seluruh dunia. AWS Cloud Pelanggan dapat mengaksesnya APIs dengan AWS kredensial. Berbeda dengan kontrol akses on-premise, kredensial ini tidak harus terikat oleh jaringan atau domain Microsoft Active Directory. Kredensial malah dikaitkan dengan prinsipal IAM di dalam akun. AWS Titik akhir API ini dapat diakses di luar jaringan perusahaan Anda, yang penting untuk dipahami ketika Anda merespons insiden di mana kredensial digunakan di luar jaringan atau geografi yang Anda harapkan.

Karena sifat berbasis API AWS, sumber log penting untuk menanggapi peristiwa keamanan adalah AWS CloudTrail, yang melacak panggilan API manajemen yang dibuat di AWS akun Anda dan di mana Anda dapat menemukan informasi tentang lokasi sumber panggilan API.

Perbedaan #4: Sifat dinamis cloud

Cloud bersifat dinamis; memungkinkan Anda membuat dan menghapus sumber daya dengan cepat. Dengan penskalaan otomatis, sumber daya dapat diputar dan diputar berdasarkan peningkatan lalu lintas. Dengan infrastruktur berumur pendek dan perubahan yang serbacepat, sumber daya yang Anda selidiki mungkin sudah tidak ada lagi atau mungkin telah dimodifikasi. Memahami sifat AWS sumber daya yang fana dan bagaimana Anda dapat melacak pembuatan dan penghapusan AWS sumber daya akan menjadi penting untuk analisis insiden. Anda dapat menggunakan [AWS Config](#) untuk melacak riwayat konfigurasi AWS sumber daya Anda.

Perbedaan #5: Akses data

Akses data juga berbeda di cloud. Anda tidak dapat terhubung ke server untuk mengumpulkan data yang Anda butuhkan untuk penyelidikan keamanan. Data dikumpulkan melalui kabel dan melalui panggilan API. Anda harus berlatih dan memahami cara melakukan pengumpulan data agar siap menghadapi shift ini, dan memverifikasi penyimpanan yang sesuai untuk pengumpulan dan akses yang efektif. APIs

Perbedaan #6: Pentingnya otomatisasi

Agar pelanggan dapat sepenuhnya menyadari manfaat adopsi cloud, strategi operasional mereka harus menerapkan otomatisasi. Infrastructure as code (IaC) adalah pola lingkungan otomatis yang sangat efisien di mana AWS layanan dikerahkan, dikonfigurasi, dikonfigurasi ulang, dan dihancurkan menggunakan kode yang difasilitasi oleh layanan IaC asli seperti atau solusi pihak ketiga. [AWS CloudFormation](#) Hal ini mendorong implementasi respons insiden menjadi sangat otomatis, yang diinginkan untuk menghindari kesalahan manusia, terutama saat menangani bukti. Meskipun otomatisasi digunakan di lingkungan on-premise, otomatisasi sangat penting dan lebih sederhana di AWS Cloud.

Mengatasi perbedaan-perbedaan ini

Untuk mengatasi perbedaan ini, ikuti langkah-langkah yang diuraikan di bagian berikutnya untuk memverifikasi bahwa program respons insiden Anda untuk orang, proses, dan teknologi dipersiapkan dengan baik.

Persiapan

Persiapan untuk menghadapi insiden merupakan hal yang sangat penting agar respons insiden bisa dilakukan dengan cepat dan efektif. Persiapan dilakukan di tiga domain:

- **Orang** – Dalam mempersiapkan orang-orang Anda untuk menghadapi insiden keamanan, pemangku kepentingan yang relevan perlu diidentifikasi untuk respons insiden, dan dilatih tentang respons insiden dan teknologi cloud.
- **Proses** – Dalam mempersiapkan proses Anda untuk menghadapi insiden keamanan, perlu adanya pendokumentasian arsitektur, pengembangan rencana respons insiden menyeluruh, dan pembuatan playbook agar respons terhadap peristiwa keamanan bisa dilakukan secara konsisten.
- **Teknologi** – Dalam mempersiapkan teknologi Anda untuk menghadapi insiden keamanan, perlu adanya pengaturan akses, agregasi dan pemantauan log yang diperlukan, penerapan mekanisme peringatan yang efektif, dan pengembangan respons serta kemampuan penyelidikan.

Setiap domain ini sama pentingnya agar respons insiden berjalan efektif. Tanpa ketiga domain ini, program respons insiden tidak akan lengkap atau efektif. Anda perlu mempersiapkan orang, proses, dan teknologi dengan integrasi yang erat agar siap menghadapi suatu insiden.

Orang

Untuk merespons peristiwa keamanan, Anda perlu mengidentifikasi pemangku kepentingan yang akan mendukung respons terhadap peristiwa keamanan. Selain itu, sangat penting untuk respons yang efektif agar mereka dilatih tentang AWS teknologi dan AWS lingkungan Anda.

Menentukan peran dan tanggung jawab

Menangani peristiwa keamanan membutuhkan disiplin lintas organisasi dan komitmen untuk bertindak. Dalam struktur organisasi Anda, harus ada banyak orang yang bertanggung jawab, akuntabel, dimintai pendapat, atau diinformasikan saat terjadi insiden, seperti perwakilan dari sumber daya manusia (SDM), tim eksekutif, dan hukum. Pertimbangkan peran dan tanggung jawab ini, dan apakah ada pihak ketiga yang harus dilibatkan. Perhatikan bahwa di banyak geografi, ada hukum setempat yang mengatur apa yang harus dan tidak boleh dilakukan. Meskipun upaya untuk membangun bagan yang bertanggung jawab, akuntabel, berdasarkan konsultasi, dan terinformasi (RACI) untuk rencana respons keamanan Anda terasa birokratis, hal itu memungkinkan komunikasi yang cepat dan langsung serta dengan jelas menguraikan kepemimpinan di berbagai tahap peristiwa.

Selama insiden, termasuk aplikasi dan sumber daya yang terkena dampak adalah kunci karena mereka adalah ahli materi pelajaran (SMEs) yang dapat memberikan informasi dan konteks untuk membantu dalam mengukur dampak. owners/developers Pastikan untuk mempraktikkan dan membangun hubungan dengan developer serta pemilik aplikasi sebelum Anda mengandalkan keahlian mereka untuk respons insiden. Pemilik aplikasi atau SMEs, seperti administrator atau insinyur cloud Anda, mungkin perlu bertindak dalam situasi di mana lingkungan tidak dikenal atau memiliki kompleksitas, atau di mana responden tidak memiliki akses.

Terakhir, hubungan tepercaya mungkin terlibat dalam penyelidikan atau tanggapan karena mereka dapat memberikan keahlian tambahan dan pengawasan yang berharga. Ketika tidak ada orang yang memiliki keterampilan ini dalam tim Anda sendiri, ada baiknya Anda menyewa pihak eksternal untuk bantuan.

Melatih staf respons insiden

Melatih staf respons insiden Anda tentang teknologi yang digunakan organisasi mereka akan sangat penting agar mereka mampu merespons peristiwa keamanan secara memadai. Respons mungkin akan berlarut-larut jika anggota staf Anda tidak memahami teknologi yang mendasarinya. Selain konsep respons insiden tradisional, penting juga bagi mereka untuk memahami AWS layanan dan AWS lingkungan mereka. Ada sejumlah mekanisme tradisional untuk melatih staf insiden Anda, seperti pelatihan online dan pelatihan di ruang kelas. Anda juga dapat mempertimbangkan untuk menjalankan simulasi atau gameday sebagai mekanisme untuk pelatihan. Untuk detail tentang cara menjalankan simulasi, lihat [the section called “Menjalankan simulasi reguler”](#) bagian dokumen ini.

Memahami AWS Cloud teknologi

Untuk mengurangi ketergantungan dan memangkas waktu respons, pastikan tim keamanan dan responden Anda diedukasi tentang layanan cloud dan memiliki kesempatan untuk praktik langsung dengan lingkungan cloud spesifik yang digunakan organisasi Anda. Agar responden insiden menjadi efektif, penting untuk memahami AWS yayasan, IAM,, layanan AWS penebangan dan pemantauan, dan layanan AWS keamanan. AWS Organizations

AWS menyediakan lokakarya keamanan online (lihat [Lokakarya AWS Keamanan](#)) di mana Anda bisa mendapatkan pengalaman langsung dengan layanan AWS keamanan dan pemantauan. AWS juga menyediakan sejumlah opsi pelatihan dan jalur pembelajaran melalui pelatihan digital, pelatihan kelas, mitra AWS pelatihan, dan sertifikasi. Untuk mempelajari lebih lanjut, lihat [AWS Training and Certification](#).

AWS menyediakan pelatihan berbasis gratis dan berlangganan yang mendukung banyak persona dan area fokus. Kunjungi [AWS Skillbuilder](#) untuk mempelajari lebih lanjut.

Pahami AWS lingkungan Anda

Selain memahami AWS layanan, kasus penggunaannya, dan bagaimana mereka berintegrasi satu sama lain, sama pentingnya untuk memahami bagaimana AWS lingkungan organisasi Anda sebenarnya dirancang dan proses operasional apa yang ada. Sering kali, pengetahuan internal seperti ini tidak didokumentasikan dan hanya dipahami oleh beberapa pakar domain, yang dapat menciptakan ketergantungan, menghambat inovasi, dan memperlambat waktu respons.

Untuk menghindari ketergantungan ini dan mempercepat waktu respons, pengetahuan internal tentang lingkungan AWS Anda harus didokumentasikan, dapat diakses, dan dipahami oleh analis keamanan Anda. Memahami cakupan cloud Anda secara menyeluruh akan membutuhkan kolaborasi antara pemangku kepentingan keamanan yang relevan dan administrator cloud. Bagian dari mempersiapkan proses Anda untuk respons insiden mencakup mendokumentasikan dan memusatkan diagram arsitektur, yang [the section called “Mendokumentasikan dan memusatkan diagram arsitektur”](#) nantinya dalam laporan resmi ini. Namun, dari perspektif orang, penting bagi analis Anda untuk mengakses dan memahami diagram dan proses operasional yang terkait dengan lingkungan Anda AWS .

Memahami tim AWS respons dan dukungan

Dukungan

[Dukungan](#) menawarkan berbagai rencana yang menyediakan akses ke alat dan keahlian yang mendukung keberhasilan dan kesehatan operasional AWS solusi Anda. Jika Anda memerlukan dukungan teknis dan lebih banyak sumber daya untuk membantu merencanakan, menerapkan, dan mengoptimalkan AWS lingkungan Anda, Anda dapat memilih paket dukungan yang paling sesuai dengan kasus AWS penggunaan Anda.

Pertimbangkan [Pusat Dukungan](#) di Konsol Manajemen AWS (diperlukan login) sebagai titik kontak utama untuk mendapatkan dukungan untuk masalah yang memengaruhi AWS sumber daya Anda. Akses ke Dukungan dikendalikan oleh IAM. Untuk informasi selengkapnya tentang mendapatkan akses ke fitur AWS Support, lihat [Memulai dengan Dukungan](#).

Selain itu, jika Anda perlu melaporkan penyalahgunaan, hubungi [tim AWS Trust and Safety](#).

Insinyur Respons Insiden Keamanan

Insinyur Security Incident Response adalah AWS tim global khusus yang selalu tersedia yang memberikan dukungan kepada pelanggan selama acara keamanan aktif di sisi pelanggan [Model Tanggung Jawab AWS Bersama](#).

Ketika teknisi Security Incident Response mendukung Anda, Anda akan menerima bantuan dengan triase dan pemulihan untuk acara keamanan aktif. AWS Mereka akan membantu dalam analisis akar penyebab melalui penggunaan log AWS layanan dan memberi Anda rekomendasi untuk pemulihan. Mereka juga akan memberikan rekomendasi keamanan dan praktik terbaik untuk membantu Anda menghindari peristiwa keamanan ke depannya.

AWS pelanggan dapat melibatkan insinyur Respons Insiden Keamanan melalui [kasus AWS dukungan](#).

- Semua Pelanggan:
 1. Akun dan penagihan
 2. Layanan: Akun
 3. Kategori: Keamanan
 4. Keparahan: Pertanyaan umum

- Pelanggan dengan Dukungan paket Pengembang:
 1. Akun dan penagihan
 2. Layanan: Akun
 3. Kategori: Keamanan
 4. Keparahan: Pertanyaan penting

- Pelanggan dengan Dukungan rencana Bisnis:
 1. Akun dan penagihan
 2. Layanan: Akun
 3. Kategori: Keamanan
 4. Keparahan: Pertanyaan berdampak bisnis yang mendesak

- Pelanggan dengan Dukungan paket Enterprise:
 1. Akun dan penagihan
 2. Layanan: Akun
 3. Kategori: Keamanan
 4. Keparahan: Pertanyaan risiko bisnis kritis

- Pelanggan dengan Respons Insiden Keamanan AWS langganan: Buka konsol Respons Insiden Keamanan di <https://console.aws.amazon.com/security-ir/>

DDoS Dukungan respons S

AWS menawarkan [AWS Shield](#), yang menyediakan layanan perlindungan penolakan layanan terdistribusi (DDoS) terkelola yang melindungi aplikasi web yang berjalan. AWS Shield menyediakan deteksi selalu aktif dan mitigasi inline otomatis yang dapat meminimalkan waktu henti dan latensi aplikasi, sehingga tidak perlu terlibat untuk mendapatkan manfaat dari perlindungan S. Dukungan DDoS Ada dua tingkatan AWS Shield: Shield Standard dan Shield Advanced. Untuk mengetahui perbedaan antara kedua tingkatan ini, lihat [Dokumentasi fitur Shield](#).

AWS Managed Services (AMS)

[AWS Managed Services](#) (AMS) menyediakan pengelolaan AWS infrastruktur yang berkelanjutan sehingga Anda dapat fokus pada aplikasi Anda. Dengan menerapkan praktik terbaik untuk memelihara infrastruktur Anda, AMS membantu mengurangi biaya operasional dan risiko Anda. AMS mengotomatiskan aktivitas umum seperti permintaan perubahan, pemantauan, manajemen patch, keamanan, dan layanan pencadangan, serta menyediakan layanan siklus hidup penuh untuk menyediakan, menjalankan, dan mendukung infrastruktur Anda.

AMS bertanggung jawab untuk menyebarkan serangkaian kontrol detektif keamanan dan memberikan respons pertama setiap hari terhadap peringatan. Saat peringatan dimulai, AMS mengikuti seperangkat standar playbook otomatis dan manual untuk memverifikasi respons yang konsisten. Playbook ini dibagikan kepada pelanggan AMS saat orientasi agar mereka dapat mengembangkan dan mengoordinasikan respons dengan AMS.

Proses

Mengembangkan proses respons insiden yang menyeluruh dan jelas adalah kunci untuk program respons insiden yang sukses dan terukur. Ketika peristiwa keamanan terjadi, langkah dan alur kerja yang jelas akan membantu Anda merespons secara tepat waktu. Anda mungkin sudah memiliki proses respons insiden yang ada. Terlepas dari keadaan saat ini, penting untuk memperbarui, mengulangi, dan menguji proses respons insiden Anda secara teratur.

Mengembangkan dan menguji rencana respons insiden

Dokumen pertama yang dikembangkan untuk respons insiden adalah rencana respons insiden. Rencana respons insiden dirancang untuk menjadi dasar bagi program dan strategi respons insiden

Anda. Rencana respons insiden adalah dokumen komprehensif yang biasanya mencakup bagian-bagian ini:

- ikhtisar tim respons insiden – Menguraikan tujuan dan fungsi tim respons insiden
- Peran dan tanggung jawab – Membuat daftar pemangku kepentingan respons insiden dan menjabarkan peran mereka ketika insiden terjadi
- Rencana komunikasi – Detail informasi kontak dan bagaimana mekanisme komunikasi selama insiden

Ini adalah praktik terbaik untuk memiliki out-of-band komunikasi sebagai cadangan untuk komunikasi insiden. Contoh aplikasi yang menyediakan saluran out-of-band komunikasi aman adalah [AWS Wickr](#).

- Fase respons insiden dan tindakan yang harus diambil - Menghitung fase respons insiden - misalnya, mendeteksi, menganalisis, memberantas, menahan, dan memulihkan - termasuk tindakan tingkat tinggi yang harus diambil dalam fase-fase tersebut
- Definisi keparahan insiden dan prioritas – Memerinci cara mengklasifikasikan tingkat keparahan suatu insiden, bagaimana memprioritaskan insiden, lalu bagaimana definisi keparahan mempengaruhi prosedur eskalasi

Meskipun bagian-bagian ini umumnya ada di perusahaan dalam berbagai ukuran dan industri yang berbeda, rencana respons insiden akan berbeda-beda di setiap organisasi. Anda perlu membuat rencana respons insiden yang paling sesuai untuk organisasi Anda.

Mendokumentasikan dan memusatkan diagram arsitektur

Untuk merespons peristiwa keamanan dengan cepat dan akurat, Anda perlu memahami bagaimana sistem dan jaringan Anda dirancang. Memahami pola internal ini tidak hanya penting untuk respons insiden, tetapi juga untuk memverifikasi konsistensi di seluruh aplikasi yang dirancang dengan pola tersebut, sesuai dengan praktik terbaik. Anda juga harus memverifikasi bahwa dokumentasi ini aktual dan diperbarui secara berkala sesuai pola arsitektur baru. Anda sebaiknya mengembangkan dokumentasi dan repositori internal yang menjabarkan item-item seperti:

- AWS struktur akun - Anda perlu tahu:
 - Berapa banyak AWS akun yang Anda miliki?
 - Bagaimana AWS akun-akun itu diatur?
 - Siapa pemilik bisnis AWS akun tersebut?

- Apakah Anda menggunakan Kebijakan Kontrol Layanan (SCPs)? Jika demikian, pagar pembatas organisasi apa yang diterapkan dengan menggunakan SCPs
- Apakah Anda membatasi Wilayah dan layanan yang dapat digunakan?
- Apa perbedaan antara unit bisnis dan lingkungan (dev/test/prod)?
- AWS pola layanan
 - AWS Layanan apa yang Anda gunakan?
 - Apa AWS layanan yang paling banyak digunakan?
- Pola arsitektur
 - Arsitektur cloud apa yang Anda gunakan?
- AWS pola otentikasi
 - Bagaimana developer Anda biasanya mengautentikasi ke AWS?
 - Apakah Anda menggunakan pengguna atau peran IAM (atau keduanya)? Apakah otentikasi Anda AWS terhubung ke penyedia identitas (iDP)?
 - Bagaimana Anda memetakan pengguna atau peran IAM ke karyawan atau sistem?
 - Bagaimana cara akses dicabut ketika seseorang tidak lagi diotorisasi?
- AWS pola otorisasi
 - Kebijakan IAM apa yang digunakan developer Anda?
 - Apakah Anda menggunakan kebijakan berbasis sumber daya?
- Pencatatan dan pemantauan
 - Sumber pencatatan apa yang Anda gunakan dan di mana sumber tersebut disimpan?
 - Apakah Anda mengumpulkan AWS CloudTrail log? Jika iya, di mana log tersebut disimpan?
 - Bagaimana Anda menanyakan CloudTrail log?
 - Apakah Anda GuardDuty mengaktifkan Amazon?
 - Bagaimana Anda mengakses GuardDuty temuan (misalnya, konsol, sistem tiket, SIEM)?
 - Apakah temuan atau peristiwa dikumpulkan dalam SIEM?
 - Apakah tiket dibuat secara otomatis?
 - Alat apa yang ada untuk menganalisis log dalam sebuah penyelidikan?
- Topologi jaringan
 - Bagaimana perangkat, titik akhir, dan koneksi di jaringan Anda diatur secara fisik atau logis?
 - Bagaimana jaringan Anda terhubung AWS?

- Infrastruktur eksternal
 - Bagaimana aplikasi yang menghadap ke luar digunakan?
 - AWS Sumber daya apa yang dapat diakses publik?
 - AWS Akun apa yang mengandung infrastruktur yang dihadapi secara eksternal?
 - Apa DDoS atau penyaringan eksternal yang ada?

Mendokumentasikan diagram dan proses teknis internal memudahkan pekerjaan analis respons insiden, membantu mereka dengan cepat memperoleh pengetahuan kelembagaan untuk merespons peristiwa keamanan. Dokumentasi proses teknis internal secara menyeluruh tidak hanya menyederhanakan investigasi keamanan, tetapi juga menyesuaikan rasionalisasi dan evaluasi proses.

Mengembangkan playbook respons insiden

Bagian penting dari mempersiapkan proses respons insiden Anda adalah mengembangkan playbook. Playbook respons insiden memberikan serangkaian panduan preskriptif dan langkah-langkah yang harus diikuti ketika terjadi peristiwa keamanan. Struktur dan langkah yang jelas akan menyederhanakan respons dan mengurangi kemungkinan kesalahan manusia.

Untuk apa saja playbook dibuat

Playbook sebaiknya dibuat untuk skenario insiden seperti:

- Insiden yang diantisipasi – Playbook harus dibuat untuk insiden yang Anda antisipasi. Hal ini termasuk ancaman seperti denial of service (DoS), ransomware, dan pembobolan kredensial.
- Temuan atau peringatan keamanan yang diketahui — Buku pedoman harus dibuat untuk temuan dan peringatan keamanan Anda yang diketahui, seperti temuan. GuardDuty Anda mungkin menerima GuardDuty temuan dan berpikir, “Sekarang apa?” Untuk mencegah kesalahan penanganan GuardDuty temuan atau mengabaikan temuan, buat buku pedoman untuk setiap temuan potensial. GuardDuty Beberapa rincian remediasi dan panduan dapat ditemukan dalam [GuardDuty dokumentasi](#). Perlu dicatat bahwa tidak GuardDuty diaktifkan secara default dan menimbulkan biaya. Detail lebih lanjut tentang GuardDuty dapat ditemukan di Lampiran A: Definisi kemampuan cloud -. [the section called “Visibilitas dan peringatan”](#)

Apa saja yang perlu dimasukkan dalam playbook

Playbook harus berisi langkah-langkah teknis yang akan dijalankan oleh analis keamanan untuk menyelidiki dan merespons insiden keamanan potensial secara memadai.

Item yang akan disertakan dalam playbook meliputi:

- Gambaran umum playbook – Skenario risiko atau insiden apa yang ditangani oleh playbook ini? Apa tujuan dari playbook ini?
- Prasyarat – Log dan mekanisme deteksi apa yang diperlukan untuk skenario insiden ini? Apa notifikasi yang diharapkan?
- Informasi pemangku kepentingan – Siapa yang terlibat dan apa informasi kontak mereka? Apa saja tanggung jawab setiap pemangku kepentingan?
- Langkah respons – Di seluruh fase respons insiden, langkah taktis apa yang perlu diambil? Kueri apa yang perlu dijalankan analisis? Kode apa yang perlu dijalankan untuk mencapai hasil yang diinginkan?
 - Deteksi – Bagaimana insiden tersebut akan terdeteksi?
 - Analisis – Bagaimana cakupan dampak akan ditentukan?
 - Tahan – Bagaimana insiden akan diisolasi untuk membatasi cakupan?
 - Berantas – Bagaimana ancaman akan dihilangkan dari lingkungan?
 - Pulihkan – Bagaimana sistem atau sumber daya yang terpengaruh akan dibawa kembali ke produksi?
- Hasil yang diharapkan – Setelah kueri dan kode dijalankan, apa hasil yang diharapkan dari playbook tersebut?

Untuk memverifikasi informasi yang konsisten di setiap playbook, sebaiknya buat templat playbook yang dapat digunakan di seluruh playbook keamanan Anda yang lainnya. Beberapa item yang sudah terdaftar, seperti informasi pemangku kepentingan, dapat digunakan di beberapa playbook. Jika demikian, Anda dapat membuat dokumentasi terpusat untuk informasi tersebut dan merujuknya di dalam playbook, lalu menyebutkan perbedaan eksplisitnya di dalam playbook. Dengan begitu, Anda tidak perlu memperbarui informasi yang sama di setiap playbook Anda. Dengan membuat templat dan mengidentifikasi informasi umum atau bersama di playbook, Anda dapat menyederhanakan dan mempercepat pengembangan playbook. Terakhir, playbook Anda kemungkinan akan berkembang seiring waktu; setelah Anda memastikan bahwa langkah-langkahnya konsisten, hal ini membentuk persyaratan untuk otomatisasi.

Contoh playbook

Sejumlah contoh playbook dapat ditemukan di Lampiran B di [the section called “Sumber daya playbook”](#). Contoh-contoh di sini dapat digunakan sebagai referensi Anda untuk playbook apa yang perlu dibuat dan apa yang perlu disertakan dalam playbook Anda. Namun, penting bagi Anda untuk

membuat playbook yang menggabungkan risiko yang paling relevan dengan bisnis Anda. Anda perlu memverifikasi bahwa langkah-langkah dan alur kerja dalam playbook Anda mencakup teknologi dan proses Anda.

Menjalankan simulasi reguler

Organisasi tumbuh dan berkembang dari waktu ke waktu, begitu pun halnya dengan ancaman. Karena itu, penting bagi Anda untuk terus meninjau kemampuan respons insiden Anda. Simulasi adalah salah satu metode yang dapat digunakan untuk melakukan penilaian ini. Simulasi menggunakan skenario peristiwa keamanan dunia nyata yang dirancang untuk meniru taktik, teknik, dan prosedur aktor ancaman (TTPs) dan memungkinkan organisasi untuk melatih dan mengevaluasi kemampuan respons insiden mereka dengan menanggapi peristiwa cyber tiruan ini karena mungkin terjadi dalam kenyataan.

Simulasi memiliki berbagai manfaat, termasuk:

- Memvalidasi kesiapan siber dan mengembangkan kepercayaan diri responden insiden Anda.
- Menguji akurasi dan efisiensi alat serta alur kerja.
- Menyempurnakan metode komunikasi dan eskalasi yang selaras dengan rencana respons insiden Anda.
- Memberikan kesempatan untuk merespons vektor yang kurang umum.

Jenis simulasi

Ada tiga jenis simulasi utama:

- Latihan meja – Pendekatan latihan meja dalam simulasi adalah sesi berbasis diskusi yang melibatkan berbagai pemangku kepentingan respons insiden untuk mempraktikkan peran dan tanggung jawab serta menggunakan alat komunikasi dan playbook yang telah ditetapkan. Fasilitas latihan biasanya dapat dilakukan dalam sehari penuh di tempat virtual, tempat fisik, atau kombinasi. Karena sifatnya yang berbasis diskusi, latihan meja berfokus pada proses, orang, dan kolaborasi. Teknologi adalah bagian integral dari diskusi; tetapi, latihan meja umumnya tidak menggunakan alat atau skrip respons insiden yang sebenarnya.
- Latihan Tim Ungu – Latihan Tim Ungu meningkatkan level kolaborasi antara tim responden insiden (Tim Biru) dan tim aktor ancaman simulasi (Tim Merah). Tim Biru umumnya terdiri dari anggota Security Operations Center (SOC), tetapi juga dapat mencakup pemangku kepentingan lain yang akan terlibat dalam peristiwa siber yang sebenarnya. Tim Merah umumnya terdiri dari tim uji penetrasi atau pemangku kepentingan utama yang dilatih dalam keamanan ofensif. Tim Merah

bekerja secara kolaboratif dengan fasilitator latihan dalam merancang skenario yang akurat dan memungkinkan. Selama latihan Tim Ungu, fokus utamanya adalah pada mekanisme deteksi, alat, dan prosedur operasi standar (SOPs) yang mendukung upaya respons insiden.

- Latihan Tim Merah – Dalam latihan Tim Merah, penyerang (Tim Merah) melakukan simulasi untuk mencapai tujuan tertentu atau serangkaian tujuan dari cakupan yang telah ditentukan sebelumnya. Pembela (Tim Biru) belum tentu mengetahui ruang lingkup dan durasi latihan, yang memberikan penilaian yang lebih realistis tentang bagaimana mereka akan menanggapi insiden yang sebenarnya. Karena latihan Tim Merah dapat menjadi uji invasif, Anda harus berhati-hati dan menerapkan kontrol untuk memverifikasi bahwa latihan tersebut tidak menyebabkan kerusakan nyata pada lingkungan Anda.

Note

AWS mengharuskan pelanggan untuk meninjau kebijakan pengujian penetrasi yang tersedia di [situs web Pengujian Penetrasi](#) sebelum mereka melakukan latihan Tim Ungu atau Tim Merah.

Tabel 1 merangkum beberapa perbedaan utama dalam jenis simulasi ini. Penting untuk dicatat bahwa definisinya secara umum dianggap lentur dan dapat disesuaikan dengan kebutuhan organisasi Anda.

Tabel 1 — Jenis simulasi

	Latihan meja	Latihan Tim Ungu	Latihan Tim Merah
Ringkasan	Latihan berbasis kertas yang berfokus pada satu skenario insiden keamanan tertentu. Latihan ini dapat berupa latihan tingkat tinggi atau teknis, dan dijalankan dengan serangkaian skenario tertulis.	Penawaran yang lebih realistis dibandingkan dengan latihan meja. Selama latihan Tim Ungu, fasilitator bekerja secara kolaboratif dengan para peserta untuk meningkatkan keterlibatan latihan dan menawarkan	Penawaran simulasi yang umumnya lebih canggih. Biasanya ada informasi yang disamarkan, sehingga para peserta mungkin tidak mengetahui semua detail latihan.

	Latihan meja	Latihan Tim Ungu	Latihan Tim Merah
		n pelatihan jika diperlukan.	
Sumber daya yang diperlukan	Diperlukan sumber daya teknis terbatas	Diperlukan berbagai pemangku kepentingan dan sumber daya teknis tingkat tinggi	Diperlukan berbagai pemangku kepentingan dan sumber daya teknis tingkat tinggi
Kompleksitas	Rendah	Sedang	Tinggi

Pertimbangkan untuk memfasilitasi simulasi siber secara reguler. Setiap jenis latihan dapat memberikan manfaat tersendiri bagi peserta dan organisasi secara keseluruhan, sehingga Anda dapat memilih untuk memulai dengan jenis simulasi yang kurang kompleks (seperti latihan meja) lalu beralih ke jenis simulasi yang lebih kompleks (latihan Tim Merah). Anda sebaiknya memilih jenis simulasi berdasarkan kematangan keamanan, sumber daya, dan hasil yang Anda inginkan. Beberapa pelanggan mungkin tidak memilih untuk melakukan latihan Tim Merah karena kompleksitas dan biayanya.

Siklus hidup latihan

Apa pun jenis simulasi yang Anda pilih, simulasi umumnya mengikuti langkah-langkah berikut:

1. Menentukan elemen latihan inti – Tentukan skenario simulasi dan tujuan simulasi. Dua hal ini harus disetujui oleh kepemimpinan.
2. Mengidentifikasi pemangku kepentingan utama – Latihan setidaknya membutuhkan fasilitator dan peserta latihan. Tergantung skenarionya, pemangku kepentingan tambahan seperti pimpinan dari departemen hukum, komunikasi, atau eksekutif dapat dilibatkan.
3. Membangun dan menguji skenario – Skenario mungkin perlu disesuaikan jika elemen tertentu tidak memungkinkan dalam pengembangannya. Tahap ini diharapkan menghasilkan skenario final.
4. Memfasilitasi simulasi – Jenis simulasi menentukan fasilitas yang digunakan (skenario tertulis atau skenario simulasi yang sangat teknis). Fasilitator harus menyelaraskan taktik fasilitasi mereka dengan objek latihan dan harus sebisa mungkin melibatkan semua peserta latihan agar hasilnya bisa optimal.
5. Mengembangkan laporan setelah tindakan (AAR) – Identifikasi area yang berjalan dengan baik, area yang dapat ditingkatkan lagi, dan potensi kesenjangan. AAR harus mengukur efektivitas

simulasi serta respons tim terhadap peristiwa simulasi agar kemajuan dapat dilacak dari waktu ke waktu dengan simulasi mendatang.

Teknologi

Jika Anda mengembangkan dan menerapkan teknologi yang tepat sebelum insiden keamanan, staf respons insiden Anda akan dapat menyelidiki, memahami ruang lingkup, dan mengambil tindakan tepat waktu.

Kembangkan struktur AWS akun

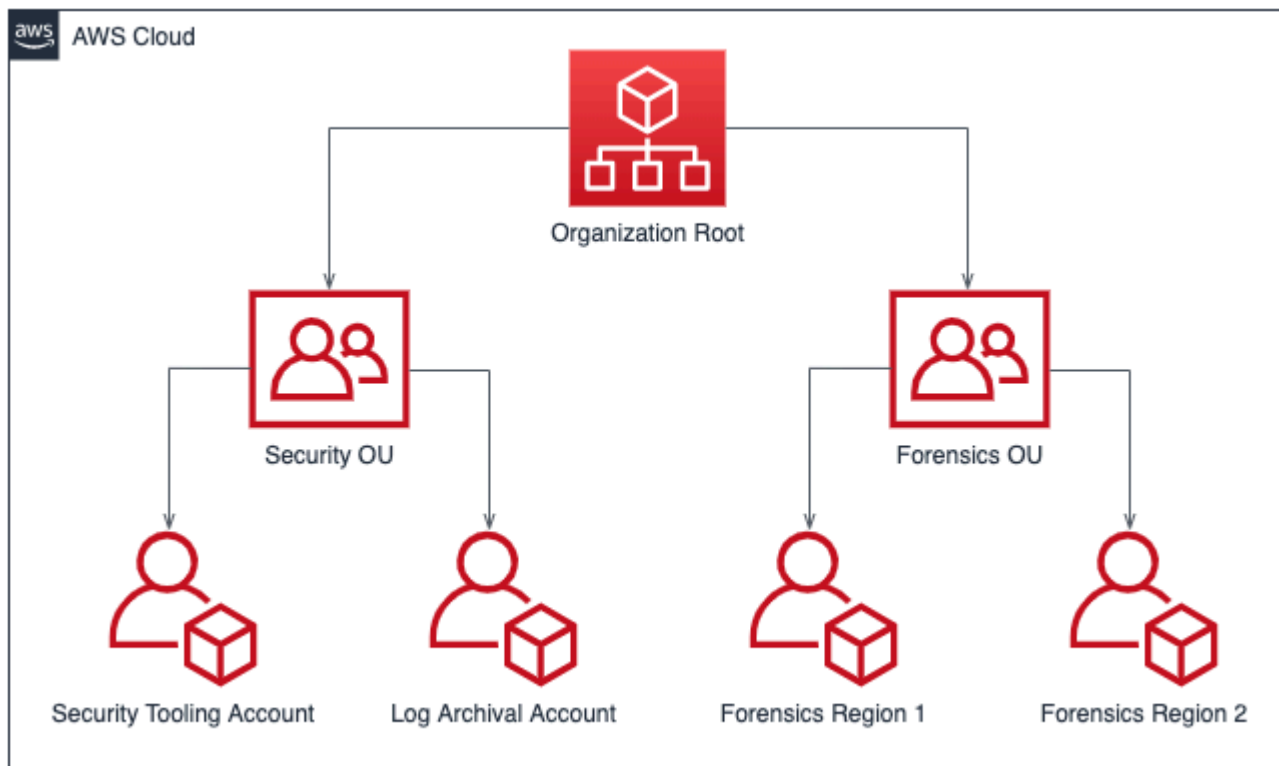
[AWS Organizations](#) membantu mengelola dan mengatur AWS lingkungan secara terpusat saat Anda tumbuh dan meningkatkan AWS sumber daya. AWS Organisasi mengkonsolidasikan AWS akun Anda sehingga Anda dapat mengelolanya sebagai satu unit. Anda dapat menggunakan unit organisasi (OUs) untuk mengelompokkan akun bersama untuk mengelola sebagai satu unit.

Untuk respons insiden, akan sangat membantu untuk memiliki struktur AWS akun yang mendukung fungsi respons insiden, yang mencakup OU keamanan dan OU forensik. Dalam unit organisasi keamanan, Anda harus memiliki akun untuk:

- Pengarsipan log – Menggabungkan log dalam akun AWS pengarsipan.
- Perangkat keamanan — Memusatkan layanan keamanan di akun alat AWS keamanan. Akun ini beroperasi sebagai administrator yang didelegasikan untuk layanan keamanan.

Dalam forensik unit organisasi, Anda memiliki opsi untuk menerapkan satu akun forensik atau akun-akun untuk setiap Wilayah tempat Anda beroperasi, bergantung pada mana yang paling sesuai untuk model bisnis dan operasional Anda. Untuk contoh pendekatan akun per Wilayah, jika Anda hanya beroperasi di AS Timur (Virginia Utara) (us-east-1) dan AS Barat (Oregon) (us-west-2), Anda akan memiliki dua akun di forensik unit organisasi: satu untuk us-east-1 dan satu untuk us-west-2. Karena penyediaan akun baru membutuhkan waktu, akun forensik harus dibuat dan digunakan jauh sebelum insiden, sehingga bisa siap digunakan oleh responden secara efektif ketika merespons insiden.

Diagram berikut menampilkan struktur akun sampel, termasuk unit organisasi forensik dengan akun forensik per Wilayah:



Struktur akun per wilayah untuk respons insiden

Mengembangkan dan menerapkan strategi pemberian tag

Memperoleh informasi kontekstual tentang kasus penggunaan bisnis dan pemangku kepentingan internal yang relevan di sekitar AWS sumber daya bisa jadi sulit. Salah satu cara untuk melakukannya adalah dalam bentuk tag, yang menetapkan metadata ke AWS sumber daya Anda dan terdiri dari kunci dan nilai yang ditentukan pengguna. Anda dapat menggunakan tag untuk mengelompokkan sumber daya berdasarkan tujuan, pemilik, lingkungan, jenis data yang diproses, dan kriteria lainnya yang Anda pilih.

Memiliki strategi penandaan yang konsisten dapat mempercepat waktu respons dengan memungkinkan Anda mengidentifikasi dan membedakan informasi kontekstual tentang sumber daya dengan cepat. AWS Tag juga dapat berfungsi sebagai mekanisme untuk memulai otomatisasi respons. Untuk informasi lebih lanjut tentang apa yang harus diberi tag, lihat [dokumentasi tentang AWS sumber daya penandaan](#). Anda harus terlebih dahulu menentukan tag yang ingin Anda terapkan di organisasi Anda. Setelah itu, Anda akan menerapkan dan menegakkan strategi pemberian tag ini. Detail tentang implementasi dan penegakan dapat ditemukan di AWS blog [Menerapkan strategi penandaan AWS sumber daya menggunakan Kebijakan AWS Tag dan Kebijakan Kontrol Layanan \(SCPs\)](#).

Perbarui informasi kontak AWS akun

Untuk setiap AWS akun Anda, penting untuk memiliki informasi up-to-date kontak yang akurat sehingga pemangku kepentingan yang benar menerima pemberitahuan penting dari AWS topik seperti keamanan, penagihan, dan operasi. Untuk setiap AWS akun, Anda memiliki kontak utama dan kontak alternatif untuk keamanan, penagihan, dan operasi. Perbedaan antara kontak ini dapat ditemukan di [Panduan Referensi Manajemen AWS Akun](#).

Untuk detail tentang mengelola kontak alternatif, lihat [AWS dokumentasi tentang menambahkan, mengubah, atau menghapus kontak alternatif](#). Jika tim Anda mengelola penagihan, operasi, dan masalah terkait keamanan, penggunaan daftar distribusi email merupakan praktik terbaik. Dengan daftar distribusi email, ketergantungan pada satu orang bisa dihindari, karena hal ini dapat menyulitkan apabila orang tersebut sedang tidak di kantor atau sudah keluar dari perusahaan. Anda juga harus memverifikasi bahwa informasi kontak email dan akun, termasuk nomor telepon, terlindungi dengan baik untuk berjaga-jaga jika terjadi pengaturan ulang kata sandi akun root dan pengaturan ulang autentikasi multi-faktor (MFA).

Untuk pelanggan yang menggunakan AWS Organizations, administrator organisasi dapat secara terpusat mengelola kontak alternatif untuk akun anggota menggunakan akun manajemen atau akun administrator yang didelegasikan tanpa memerlukan kredensial untuk setiap akun. AWS Anda juga perlu memverifikasi bahwa akun yang baru dibuat memiliki informasi kontak yang akurat. Lihat [Perbarui kontak alternatif secara otomatis untuk posting Akun AWS blog yang baru dibuat](#).

Siapkan akses ke Akun AWS

Selama insiden, tim respons insiden Anda harus memiliki akses ke lingkungan dan sumber daya yang terlibat dalam insiden tersebut. Pastikan tim Anda memiliki akses yang tepat untuk melakukan tugas mereka sebelum suatu peristiwa terjadi. Untuk melakukan itu, Anda harus tahu tingkat akses apa yang dibutuhkan anggota tim Anda (misalnya, jenis tindakan apa yang mungkin mereka ambil) dan harus memberikan akses hak istimewa paling sedikit terlebih dahulu.

Untuk menerapkan dan menyediakan akses ini, Anda harus mengidentifikasi dan mendiskusikan strategi akun AWS dan strategi identitas cloud dengan arsitek cloud organisasi Anda untuk memahami metode autentikasi dan otorisasi yang dikonfigurasi. Karena kredensial ini bersifat istimewa, Anda sebaiknya mempertimbangkan untuk menggunakan alur persetujuan atau mengambil kredensial dari brankas sebagai bagian dari implementasi Anda. Setelah implementasi, Anda perlu mendokumentasikan dan menguji akses anggota tim dengan baik sebelum peristiwa terjadi untuk memastikan mereka dapat merespons tanpa penundaan.

Terakhir, pengguna yang dibuat khusus untuk merespons insiden keamanan sering kali diberi hak istimewa agar dapat memiliki akses yang memadai. Oleh karena itu, penggunaan kredensial ini harus dibatasi, dipantau, dan tidak digunakan untuk kegiatan sehari-hari.

Memahami lanskap ancaman

Mengembangkan model ancaman

Dengan mengembangkan model ancaman, organisasi dapat mengidentifikasi ancaman dan mitigasi sebelum pengguna yang tidak sah dapat melakukannya. Ada sejumlah strategi dan pendekatan untuk pemodelan ancaman; lihat posting blog [How to approach threat modeling](#). Untuk respons insiden, model ancaman dapat membantu mengidentifikasi vektor serangan yang mungkin digunakan aktor ancaman dalam insiden. Memahami apa yang Anda pertahankan akan sangat penting agar dapat merespons dengan segera. Anda juga dapat menggunakan pemodelan AWS Partner untuk ancaman. Untuk mencari AWS pasangan, gunakan [AWS Partner Network](#).

Mengintegrasikan dan menggunakan intelijen ancaman siber

Intelijen ancaman siber adalah data dan analisis intensi, peluang, dan kemampuan aktor ancaman. Memperoleh dan menggunakan intelijen ancaman sangat membantu untuk mendeteksi insiden sejak dini dan memahami perilaku aktor ancaman dengan lebih baik. Intelijen ancaman siber mencakup indikator statis seperti alamat IP atau hash file malware. Hal ini juga mencakup informasi tingkat tinggi, seperti pola perilaku dan intensi. Anda dapat mengumpulkan intelijen ancaman dari sejumlah vendor keamanan siber dan dari repositori sumber terbuka.

Untuk mengintegrasikan dan memaksimalkan kecerdasan ancaman untuk AWS lingkungan Anda, Anda dapat menggunakan beberapa out-of-the-box kemampuan dan mengintegrasikan daftar intelijen ancaman Anda sendiri. Amazon GuardDuty menggunakan sumber intelijen ancaman AWS internal dan pihak ketiga. AWS Layanan lain, seperti firewall dan AWS WAF aturan DNS, juga mengambil masukan dari AWS'kelompok intelijen ancaman canggih. Beberapa GuardDuty temuan dipetakan ke [MITRE ATT&CK Framework](#), yang memberikan informasi tentang pengamatan dunia nyata tentang taktik dan teknik musuh.

Memilih dan mengatur log untuk analisis dan peringatan

Selama penyelidikan keamanan, Anda harus dapat meninjau log yang relevan untuk mencatat dan memahami cakupan serta garis waktu lengkap insiden tersebut. Log juga diperlukan untuk pembuatan peringatan, yang menunjukkan terjadinya tindakan tertentu yang menarik. Sangat penting untuk memilih, mengaktifkan, menyimpan, serta mengatur mekanisme kueri dan pengambilan,

serta mengatur peringatan. Setiap tindakan ini ditinjau di bagian ini. Untuk detail selengkapnya, lihat posting AWS blog [Strategi pencatatan untuk respons insiden keamanan](#).

Memilih dan mengaktifkan sumber log

Menjelang penyelidikan keamanan, Anda perlu menangkap log yang relevan untuk merekonstruksi aktivitas secara surut di akun. AWS Pilih dan aktifkan sumber log yang relevan dengan beban kerja AWS akun mereka.

AWS CloudTrail adalah layanan logging yang melacak panggilan API yang dilakukan terhadap aktivitas AWS layanan pengambilan AWS akun. Ini diaktifkan secara default dengan retensi 90 hari peristiwa manajemen yang dapat [diambil melalui CloudTrail fasilitas Riwayat Acara](#) menggunakan Konsol Manajemen AWS, AWS CLI, atau SDK. AWS Untuk retensi dan visibilitas peristiwa data yang lebih lama, Anda perlu [membuat CloudTrail Trail](#) dan dikaitkan dengan bucket Amazon S3, dan secara opsional, dengan CloudWatch grup log. Atau, Anda dapat membuat [CloudTrail Danau](#), yang menyimpan CloudTrail log hingga tujuh tahun dan menyediakan fasilitas kueri berbasis SQL.

AWS merekomendasikan agar pelanggan yang menggunakan VPC mengaktifkan lalu lintas jaringan dan log DNS masing-masing menggunakan Log [Aliran VPC dan log kueri penyelesai Amazon Route 53, mengalirkannya ke bucket Amazon S3 atau grup log](#). CloudWatch Anda dapat membuat log alur VPC untuk VPC, subnet, atau antarmuka jaringan. Untuk Log Alur VPC, Anda dapat bersikap selektif tentang bagaimana dan di mana Anda mengaktifkan Log Alur untuk mengurangi biaya.

AWS CloudTrail Log, Log Aliran VPC, dan log kueri resolver Route 53 adalah trifecta logging dasar untuk mendukung penyelidikan keamanan di. AWS

AWS layanan dapat menghasilkan log yang tidak ditangkap oleh trifecta logging dasar, seperti log Elastic Load Balancing AWS WAF , log, log perekam, temuan Amazon AWS Config , log audit GuardDuty Amazon Elastic Kubernetes Service (Amazon EKS), dan sistem operasi instans Amazon EC2 dan log aplikasi. Lihat daftar lengkap opsi pencatatan log dan pemantauan di [the section called "Lampiran A: Definisi kemampuan cloud"](#).

Memilih penyimpanan log

Pilihan penyimpanan log umumnya terkait dengan alat kueri yang Anda gunakan, kemampuan retensi, pemahaman, dan biaya. Saat Anda mengaktifkan log AWS layanan, sediakan fasilitas penyimpanan; biasanya bucket atau grup CloudWatch log Amazon S3.

Bucket Amazon S3 menyediakan penyimpanan tahan lama yang hemat biaya dengan kebijakan siklus hidup opsional. Log yang disimpan di bucket Amazon S3 dapat dikueri secara native

menggunakan layanan seperti Amazon Athena. Grup CloudWatch log menyediakan penyimpanan yang tahan lama dan fasilitas kueri bawaan melalui Wawasan CloudWatch Log.

Mengidentifikasi retensi log yang sesuai

Bila Anda menggunakan bucket S3 atau grup CloudWatch log untuk menyimpan log, Anda harus menetapkan siklus hidup yang memadai untuk setiap sumber log guna mengoptimalkan biaya penyimpanan dan pengambilan. Pelanggan umumnya memiliki antara 3 dan 12 bulan log yang tersedia untuk kueri, dengan retensi hingga tujuh tahun. Pilihan ketersediaan dan retensi harus selaras dengan persyaratan keamanan Anda serta gabungan mandat hukum, peraturan, dan bisnis.

Memilih dan menerapkan mekanisme kueri untuk log

Di AWS, layanan utama yang dapat Anda gunakan untuk menanyakan [CloudWatch log adalah Wawasan Log](#) untuk data yang disimpan dalam grup CloudWatch log, serta [Amazon Athena](#) dan Layanan [OpenSearch Amazon](#) untuk data yang disimpan di Amazon S3. Anda juga dapat menggunakan alat kueri pihak ketiga seperti informasi keamanan dan manajemen peristiwa (SIEM).

Proses untuk memilih alat kueri log harus mempertimbangkan aspek orang, proses, dan teknologi dalam operasi keamanan Anda. Pilih alat yang memenuhi persyaratan operasional, bisnis, dan keamanan, serta dapat diakses dan dipelihara dalam jangka panjang. Perlu diingat bahwa alat kueri log bekerja secara optimal ketika jumlah log yang akan dipindai tidak melebihi batas alat. Tidak jarang pelanggan memiliki beberapa alat kueri karena kendala biaya atau teknis. Misalnya, pelanggan mungkin menggunakan SIEM pihak ketiga untuk melakukan kueri data selama 90 hari terakhir, dan menggunakan Athena untuk melakukan kueri melebihi 90 hari karena biaya penyerapan log SIEM. Apa pun implementasinya, verifikasi bahwa pendekatan Anda meminimalkan jumlah alat yang diperlukan untuk memaksimalkan efisiensi operasional, terutama selama penyelidikan peristiwa keamanan.

Menggunakan log untuk peringatan

AWS secara native memberikan peringatan melalui layanan keamanan, seperti Amazon GuardDuty [AWS Security Hub CSPM](#), dan AWS Config. Anda juga dapat menggunakan mesin pembuat peringatan kustom untuk peringatan keamanan yang tidak tercakup oleh layanan ini atau untuk peringatan spesifik yang relevan dengan lingkungan Anda. Membangun peringatan dan deteksi ini tercakup dalam bagian bernama [the section called “Deteksi”](#) dalam dokumen ini.

Mengembangkan kemampuan forensik

Menjelang insiden keamanan, pertimbangkan untuk mengembangkan kemampuan forensik guna mendukung investigasi peristiwa keamanan. [Guide to Integrating Forensic Techniques into Incident Response](#) dari NIST menyediakan panduan tersebut.

Forensik pada AWS

Konsep dari forensik lokal tradisional berlaku untuk. AWS [Strategi lingkungan investigasi forensik dalam](#) posting AWS Cloud blog memberi Anda informasi penting untuk mulai memigrasikan keahlian forensik mereka ke. AWS

Setelah lingkungan dan struktur AWS akun Anda disiapkan untuk forensik, Anda akan ingin menentukan teknologi yang diperlukan untuk secara efektif melakukan metodologi forensik yang sehat di empat fase:

- Koleksi — Kumpulkan AWS log yang relevan, seperti AWS CloudTrail, AWS Config, Log Aliran VPC, dan log tingkat host. Kumpulkan snapshot, backup, dan dump memori dari sumber daya yang terkena dampak. AWS
- Pemeriksaan – Memeriksa data yang dikumpulkan dengan mengekstraksi dan menilai informasi yang relevan.
- Analisis – Menganalisis data yang dikumpulkan untuk memahami insiden dan menarik kesimpulan dari insiden tersebut.
- Pelaporan – Menyajikan informasi yang dihasilkan dari fase analisis.

Menangkap cadangan dan snapshot

Menyiapkan cadangan sistem kunci dan basis data sangat penting untuk pemulihan dari insiden keamanan dan untuk tujuan forensik. Dengan memiliki cadangan, Anda dapat memulihkan sistem Anda ke keadaan aman sebelumnya. Pada AWS, Anda dapat mengambil snapshot dari berbagai sumber daya. Snapshot memberi Anda point-in-time cadangan sumber daya tersebut. Ada banyak layanan AWS yang dapat mendukung Anda dalam pencadangan dan pemulihan. Lihat [Panduan Preskriptif Pencadangan dan Pemulihan](#) untuk detail tentang layanan ini dan pendekatan untuk pencadangan dan pemulihan. Untuk detail selengkapnya, lihat posting blog [Use backups to recover from security incidents](#).

Terutama ketika berhubungan dengan situasi seperti ransomware, sangat penting agar cadangan Anda dilindungi dengan baik. Lihat [10 praktik terbaik keamanan teratas untuk mengamankan cadangan di](#) posting AWS blog untuk panduan mengamankan cadangan Anda. Selain mengamankan

cadangan, Anda juga sebaiknya menguji proses pencadangan dan pemulihan Anda secara teratur untuk memverifikasi bahwa teknologi dan proses yang Anda miliki berfungsi sesuai harapan.

Otomatisasi forensik pada AWS

Ketika terjadi peristiwa keamanan, tim respons insiden Anda harus dapat mengumpulkan dan menganalisis bukti dengan cepat sambil mempertahankan akurasi untuk periode waktu yang mengitari peristiwa tersebut. Mengumpulkan bukti yang relevan di lingkungan cloud, terutama di sejumlah besar contoh dan akun secara manual merupakan hal yang menyulitkan sekaligus memakan waktu bagi tim respons insiden. Selain itu, kesalahan manusia rentan terjadi dalam pengumpulan secara manual. Untuk alasan ini, pelanggan harus mengembangkan dan menerapkan otomatisasi untuk forensik.

AWS menawarkan sejumlah sumber daya otomatisasi untuk forensik, yang dikonsolidasikan dalam Lampiran di bawah. [the section called “Sumber daya forensik”](#) Sumber daya ini adalah contoh pola forensik yang telah kami kembangkan dan telah diterapkan pelanggan. Meskipun sumber daya ini mungkin merupakan arsitektur referensi yang berguna untuk memulai, pertimbangkan untuk memodifikasinya atau membuat pola otomatisasi forensik baru berdasarkan lingkungan, persyaratan, alat, dan proses forensik Anda.

Ringkasan item persiapan

Persiapan menyeluruh untuk merespons peristiwa keamanan sangat penting agar respons insiden bisa dilakukan tepat waktu dan efektif. Persiapan respons insiden melibatkan orang, proses, dan teknologi. Ketiga domain ini sama pentingnya dalam persiapan. Anda harus mempersiapkan dan mengembangkan program respons insiden Anda di ketiga domain tersebut.

Tabel 2 merangkum item persiapan yang dijabarkan dalam bagian ini.

Tabel 2 – Item persiapan respons insiden

Domain	Item persiapan	Item tindakan
Orang	Menentukan peran dan tanggung jawab.	<ul style="list-style-type: none"> • Mengidentifikasi pemangku kepentingan respons insiden yang relevan. • Mengembangkan bagan yang bertanggung jawab, akuntabel, terinformasi,

Domain	Item persiapan	Item tindakan
		<p>berdasarkan konsultasi (RACI) untuk suatu insiden.</p>
Orang	<p>Latih staf respons insiden di AWS.</p>	<ul style="list-style-type: none"> • Melatih pemangku kepentingan respons insiden di AWS yayasan. • Melatih pemangku kepentingan respons insiden pada layanan AWS keamanan dan pemantauan. • Latih pemangku kepentingan respons insiden di AWS lingkungan Anda dan bagaimana hal itu dirancang.
Orang	<p>Memahami opsi AWS dukungan.</p>	<ul style="list-style-type: none"> • Memahami perbedaan dalam AWS dukungan, insinyur Respons Insiden Keamanan, tim respons DDoS (DRT) dan AMS. • Memahami jalur triase dan eskalasi untuk menjangkau teknisi Security Incident Response selama acara keamanan aktif jika diperlukan.

Domain	Item persiapan	Item tindakan
Proses	Mengembangkan rencana respons insiden.	<ul style="list-style-type: none"> • Buat dokumen tingkat tinggi yang mendefinisikan program dan strategi respons insiden Anda. • Sertakan RACI, rencana komunikasi, definisi insiden, dan fase respons insiden dalam rencana respons insiden.
Proses	Mendokumentasikan dan memusatkan diagram arsitektur.	<ul style="list-style-type: none"> • Dokumentasikan detail tentang bagaimana AWS lingkungan Anda dikonfigurasi di seluruh struktur akun, penggunaan layanan, pola IAM, dan fungsionalitas inti lainnya ke konfigurasi Anda AWS . • Mengembangkan diagram arsitektur untuk arsitektur cloud Anda.
Proses	Mengembangkan playbook respons insiden.	<ul style="list-style-type: none"> • Buat template untuk struktur buku pedoman Anda. • Membuat playbook untuk peristiwa keamanan yang diharapkan. • Buat buku pedoman untuk peringatan keamanan yang diketahui, seperti GuardDuty temuan.

Domain	Item persiapan	Item tindakan
Proses	Menjalankan simulasi reguler.	<ul style="list-style-type: none"> • Mengembangkan jadwal reguler untuk menjalankan simulasi insiden. • Menggunakan output dan pelajaran yang didapatkan untuk mengiterasi program respons insiden Anda.
Teknologi	Kembangkan struktur AWS akun.	<ul style="list-style-type: none"> • Rencanakan struktur akun untuk bagaimana beban kerja dipisahkan oleh AWS akun. • Membuat unit organisasi keamanan dengan alat keamanan dan akun pengarsipan log. • Membuat unit organisasi forensik dengan akun forensik untuk setiap Wilayah tempat Anda beroperasi.
Teknologi	Mengembangkan dan menerapkan strategi pemberian tag yang membantu responden untuk mengidentifikasi kepemilikan dan konteks temuan.	<ul style="list-style-type: none"> • Rencanakan strategi untuk menandai dan tag apa yang Anda inginkan terkait dengan AWS sumber daya Anda. • Menerapkan dan menegakkan strategi pemberian tag.

Domain	Item persiapan	Item tindakan
Teknologi	Perbarui informasi kontak AWS akun.	<ul style="list-style-type: none"> • Verifikasi bahwa AWS akun memiliki informasi kontak yang terdaftar. • Membuat daftar distribusi email untuk informasi kontak untuk menghapus satu titik kegagalan. • Lindungi akun email yang terkait dengan informasi AWS akun.
Teknologi	Siapkan akses ke AWS akun.	<ul style="list-style-type: none"> • Menentukan apa yang diperlukan oleh responden akses insiden untuk merespons suatu insiden. • Melaksanakan, menguji, dan memantau akses.
Teknologi	Memahami lanskap ancaman.	<ul style="list-style-type: none"> • Mengembangkan model ancaman untuk lingkungan dan aplikasi Anda. • Mengintegrasikan dan menggunakan intelijen ancaman siber.

Domain	Item persiapan	Item tindakan
Teknologi	Memilih dan mengatur log.	<ul style="list-style-type: none"> • Mengidentifikasi dan mengaktifkan log untuk penyelidikan. • Memilih penyimpanan log. • Mengidentifikasi dan menerapkan retensi log. • Mengembangkan mekanisme untuk mengambil dan query log dan artefak. • Menggunakan log untuk peringatan.
Teknologi	Mengembangkan kemampuan forensik.	<ul style="list-style-type: none"> • Mengidentifikasi artefak yang diperlukan untuk pengumpulan forensik. • Menangkap dan mengamankan cadangan sistem kunci. • Menentukan mekanisme untuk analisis log dan artefak yang diidentifikasi. • Menerapkan otomatisasi untuk analisis forensik.

Pendekatan berulang direkomendasikan untuk persiapan respons insiden. Semua item persiapan ini tidak dapat dilakukan dalam waktu singkat; Anda harus membuat rencana untuk memulai dari yang kecil dan terus meningkatkan kemampuan respons insiden Anda dari waktu ke waktu.

Operasi

Operasi adalah hal inti dalam melakukan respons insiden. Di sinilah tindakan merespons dan meremediasi insiden keamanan terjadi. Operasi meliputi lima fase berikut: deteksi, analisis,

penahanan, pemberantasan, dan pemulihan. Deskripsi fase dan tujuan ini dapat ditemukan pada Tabel 3.

Tabel 3 – Fase operasi

Fase	Tujuan
Deteksi	Mengidentifikasi peristiwa keamanan potensial.
Analisis	Tentukan apakah peristiwa keamanan adalah insiden dan menilai ruang lingkup insiden tersebut.
Penahanan	Meminimalkan dan membatasi cakupan peristiwa keamanan.
Pemberantasan	Menghapus sumber daya atau artefak tidak sah yang terkait dengan peristiwa keamanan. Menerapkan mitigasi yang menyebabkan insiden keamanan tersebut.
Pemulihan	Kembalikan sistem ke keadaan aman yang diketahui dan pantau sistem ini untuk memverifikasi bahwa ancaman tidak kembali.

Fase-fase ini akan berfungsi sebagai panduan ketika Anda merespons dan beroperasi pada insiden keamanan untuk merespons dengan cara yang efektif dan kuat. Tindakan aktual yang Anda ambil akan bervariasi, tergantung insiden Anda. Insiden yang melibatkan ransomware, misalnya, akan memiliki serangkaian langkah respons yang berbeda untuk diikuti dibandingkan insiden yang melibatkan bucket Amazon S3 publik. Selain itu, fase-fase ini tidak selalu terjadi secara berurutan. Setelah penahanan dan pemberantasan, Anda mungkin perlu kembali ke analisis untuk mengetahui apakah tindakan Anda efektif.

Deteksi

Peringatan adalah komponen utama dari fase deteksi. Ini menghasilkan pemberitahuan untuk memulai proses respons insiden berdasarkan aktivitas ancaman AWS akun yang menarik.

Akurasi peringatan merupakan hal yang menantang; terjadinya, berlangsungnya, atau akan terjadinya suatu insiden tidak selalu dapat ditentukan dengan pasti. Berikut ini beberapa alasannya:

- Mekanisme deteksi didasarkan pada simpangan dasar, pola yang diketahui, dan pemberitahuan dari entitas internal atau eksternal.
- Karena sifat teknologi dan manusia yang tidak dapat diprediksi, yaitu cara dan aktor insiden keamanan, garis dasar berubah seiring waktu. Pola nakal muncul melalui taktik, teknik, dan prosedur aktor ancaman baru atau yang dimodifikasi (TTPs).
- Perubahan pada orang, teknologi, dan proses tidak segera dimasukkan ke dalam proses respons insiden. Sebagian di antaranya ditemukan dalam proses penyelidikan.

Sumber peringatan

Anda sebaiknya mempertimbangkan sumber berikut untuk menentukan peringatan:

- Temuan — AWS layanan seperti [Amazon GuardDuty](#), [Amazon Macie](#), [AWS Security Hub CSPM](#), [Amazon Inspector](#), [IAM Access Analyzer](#), [AWS Config](#), dan [Network Access Analyzer](#) menghasilkan temuan yang dapat digunakan untuk membuat peringatan.
- Log — log AWS layanan, infrastruktur, dan aplikasi yang disimpan di bucket Amazon S3 dan grup CloudWatch log dapat diuraikan dan dikorelasikan untuk menghasilkan peringatan.
- Aktivitas penagihan – Perubahan mendadak dalam aktivitas penagihan dapat mengindikasikan adanya peristiwa keamanan. Ikuti dokumentasi tentang [Membuat alarm penagihan untuk memantau perkiraan AWS biaya Anda](#) untuk memantau hal ini.
- Intelijen ancaman siber – Jika Anda berlangganan feed intelijen ancaman siber pihak ketiga, Anda dapat menghubungkan informasi tersebut dengan alat pencatatan dan pemantauan lainnya untuk mengidentifikasi indikator potensial peristiwa.
- Alat partner – Partner di AWS Partner Network (APN) menawarkan produk unggulan yang dapat membantu Anda memenuhi tujuan keamanan Anda. Untuk respons insiden, produk partner dengan deteksi dan respons titik akhir (EDR) atau SIEM dapat membantu mendukung tujuan respons insiden Anda. Untuk informasi selengkapnya, lihat [Solusi Partner Keamanan](#) dan [Solusi Keamanan di AWS Marketplace](#).
- AWS kepercayaan dan keamanan — Dukungan dapat menghubungi pelanggan jika kami mengidentifikasi aktivitas kasar atau berbahaya.
- Sekali kontak – Karena sesuatu yang tidak biasa mungkin saja diperhatikan oleh pelanggan, developer, atau staf lain di organisasi Anda, penting agar Anda memiliki metode yang dikenali dan dipublikasikan dengan baik untuk menghubungi tim keamanan Anda. Pilihan populer

termasuk sistem tiket, alamat email kontak, dan formulir web. Jika organisasi Anda bekerja dengan masyarakat umum, Anda mungkin juga memerlukan mekanisme kontak keamanan yang digunakan publik.

Untuk informasi selengkapnya tentang kemampuan cloud yang dapat Anda gunakan selama penyelidikan, lihat [the section called “Lampiran A: Definisi kemampuan cloud”](#) di dokumen ini.

Deteksi sebagai bagian dari rekayasa kontrol keamanan

Mekanisme deteksi merupakan bagian integral dari pengembangan kontrol keamanan. Ketika kontrol direktif dan pencegahan ditentukan, kontrol detektif dan responsif terkait harus dibangun. Sebagai contoh, sebuah organisasi menetapkan kontrol direktif yang terkait dengan pengguna root AWS akun, yang seharusnya hanya digunakan untuk aktivitas spesifik dan sangat terdefinisi dengan baik. Mereka mengaitkannya dengan kontrol preventif yang diterapkan dengan menggunakan kebijakan kontrol layanan AWS organisasi (SCP). Jika aktivitas pengguna root di luar baseline yang diharapkan terjadi, kontrol detektif yang diterapkan dengan EventBridge aturan dan topik SNS akan memperingatkan pusat operasi keamanan (SOC). Dalam kontrol responsif, SOC memilih playbook yang sesuai, melakukan analisis, dan bekerja sampai insiden terselesaikan.

Kontrol keamanan paling baik ditentukan oleh pemodelan ancaman beban kerja yang berjalan di AWS. Tingkat kekritisannya kontrol detektif akan ditetapkan dengan melihat analisis dampak bisnis (BIA) untuk beban kerja tertentu. Peringatan yang dihasilkan oleh kontrol detektif tidak ditangani saat masuk, melainkan berdasarkan kekritisannya awalnya, untuk disesuaikan selama analisis. Set kekritisannya awal adalah bantuan untuk menentukan prioritas; konteks terjadinya peringatan akan menentukan kekritisannya sebenarnya. Sebagai contoh, sebuah organisasi menggunakan Amazon GuardDuty sebagai komponen kontrol detektif yang digunakan untuk instans EC2 yang merupakan bagian dari beban kerja. Temuan `Impact:EC2/SuspiciousDomainRequest.Reputation` ini dibuat, menginformasikan Anda bahwa instans Amazon EC2 yang terdaftar dalam beban kerja Anda sedang melakukan kueri terhadap nama domain yang dicurigai berbahaya. Peringatan ini ditetapkan secara default sebagai tingkat keparahan rendah, dan saat fase analisis berlangsung, ditentukan bahwa beberapa ratus instans EC2 jenis `p4d.24xlarge` telah digunakan oleh aktor yang tidak memiliki otorisasi, meningkatkan biaya operasi organisasi tersebut secara signifikan. Pada titik ini, tim respons insiden membuat keputusan untuk menyesuaikan kekritisannya peringatan ini menjadi tinggi, meningkatkan rasa urgensi dan mempercepat tindakan lebih lanjut. Perhatikan bahwa tingkat keparahan GuardDuty temuan tidak dapat diubah.

Menerapkan kontrol detektif

Penting untuk memahami bagaimana kontrol detektif diterapkan karena kontrol tersebut membantu menentukan bagaimana peringatan akan digunakan untuk peristiwa tertentu. Ada dua implementasi utama untuk kontrol detektif teknis:

- Deteksi perilaku bergantung pada model matematika yang biasa disebut sebagai machine learning (ML) atau kecerdasan buatan (AI). Deteksi dilakukan dengan inferensi; oleh karena itu, peringatan mungkin tidak mencerminkan peristiwa yang sebenarnya.
- Deteksi berbasis aturan bersifat deterministik; pelanggan dapat mengatur parameter yang tepat dari aktivitas apa yang akan memunculkan peringatan, dan itu bersifat pasti.

Implementasi modern sistem detektif, seperti sistem deteksi intrusi (IDS), umumnya memiliki dengan kedua mekanisme tersebut. Berikut adalah beberapa contoh untuk deteksi berbasis aturan dan perilaku dengan GuardDuty

- Ketika temuan `Exfiltration:IAMUser/AnomalousBehavior` dibuat, temuan tersebut menginformasikan bahwa “terdapat permintaan API anomali di akun Anda”. Saat Anda melihat lebih jauh ke dalam dokumentasi, ia memberi tahu Anda bahwa “Model ML mengevaluasi semua permintaan API di akun Anda dan mengidentifikasi peristiwa anomali yang terkait dengan teknik yang digunakan oleh musuh,” yang menunjukkan bahwa temuan ini bersifat perilaku.
- Untuk temuan GuardDuty ini `Impact:S3/MaliciousIPCaller`, menganalisis panggilan API dari layanan Amazon S3 di CloudTrail, membandingkan elemen `SourceIPAddress` log dengan tabel alamat IP publik yang mencakup umpan intelijen ancaman. Setelah menemukan kecocokan langsung dengan sebuah entri, temuan akan dihasilkan.

Kami merekomendasikan untuk menerapkan campuran peringatan berbasis perilaku dan aturan, karena menerapkan peringatan berbasis aturan untuk setiap aktivitas dalam model ancaman Anda bukanlah hal yang selalu memungkinkan.

Deteksi berbasis orang

Pada titik ini, kita telah membahas deteksi berbasis teknologi. Sumber deteksi penting lainnya berasal dari orang-orang di dalam atau di luar organisasi pelanggan. Orang dalam dapat didefinisikan sebagai karyawan atau kontraktor, dan orang luar adalah entitas seperti peneliti keamanan, penegak hukum, berita, dan media sosial.

Meskipun deteksi berbasis teknologi dapat dikonfigurasi secara sistematis, deteksi berbasis orang datang dalam berbagai bentuk seperti email, tiket, surat, kiriman berita, panggilan telepon, dan interaksi langsung. Notifikasi deteksi berbasis teknologi dapat diharapkan untuk dikirimkan secara hampir waktu nyata, tetapi deteksi berbasis orang tidak memiliki jadwal yang bisa diacu secara pasti. Sangat penting bahwa budaya keamanan menggabungkan, memfasilitasi, dan memberdayakan mekanisme deteksi berbasis orang untuk pendekatan pertahanan yang mendalam terhadap keamanan.

Ringkasan

Dengan deteksi, penting untuk memiliki campuran peringatan berbasis aturan dan perilaku. Selain itu, Anda harus memiliki mekanisme untuk orang, baik secara internal maupun eksternal, untuk mengirimkan tiket tentang masalah keamanan. Manusia dapat menjadi salah satu sumber paling berharga untuk peristiwa keamanan, jadi penting untuk memiliki proses bagi orang untuk mengeskalsikan kekhawatirannya. Anda sebaiknya menggunakan model ancaman lingkungan Anda untuk mulai membangun deteksi. Model ancaman akan membantu Anda membangun peringatan berdasarkan ancaman yang paling relevan dengan lingkungan Anda. Terakhir, Anda dapat menggunakan kerangka kerja seperti MITRE ATT&CK untuk memahami taktik, teknik, dan prosedur aktor ancaman (). TTPs Kerangka kerja MITRE ATT&CK dapat membantu untuk digunakan sebagai bahasa umum di berbagai mekanisme deteksi Anda.

Analisis

Log, kemampuan kueri, dan intelijen ancaman adalah beberapa komponen pendukung yang dibutuhkan oleh fase analisis. Banyak log yang digunakan untuk deteksi juga digunakan untuk analisis, dan akan memerlukan orientasi dan konfigurasi alat kueri.

Memvalidasi, menentukan cakupan, dan menilai dampak peringatan

Selama fase analisis, analisis log komprehensif dilakukan dengan tujuan untuk memvalidasi peringatan, menentukan ruang lingkup, dan menilai dampak dari kemungkinan kompromi.

- Validasi peringatan adalah titik masuk fase analisis. Responden insiden akan mencari entri log dari berbagai sumber dan langsung terlibat dengan pemilik beban kerja yang terdampak.
- Pencakupan adalah langkah berikutnya, ketika semua sumber daya yang terlibat diinventarisasi dan kekritisannya disesuaikan setelah pemangku kepentingan setuju bahwa peringatan tersebut tidak mungkin bersifat positif palsu.
- Terakhir, analisis dampak memerinci gangguan yang sebenarnya pada bisnis.

Setelah komponen beban kerja yang terpengaruh diidentifikasi, hasil pencakupan dapat dikorelasikan dengan sasaran titik pemulihan (RPO) beban kerja terkait dan sasaran waktu pemulihan (RTO), menyesuaikan tingkat kekritisan peringatan, yang akan memulai alokasi sumber daya dan semua aktivitas yang terjadi selanjutnya. Tidak semua insiden akan secara langsung mengganggu operasi beban kerja yang mendukung proses bisnis. Insiden seperti pengungkapan data sensitif, pencurian kekayaan intelektual, atau pembajakan sumber daya (seperti dalam penambangan mata uang kripto) mungkin tidak segera menghentikan atau melemahkan proses bisnis, tetapi dapat mengakibatkan konsekuensi ke depannya.

Memperkaya log dan temuan keamanan

Pengayaan dengan intelijen ancaman dan konteks organisasi

Selama proses analisis, hal yang menarik untuk diamati memerlukan pengayaan untuk meningkatkan kontekstualisasi peringatan. Sebagaimana dinyatakan dalam bagian Persiapan, mengintegrasikan dan memanfaatkan intelijen ancaman siber dapat membantu untuk memahami lebih lanjut tentang temuan keamanan. Layanan intelijen ancaman digunakan untuk menetapkan reputasi dan atribut kepemilikan ke alamat IP publik, nama domain, dan hash file. Alat-alat ini tersedia sebagai layanan berbayar dan tanpa biaya.

Pelanggan yang mengadopsi Amazon Athena sebagai alat kueri log mendapatkan keuntungan dari pekerjaan AWS Glue untuk memuat informasi intelijen ancaman sebagai tabel. Tabel intelijen ancaman dapat digunakan dalam kueri SQL untuk menghubungkan elemen log seperti alamat IP dan nama domain, sehingga memberikan tampilan yang diperkaya dari data yang akan dianalisis.

AWS tidak memberikan intelijen ancaman langsung kepada pelanggan, tetapi layanan seperti Amazon GuardDuty memanfaatkan intelijen ancaman untuk pengayaan dan generasi pencarian. Anda juga dapat mengunggah daftar ancaman khusus GuardDuty berdasarkan intelijen ancaman Anda sendiri.

Pengayaan dengan otomatisasi

Otomasi merupakan bagian integral dari AWS Cloud tata kelola. Hal ini dapat digunakan di berbagai fase siklus respons insiden.

Untuk fase deteksi, otomatisasi berbasis aturan mencocokkan pola yang menarik dari model ancaman dalam log dan mengambil tindakan yang sesuai, seperti mengirim pemberitahuan. Fase analisis dapat memanfaatkan mekanisme deteksi dan meneruskan isi peringatan ke mesin yang mampu mengueri log dan memperkaya hal-hal yang dapat diamati untuk kontekstualisasi peristiwa.

Isi peringatan, dalam bentuk fundamentalnya, terdiri dari sumber daya dan identitas. Sebagai contoh, Anda dapat menerapkan otomatisasi CloudTrail untuk kueri aktivitas AWS API yang dilakukan oleh identitas atau sumber daya badan peringatan di sekitar waktu peringatan, memberikan wawasan tambahan termasuk `eventSource`, `eventNameSourceIPAddress`, dan aktivitas API `userAgent` yang diidentifikasi. Dengan melakukan kueri ini secara otomatis, responden dapat menghemat waktu selama triase dan mendapatkan konteks tambahan untuk membantu membuat keputusan yang lebih tepat.

Lihat [Cara memperkaya temuan AWS Security Hub dengan posting blog metadata akun](#) untuk contoh tentang cara menggunakan otomatisasi untuk memperkaya temuan keamanan dan menyederhanakan analisis.

Mengumpulkan dan menganalisis bukti forensik

Forensik, sebagaimana disebutkan di bagian [the section called “Persiapan”](#) dokumen ini, adalah proses mengumpulkan dan menganalisis artefak selama respons insiden. Pada AWS, ini berlaku untuk sumber daya domain infrastruktur seperti tangkapan paket lalu lintas jaringan, dump memori sistem operasi, dan untuk sumber daya domain layanan seperti log. AWS CloudTrail

Proses forensik memiliki karakteristik mendasar sebagai berikut:

- Konsisten – Mengikuti langkah-langkah tepat yang didokumentasikan, tanpa menyimpang.
- Dapat Diulang – Menciptakan hasil yang sama persis ketika diulang terhadap artefak yang sama.
- Menjadi Norma – Didokumentasikan secara publik dan diadopsi secara luas.

Penting untuk mempertahankan rantai penahanan untuk artefak yang dikumpulkan selama respons insiden. Menggunakan otomatisasi dan membuat dokumentasi otomatis dari pengumpulan ini dapat membantu, selain menyimpan artefak dalam repositori hanya-baca. Analisis hanya boleh dilakukan pada replika yang tepat dari artefak yang dikumpulkan untuk menjaga integritas.

Mengumpulkan artefak yang relevan

Dengan mempertimbangkan karakteristik ini, dan berdasarkan peringatan yang relevan serta penilaian dampak dan cakupannya, Anda perlu mengumpulkan data yang relevan untuk penyelidikan dan analisis lebih lanjut. Berbagai jenis dan sumber data yang mungkin relevan dengan investigasi, termasuk log service/control pesawat (, peristiwa data Amazon S3CloudTrail, Log Aliran VPC), data (metadata dan objek Amazon S3), dan sumber daya (database, instans Amazon EC2).

Service/control log pesawat dapat dikumpulkan untuk analisis lokal atau, idealnya, langsung ditanyakan menggunakan AWS layanan asli (jika berlaku). Data (termasuk metadata) dapat langsung

ditanyakan untuk mendapatkan informasi yang relevan atau untuk memperoleh objek sumber; misalnya, gunakan untuk memperoleh bucket Amazon S3 dan metadata objek dan langsung memperoleh objek sumber. AWS CLI Sumber daya perlu dikumpulkan dengan cara yang konsisten dengan jenis sumber daya dan metode analisis yang dimaksudkan. Misalnya, database dapat dikumpulkan dengan membuat sistem yang copy/snapshot menjalankan database, membuat seluruh database itu sendiri, atau menanyakan dan mengekstrak data dan log tertentu dari database yang relevan dengan penyelidikan. copy/snapshot

Untuk instans Amazon EC2, ada set data tertentu yang harus dikumpulkan dan urutan spesifik untuk pengumpulan yang harus dilakukan guna memperoleh dan mempertahankan jumlah data terbanyak untuk analisis dan penyelidikan.

Secara khusus, urutan respon untuk memperoleh dan mempertahankan jumlah data terbanyak dari instans Amazon EC2 adalah sebagai berikut:

1. Dapatkan metadata instans — Dapatkan metadata instans yang relevan dengan penyelidikan dan kueri data (ID instans, jenis, alamat IP, ID, Wilayah VPC/subnet, ID Amazon Machine Image (AMI), grup keamanan yang dilampirkan, waktu peluncuran).
2. Mengaktifkan perlindungan instans dan tag – Aktifkan perlindungan instans seperti perlindungan dari penghentian, mengatur perilaku shutdown agar berhenti (jika diatur untuk melakukan penghentian), menonaktifkan atribut Delete on Termination untuk volume EBS yang terlampir, dan menerapkan tag yang sesuai untuk denotasi visual dan penggunaan dalam kemungkinan otomatisasi respon (misalnya, setelah menerapkan tag dengan nama Status dan nilai Quarantine, melakukan akuisisi data secara forensik dan mengisolasi instans).
3. Mendapatkan disk (snapshot EBS) – Dapatkan snapshot EBS dari volume EBS yang terlampir. Setiap snapshot berisi informasi yang Anda perlukan untuk memulihkan data Anda (dari saat ketika snapshot diambil) ke volume EBS baru. Lihat langkah untuk melakukan response/artifact koleksi langsung jika Anda menggunakan volume penyimpanan instance.
4. Memperoleh memori – Karena snapshot EBS hanya menangkap data yang telah ditulis ke volume Amazon EBS Anda, yang mungkin mengecualikan data yang disimpan atau di-cache dalam memori oleh aplikasi atau OS Anda, sangat penting untuk memperoleh gambar memori sistem menggunakan alat sumber terbuka atau komersial pihak ketiga yang sesuai untuk memperoleh data yang tersedia dari sistem.
5. (Opsional) Lakukan pengumpulan respon langsung/artefak — Lakukan pengumpulan data yang ditargetkan (disk/memori/logs) melalui respon langsung pada sistem hanya jika disk atau memori tidak dapat diperoleh sebaliknya, atau ada alasan bisnis atau operasional yang valid. Melakukan hal ini akan memodifikasi data sistem dan artefak yang berharga.

6. Menonaktifkan instance — Lepaskan instance dari grup Auto Scaling, deregister instance dari load balancer, dan sesuaikan atau terapkan profil instans bawaan dengan izin yang diminimalkan atau tanpa izin.
7. Mengisolasi atau memuat instans – Verifikasi bahwa instans secara efektif diisolasi dari sistem dan sumber daya lain dalam lingkungan dengan mengakhiri dan mencegah koneksi saat ini dan mendatang ke dan dari instans tersebut. Lihat bagian [the section called “Penahanan”](#) dari dokumen ini untuk lebih jelasnya.
8. Pilihan responden – Berdasarkan situasi dan tujuan, pilih salah satu dari yang berikut ini:
 - Nonaktifkan dan matikan sistem (disarankan).

Matikan sistem setelah bukti yang tersedia diperoleh untuk memverifikasi mitigasi paling efektif terhadap kemungkinan dampak masa depan terhadap lingkungan oleh instans.

- Terus jalankan instans dalam lingkungan terisolasi yang diinstrumentasi untuk pemantauan.

Meskipun tidak direkomendasikan sebagai pendekatan standar, jika suatu situasi memerlukan pengamatan lanjutan dari instance (seperti ketika data atau indikator tambahan diperlukan untuk melakukan penyelidikan dan analisis komprehensif instance), Anda dapat mempertimbangkan untuk mematikan instance, membuat AMI dari instance, dan meluncurkan kembali instance di akun forensik khusus Anda dalam lingkungan kotak pasir yang telah diinstrumentasi sebelumnya untuk sepenuhnya diisolasi dan dikonfigurasi dengan instrumentasi untuk memfasilitasi hampir berkelanjutan pemantauan instance (untuk contoh, VPC Flow Logs atau VPC Traffic Mirroring).

Note

Sangat penting untuk mengambil memori sebelum aktivitas respons langsung atau isolasi sistem atau mematikan sistem untuk mengambil data yang mudah menguap (dan berharga) yang tersedia.

Mengembangkan narasi

Selama analisis dan investigasi, dokumentasikan tindakan yang diambil, analisis yang dilakukan, dan informasi yang diidentifikasi, untuk digunakan oleh fase berikutnya dan laporan final. Narasi ini harus ringkas dan presisi, menegaskan bahwa informasi yang relevan disertakan untuk memverifikasi pemahaman yang efektif tentang insiden tersebut dan untuk mempertahankan garis waktu yang akurat. Narasi juga membantu ketika Anda melibatkan orang-orang di luar tim respons insiden inti. Inilah contohnya:

i Departemen pemasaran dan penjualan menerima surat pemerasan pada 15 Maret 2022 yang menuntut pembayaran dalam mata uang kripto jika tidak ingin data yang berpotensi sensitif dibocorkan ke publik. SOC menetapkan bahwa basis data Amazon RDS milik pemasaran dan penjualan dapat diakses publik pada 20 Februari 2022. SOC mengueri log akses RDS dan menentukan bahwa alamat IP 198.51.100.23 digunakan pada 20 Februari 2022 dengan kredensial *mm03434* milik Major Mary, salah satu developer web. SOC mengueri Log Alur VPC dan menentukan bahwa data berukuran sekitar 256 MB keluar ke alamat IP yang sama pada tanggal yang sama (cap waktu 2022-02-20T15:50+00Z). SOC menentukan melalui intelijen ancaman sumber terbuka bahwa kredensial saat ini tersedia dalam teks biasa di repositori publik [https\[:\]//example\[.\]com/majormary/rds-utils](https[:]//example[.]com/majormary/rds-utils).

Penahanan

Salah satu definisi penahanan, yang berkaitan dengan respons insiden, adalah proses atau implementasi strategi selama penanganan peristiwa keamanan yang bertindak untuk meminimalkan cakupan peristiwa keamanan dan menahan efek penggunaan yang tidak sah dalam lingkungan.

Strategi penahanan tergantung pada segudang faktor dan penerapan taktik penahanan, waktu, dan tujuannya dapat berbeda dari satu organisasi ke organisasi lain. [Panduan Penanganan Insiden Keamanan Komputer NIST SP 800-61](#) menguraikan beberapa kriteria untuk menentukan strategi penahanan yang tepat, yang meliputi:

- Potensi kerusakan dan pencurian sumber daya
- Kebutuhan preservasi bukti
- Ketersediaan layanan (konektivitas jaringan, layanan yang diberikan kepada pihak eksternal)
- Waktu dan sumber daya yang dibutuhkan untuk mengimplementasikan strategi
- Efektivitas strategi (penahanan sebagian atau penuh)
- Durasi solusi (solusi darurat akan dihapus dalam empat jam, solusi sementara akan dihapus dalam dua minggu, solusi permanen)

Mengenai layanan AWS, bagaimanapun, langkah-langkah penahanan mendasar dapat disuling menjadi tiga kategori:

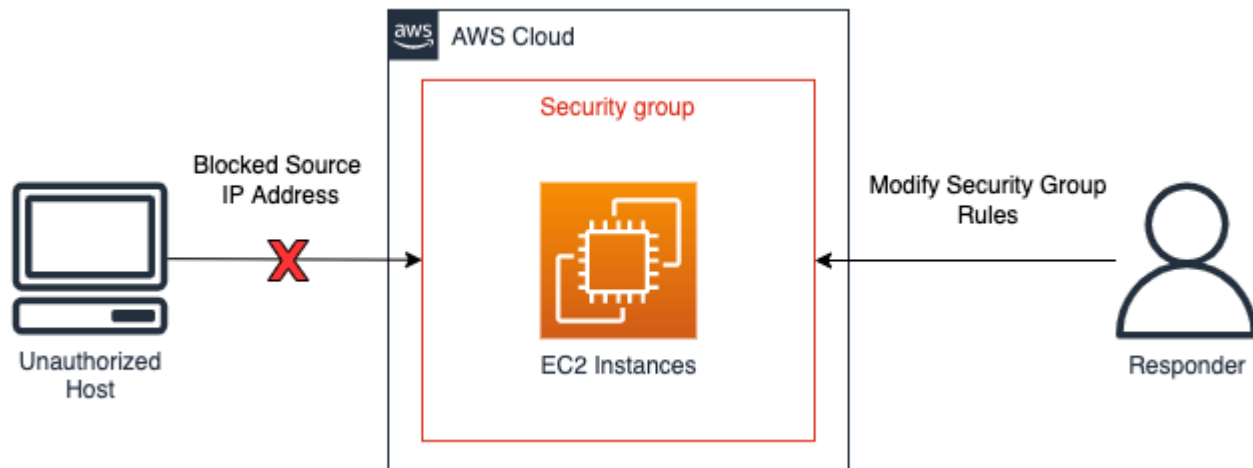
- Penahanan sumber – Gunakan penyaringan dan perutean untuk mencegah akses dari sumber tertentu.
- Teknik dan penahanan akses – Hapus akses untuk mencegah akses tidak sah ke sumber daya yang terpengaruh.
- Penahanan tujuan – Gunakan penyaringan dan perutean untuk mencegah akses ke sumber daya target.

Penahanan sumber

Penahanan sumber adalah penggunaan dan aplikasi penyaringan atau perutean dalam suatu lingkungan untuk mencegah akses ke sumber daya dari alamat IP sumber tertentu atau jangkauan jaringan. Contoh penahanan sumber menggunakan AWS layanan disorot di sini:

- Grup keamanan — Membuat dan menerapkan grup keamanan isolasi ke instans Amazon EC2 atau menghapus aturan dari grup keamanan yang ada dapat membantu memuat lalu lintas tidak sah ke instans atau sumber daya Amazon EC2. AWS Penting untuk dicatat bahwa koneksi terlacak yang ada tidak akan dimatikan sebagai akibat dari perubahan grup keamanan - hanya lalu lintas mendatang yang akan diblokir secara efektif oleh grup keamanan baru (lihat [Playbook Respons Insiden ini](#) dan [Pelacakan koneksi grup keamanan](#) untuk informasi tambahan tentang koneksi terlacak dan tidak terlacak).
- Kebijakan – Kebijakan bucket Amazon S3 dapat dikonfigurasi untuk memblokir atau mengizinkan lalu lintas dari alamat IP, rentang jaringan, atau titik akhir VPC. Kebijakan menciptakan kemampuan untuk memblokir alamat dan akses yang mencurigakan ke bucket Amazon S3. Informasi selengkapnya tentang kebijakan bucket dapat dilihat di [Menambahkan kebijakan bucket menggunakan konsol Amazon S3](#).
- AWS WAF Daftar kontrol akses web (web ACLs) dapat dikonfigurasi AWS WAF untuk memberikan kontrol halus atas permintaan web yang ditanggapi sumber daya. Anda dapat menambahkan alamat IP atau rentang jaringan ke set IP yang dikonfigurasi AWS WAF, dan menerapkan kondisi kecocokan, seperti blok, ke set IP. Hal ini akan memblokir permintaan web ke sumber daya jika alamat IP atau rentang jaringan dari lalu lintas asal sesuai dengan yang dikonfigurasi dalam aturan set IP.

Contoh penahanan sumber dapat dilihat pada diagram berikut ini dengan analisis respons insiden yang memodifikasi grup keamanan pada instans Amazon EC2 untuk membatasi koneksi baru hanya untuk alamat IP tertentu. Sebagaimana dinyatakan dalam poin grup keamanan, koneksi terlacak yang ada tidak akan dimatikan sebagai akibat dari perubahan grup keamanan.



Contoh penahanan sumber

Note

Grup Keamanan dan ACL Jaringan tidak memfilter lalu lintas ke Amazon Route 53. Saat berisi instans EC2, jika Anda ingin mencegahnya menghubungi host eksternal, pastikan Anda juga memblokir komunikasi DNS secara eksplisit.

Teknik dan penahanan akses

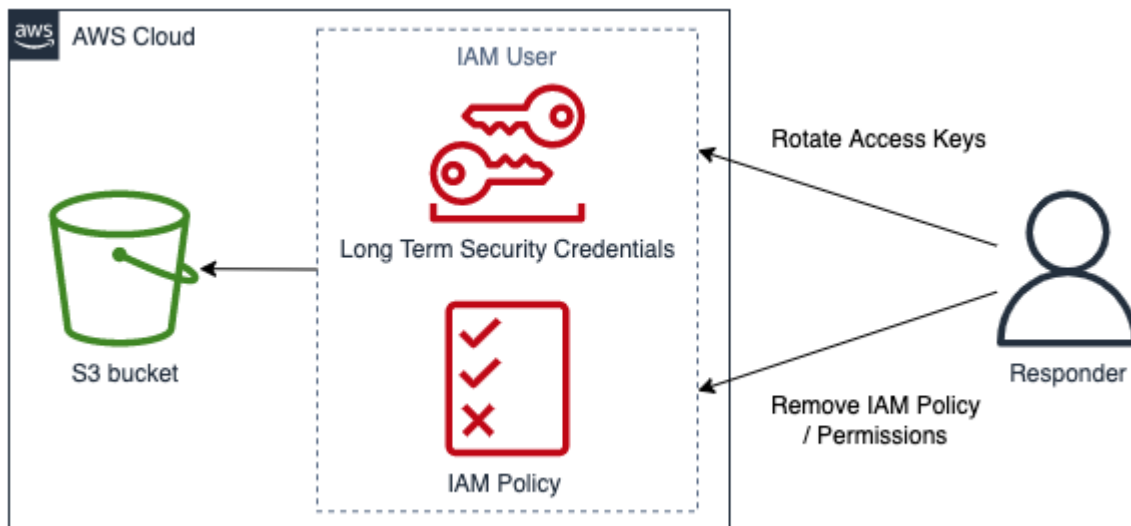
Mencegah penggunaan sumber daya yang tidak sah dengan membatasi fungsi dan pengguna utama IAM dengan akses ke sumber daya. Hal ini termasuk membatasi izin pengguna utama IAM yang memiliki akses ke sumber daya; juga termasuk pencabutan kredensial keamanan sementara. Contoh teknik dan akses penahanan menggunakan AWS layanan disorot di sini:

- **Membatasi izin** – Izin yang ditetapkan ke pengguna utama IAM harus mengikuti [Prinsip Hak Akses Paling Rendah](#). Namun, selama peristiwa keamanan aktif, Anda mungkin perlu membatasi akses ke sumber daya yang ditargetkan dari pengguna utama IAM tertentu lebih jauh. Dalam hal ini, akses ke sumber daya bisa ditahan dengan menghapus izin dari pengguna utama IAM yang akan ditahan. Ini dilakukan dengan layanan IAM dan dapat diterapkan menggunakan Konsol Manajemen AWS, AWS CLI, atau AWS SDK.
- **Mencabut kunci** – Kunci akses IAM digunakan oleh pengguna utama IAM untuk mengakses atau mengelola sumber daya. [Ini adalah kredensial statis jangka panjang untuk menandatangani permintaan terprogram ke AWS CLI atau AWS API dan dimulai dengan awalan AKIA \(untuk informasi tambahan, lihat bagian Memahami awalan ID unik di pengidentifikasi IAM\)](#). Untuk

menahan akses bagi pengguna utama IAM yang kunci akses IAM-nya telah disusupi, kunci akses dapat dinonaktifkan atau dihapus. Penting untuk memperhatikan hal-hal berikut ini:

- Kunci akses dapat diaktifkan kembali setelah dinonaktifkan.
- Kunci akses tidak dapat dipulihkan setelah dihapus.
- Seorang pengguna utama IAM dapat memiliki hingga dua kunci akses kapan saja.
- Pengguna atau aplikasi yang menggunakan kunci akses akan kehilangan akses setelah kunci tersebut dinonaktifkan atau dihapus.
- Mencabut kredensial keamanan sementara — Kredensial [keamanan sementara dapat digunakan oleh organisasi untuk mengontrol akses ke AWS sumber daya dan mulai dengan awalan ASIA \(untuk informasi tambahan, lihat bagian Memahami awalan ID unik di pengenalan IAM\)](#). Kredensial sementara biasanya digunakan oleh peran IAM dan tidak harus dirotasi atau dicabut secara eksplisit karena masa pakainya terbatas. Jika terjadi peristiwa keamanan yang melibatkan kredensial keamanan sementara sebelum masa berlaku kredensial keamanan sementara habis, Anda mungkin perlu mengubah izin efektif kredensial keamanan sementara yang ada. Hal ini dapat diselesaikan [menggunakan layanan IAM di dalam Konsol Manajemen AWS](#). Kredensial keamanan sementara juga dapat dikeluarkan untuk pengguna IAM (berlawanan dengan peran IAM); namun, pada saat artikel ini ditulis, tidak ada opsi untuk mencabut kredensial keamanan sementara untuk pengguna IAM di dalam Konsol Manajemen AWS. Untuk peristiwa keamanan di mana kunci akses IAM pengguna disusupi oleh pengguna yang tidak sah yang membuat kredensial keamanan sementara, kredensial keamanan sementara dapat dicabut menggunakan dua metode:
 - Lampirkan kebijakan sebaris ke pengguna IAM yang mencegah akses berdasarkan waktu penerbitan token keamanan (lihat bagian Menolak akses ke kredensial keamanan sementara yang dikeluarkan sebelum waktu spesifik di [Menonaktifkan izin untuk kredensial keamanan sementara](#) untuk detail selengkapnya).
 - Hapus pengguna IAM yang memiliki kunci akses yang disusupi. Buat ulang pengguna jika diperlukan.
- AWS WAF- Teknik tertentu yang digunakan oleh pengguna yang tidak sah termasuk pola lalu lintas berbahaya yang umum, seperti permintaan yang berisi injeksi SQL dan skrip lintas situs (XSS). AWS WAF dapat dikonfigurasi untuk mencocokkan dan menolak lalu lintas menggunakan teknik ini menggunakan pernyataan aturan AWS WAF bawaan.

Contoh teknik dan penahanan akses dapat dilihat pada diagram berikut, dengan responden insiden merotasi kunci akses atau menghapus kebijakan IAM untuk mencegah pengguna IAM mengakses bucket Amazon S3.



Contoh teknik dan penahanan akses

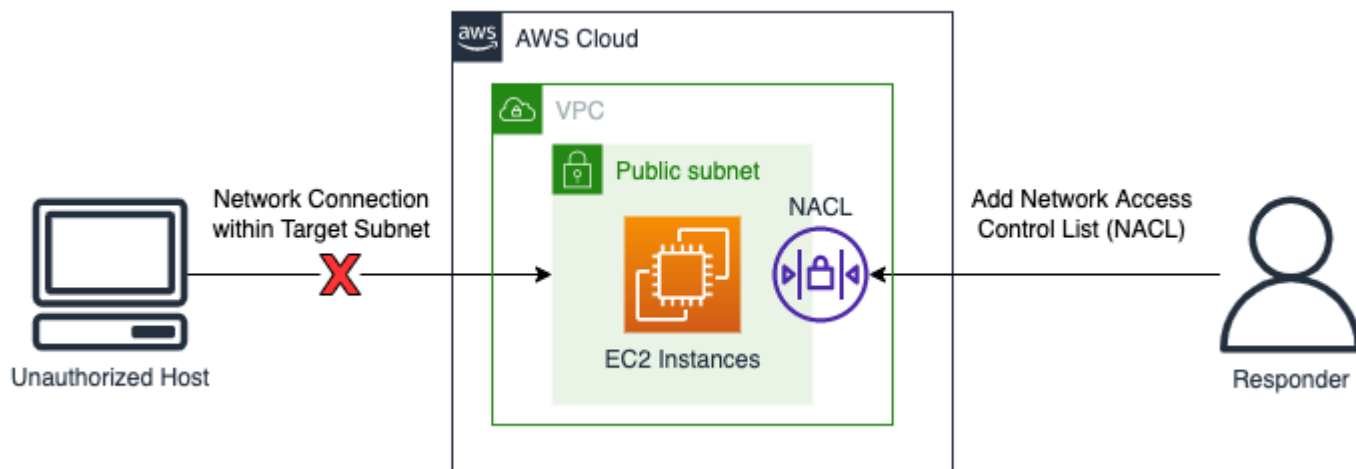
Penahanan tujuan

Penahanan tujuan adalah aplikasi penyaringan atau perutean dalam suatu lingkungan untuk mencegah akses ke host atau sumber daya yang ditargetkan. Dalam beberapa kasus, penahanan tujuan juga melibatkan suatu bentuk ketahanan untuk memverifikasi bahwa sumber daya yang sah direplikasi untuk ketersediaan; sumber daya harus dilepaskan dari bentuk-bentuk ketahanan ini untuk isolasi dan penahanan. Contoh penahanan tujuan menggunakan AWS layanan meliputi:

- Jaringan ACLs — Jaringan ACLs (jaringan ACLs) yang dikonfigurasi pada subnet yang berisi AWS sumber daya dapat memiliki aturan penolakan yang ditambahkan. Aturan penolakan ini dapat diterapkan untuk mencegah akses ke AWS sumber daya tertentu; Namun, menerapkan daftar kontrol akses jaringan (ACL jaringan) akan memengaruhi setiap sumber daya di subnet, tidak hanya sumber daya yang diakses tanpa otorisasi. Aturan yang tercantum dalam ACL jaringan diproses dalam urutan top-down, sehingga aturan pertama dalam ACL jaringan yang ada harus dikonfigurasi untuk menolak lalu lintas yang tidak sah ke sumber daya dan subnet yang ditargetkan. Atau, ACL jaringan yang sama sekali baru dapat dibuat dengan aturan penolakan tunggal untuk lalu lintas masuk dan keluar dan terkait dengan subnet yang berisi sumber daya yang ditargetkan untuk mencegah akses ke subnet menggunakan ACL jaringan baru.
- Mematikan sumber daya – Mematikan sumber daya sepenuhnya dapat efektif dalam menahan efek penggunaan yang tidak sah. Mematikan sumber daya juga akan mencegah akses yang sah untuk kebutuhan bisnis dan mencegah diperolehnya data forensik yang mudah berubah, jadi ini harus merupakan keputusan yang disengaja dan harus dinilai berdasarkan kebijakan keamanan organisasi.

- **Isolasi VPCs** — Isolasi VPC dapat digunakan untuk menyediakan penahanan sumber daya yang efektif sambil menyediakan akses ke lalu lintas yang sah (seperti solusi anti-virus (AV) atau EDR yang memerlukan akses ke internet atau konsol manajemen eksternal). VPC isolasi dapat dikonfigurasi terlebih dahulu sebelum peristiwa keamanan untuk mengizinkan alamat IP dan port yang valid, dan sumber daya yang ditargetkan dapat segera dipindahkan ke dalam VPC isolasi ini selama peristiwa keamanan aktif untuk menahan sumber daya sambil memungkinkan lalu lintas yang sah dikirim dan diterima oleh sumber daya yang ditargetkan selama fase respons insiden berikutnya. Aspek penting dalam menggunakan VPC isolasi adalah sumber daya, seperti instans EC2, harus dimatikan dan diluncurkan kembali di VPC isolasi yang baru sebelum digunakan. Instans EC2 yang ada tidak dapat dipindahkan ke VPC atau Zona Ketersediaan lainnya. Untuk melakukannya, ikuti langkah-langkah yang diuraikan dalam [Bagaimana cara memindahkan instans Amazon EC2 saya ke subnet, Zona Ketersediaan, atau VPC lainnya?](#)
- **Grup Auto Scaling dan penyeimbang beban** — AWS sumber daya yang melekat pada grup Auto Scaling dan penyeimbang beban harus dilepas dan dideregistrasi sebagai bagian dari prosedur penahanan tujuan. Detasemen dan deregistrasi AWS sumber daya dapat dilakukan dengan menggunakan, dan SDK. Konsol Manajemen AWS AWS CLI AWS

Contoh penahanan tujuan ditunjukkan dalam diagram berikut dengan analisis respons insiden menambahkan ACL jaringan ke subnet untuk memblokir permintaan koneksi jaringan dari host yang tidak sah.



Contoh penahanan tujuan

Ringkasan

Penahanan adalah salah satu langkah dari proses respons insiden dan dapat dilakukan secara manual atau otomatis. Strategi penahanan keseluruhan harus selaras dengan kebijakan keamanan

organisasi dan kebutuhan bisnis, dan memverifikasi bahwa efek negatif dikurangi seefisien mungkin sebelum pemberantasan dan pemulihan.

Pemberantasan

Pemberantasan, dalam kaitannya dengan respons insiden keamanan, adalah penghapusan sumber daya yang mencurigakan atau tidak sah dalam upaya mengembalikan akun ke kondisi aman yang diketahui. Strategi pemberantasan bergantung pada beberapa faktor, yang berkaitan dengan persyaratan bisnis untuk organisasi Anda.

Beberapa langkah pemberantasan tersedia di [NIST SP 800-61 Computer Security Incident Handling Guide](#):

1. Identifikasi dan mitigasi semua kerentanan yang dieksploitasi.
2. Hapus malware, materi yang tidak pantas, dan komponen lainnya.
3. Jika ternyata ada banyak host yang terpengaruh (misalnya, infeksi malware baru), ulangi langkah-langkah deteksi dan analisis untuk mengidentifikasi semua host lain yang terkena dampak, lalu tahan dan berantas insiden untuk host-host tersebut.

Untuk AWS sumber daya, ini dapat disempurnakan lebih lanjut melalui peristiwa yang terdeteksi dan dianalisis melalui log yang tersedia atau perkakas otomatis seperti CloudWatch Log dan Amazon GuardDuty. Peristiwa-peristiwa tersebut harus menjadi dasar untuk menentukan remediasi mana yang harus dilakukan untuk memulihkan lingkungan ke kondisi aman yang diketahui.

Langkah pertama pemberantasan adalah menentukan sumber daya mana yang terpengaruh dalam akun. AWS Hal ini dicapai melalui analisis sumber data log yang tersedia, sumber daya, dan alat otomatis.

- Identifikasi tindakan tidak sah yang diambil oleh identitas IAM di akun Anda.
- Identifikasi akses yang tidak sah atau perubahan pada akun Anda.
- Identifikasi pembuatan sumber daya atau pengguna IAM yang tidak sah.
- Identifikasi sistem atau sumber daya dengan perubahan yang tidak sah.

Setelah daftar sumber daya diidentifikasi, Anda harus menilai setiap sumber daya untuk menentukan dampak bisnis jika sumber daya dihapus atau dipulihkan. Sebagai contoh, jika server web menghosting aplikasi bisnis Anda dan menghapus server tersebut akan menyebabkan waktu henti, Anda harus mempertimbangkan untuk memulihkan sumber daya dari cadangan aman yang

diverifikasi atau meluncurkan ulang sistem dari AMI yang bersih sebelum menghapus server yang terkena dampak.

Setelah Anda menyimpulkan analisis dampak bisnis Anda, maka, dengan menggunakan peristiwa dari analisis log Anda, Anda harus masuk ke akun dan melakukan remediasi yang sesuai, seperti:

- Merotasi atau menghapus kunci - langkah ini menghilangkan kemampuan aktor untuk terus melakukan aktivitas di dalam akun.
- Merotasi kredensial pengguna IAM yang berpotensi tidak sah.
- Menghapus sumber daya yang tidak dikenal atau tidak sah.

Important

Jika Anda harus menyimpan sumber daya untuk penyelidikan Anda, pertimbangkan untuk mencadangkan sumber daya tersebut. Misalnya, jika Anda harus mempertahankan instans Amazon EC2 untuk alasan peraturan, kepatuhan, atau hukum, [buat snapshot Amazon EBS](#) sebelum menghapus instans tersebut.

- Untuk infeksi malware, Anda mungkin perlu menghubungi vendor AWS Partner atau vendor lain. AWS tidak menawarkan alat asli untuk analisis atau penghapusan malware. Namun, jika Anda menggunakan modul GuardDuty Malware untuk Amazon EBS, maka rekomendasi mungkin tersedia untuk temuan yang disediakan.

Setelah Anda menghapus sumber daya yang teridentifikasi, AWS sarankan Anda melakukan tinjauan keamanan akun Anda. Ini dapat dilakukan dengan menggunakan AWS Config aturan, menggunakan solusi open-source seperti Prowler dan ScoutSuite, atau melalui vendor lain. Anda juga dapat mempertimbangkan untuk melakukan pemindaian kerentanan terhadap sumber daya yang digunakan publik (internet) untuk menilai risiko residual.

Pemberantasan adalah salah satu langkah dari proses respons insiden dan dapat dilakukan secara manual atau otomatis, tergantung insiden dan sumber daya yang terpengaruh. Strategi keseluruhan harus selaras dengan kebijakan keamanan dan kebutuhan bisnis organisasi, dan memverifikasi bahwa efek negatif dimitigasi saat sumber daya atau konfigurasi yang tidak sesuai dihapus.

Pemulihan

Pemulihan adalah proses memulihkan sistem ke keadaan aman yang diketahui, memvalidasi bahwa cadangan aman atau tidak terpengaruh oleh insiden sebelum restorasi, pengujian untuk

memverifikasi bahwa sistem berfungsi dengan baik setelah restorasi, dan mengatasi kerentanan yang terkait dengan peristiwa keamanan.

Urutan pemulihan bergantung pada kebutuhan organisasi Anda. Sebagai bagian dari proses pemulihan, Anda harus melakukan analisis dampak bisnis untuk menentukan, setidaknya:

- Prioritas bisnis atau dependensi
- Rencana restorasi
- Autentikasi dan otorisasi

NIST SP 800-61 Computer Security Incident Handling Guide menyediakan beberapa langkah untuk memulihkan sistem, termasuk:

- Memulihkan sistem dari cadangan bersih.
 - Verifikasi bahwa cadangan dievaluasi sebelum memulihkan ke sistem untuk memastikan bahwa infeksi tidak ada dan untuk mencegah kebangkitan peristiwa keamanan.

Cadangan harus dievaluasi secara teratur sebagai bagian dari pengujian pemulihan bencana untuk memverifikasi bahwa mekanisme cadangan berfungsi dengan baik dan integritas data memenuhi tujuan titik pemulihan.

- Jika memungkinkan, gunakan cadangan dari sebelum stempel waktu kejadian pertama yang diidentifikasi sebagai bagian dari analisis akar masalah.
- Membangun kembali sistem dari awal, termasuk memindahkan dari sumber tepercaya menggunakan otomatisasi, kadang-kadang di akun baru. AWS
- Mengganti file yang disusupi dengan versi bersih.

Anda harus sangat berhati-hati saat melakukan ini. Anda harus benar-benar yakin bahwa file yang Anda pulihkan diketahui aman dan tidak terpengaruh oleh insiden tersebut

- Menginstal patch.
- Mengubah kata sandi.
 - Hal ini termasuk kata sandi untuk pengguna utama IAM yang mungkin telah disalahgunakan.
 - Jika memungkinkan, sebaiknya gunakan peran untuk pengguna utama dan federasi IAM sebagai bagian dari strategi hak akses paling rendah.
- Memperketat keamanan perimeter jaringan (aturan firewall, daftar kontrol akses router batas).

Setelah sumber daya dipulihkan, penting untuk mengambil pelajaran yang dapat dipetik untuk memperbarui kebijakan, prosedur, dan panduan respons insiden.

Singkatnya, sangat penting untuk menerapkan proses pemulihan yang memfasilitasi kembalinya ke operasi aman yang diketahui. Pemulihan dapat memakan waktu lama dan membutuhkan hubungan yang erat dengan strategi penahanan untuk menyeimbangkan dampak bisnis terhadap risiko infeksi ulang. Prosedur pemulihan harus mencakup langkah-langkah untuk memulihkan sumber daya dan layanan, pengguna utama IAM, dan melakukan tinjauan keamanan akun untuk menilai risiko residual.

Kesimpulan

Setiap fase operasi memiliki tujuan, teknik, metodologi, dan strategi yang unik. Tabel 4 merangkum fase-fase ini dan beberapa teknik serta metodologi yang tercakup dalam bagian ini.

Tabel 4 – Fase operasi: Tujuan, teknik, dan metodologi

Fase	Tujuan	Teknik dan metodologi
Deteksi	Mengidentifikasi peristiwa keamanan potensial.	<ul style="list-style-type: none"> • Kontrol keamanan untuk deteksi • Deteksi berbasis perilaku dan aturan • Deteksi berbasis orang
Analisis	Menentukan apakah peristiwa keamanan tersebut merupakan insiden dan menilai cakupan insiden tersebut.	<ul style="list-style-type: none"> • Memvalidasi dan membuat cakupan peringatan • Log kueri • Intelijen ancaman • Otomatisasi
Penahanan	Meminimalkan dan membatasi dampak peristiwa keamanan.	<ul style="list-style-type: none"> • Penahanan sumber • Teknik dan penahanan akses • Penahanan tujuan
Pemberantasan	Menghapus sumber daya atau artefak tidak sah yang terkait dengan peristiwa keamanan.	<ul style="list-style-type: none"> • Rotasi atau penghapusan kredensial yang disusupi atau tidak sah

Fase	Tujuan	Teknik dan metodologi
		<ul style="list-style-type: none"> • Penghapusan sumber daya yang tidak sah • Penghapusan malware • Pemindaian keamanan
Pemulihan	Mengembalikan sistem ke kondisi yang diketahui baik dan pantau sistem ini untuk memastikan ancaman tidak kembali.	<ul style="list-style-type: none"> • Pemulihan sistem dari cadangan • Sistem dibangun kembali dari awal • File yang disusupi diganti dengan versi bersih

Aktivitas pascainsiden

Lanskap ancaman terus berubah dan penting agar organisasi Anda memiliki kemampuan yang juga dinamis untuk melindungi lingkungan Anda secara efektif. Kunci untuk perbaikan berkelanjutan adalah mengulangi hasil insiden dan simulasi Anda untuk meningkatkan kemampuan Anda untuk secara efektif mendeteksi, merespons, dan menyelidiki kemungkinan insiden keamanan, mengurangi kemungkinan kerentanan Anda, waktu untuk merespons, dan kembali ke operasi yang aman. Mekanisme berikut dapat membantu Anda memverifikasi bahwa organisasi Anda tetap siap dengan kemampuan dan pengetahuan terbaru untuk merespons secara efektif, apa pun situasinya.

Menetapkan kerangka kerja untuk belajar dari insiden

Menerapkan kerangka kerja dan metodologi pembelajaran tidak hanya akan membantu meningkatkan kemampuan respons insiden, tetapi juga membantu mencegah insiden terulang kembali. Dengan belajar dari setiap kejadian, Anda dapat membantu menghindari terulangnya kesalahan, eksposur, atau kesalahan konfigurasi, yang tidak hanya meningkatkan postur keamanan Anda, tetapi juga meminimalkan waktu yang terbuang untuk situasi yang dapat dicegah.

Penting untuk menerapkan kerangka kerja pembelajaran dan meraih poin-poin berikut di tingkatan tinggi:

- Kapan pembelajaran diadakan?
- Apa saja yang terlibat dalam proses pembelajaran tersebut?

- Bagaimana pembelajaran dilakukan?
- Siapa yang terlibat dalam proses tersebut dan bagaimana caranya?
- Bagaimana cara mengenali area yang perlu ditingkatkan?
- Bagaimana Anda memastikan perbaikan dilacak dan diimplementasikan secara efektif?

Selain dari hasil tingkat tinggi yang tercantum di atas, penting untuk memastikan bahwa Anda mengajukan pertanyaan yang tepat untuk mendapatkan nilai terbaik (informasi yang mengarah pada peningkatan yang dapat ditindaklanjuti) dari proses tersebut. Pertimbangkan pertanyaan-pertanyaan ini untuk membantu Anda memulai dalam mendorong diskusi pembelajaran Anda:

- Apa insiden yang terjadi?
- Kapan insiden tersebut pertama kali diidentifikasi?
- Bagaimana insiden tersebut diidentifikasi?
- Sistem apa yang memunculkan peringatan tentang aktivitas tersebut?
- Sistem, layanan, dan data apa yang terlibat?
- Secara khusus, apa yang terjadi?
- Apa yang berjalan dengan baik?
- Apa yang tidak berjalan dengan baik?
- Proses atau prosedur mana yang gagal atau tidak dapat diskalakan untuk merespons insiden tersebut?
- Apa yang dapat ditingkatkan dalam bidang berikut:
 - Orang
 - Apakah orang-orang yang perlu dihubungi benar-benar tersedia dan apakah daftar kontak sudah aktual?
 - Apakah orang-orang tidak mendapatkan pelatihan atau tidak memiliki kemampuan yang diperlukan untuk merespons dan menyelidiki insiden tersebut secara efektif?
 - Apakah sumber daya yang sesuai siap dan tersedia?
 - Proses
 - Apakah proses dan prosedur diikuti?
 - Apakah proses dan prosedur didokumentasikan dan tersedia untuk (jenis) insiden ini?
 - Apakah proses dan prosedur yang diperlukan tidak ada?
 - Apakah responden dapat memperoleh akses tepat waktu ke informasi yang diperlukan untuk merespons masalah ini?

- Teknologi
 - Apakah sistem peringatan yang ada mampu mengidentifikasi dan memperingatkan tentang aktivitas tersebut secara efektif?
 - Apakah peringatan yang ada perlu ditingkatkan atau apakah peringatan baru perlu dibangun untuk (jenis) insiden ini?
 - Apakah alat yang ada membuat penyelidikan (pencarian/analisis) insiden tersebut dapat dilakukan secara efektif?
- Apa yang dapat dilakukan untuk membantu mengidentifikasi (jenis) insiden ini lebih cepat?
- Apa yang dapat dilakukan untuk membantu mencegah (jenis) insiden ini terjadi lagi?
- Siapa yang bertanggung jawab atas rencana peningkatan dan bagaimana cara untuk menguji apakah rencana tersebut telah diimplementasikan?
- Apa timeline untuk monitoring/preventative kontrol/proses tambahan yang akan diimplementasikan dan diuji?

Daftar ini tidak mencakup semua; hal ini dimaksudkan untuk berfungsi sebagai titik awal guna mengidentifikasi kebutuhan organisasi dan bisnis dan bagaimana Anda dapat menganalisisnya agar dapat belajar secara efektif dari insiden dan terus meningkatkan postur keamanan Anda. Yang paling penting adalah memulai dengan memasukkan pembelajaran yang diambil sebagai bagian standar dari proses respons insiden, dokumentasi, dan ekspektasi di seluruh pemangku kepentingan.

Menetapkan metrik keberhasilan

Metrik diperlukan untuk mengukur, menilai, dan meningkatkan kemampuan respons insiden Anda secara efektif. Tanpa metrik, Anda tidak memiliki referensi untuk mengukur secara akurat atau bahkan mengidentifikasi seberapa baik (atau buruk) performa organisasi Anda. Ada beberapa metrik umum untuk respons insiden yang merupakan titik awal yang baik bagi organisasi yang ingin menetapkan ekspektasi serta referensi untuk berupaya mewujudkan keunggulan operasional.

Waktu rata-rata untuk mendeteksi

Waktu rata-rata untuk mendeteksi adalah waktu rata-rata yang diperlukan untuk menemukan kemungkinan insiden keamanan. Secara khusus, ini adalah waktu antara terjadinya indikator penyusupan pertama dan identifikasi atau peringatan awal.

Anda dapat menggunakan metrik ini untuk melacak seberapa efektif performa sistem deteksi dan peringatan Anda. Mekanisme deteksi dan peringatan yang efektif adalah kunci untuk memverifikasi bahwa kemungkinan insiden keamanan tidak berlangsung lama di lingkungan Anda.

Makin tinggi waktu rata-rata deteksi, makin besar kebutuhan untuk membangun peringatan dan mekanisme tambahan atau yang lebih efektif untuk mengidentifikasi dan menemukan kemungkinan insiden keamanan. Makin rendah waktu rata-rata deteksi, makin baik fungsi mekanisme deteksi dan peringatan Anda.

Waktu rata-rata untuk mengakui

Waktu rata-rata untuk mengakui adalah waktu rata-rata yang diperlukan untuk mengakui dan memprioritaskan kemungkinan insiden keamanan. Secara khusus, ini adalah waktu antara pembuatan peringatan dan anggota SOC Anda atau staf respons insiden mengidentifikasi dan memprioritaskan peringatan untuk diproses.

Anda dapat menggunakan metrik ini untuk melacak seberapa baik tim Anda memproses dan memprioritaskan peringatan. Jika tim Anda tidak dapat mengidentifikasi dan memprioritaskan peringatan secara efektif, respons akan tertunda dan menjadi tidak efektif.

Makin tinggi waktu rata-rata untuk mengakui, makin besar kebutuhan untuk memverifikasi bahwa tim Anda memiliki sumber daya yang memadai dan terlatih untuk dengan cepat mengetahui dan memprioritaskan kemungkinan insiden keamanan untuk direspons. Makin rendah waktu rata-rata untuk mengakui, makin baik tim Anda dalam merespons peringatan keamanan, yang menunjukkan bahwa mereka melakukan persiapan secara efektif dan mampu menentukan prioritas dengan baik.

Waktu rata-rata untuk merespons

Waktu rata-rata untuk merespons adalah waktu rata-rata yang diperlukan untuk memulai respons awal terhadap kemungkinan insiden keamanan. Secara khusus, ini adalah waktu antara peringatan awal atau penemuan kemungkinan insiden keamanan dan tindakan pertama yang diambil untuk merespons. Ini mirip dengan waktu rata-rata untuk mengakui, tetapi ini merupakan pengukuran tindakan responsif tertentu (misalnya, memperoleh data sistem, menahan sistem), bukan pengenalan atau pengakuan sederhana atas situasinya.

Anda dapat menggunakan metrik ini untuk melacak kesiapan Anda dalam merespons insiden keamanan. Seperti disebutkan, persiapan adalah kunci untuk respons yang efektif. Lihat bagian [the section called “Persiapan”](#) dari dokumen ini.

Makin tinggi waktu rata-rata untuk merespons, makin besar kebutuhan untuk memverifikasi bahwa tim Anda dilatih dengan baik tentang cara merespons sehingga proses respons didokumentasikan dan digunakan secara efektif. Makin rendah waktu rata-rata untuk merespons, makin baik tim Anda dalam mengidentifikasi respons yang tepat terhadap peringatan yang teridentifikasi dan melakukan tindakan responsif yang diperlukan untuk memulai pengembalian ke operasi yang aman.

Waktu rata-rata untuk menahan

Waktu rata-rata untuk menahan adalah waktu rata-rata yang diperlukan untuk menahan kemungkinan insiden keamanan. Secara khusus, ini adalah waktu antara peringatan awal atau penemuan kemungkinan insiden keamanan dan penyelesaian tindakan responsif yang secara efektif mencegah penyerang atau sistem yang dikompromikan dari melakukan kerusakan lebih lanjut.

Anda dapat menggunakan metrik ini untuk melacak seberapa baik tim Anda dapat memitigasi atau menahan kemungkinan insiden keamanan. Ketidakmampuan untuk menahan kemungkinan insiden keamanan secara cepat dan efektif akan meningkatkan dampak, cakupan, dan eksposur dari kemungkinan penyusupan lebih lanjut.

Makin tinggi waktu rata-rata untuk menahan, makin besar kebutuhan untuk membangun pengetahuan dan kemampuan agar dapat mengurangi dan menahan insiden keamanan yang Anda alami dengan cepat dan efektif. Makin rendah waktu rata-rata untuk menahan, makin baik tim Anda dalam memahami dan menggunakan langkah-langkah yang diperlukan untuk memitigasi dan menahan ancaman yang teridentifikasi guna mengurangi dampak, cakupan, dan risiko terhadap bisnis.

Waktu rata-rata untuk pulih

Waktu rata-rata untuk memulihkan adalah waktu rata-rata yang diperlukan untuk sepenuhnya kembali ke operasi yang aman dari kemungkinan insiden keamanan. Secara khusus, ini adalah waktu antara peringatan awal atau penemuan kemungkinan insiden keamanan dan ketika bisnis kembali beroperasi secara normal dan aman tanpa terpengaruh oleh insiden tersebut.

Anda dapat menggunakan metrik ini untuk melacak seberapa efektif tim Anda dalam mengembalikan sistem, akun, dan lingkungan ke operasi yang aman setelah insiden keamanan terjadi. Ketidakmampuan untuk kembali ke operasi yang aman dengan cepat atau efektif tidak hanya dapat berdampak pada keamanan, tetapi juga dapat meningkatkan dampak dan biaya bagi bisnis dan operasinya.

Semakin tinggi waktu rata-rata untuk pulih, semakin besar kebutuhan untuk mempersiapkan tim dan lingkungan Anda untuk memiliki mekanisme yang sesuai (misalnya, proses failover dan CI/CD saluran pipa untuk menerapkan kembali sistem bersih yang aman) untuk meminimalkan dampak insiden keamanan terhadap operasi dan bisnis. Makin rendah waktu rata-rata untuk pulih, makin efektif tim Anda dalam meminimalkan dampak insiden keamanan pada operasi dan bisnis Anda.

Waktu tinggal penyerang

Waktu tinggal penyerang adalah waktu rata-rata bahwa pengguna yang tidak sah memiliki akses ke sistem atau lingkungan. Hal ini mirip dengan waktu rata-rata untuk menahan, tetapi kerangka waktu ini dimulai dengan waktu awal penyerang memperoleh akses ke sistem atau lingkungan, yang mungkin lebih awal dari peringatan atau penemuan awal.

Anda dapat menggunakan metrik ini untuk melacak seberapa baik sistem dan mekanisme Anda bekerja sama untuk mengurangi jumlah waktu, akses, dan kesempatan yang dimiliki penyerang atau ancaman untuk memengaruhi lingkungan Anda. Mengurangi waktu tinggal penyerang harus menjadi prioritas utama bagi tim dan bisnis Anda.

Makin tinggi waktu tinggal penyerang, makin besar kebutuhan untuk mengidentifikasi bagian mana dari proses respons insiden yang perlu ditingkatkan untuk memastikan kemampuan tim Anda dalam meminimalkan dampak dan cakupan ancaman atau serangan di lingkungan Anda. Makin rendah waktu tinggal penyerang, makin baik tim Anda meminimalkan waktu dan peluang yang dimiliki ancaman atau penyerang dalam lingkungan Anda, yang pada akhirnya mengurangi risiko dan dampak terhadap operasi dan bisnis Anda.

Ringkasan metrik

Membuat dan melacak metrik untuk respons insiden memungkinkan Anda mengukur, menilai, dan meningkatkan kemampuan respons insiden secara efektif. Untuk mencapai hal ini, ada sejumlah metrik respons insiden umum yang disorot di bagian ini. Tabel 5 merangkum metrik-metrik ini.

Tabel 5 – Metrik respons insiden

Metrik	Deskripsi
Waktu rata-rata untuk mendeteksi	Waktu rata-rata yang diperlukan untuk menemukan kemungkinan insiden keamanan
Waktu rata-rata untuk mengakui	Waktu rata-rata yang diperlukan untuk mengakui (dan memprioritaskan) kemungkinan insiden keamanan
Waktu rata-rata untuk merespons	Waktu rata-rata yang diperlukan untuk memulai respons awal terhadap kemungkinan insiden keamanan

Metrik	Deskripsi
Waktu rata-rata untuk menahan	Waktu rata-rata yang diperlukan untuk menahan kemungkinan insiden keamanan
Waktu rata-rata untuk pulih	Waktu rata-rata yang diperlukan untuk sepenuhnya kembali ke operasi yang aman dari kemungkinan insiden keamanan
Waktu tinggal penyerang	Waktu rata-rata pengguna yang tidak sah memiliki akses ke sistem atau lingkungan

Gunakan indikator kompromi (IOC)

Indikator kompromi (IOC) adalah artefak yang diamati di dalam atau pada jaringan, sistem, atau lingkungan yang dapat (dengan tingkat kepercayaan tinggi) mengidentifikasi aktivitas berbahaya atau insiden keamanan. IOCs dapat ada dalam berbagai bentuk, termasuk alamat IP, domain, artefak tingkat jaringan seperti bendera atau muatan TCP, artefak sistem atau tingkat host seperti executable, nama file dan hash, entri file log, atau entri registri, dan banyak lagi. IOC juga dapat berupa kombinasi item atau aktivitas, seperti keberadaan item atau artefak tertentu pada sistem (file tertentu atau set file dan item registri), tindakan yang dilakukan dalam urutan tertentu (masuk ke sistem dari IP tertentu diikuti oleh perintah anomali tertentu), atau aktivitas jaringan (lalu lintas masuk atau keluar anomali ke atau dari domain tertentu) yang dapat menunjukkan ancaman, serangan, atau metodologi penyerang tertentu.

Saat Anda bekerja untuk meningkatkan program respons insiden secara berulang, Anda harus menerapkan kerangka kerja untuk mengumpulkan, mengelola, dan memanfaatkan IOCs sebagai mekanisme untuk terus membangun dan meningkatkan deteksi dan peringatan serta meningkatkan kecepatan dan kemanjuran investigasi. Anda dapat mulai dengan memasukkan pengumpulan dan pengelolaan IOCs ke dalam fase analisis dan investigasi dari proses respons insiden Anda. Dengan secara proaktif mengidentifikasi, mengumpulkan, dan menyimpan IOCs sebagai bagian standar dari proses Anda, Anda dapat membangun repositori data (sebagai bagian dari program intelijen ancaman yang lebih komprehensif) yang pada gilirannya dapat digunakan untuk meningkatkan deteksi dan peringatan yang ada, membangun deteksi dan peringatan tambahan, mengidentifikasi di mana dan kapan artefak terlihat sebelumnya, membangun dan mereferensikan dokumentasi tentang bagaimana investigasi sebelumnya dilakukan yang melibatkan pencocokan, dan banyak lagi. IOCs

Pendidikan dan pelatihan berkelanjutan

Pendidikan dan pelatihan merupakan upaya yang terus berkembang dan berkelanjutan yang harus diupayakan dan dipertahankan. Ada berbagai mekanisme untuk memverifikasi bahwa tim Anda menjaga kewaspadaan, pengetahuan, dan kemampuan yang sejalan dengan perkembangan teknologi serta lanskap ancaman.

Salah satu mekanismenya adalah menggunakan pendidikan berkelanjutan sebagai bagian standar dari tujuan dan operasi tim Anda. Seperti yang disebutkan di bagian Persiapan, staf dan pemangku kepentingan respons insiden Anda harus dilatih secara efektif dalam mendeteksi, menanggapi, dan menyelidiki insiden di dalamnya. AWS Namun, pendidikan bukanlah upaya yang “sekali jadi”. Pendidikan harus terus dijalankan untuk memverifikasi bahwa tim Anda dapat mengikuti kemajuan teknologi terbaru, informasi terbaru, dan peningkatan yang dapat dimanfaatkan untuk meningkatkan efektivitas dan efisiensi respons, serta penambahan atau pembaruan pada data yang dapat dimanfaatkan untuk meningkatkan penyelidikan dan analisis.

Mekanisme lain adalah memverifikasi bahwa simulasi dilakukan secara teratur (misalnya, setiap triwulan) dan berfokus pada hasil spesifik untuk bisnis. Lihat bagian [the section called “Menjalankan simulasi reguler”](#) dari dokumen ini.

Meskipun menjalankan latihan meja awal adalah cara terbaik untuk menghasilkan dasar awal untuk perbaikan, pengujian berkelanjutan adalah kunci untuk perbaikan berkelanjutan dan mempertahankan refleksi yang up-to-date akurat dari keadaan operasi saat ini. Menguji situasi keamanan terbaru dan paling kritis dan kemampuan respons yang paling penting atau terbaru, dan memasukkan pelajaran yang dipetik kembali ke dalam pendidikan, operasi, dan processes/procedures akan memverifikasi bahwa Anda dapat terus meningkatkan proses dan program respons Anda secara keseluruhan.

Kesimpulan

Saat Anda melanjutkan perjalanan cloud Anda, penting bagi Anda untuk mempertimbangkan konsep respons insiden keamanan mendasar untuk AWS lingkungan Anda. Anda dapat menggabungkan kontrol yang tersedia, kemampuan cloud, dan opsi remediasi untuk membantu Anda meningkatkan keamanan lingkungan cloud Anda. Anda juga dapat memulai dari yang kecil dan melakukan iterasi saat Anda mengadopsi kemampuan otomatisasi yang meningkatkan kecepatan respons Anda, sehingga Anda menjadi lebih siap saat peristiwa keamanan terjadi.

Kontributor

Kontributor saat ini dan terdahulu untuk dokumen ini meliputi:

- Anna McAbee, Arsitek Solusi Keamanan Senior, Amazon Web Services
- Freddy Kasprzykowski, Senior Security Consultant, Amazon Web Services
- Jason Hurst, Insinyur Keamanan Senior, Amazon Web Services
- Jonathon Poling, Principal Security Consultant, Amazon Web Services
- Josh Du Lac, Senior Manager, Security Solutions Architecture, Amazon Web Services
- Paco Hope, Insinyur Keamanan Utama, Amazon Web Services
- Ryan Tick, Senior Security Engineer, Amazon Web Services
- Steve de Vera, Insinyur Keamanan Senior, Amazon Web Services

Lampiran A: Definisi kemampuan cloud

AWS menawarkan lebih dari 200 layanan cloud dan ribuan fitur. Banyak di antaranya menyediakan kemampuan detektif, pencegahan, dan responsif native, dan lainnya dapat digunakan untuk merancang solusi keamanan khusus. Bagian ini mencakup sebagian dari layanan yang paling relevan dengan respons insiden di cloud.

Topik

- [Pencatatan log dan peristiwa](#)
- [Visibilitas dan peringatan](#)
- [Otomatisasi](#)
- [Penyimpanan aman](#)
- [Kemampuan Keamanan Masa Depan dan Kustom](#)

Pencatatan log dan peristiwa

[AWS CloudTrail](#)— AWS CloudTrail layanan yang memungkinkan tata kelola, kepatuhan, audit operasional, dan audit risiko akun. AWS Dengan CloudTrail, Anda dapat log, terus memantau, dan mempertahankan aktivitas akun yang terkait dengan tindakan di seluruh AWS layanan. CloudTrail menyediakan riwayat peristiwa aktivitas AWS akun Anda, termasuk tindakan yang diambil melalui Konsol Manajemen AWS, AWS SDKs, alat baris perintah, dan AWS layanan lainnya. Riwayat

peristiwa ini menyederhanakan analisis keamanan, pelacakan perubahan sumber daya, dan pemecahan masalah. CloudTrail mencatat dua jenis tindakan AWS API yang berbeda:

- CloudTrail Peristiwa manajemen (juga dikenal sebagai operasi pesawat kontrol) menunjukkan operasi manajemen yang dilakukan pada sumber daya di AWS akun Anda. Hal ini termasuk tindakan seperti membuat bucket Amazon S3 dan menyiapkan pencatatan log.
- CloudTrail Peristiwa data (juga dikenal sebagai operasi bidang data) menunjukkan operasi sumber daya yang dilakukan pada atau di dalam sumber daya di AWS akun Anda. Operasi ini sering kali merupakan aktivitas bervolume tinggi. Hal ini mencakup tindakan seperti aktivitas API tingkat objek Amazon S3 (misalnya, operasi API `GetObject`, `DeleteObject`, dan `PutObject`) dan aktivitas invokasi fungsi Lambda.

[AWS Config](#)— AWS Config adalah layanan yang memungkinkan pelanggan menilai, mengaudit, dan mengevaluasi konfigurasi sumber daya Anda AWS . 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 AWS Config, pelanggan dapat meninjau perubahan konfigurasi dan hubungan antar AWS sumber daya, secara manual atau otomatis, riwayat konfigurasi sumber daya terperinci, dan menentukan kepatuhan keseluruhan terhadap konfigurasi yang ditentukan dalam pedoman pelanggan. Hal ini memungkinkan penyederhanaan audit kepatuhan, analisis keamanan, manajemen perubahan, dan pemecahan masalah operasional.

[Amazon EventBridge](#) — Amazon EventBridge memberikan aliran peristiwa sistem yang mendekati real-time yang menjelaskan perubahan AWS sumber daya, atau saat panggilan API dipublikasikan oleh AWS CloudTrail. Dengan menggunakan aturan sederhana yang dapat Anda atur dengan cepat, Anda dapat mencocokkan acara dan mengarahkannya ke satu atau lebih fungsi atau aliran target. EventBridge menjadi sadar akan perubahan operasional saat terjadi. EventBridge dapat menanggapi perubahan operasional ini dan mengambil tindakan korektif seperlunya, dengan mengirim pesan untuk merespons lingkungan, mengaktifkan fungsi, membuat perubahan, dan menangkap informasi negara. Beberapa layanan keamanan, seperti Amazon GuardDuty, menghasilkan output mereka dalam bentuk EventBridge acara. Banyak layanan keamanan juga menyediakan opsi untuk mengirim output-nya ke Amazon S3.

Log akses Amazon S3 – Jika informasi sensitif disimpan dalam bucket Amazon S3, pelanggan dapat mengaktifkan log akses Amazon S3 untuk merekam setiap unggahan, unduhan, dan modifikasi data tersebut. Log ini terpisah dari, dan sebagai tambahan, CloudTrail log yang mencatat perubahan pada bucket itu sendiri (seperti mengubah kebijakan akses dan kebijakan siklus hidup). Perlu diketahui bahwa catatan log akses server disampaikan atas dasar upaya terbaik. Sebagian besar permintaan

bucket yang dikonfigurasi dengan benar untuk mencatat hasil dalam catatan log yang dikirim. Kelengkapan dan ketepatan waktu pencatatan server tidak dijamin.

[CloudWatch Log Amazon](#) — Pelanggan dapat menggunakan CloudWatch Log Amazon untuk memantau, menyimpan, dan mengakses file log yang berasal dari sistem operasi, aplikasi, dan sumber lain yang berjalan di instans Amazon EC2 dengan CloudWatch agen Log. CloudWatch Log dapat menjadi tujuan untuk AWS CloudTrail, Kueri DNS Route 53, Log Aliran VPC, fungsi Lambda, dan lainnya. Pelanggan kemudian dapat mengambil data log terkait dari CloudWatch Log.

[Log Alur Amazon VPC](#) – Log Alur VPC memungkinkan pelanggan untuk menangkap informasi tentang lalu lintas IP ke dan dari antarmuka jaringan di VPC. Setelah mengaktifkan flow log, mereka dapat dialirkan ke Amazon CloudWatch Logs dan Amazon S3. Log Alur VPC membantu pelanggan dengan sejumlah tugas seperti pemecahan masalah lalu lintas tertentu yang tidak mencapai instans, mendiagnosis aturan grup keamanan yang terlalu ketat, dan menggunakannya sebagai alat keamanan untuk memantau lalu lintas ke instans EC2. Gunakan pencatatan alur VPC versi terbaru untuk mendapatkan bidang yang paling kuat.

[AWS WAF Log](#) — AWS WAF mendukung pencatatan penuh dari semua permintaan web yang diperiksa oleh layanan. Pelanggan dapat menyimpannya di Amazon S3 untuk memenuhi persyaratan kepatuhan dan audit, serta debugging dan forensik. Log ini membantu pelanggan menentukan akar penyebab aturan yang dimulai dan permintaan web yang diblokir. Log dapat diintegrasikan dengan SIEM pihak ketiga dan alat analisis log.

[Log kueri Route 53 Resolver](#) – Log kueri Route 53 Resolver akan memungkinkan Anda mencatat semua kueri DNS yang dibuat oleh sumber daya dalam Amazon Virtual Private Cloud (Amazon VPC). Baik itu instans Amazon EC2, AWS Lambda fungsi, atau wadah, jika itu hidup di VPC Amazon Anda dan membuat kueri DNS, maka fitur ini akan mencatatnya; Anda kemudian dapat menjelajahi dan lebih memahami bagaimana aplikasi Anda beroperasi.

AWS Log lain — AWS terus merilis fitur dan kemampuan layanan untuk pelanggan dengan kemampuan logging dan pemantauan baru. Untuk informasi tentang fitur yang tersedia untuk setiap AWS layanan, lihat dokumentasi publik kami.

Visibilitas dan peringatan

[Respons Insiden Keamanan AWS](#)- Respons Insiden Keamanan AWS adalah layanan komprehensif yang membantu organisasi menangani peristiwa keamanan sepanjang siklus hidup mereka dengan menggabungkan kemampuan otomatis dengan dukungan manusia ahli. Layanan ini memanfaatkan fitur pemantauan dan investigasi otomatis untuk membebaskan sumber daya organisasi sambil mempertahankan pengawasan keamanan yang waspada, dan ketika peristiwa keamanan terjadi,

ini memfasilitasi komunikasi dan koordinasi yang dipercepat di antara para pemangku kepentingan untuk waktu respons yang cepat. Layanan ini mendukung beberapa kasus penggunaan, termasuk persiapan dan simulasi peristiwa keamanan, respons terhadap insiden aktif, dan pelaporan dan analisis pasca-insiden yang efisien, memastikan organisasi dilengkapi dengan baik untuk menangani tantangan keamanan di setiap tahap.

[AWS Security Hub CSPM](#)— AWS Security Hub CSPM memberi pelanggan pandangan komprehensif tentang peringatan keamanan prioritas tinggi dan status kepatuhan di seluruh akun. AWS Security Hub CSPM mengumpulkan, mengatur, dan memprioritaskan temuan ancaman dari layanan AWS seperti Amazon Inspector, GuardDuty Amazon Macie, dan solusi AWS Partner Temuan dirangkum secara visual pada dasbor terintegrasi dengan grafik dan tabel yang dapat ditindaklanjuti. Anda juga dapat terus memantau lingkungan Anda menggunakan pemeriksaan kepatuhan otomatis berdasarkan praktik AWS terbaik dan standar industri yang diikuti organisasi Anda.

[Amazon GuardDuty](#) GuardDuty adalah layanan deteksi ancaman terkelola yang terus memantau perilaku berbahaya atau tidak sah untuk membantu pelanggan melindungi AWS akun dan beban kerja. Layanan ini memantau aktivitas seperti panggilan API yang tidak biasa atau deployment yang berpotensi tidak sah yang menunjukkan kemungkinan pembobolan akun atau sumber daya instans Amazon EC2, bucket Amazon S3, atau pengintaian oleh pihak yang tidak bertanggung jawab.

GuardDuty mengidentifikasi tersangka pelaku jahat melalui umpan intelijen ancaman terintegrasi menggunakan pembelajaran mesin untuk mendeteksi anomali dalam aktivitas akun dan beban kerja. Ketika ancaman potensial terdeteksi, layanan memberikan peringatan keamanan terperinci ke GuardDuty konsol dan CloudWatch Acara. Hal ini membuat peringatan dapat ditindaklanjuti dan mudah diintegrasikan ke dalam manajemen peristiwa dan sistem alur kerja yang ada.

GuardDuty juga menawarkan dua add-on untuk memantau ancaman dengan layanan tertentu: Amazon GuardDuty untuk perlindungan Amazon S3 dan Amazon GuardDuty untuk perlindungan Amazon EKS. Perlindungan Amazon S3 memungkinkan GuardDuty untuk memantau operasi API tingkat objek untuk mengidentifikasi potensi risiko keamanan untuk data dalam bucket Amazon S3. Perlindungan Kubernetes memungkinkan GuardDuty untuk mendeteksi aktivitas mencurigakan dan potensi kompromi kluster Kubernetes di Amazon EKS.

[Amazon Macie](#) - Amazon Macie adalah layanan keamanan bertenaga AI yang membantu mencegah kehilangan data dengan secara otomatis menemukan, mengklasifikasikan, dan melindungi data sensitif yang disimpan. AWS Macie menggunakan machine learning (ML) untuk mengenali data sensitif seperti informasi pengenal pribadi (PII) atau kekayaan intelektual, menetapkan nilai bisnis, dan memberikan visibilitas ke tempat data ini disimpan dan bagaimana data tersebut digunakan dalam organisasi Anda. Amazon Macie terus memantau adanya anomali dalam aktivitas akses data,

dan memberikan peringatan ketika mendeteksi risiko akses tidak sah atau kebocoran data yang tidak disengaja.

[Aturan AWS Config](#) AWS Config Aturan mewakili konfigurasi yang disukai untuk sumber daya dan dievaluasi terhadap perubahan konfigurasi pada sumber daya yang relevan, seperti yang dicatat oleh. AWS Config Anda dapat melihat hasil evaluasi aturan terhadap konfigurasi sumber daya di dasbor. Dengan menggunakan AWS Config aturan, Anda dapat menilai kepatuhan dan status risiko secara keseluruhan dari perspektif konfigurasi, melihat tren kepatuhan dari waktu ke waktu, dan menemukan perubahan konfigurasi mana yang menyebabkan sumber daya tidak sesuai dengan aturan.

[AWS Trusted Advisor](#)— AWS Trusted Advisor adalah sumber daya online untuk membantu Anda mengurangi biaya, meningkatkan kinerja, dan meningkatkan keamanan dengan mengoptimalkan AWS lingkungan Anda. Trusted Advisor memberikan panduan waktu nyata untuk membantu Anda menyediakan sumber daya Anda dengan mengikuti praktik AWS terbaik. Set lengkap Trusted Advisor pemeriksaan, termasuk integrasi CloudWatch Acara, tersedia untuk pelanggan paket Business and Enterprise Support.

[Amazon CloudWatch](#) — Amazon CloudWatch adalah layanan pemantauan untuk AWS Cloud sumber daya dan aplikasi yang Anda jalankan AWS. Anda dapat menggunakannya CloudWatch untuk mengumpulkan dan melacak metrik, mengumpulkan dan memantau file log, mengatur alarm, dan secara otomatis bereaksi terhadap perubahan sumber daya Anda AWS . CloudWatch dapat memantau AWS sumber daya, seperti instans Amazon EC2, tabel Amazon DynamoDB, dan instans Amazon RDS DB, serta metrik khusus yang dihasilkan oleh aplikasi dan layanan Anda, dan file log apa pun yang dihasilkan aplikasi Anda. Anda dapat menggunakan Amazon CloudWatch untuk mendapatkan visibilitas seluruh sistem ke dalam pemanfaatan sumber daya, kinerja aplikasi, dan kesehatan operasional. Anda dapat menggunakan wawasan ini untuk bereaksi dengan tepat dan menjaga aplikasi Anda tetap berjalan dengan lancar.

[Amazon Inspector](#) - Amazon Inspector adalah layanan penilaian keamanan otomatis yang membantu meningkatkan keamanan dan kepatuhan aplikasi yang digunakan. AWS Amazon Inspector secara otomatis menilai kerentanan atau penyimpangan dari praktik terbaik pada aplikasi. Setelah melakukan penilaian, Amazon Inspector menghasilkan daftar detail temuan keamanan yang diprioritaskan berdasarkan tingkat keparahan. Temuan ini dapat ditinjau secara langsung atau sebagai bagian dari laporan penilaian terperinci yang tersedia melalui konsol Amazon Inspector atau API.

[Amazon Detective](#) — Amazon Detective adalah layanan keamanan yang secara otomatis mengumpulkan data log dari AWS sumber daya Anda dan menggunakan pembelajaran mesin,

analisis statistik, dan teori grafik untuk membangun kumpulan data terkait yang memungkinkan Anda melakukan investigasi keamanan yang lebih cepat dan lebih efisien. Detective dapat menganalisis triliunan peristiwa dari berbagai sumber data seperti VPC Flow Logs, dan, dan CloudTrail GuardDuty, dan secara otomatis membuat tampilan interaktif terpadu dari sumber daya, pengguna, dan interaksi Anda di antara mereka dari waktu ke waktu. Dengan pandangan terpadu ini, Anda dapat memvisualisasikan semua detail dan konteks di satu tempat untuk mengidentifikasi alasan yang mendasari temuan, menggali aktivitas historis yang relevan, dan menentukan akar penyebabnya dengan cepat.

Otomatisasi

[AWS Lambda](#)— AWS Lambda adalah layanan komputasi tanpa server yang menjalankan kode Anda sebagai respons terhadap peristiwa, dan secara otomatis mengelola sumber daya komputasi yang mendasarinya untuk Anda. Anda dapat menggunakan Lambda untuk memperluas AWS layanan lain dengan logika khusus, atau membuat layanan backend Anda sendiri yang beroperasi pada AWS skala, kinerja, dan keamanan. Lambda menjalankan kode Anda pada infrastruktur komputasi dengan ketersediaan tinggi dan melakukan administrasi sumber daya komputasi untuk Anda. Hal ini termasuk pemeliharaan server dan sistem operasi, penyediaan kapasitas dan penskalaan otomatis, deployment kode dan patch keamanan, serta pemantauan dan pencatatan kode. Anda hanya tinggal menyediakan kode.

[AWS Step Functions](#)— AWS Step Functions membuatnya mudah untuk mengoordinasikan komponen aplikasi terdistribusi dan layanan mikro menggunakan alur kerja visual. Step Functions menyediakan konsol grafis bagi Anda untuk mengatur dan memvisualisasikan komponen aplikasi Anda sebagai serangkaian langkah. Hal ini memudahkan Anda untuk membangun dan menjalankan aplikasi multilangkah. Step Functions secara otomatis memulai dan melacak setiap langkah, dan mencoba kembali ketika ada kesalahan, sehingga aplikasi Anda berjalan sesuai urutan dan seperti yang diharapkan.

Step Functions mencatat status setiap langkah, jadi ketika terjadi kesalahan, Anda dapat mendiagnosis dan melakukan debug masalah dengan cepat. Anda dapat mengubah dan menambahkan langkah-langkah tanpa menulis kode, sehingga Anda dapat mengembangkan aplikasi Anda dan berinovasi lebih cepat. AWS Step Functions adalah bagian dari AWS Tanpa Server, dan membuatnya mudah untuk mengatur fungsi untuk aplikasi tanpa server. AWS Lambda Anda juga dapat menggunakan Step Functions untuk orkestrasi layanan mikro menggunakan sumber daya komputasi seperti Amazon EC2 dan Amazon ECS.

[AWS Systems Manager](#) — AWS Systems Manager memberi Anda visibilitas dan kontrol atas AWS infrastruktur Anda. Systems Manager menyediakan antarmuka pengguna terpadu sehingga

Anda dapat melihat data operasional dari beberapa AWS layanan, dan memungkinkan Anda untuk mengotomatiskan tugas operasional di seluruh sumber daya Anda AWS . Dengan Systems Manager, Anda dapat mengelompokkan sumber daya berdasarkan aplikasi, melihat data operasional untuk pemantauan dan pemecahan masalah, dan bertindak pada kelompok sumber daya Anda. Systems Manager dapat menyimpan instans Anda dalam status yang ditentukan, melakukan perubahan sesuai permintaan, seperti memperbarui aplikasi atau menjalankan skrip shell, serta melakukan tugas otomatisasi dan patching lainnya.

Penyimpanan aman

[Amazon Simple Storage Service](#) – Amazon S3 adalah penyimpanan objek yang dibuat untuk menyimpan dan mengambil sejumlah data dari mana saja. Penyimpanan ini dirancang untuk memberikan daya tahan 99,999999999%, dan menyimpan data untuk jutaan aplikasi yang digunakan oleh para pemimpin pasar di setiap industri. Amazon S3 memberikan keamanan komprehensif dan dirancang untuk membantu Anda memenuhi persyaratan peraturan Anda. Ini memberi pelanggan fleksibilitas dalam metode yang mereka gunakan untuk mengelola data untuk pengoptimalan biaya, kontrol akses, dan kepatuhan. Amazon S3 menyediakan query-in-place fungsionalitas, yang memungkinkan Anda menjalankan analitik yang kuat langsung pada data Anda saat istirahat di Amazon S3. Amazon S3 adalah layanan penyimpanan cloud yang sangat didukung, dengan integrasi dari salah satu komunitas terbesar solusi pihak ketiga, mitra integrator sistem, dan layanan lainnya.

AWS

[Amazon Glacier — Amazon](#) Glacier adalah layanan penyimpanan cloud yang aman, tahan lama, dan sangat murah untuk pengarsipan data dan pencadangan jangka panjang. Layanan ini dirancang untuk memberikan ketahanan 99,999999999%, keamanan komprehensif dan dirancang untuk membantu Anda memenuhi persyaratan peraturan Anda. Amazon Glacier query-in-place menyediakan fungsionalitas, yang memungkinkan Anda menjalankan analitik yang kuat secara langsung pada data arsip Anda saat istirahat. Untuk menjaga biaya tetap rendah namun cocok untuk berbagai kebutuhan pengambilan, Amazon Glacier menyediakan tiga opsi untuk akses ke arsip, dari beberapa menit hingga beberapa jam.

Kemampuan Keamanan Masa Depan dan Kustom

Layanan dan fitur yang disebutkan di atas bukanlah daftar lengkap. AWS terus menambahkan kemampuan baru. Untuk informasi lebih lanjut, kami mendorong Anda untuk meninjau halaman [Apa yang Baru di AWS](#) dan [Keamanan AWS Cloud](#). Selain layanan keamanan yang AWS menawarkan layanan cloud asli, Anda mungkin tertarik untuk membangun kemampuan Anda sendiri di atas AWS layanan.

Meskipun kami menyarankan untuk mengaktifkan serangkaian layanan keamanan dasar dalam akun Anda, seperti Amazon AWS CloudTrail GuardDuty, dan Amazon Macie, Anda mungkin ingin memperluas kemampuan ini untuk mendapatkan nilai tambahan dari aset log Anda. Ada sejumlah alat partner yang tersedia, seperti yang tercantum dalam program Kompetensi Keamanan APN kami. Anda mungkin juga ingin menulis kueri Anda sendiri untuk mencari log Anda. Dengan banyaknya layanan terkelola yang AWS menawarkan, ini tidak pernah semudah ini. Ada banyak AWS layanan tambahan yang dapat membantu Anda dengan penyelidikan yang berada di luar cakupan paper ini, seperti Amazon Athena, Amazon OpenSearch Service, Amazon Quick, Amazon Machine Learning, dan Amazon EMR.

Lampiran B: sumber daya respons AWS insiden

AWS menerbitkan sumber daya untuk membantu pelanggan mengembangkan kemampuan respons insiden. Sebagian besar contoh kode dan prosedur dapat ditemukan di repositori GitHub publik AWS eksternal. Berikut ini adalah beberapa sumber daya yang memberikan contoh cara melakukan respons insiden.

Sumber daya playbook

- [Framework for Incident Response Playbooks](#) - Contoh kerangka kerja bagi pelanggan untuk membuat, mengembangkan, dan mengintegrasikan buku pedoman keamanan dalam persiapan untuk skenario serangan potensial saat menggunakan AWS layanan.
- [Sampel Playbook Respon Insiden](#) - Buku pedoman yang mencakup skenario umum yang dihadapi oleh AWS pelanggan.
- [AWS mengumumkan rilis lima lokakarya yang tersedia untuk umum.](#)

Sumber daya forensik

- [Automated Incident Response and Forensics Framework](#) – Kerangka kerja dan solusi ini menyediakan proses forensik digital standar, yang terdiri dari fase-fase berikut: penahanan, akuisisi, pemeriksaan, dan analisis. Ini memanfaatkan fungsi AWS Λ untuk memicu proses respons insiden dengan cara berulang otomatis. Hal ini menyediakan segregasi akun untuk mengoperasikan langkah-langkah otomatisasi, menyimpan artefak, dan menciptakan lingkungan forensik.
- [Orkestrator Forensik Otomatis untuk Amazon EC2](#) – Panduan implementasi ini menyediakan solusi otomatis untuk menangkap dan memeriksa data dari instans EC2 dan volume terlampir untuk

analisis forensik jika terjadi potensi masalah keamanan yang terdeteksi. Ada AWS CloudFormation template untuk menyebarkan solusi.

- [Cara mengotomatiskan pengumpulan disk forensik di AWS](#) — AWS Blog ini merinci cara mengatur alur kerja otomatisasi untuk menangkap bukti disk untuk analisis guna menentukan ruang lingkup dan dampak potensi insiden keamanan. Ada juga AWS CloudFormation template yang disertakan untuk menyebarkan solusi.

Pemberitahuan

Pelanggan bertanggung jawab untuk membuat penilaian independen mereka sendiri atas informasi dalam dokumen ini. Dokumen ini: (a) hanya untuk tujuan informasi, (b) mewakili penawaran dan praktik AWS produk saat ini, yang dapat berubah tanpa pemberitahuan, dan (c) tidak membuat komitmen atau jaminan apa pun dari AWS dan afiliasinya, pemasok, atau pemberi lisensinya. AWS produk atau layanan disediakan “sebagaimana adanya” tanpa jaminan, representasi, atau kondisi apa pun, baik tersurat maupun tersirat. Tanggung jawab dan kewajiban AWS kepada pelanggannya dikendalikan oleh AWS perjanjian, dan dokumen ini bukan bagian dari, juga tidak mengubah, perjanjian apa pun antara AWS dan pelanggannya.

© 2024 Amazon Web Services, Inc. atau afiliasinya. Semua hak dilindungi undang-undang.

Riwayat dokumen

Tabel berikut menjelaskan penambahan penting pada dokumentasi Respons Insiden AWS Keamanan, mulai 1 Januari 2026. Untuk notifikasi tentang pembaruan-pembaruan dokumentasi ini, Anda dapat berlangganan ke sebuah umpan RSS.

Perubahan	Deskripsi	Tanggal
Mengganti nama laporan insiden Post menjadi laporan Bulanan	Mengganti nama bagian Laporan Insiden Post menjadi laporan Bulanan. Memperbarui bagian untuk mengklarifikasi bahwa laporan dikirim ke semua kontak di tim Respons Insiden, termasuk waktu pengiriman, dan mendokumentasikan format baris subjek email.	13 Mei 2026
Dokumentasi orientasi yang diperbarui	Memperbarui topik Aktifkan Respons Insiden AWS AWS Keamanan untuk memperjelas bahwa Respons Insiden Keamanan secara otomatis membuat peran <code>AWSServiceRoleForSecurityIncidentResponse_Triage</code> terkait layanan di akun AWS Organizations manajemen saat menggunakan konsol. Menambahkan tautan ke instruksi untuk mengaktifkan Respons Insiden Keamanan menggunakan API/CLI	7 Mei 2026

<p><u>Menambahkan Aktifkan Respons Insiden Keamanan menggunakan API/CLI topik</u></p>	<p>Menambahkan topik baru dengan petunjuk CLI langkah demi langkah untuk mengaktifkan Respons Insiden AWS Keamanan menggunakan metode pendaftaran Administrator Delegasi dan pendaftaran akun manajemen.</p>	<p>7 Mei 2026</p>
<p><u>Persyaratan respons proaktif yang diklarifikasi untuk Amazon GuardDuty dan temuan pihak ketiga</u></p>	<p>Diklarifikasi bahwa Amazon tidak GuardDuty diharuskan menggunakan respons proaktif. AWS Security Incident Response juga dapat memantau dan menyelidiki peringatan ancaman dari alat deteksi ancaman pihak ketiga menggunakan integrasi CSPM Security Hub. Memperbarui bagian untuk secara akurat menjelaskan persyaratan layanan deteksi dan nilai konfigurasi konsumsi temuan.</p>	<p>5 Mei 2026</p>
<p><u>Menambahkan sistem operasi yang didukung untuk EC2 Triage</u></p>	<p>Menambahkan daftar sistem operasi yang didukung untuk kemampuan Triage EC2, termasuk distribusi Linux (Amazon Linux 2, Amazon Linux 2023, Ubuntu, RHEL, CentOS, SLES, dan Debian) dan versi Windows Server.</p>	<p>April 29, 2026</p>
<p><u>Perbarui deskripsi kebijakan untuk AWSSecurityIncidentResponseReadOnlyAccess</u></p>	<p>Kebijakan yang diperbarui untuk menambahkan <code>security-ir:ListInvestigations</code> tindakan.</p>	<p>April 22, 2026</p>

<u>Perbarui deskripsi kebijakan untuk AWS Security Incident Response Full Access</u>	<p>Kebijakan yang diperbarui untuk menambahkan AWS Organizations izin dan menghapus kondisi MFA.</p>	<p>April 22, 2026</p>
<u>Perbarui deskripsi kebijakan untuk AWS Security Incident Response Case Full Access</u>	<p>Kebijakan yang diperbarui untuk menambah security-ir:ListInvestigations dan security-ir:SendFeedback bertindak serta menghapus kondisi MFA.</p>	<p>April 22, 2026</p>
<u>Fitur EC2 Triage untuk Respons Insiden AWS Keamanan</u>	<p>Menambahkan kemampuan Triage EC2 yang memungkinkan AWS Security Incident Response mengumpulkan informasi investigasi dari instans Amazon Elastic Compute Cloud menggunakan AWS Systems Manager Run Command selama penyelidikan keamanan. Halaman Deteksi dan Analisis yang Diperbarui untuk mendokumentasikan prasyarat dan kemampuan Triage EC2.</p>	<p>April 20, 2026</p>

[Fitur EC2 Triage untuk Respons Insiden AWS Keamanan](#)

CloudFormation StackSets
Dokumentasi diperbarui untuk menyediakan dua pilihan template: Containment only dan Containment dengan EC2 Triage. Template Containment with EC2 Triage menyertakan izin tambahan untuk pengumpulan data investigasi dari instans Amazon EC2.

April 20, 2026

[Pengumpulan data, perilaku regional, dan panduan kepatuhan untuk pelanggan yang diatur](#)

Menambahkan bagian baru tentang pengumpulan dan penggunaan data, residensi data dan perilaku Regional, serta akses dan izin data. Memperluas bagian validasi kepatuhan dengan tanggung jawab bersama dan panduan klasifikasi metadata untuk pelanggan di industri yang diatur.

April 17, 2026

[Panduan orientasi yang diperbarui](#)

Memperbarui panduan orientasi dengan struktur langkah demi langkah baru, termasuk langkah-langkah persiapan, prasyarat, dan alur kerja konfigurasi yang disederhanakan untuk tim respons insiden, jenis kasus, dan integrasi alat.

April 7, 2026

<p>Memperbarui deskripsi kebijakan untuk Kebijakan Peran Layanan Triase Respons Insiden AWS Keamanan</p>	<p>Perbarui deskripsi kebijakan untuk Kebijakan Peran Layanan Triase Respons Insiden AWS Keamanan untuk mencerminkan perubahan yang memungkinkan layanan meningkatkan penyetalan layanan dan mengumpulkan informasi untuk menyelidiki potensi insiden.</p>	<p>Maret 27, 2026</p>
<p>Kirim metadata</p>	<p>Menambahkan instruksi untuk mengirimkan metadata melalui kasus. AWS Dukungan</p>	<p>Maret 27, 2026</p>
<p>Kirim preferensi penahanan</p>	<p>Menambahkan instruksi untuk mengirimkan preferensi penahanan melalui kasus. AWS Dukungan</p>	<p>Maret 27, 2026</p>
<p>Templat penahanan StackSet</p>	<p>Diperbarui StackSet CloudFormation template penahanan.</p>	<p>Maret 27, 2026</p>
<p>Wilayah AWS Pertimbangan yang diklarifikasi untuk akun administrator yang didelegasikan</p>	<p>Mengklarifikasi bahwa saat Anda menetapkan akun administrator Respons Insiden AWS Keamanan yang didelegasikan menjadi satu Wilayah AWS selama penyiapan awal, layanan ini menyediakan cakupan seluruh organisasi di semua yang didukung. Wilayah AWS</p>	<p>Maret 20, 2026</p>
<p>Tentukan preferensi tindakan penahanan</p>	<p>Memperbarui bagian preferensi tindakan penahanan agar sesuai dengan opsi saat ini.</p>	<p>Maret 19, 2026</p>

[Respon Proaktif dan Triaging Peringatan](#)

Referensi yang dihapus ke respons proaktif dan alur kerja triaging peringatan menjadi opsional.

Maret 3, 2026

[Garis Waktu Respons](#)

Garis waktu respons yang diperbarui untuk menentukan SLO 15 menit untuk pengakuan kasus dan 5 hari kerja untuk respons pelanggan sebelum penutupan kasus.

Februari 24, 2026

[Praktik Terbaik Komunikasi](#)

Garis waktu penutupan kasus yang diperbarui untuk menentukan 5 hari kerja untuk respons pelanggan terhadap permintaan informasi penting.

Februari 24, 2026

[AWS CLI referensi ditambahkan dalam Berinteraksi dengan Respons Insiden Keamanan menggunakan AWS CloudShell](#)

Menambahkan tautan ke AWS Command Line Interface Referensi untuk Respons Insiden AWS Keamanan.

Februari 24, 2026

[Matriks RACI](#)

Memperbarui “Otorisasi tindakan penahanan CIRT” menjadi “Otorisasi tindakan penahanan” dalam matriks RACI.

Februari 13, 2026

<u>Preferensi Penahanan</u>	Opsi preferensi penahanan yang diperbarui dari “Tidak ada tindakan penahanan”, “Penahanan dengan persetujuan”, dan “Penahanan otomatis” menjadi “Persetujuan Diperlukan”, “Mengandung Dikonfirmasi”, dan “Mengandung Diduga” dengan deskripsi yang direvisi.	Februari 13, 2026
<u>Pasca Penerapan Respons Insiden Keamanan</u>	Menambahkan tautan ke Respons Insiden AWS Keamanan: Integrasi Baru dan demo OU-Level Berlangganan.	Februari 4, 2026
<u>Pemantauan dan Investigasi</u>	Ditambahkan konten revisi untuk intro dan sub bagian pada halaman ini.	Februari 4, 2026
<u>Mendeteksi dan Menganalisis</u>	Ditambahkan konten revisi untuk intro dan sub bagian pada halaman ini.	Februari 4, 2026
<u>Mengandung</u>	Menambahkan konten yang direvisi ke halaman ini.	Februari 4, 2026
<u>Agen Investigasi AI</u>	Ditambahkan Penggunaan disclaimer data pelanggan ke halaman ini. Penafian: Agen Investigasi AI tidak menggunakan data pelanggan untuk pelatihan model, dan tidak membagikan data pelanggan dengan pihak ketiga.	Februari 4, 2026

Perubahan	Deskripsi	Date
Batalkan Keanggotaan	Halaman pembatalan keanggotaan yang diperbarui untuk menunjukkan bahwa keanggotaan dan layanan akan segera berakhir setelah pembatalan dan bukan sebagai akhir dari siklus penagihan.	November 20, 2025
AWS Kebijakan Terkelola	Menambahkan kasus pembaruan, membuat komentar kasus, daftar kasus, daftar komentar kasus ke daftar tindakan yang disediakan layanan.	November 19, 2025
Menggunakan Peran Terkait Layanan	Menambahkan kasus pembaruan, membuat komentar kasus, daftar kasus, daftar komentar kasus ke daftar tindakan yang disediakan layanan.	November 19, 2025
Preferensi Komunikasi	Dibuat dan Diperbarui Bagian Preferensi Komunikasi Ditambahkan untuk dokumentasi fitur baru.	November 12, 2025
Penambahan dan Pembaruan Panduan Orientasi	Dibuat dan Diperbarui Panduan orientasi Ditambahkan termasuk bagian berikut Ditambahkan Aktifkan bagian Respons Insiden Keamanan.	November 12, 2025

Perubahan	Deskripsi	Date
	<p>Menambahkan insinyur Authorize Security Incident Response untuk melakukan bagian tindakan penahanan ancaman.</p> <p>Ditambahkan Post Deployment bagian Security Incident Response.</p> <p>Ditambahkan Perbarui bagian Tim Respons Insiden.</p> <p>Menambahkan bagian GuardDuty Temuan dan Aturan Penindasan.</p> <p>Ditambahkan EventBridge bagian Amazon.</p> <p>Menambahkan bagian Integrasi dan Alur Kerja Perangkat Eksternal.</p> <p>Menambahkan bagian Alur Kerja Perangkat Eksternal.</p> <p>Ditambahkan Lampiran A: Poin bagian Kontak.</p>	

Perubahan	Deskripsi	Date
<p>Pembaruan Lanugage Kepatuhan dan Penagihan</p>	<p>Pernyataan Dihapus yang Diperbarui bahwa Respons Insiden AWS Keamanan tidak tercakup dalam kerangka kerja apa pun. AWS Security Incident Response sekarang tercakup dalam HITRUST dengan lebih banyak lagi yang akan datang di masa depan.</p> <p>Visibilitas dan Kontrol yang Diperbarui untuk menambahkan AWS Respons Insiden Keamanan</p> <p>Memperbarui Batalkan Keanggotaan untuk memperjelas periode penagihan layanan.</p> <p>Menambahkan video ke Memulai yang menyediakan konteks tambahan untuk tugas-tugas umum untuk mulai menggunakan Respons Insiden AWS Keamanan.</p>	<p>Agustus 15, 2025</p>

Perubahan	Deskripsi	Date
<p>Diperbarui - AWS Security Incident Response Service Role Policy</p>	<p>Kebijakan tersebut sekarang mencakup dua tindakan baru untuk "organizations:DescribeAccount" , "organizations:ListDelegatedAdministrators" dan kondisi baru:</p> <pre data-bbox="592 615 1029 1052"> "Condition": { "StringEquals": { "aws:ResourceAccount": "\${aws:PrincipalAccount}" } }</pre>	<p>Akan Ditentukan Kemudian</p>
<p>Pembaruan fitur: berlangganan unit organisasi tertentu (OU) atau seluruh AWS organisasi Anda</p>	<p>Panel bantuan di antarmuka pengguna telah diperbarui untuk mencerminkan pembaruan untuk berlangganan unit organisasi tertentu (OU) atau seluruh AWS organisasi Anda.</p> <p>Halaman baru dibuat untuk Mengelola keanggotaan dengan unit organisasi (OU)</p> <p>Halaman yang terkait dengan AWS Organizations diperbarui untuk mencerminkan fitur manajemen OU baru.</p>	<p>Agustus 7, 2025</p>

Perubahan	Deskripsi	Date
Service Quotas yang diperbarui	Halaman Service Quotas diperbarui untuk memandu pengguna menuju titik akhir dan kuota Panduan Referensi AWS Umum untuk Respons Insiden AWS Keamanan	Agustus 7, 2025
Pembaruan umpan balik pengguna	Menambahkan hyperlink untuk layanan ke Kasus Respons Insiden AWS Keamanan Pembaruan untuk mencerminkan Panduan Penanganan Insiden Keamanan Komputer SP 800-61 r3 aktif untuk Panduan Teknis Keamanan	Agustus 7, 2025
Menambahkan halaman untuk EventBridge integrasi Amazon dengan AWS Security Incident Response.	Bagian konten baru untuk menjelaskan bagaimana Amazon EventBridge mengintegrasikan dalam Respons Insiden AWS Keamanan.	Juni 26, 2025

Perubahan	Deskripsi	Date
<p>Pembaruan untuk SLR menambahkan izin untuk mendukung hak layanan.</p>	<p>AWS Security Incident Response Triage Service Role Policy telah diperbarui untuk menambahkan security-ir:GetMembership, security-ir:, security-ir:ListMemberships, guardduty:, guardduty:, guardduty:UpdateCase, dan guardduty: ListFilters izin. guardduty: UpdateFilter ditambahkan untuk memfasilitasi pengelolaan filter di DeleteFilter akun yang didelegasikan. GetAdministratorAccount GetAdministratorAccount GuardDuty Auto-Archival</p>	<p>02 Juni 2025</p>
<p>Pembaruan Sumber Daya.</p>	<p>Memperbarui https://docs.aws.amazon.com/security-ir/latest/userguide/appendix-b-incident-response-resources.html #playbook -resources untuk mencerminkan lokakarya aktif yang tersedia bagi pelanggan.</p>	<p>23 Mei 2025</p>
<p>Layanan mendukung bahasa Jepang.</p>	<p>Memperbarui konfigurasi yang didukung untuk mengidentifikasi dukungan bahasa Jepang di waktu setempat Jepang. Bahasa Inggris didukung secara global.</p>	<p>13 Mei 2025</p>

Perubahan	Deskripsi	Date
<p>Pembaruan konten dan umpan balik pelanggan.</p>	<p>Menambahkan catatan https://docs.aws.amazon.com/security-ir/latest/userguide/select-a-membership-account.html untuk mencerminkan tugas tambahan saat menggunakan akun administrator yang didelegasikan sebagai bagian dari penyiapan .</p> <p>Memperbarui pengalaman pelanggan saat bekerja dengan kasus yang dihasilkan layanan dan Mendeteksi dan Menganalisis.</p> <p>Detail pembatalan akun yang diperbarui untuk memberikan kejelasan yang lebih baik tentang implikasi penagihan dalam membatalkan keanggotaan.</p>	<p>9 Mei 2025</p>
<p>Menambahkan tiga wilayah baru yang didukung.</p>	<p>Menambahkan tiga wilayah baru ke https://docs.aws.amazon.com/security-ir/latest/userguide/supported-configs.html. Mumbai, Paris, dan Sao Paulo.</p>	<p>7 Mei 2025</p>

Perubahan	Deskripsi	Date
Diperbarui: Pembaruan dari komentar pelanggan pada dokumen.	<p>Kesalahan ejaan dan tata bahasa pada beberapa halaman benar.</p> <p>Diperbarui https://docs.aws.amazon.com/en_us/security-ir/latest/userguide/organizations_permissions.html untuk secara akurat mencerminkan security-ir sebagai awalan layanan.</p> <p>Menambahkan catatan https://docs.aws.amazon.com/security-ir/latest/userguide/source-containment.html tentang Route53 dan DNS.</p>	Februari 7, 2025

Perubahan	Deskripsi	Date
<p>Diperbarui: Pembaruan dari komentar pelanggan pada dokumen.</p>	<p>Diperbarui https://docs.aws.amazon.com/security-ir/latest/userguide/setup-monitoring-and-investigation-workflows.html ke template stackset.</p> <p>Entri yang diperbaiki triage.security-ir.com ke triage.security-ir.amazonaws.com</p> <p>Menambahkan catatan koneksi yang dilacak untuk aktif AWSSupport-Contain EC2Reversible https://docs.aws.amazon.com/security-ir/latest/userguide/contain.html.</p> <p>Tetap link rusak pada https://docs.aws.amazon.com/security-ir/latest/userguide/managing-associated-accounts.html.</p> <p>Menambahkan definisi untuk akun keanggotaan di https://docs.aws.amazon.com/security-ir/latest/userguide/select-a-membership-account.html.</p> <p>Menambahkan catatan klarifikasi https://docs.aws.amazon.com/en_us/security-ir/latest/userguide/using-service-linked-roles.html untuk akun AWS Organizations manajemen.</p>	<p>Desember 20, 2024</p>

Perubahan	Deskripsi	Date
<p>Diperbarui: Pembaruan dari komentar pelanggan pada dokumen.</p>	<p>Menghapus beberapa duplikat AWS AWS dalam teks.</p> <p>Memperbaiki tautan yang rusak pada https://docs.aws.amazon.com/security-ir/latest/userguide/sir_tagging.html dan https://docs.aws.amazon.com/security-ir/latest/userguide/service-name-info-in-cloudtrail.html.</p> <p>Pembaruan untuk https://docs.aws.amazon.com/security-ir/latest/userguide/contain.html. Menghapus > dari paragraf pertama. Diganti AWSSupport-ContainEC2Reversible dengan AWSSupport-ContainEC2Instance. Diganti AWSSupport-ContainIAMReversible dengan AWSSupport-ContainIAMPrincipal. Diganti AWSSupport-ContainS3Reversible dengan AWSSupport-ContainS3Resource.</p> <p>Pemformatan yang diperbarui pada https://docs.aws.amazon.com/en_us/security-ir/latest/userguide/issues.html</p>	<p>Desember 10, 2024</p>

Perubahan	Deskripsi	Date
	<p>Saat memberi tahu pelanggan untuk menghubungi respons insiden keamanan melalui tiket dukungan, https://docs.aws.amazon.com/security-ir/latest/userguide/understand-response-teams-and-support.html sekarang berikan opsi untuk memilih dalam formulir dukungan.</p> <p>CloudWatch Acara yang Dihapus dan diganti dengan EventBridge on https://docs.aws.amazon.com/security-ir/latest/userguide/logging-and-events.html.</p> <p>Pembaruan tata bahasa pada https://docs.aws.amazon.com/security-ir/latest/userguide/technique-access-containment.html.</p> <p>Tanggal publikasi dihapus dari https://docs.aws.amazon.com/security-ir/latest/userguide/security-incident-response-guide.html, digantikan oleh pembaruan dalam tabel ini.</p>	
<p>Diperbarui: kebijakan AWS terkelola dan peran terkait layanan.</p>	<p>Pembaruan kebijakan terkelola dan peran terkait layanan.</p>	<p>Desember 1, 2024</p>

Perubahan	Deskripsi	Date
Peluncuran Layanan	Dokumen layanan awal untuk peluncuran layanan di re:Invent 2024	Desember 1, 2024

Terjemahan disediakan oleh mesin penerjemah. Jika konten terjemahan yang diberikan bertentangan dengan versi bahasa Inggris aslinya, utamakan versi bahasa Inggris.