



Panduan GuardDuty Pengguna Amazon

Amazon GuardDuty



Amazon GuardDuty: Panduan GuardDuty Pengguna Amazon

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

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

Table of Contents

Apa itu GuardDuty?	1
Fitur dari GuardDuty	2
Kepatuhan PCI DSS	5
Harga di GuardDuty	6
Menggunakan uji GuardDuty coba gratis 30 hari	6
Menggunakan Perlindungan Malware untuk S3 dengan Tingkat Gratis 12 bulan	8
Mengakses GuardDuty	8
Konsep dan istilah kunci	10
Memulai	15
Sebelum Anda mulai	15
Langkah 1: Aktifkan Amazon GuardDuty	17
Langkah 2: Menghasilkan temuan sampel dan menjelajahi operasi dasar	19
Langkah 3: Konfigurasi GuardDuty temuan ekspor ke bucket Amazon S3	21
Langkah 4: Siapkan peringatan GuardDuty pencarian melalui SNS	26
Langkah selanjutnya	28
Sumber data dasar	30
AWS CloudTrail acara manajemen	30
Bagaimana GuardDuty menangani peristiwa AWS CloudTrail global	31
Log Alur VPC	32
Log kueri DNS Route53 Resolver	33
Deteksi Ancaman Diperpanjang	34
Contoh skenario ancaman urutan serangan	34
Cara kerja Extended Threat Detection	35
Mengaktifkan rencana perlindungan untuk memaksimalkan deteksi ancaman	36
Mendeteksi urutan serangan di cluster Amazon EKS	37
Mendeteksi urutan serangan di bucket Amazon S3	38
Deteksi Ancaman Diperpanjang di GuardDuty konsol	38
Memahami dan mengelola temuan urutan serangan	39
Sumber daya tambahan	39
Perlindungan EKS	40
Log audit EKS di Perlindungan EKS	41
Mengaktifkan Perlindungan EKS di lingkungan multi-akun	41
Mengaktifkan Perlindungan EKS untuk akun mandiri	49
Perlindungan S3	51

AWS CloudTrail peristiwa data untuk S3	52
Cara GuardDuty menggunakan peristiwa CloudTrail data untuk S3	52
GuardDuty menggunakan peristiwa CloudTrail data untuk S3 untuk urutan serangan	53
Mengaktifkan Perlindungan S3 di lingkungan beberapa akun	53
Mengaktifkan Perlindungan S3 untuk akun mandiri	60
Pemantauan Runtime	62
Cara kerjanya	63
Dengan cluster Amazon EKS	64
Dengan EC2 instans Amazon	70
Dengan Fargate (hanya Amazon ECS)	73
Setelah Anda mengaktifkan Runtime Monitoring	75
Uji coba gratis 30 hari	76
Saya menggunakan masa GuardDuty percobaan atau saya tidak pernah mengaktifkan EKS Runtime Monitoring	76
Saya mengaktifkan EKS Runtime Monitoring sebelum peluncuran Runtime Monitoring	77
Prasyarat	78
Sebagai EC2 contoh	79
Untuk cluster Fargate (khusus ECS)	84
Untuk kluster EKS	90
Mengaktifkan Runtime Monitoring	93
Mengaktifkan Runtime Monitoring untuk lingkungan multi-akun	94
Mengaktifkan Runtime Monitoring untuk akun mandiri	98
Mengelola agen GuardDuty keamanan	99
Agen otomatis di EC2 sumber daya Amazon	100
Manajemen agen manual untuk EC2 sumber daya Amazon	112
Agen otomatis di Fargate (hanya Amazon ECS)	128
Agen otomatis di sumber daya Amazon EKS	162
Manajemen agen manual untuk kluster Amazon EKS	200
Konfigurasi parameter add-on EKS	209
Memvalidasi konfigurasi titik akhir VPC	212
Masalah cakupan runtime dan pemecahan masalah	214
Cakupan dan pemecahan masalah untuk sumber daya Amazon EC2	214
Cakupan dan pemecahan masalah untuk kluster Amazon ECS	230
Cakupan dan pemecahan masalah untuk kluster Amazon EKS	246
Menyiapkan CPU dan pemantauan memori	262
Menggunakan VPC bersama	263

Cara kerjanya	264
Prasyarat	266
Menggunakan IAc dengan agen otomatis	267
Ikhtisar grafik ketergantungan sumber daya IAc	267
Masalah umum - Menghapus sumber daya di IAc	267
Jenis acara runtime yang dikumpulkan	269
Proses acara	269
Acara kontainer	271
AWS Fargate (Hanya Amazon ECS) peristiwa tugas	272
Acara pod Kubernetes	273
Acara Sistem Nama Domain (DNS)	273
Buka acara	274
Memuat acara modul	274
Acara Mprotect	275
Acara gunung	275
Tautkan acara	275
Acara Symlink	276
Acara Dup	276
Acara peta memori	277
Acara soket	277
Connect event	278
Proses acara VM Readv	279
Proses acara VM Writev	279
Peristiwa proses jejak (Ptrace)	280
Mengikat acara	280
Dengarkan acara	281
Ganti nama acara	281
Mengatur peristiwa ID pengguna (UID)	282
Acara Chmod	282
Agen hosting repositori Amazon ECR GuardDuty	282
Agen keamanan di host yang sama	294
Gambaran Umum	294
Dampak	295
Bagaimana GuardDuty menangani banyak agen	295
Pemantauan Runtime EKS	296
Mengkonfigurasi EKS Runtime Monitoring untuk lingkungan multi-akun (API)	296

Mengkonfigurasi EKS Runtime Monitoring untuk akun mandiri (API)	338
Migrasi dari EKS Runtime Monitoring ke Runtime Monitoring	346
GuardDuty versi rilis agen keamanan	350
Sumber daya tambahan - langkah selanjutnya	375
Menonaktifkan, menghapus instalasi, dan pembersihan sumber daya	376
Menghapus instalasi agen keamanan secara manual untuk sumber daya Amazon EC2	378
Membersihkan sumber daya agen keamanan	380
Perlindungan Malware untuk EC2	382
Membandingkan GuardDuty pemindaian malware yang dimulai dan pemindaian malware sesuai permintaan	383
Cara GuardDuty memindai volume EBS untuk deteksi malware	386
Volume EBS yang didukung	387
Ubah ID kunci KMS default	388
Mengatur retensi snapshot dan cakupan EC2 pemindaian	389
Retensi snapshot	389
Opsi pindai dengan tag yang ditentukan pengguna	391
GuardDutyExcludedTag global	395
GuardDuty-pemindaian malware yang dimulai	395
Uji coba gratis 30 hari	396
Mengaktifkan GuardDuty pemindaian malware yang dimulai di lingkungan beberapa akun ..	397
Mengaktifkan GuardDuty pemindaian malware yang dimulai untuk akun mandiri	408
Temuan yang memanggil pemindaian GuardDuty malware yang dimulai	409
Pemindaian malware sesuai permintaan	412
Cara kerja pemindaian malware sesuai permintaan	413
Memulai pemindaian malware sesuai permintaan	414
Memindai ulang instans Amazon yang dipindai sebelumnya EC2	416
Memantau status dan hasil pemindaian malware	417
GuardDuty akun layanan	419
Kuota dalam Perlindungan Malware untuk EC2	422
Perlindungan Malware untuk S3	427
Harga dan biaya penggunaan	429
Meninjau biaya penggunaan	430
Cara kerjanya	430
Gambaran Umum	430
Izin peran IAM	431
Penandaan opsional objek berdasarkan hasil pemindaian	431

Proses setelah Anda mengaktifkan Perlindungan Malware untuk S3 untuk ember	432
Kemampuan Perlindungan Malware untuk S3	434
(Opsional) Memulai dengan Perlindungan Malware hanya untuk S3 (konsol)	435
Mengonfigurasi Perlindungan Malware untuk S3 untuk bucket Anda	436
Mengaktifkan Perlindungan Malware untuk deteksi ancaman S3 untuk bucket Anda	437
Izin peran IAM	443
Memecahkan masalah kesalahan izin peran IAM	449
Langkah-langkah setelah mengaktifkan Perlindungan Malware untuk S3	450
Menggunakan kontrol akses berbasis tag (TBAC)	451
Menambahkan TBAC pada sumber daya bucket S3	452
Lihat dan pahami status bucket yang dilindungi	454
Memecahkan masalah status paket Perlindungan Malware	455
EventBridge pemberitahuan dinonaktifkan untuk bucket S3 ini	455
EventBridge aturan terkelola untuk menerima peristiwa bucket S3 tidak ada	456
Bucket S3 tidak ada lagi	457
Tidak dapat menempatkan objek uji	458
Memantau pemindaian objek S3	459
Status pemindaian potensial objek S3 dan status hasil	459
Menggunakan Amazon EventBridge	461
Menggunakan Tag Objek S3	470
Menggunakan CloudWatch alarm dan metrik	472
Mengedit paket Perlindungan Malware untuk bucket yang dilindungi	475
Menonaktifkan Perlindungan Malware untuk S3 untuk bucket yang dilindungi	477
Dukungan fitur Amazon S3	478
Perlindungan Malware untuk kuota S3	485
Perlindungan RDS	488
Database yang didukung	489
Aktivitas login RDS	490
Mengaktifkan Perlindungan RDS di lingkungan multi-akun	491
Mengaktifkan Perlindungan RDS untuk akun mandiri	497
Perlindungan Lambda	499
Pemantauan Aktivitas Jaringan Lambda	500
Mengaktifkan Perlindungan Lambda di lingkungan multi-akun	500
Mengaktifkan Perlindungan Lambda untuk akun mandiri	507
Melindungi beban kerja AI	509
Beberapa akun di GuardDuty	510

Akun administrator dan hubungan akun anggota	510
Mengelola akun dengan AWS Organizations	515
Pertimbangan dan rekomendasi	516
Izin yang diperlukan untuk menunjuk akun administrator yang didelegasikan GuardDuty	518
Menunjuk akun administrator yang didelegasikan GuardDuty	519
Menyetel preferensi aktifkan otomatis organisasi	521
Menambahkan anggota ke organisasi	525
(Opsional) Aktifkan paket perlindungan untuk akun anggota yang ada	527
Terus mengelola akun anggota Anda dalam GuardDuty	528
Penangguhan GuardDuty untuk akun anggota	529
Memutuskan (menghapus) akun anggota dari akun administrator	531
Menghapus akun anggota dari organisasi GuardDuty	532
Mengubah akun GuardDuty administrator yang didelegasikan	534
Mengelola akun dengan undangan	536
Menambahkan akun dengan undangan	538
Mengkonsolidasikan akun administrator di bawah satu organisasi	542
GuardDuty pertimbangan untuk opsi Ekspor CSV di akun	545
Tipe temuan	547
EC2 menemukan jenis	547
Backdoor:EC2/C&CActivity.B	549
Backdoor:EC2/C&CActivity.B!DNS	550
Backdoor:EC2/DenialOfService.Dns	551
Backdoor:EC2/DenialOfService.Tcp	552
Backdoor:EC2/DenialOfService.Udp	553
Backdoor:EC2/DenialOfService.UdpOnTcpPorts	553
Backdoor:EC2/DenialOfService.UnusualProtocol	554
Backdoor:EC2/Spambot	555
Behavior:EC2/NetworkPortUnusual	555
Behavior:EC2/TrafficVolumeUnusual	556
CryptoCurrency:EC2/BitcoinTool.B	556
CryptoCurrency:EC2/BitcoinTool.B!DNS	557
DefenseEvasion:EC2/UnusualDNSResolver	558
DefenseEvasion:EC2/UnusualDoHActivity	558
DefenseEvasion:EC2/UnusualDoTActivity	559
Impact:EC2/AbusedDomainRequest.Reputation	559
Impact:EC2/BitcoinDomainRequest.Reputation	560

Impact:EC2/MaliciousDomainRequest.Reputation	561
Impact:EC2/PortSweep	562
Impact:EC2/SuspiciousDomainRequest.Reputation	562
Impact:EC2/WinRMBruteForce	563
Recon:EC2/PortProbeEMRUnprotectedPort	563
Recon:EC2/PortProbeUnprotectedPort	564
Recon:EC2/Portscan	565
Trojan:EC2/BlackholeTraffic	566
Trojan:EC2/BlackholeTraffic!DNS	566
Trojan:EC2/DGADomainRequest.B	567
Trojan:EC2/DGADomainRequest.C!DNS	568
Trojan:EC2/DNSDataExfiltration	569
Trojan:EC2/DriveBySourceTraffic!DNS	569
Trojan:EC2/DropPoint	570
Trojan:EC2/DropPoint!DNS	570
Trojan:EC2/PhishingDomainRequest!DNS	571
UnauthorizedAccess:EC2/MaliciousIPCaller.Custom	571
UnauthorizedAccess:EC2/MetadataDNSRebind	572
UnauthorizedAccess:EC2/RDPBruteForce	573
UnauthorizedAccess:EC2/SSHBruteForce	574
UnauthorizedAccess:EC2/TorClient	575
UnauthorizedAccess:EC2/TorRelay	575
Tipe temuan IAM	576
CredentialAccess:IAMUser/AnomalousBehavior	577
DefenseEvasion:IAMUser/AnomalousBehavior	578
Discovery:IAMUser/AnomalousBehavior	579
Exfiltration:IAMUser/AnomalousBehavior	579
Impact:IAMUser/AnomalousBehavior	580
InitialAccess:IAMUser/AnomalousBehavior	581
PenTest:IAMUser/KaliLinux	582
PenTest:IAMUser/ParrotLinux	582
PenTest:IAMUser/Pentoolinux	583
Persistence:IAMUser/AnomalousBehavior	583
Policy:IAMUser/RootCredentialUsage	584
Policy:IAMUser/ShortTermRootCredentialUsage	585
PrivilegeEscalation:IAMUser/AnomalousBehavior	585

Recon:IAMUser/MaliciousIPCaller	586
Recon:IAMUser/MaliciousIPCaller.Custom	587
Recon:IAMUser/TorIPCaller	587
Stealth:IAMUser/CloudTrailLoggingDisabled	588
Stealth:IAMUser/PasswordPolicyChange	588
UnauthorizedAccess:IAMUser/ConsoleLoginSuccess.B	589
UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS	589
UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS	591
UnauthorizedAccess:IAMUser/MaliciousIPCaller	593
UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom	593
UnauthorizedAccess:IAMUser/TorIPCaller	594
Jenis pencarian urutan serangan	594
AttackSequence:EKS/CompromisedCluster	595
AttackSequence:IAM/CompromisedCredentials	596
AttackSequence:S3/CompromisedData	596
Jenis temuan Perlindungan S3	597
Discovery:S3/AnomalousBehavior	599
Discovery:S3/MaliciousIPCaller	599
Discovery:S3/MaliciousIPCaller.Custom	600
Discovery:S3/TorIPCaller	600
Exfiltration:S3/AnomalousBehavior	601
Exfiltration:S3/MaliciousIPCaller	602
Impact:S3/AnomalousBehavior.Delete	602
Impact:S3/AnomalousBehavior.Permission	603
Impact:S3/AnomalousBehavior.Write	604
Impact:S3/MaliciousIPCaller	605
PenTest:S3/KaliLinux	605
PenTest:S3/ParrotLinux	606
PenTest:S3/Pentoolinux	606
Policy:S3/AccountBlockPublicAccessDisabled	607
Policy:S3/BucketAnonymousAccessGranted	608
Policy:S3/BucketBlockPublicAccessDisabled	608
Policy:S3/BucketPublicAccessGranted	609
Stealth:S3/ServerAccessLoggingDisabled	610
UnauthorizedAccess:S3/MaliciousIPCaller.Custom	611
UnauthorizedAccess:S3/TorIPCaller	611

Jenis penemuan Perlindungan EKS	612
CredentialAccess:Kubernetes/MaliciousIPCaller	614
CredentialAccess:Kubernetes/MaliciousIPCaller.Custom	614
CredentialAccess:Kubernetes/SuccessfulAnonymousAccess	615
CredentialAccess:Kubernetes/TorIPCaller	616
DefenseEvasion:Kubernetes/MaliciousIPCaller	616
DefenseEvasion:Kubernetes/MaliciousIPCaller.Custom	617
DefenseEvasion:Kubernetes/SuccessfulAnonymousAccess	618
DefenseEvasion:Kubernetes/TorIPCaller	618
Discovery:Kubernetes/MaliciousIPCaller	619
Discovery:Kubernetes/MaliciousIPCaller.Custom	620
Discovery:Kubernetes/SuccessfulAnonymousAccess	620
Discovery:Kubernetes/TorIPCaller	621
Execution:Kubernetes/ExecInKubeSystemPod	622
Impact:Kubernetes/MaliciousIPCaller	622
Impact:Kubernetes/MaliciousIPCaller.Custom	623
Impact:Kubernetes/SuccessfulAnonymousAccess	624
Impact:Kubernetes/TorIPCaller	624
Persistence:Kubernetes/ContainerWithSensitiveMount	625
Persistence:Kubernetes/MaliciousIPCaller	626
Persistence:Kubernetes/MaliciousIPCaller.Custom	626
Persistence:Kubernetes/SuccessfulAnonymousAccess	627
Persistence:Kubernetes/TorIPCaller	628
Policy:Kubernetes/AdminAccessToDefaultServiceAccount	628
Policy:Kubernetes/AnonymousAccessGranted	629
Policy:Kubernetes/ExposedDashboard	630
Policy:Kubernetes/KubeflowDashboardExposed	630
PrivilegeEscalation:Kubernetes/PrivilegedContainer	631
CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed	631
PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated	632
Execution:Kubernetes/AnomalousBehavior.ExecInPod	633
PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!	
PrivilegedContainer	634
Persistence:Kubernetes/AnomalousBehavior.WorkloadDeployed!	
ContainerWithSensitiveMount	635
Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed	636

PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated	637
Discovery:Kubernetes/AnomalousBehavior.PermissionChecked	638
Jenis penemuan Runtime Monitoring	639
CryptoCurrency:Runtime/BitcoinTool.B	641
Backdoor:Runtime/C&CActivity.B	642
UnauthorizedAccess:Runtime/TorRelay	643
UnauthorizedAccess:Runtime/TorClient	644
Trojan:Runtime/BlackholeTraffic	644
Trojan:Runtime/DropPoint	645
CryptoCurrency:Runtime/BitcoinTool.B!DNS	646
Backdoor:Runtime/C&CActivity.B!DNS	647
Trojan:Runtime/BlackholeTraffic!DNS	648
Trojan:Runtime/DropPoint!DNS	649
Trojan:Runtime/DGADomainRequest.C!DNS	649
Trojan:Runtime/DriveBySourceTraffic!DNS	650
Trojan:Runtime/PhishingDomainRequest!DNS	651
Impact:Runtime/AbusedDomainRequest.Reputation	652
Impact:Runtime/BitcoinDomainRequest.Reputation	652
Impact:Runtime/MaliciousDomainRequest.Reputation	653
Impact:Runtime/SuspiciousDomainRequest.Reputation	654
UnauthorizedAccess:Runtime/MetadataDNSRebind	655
Execution:Runtime/NewBinaryExecuted	656
PrivilegeEscalation:Runtime/DockerSocketAccessed	657
PrivilegeEscalation:Runtime/RuncContainerEscape	658
PrivilegeEscalation:Runtime/CGroupsReleaseAgentModified	659
DefenseEvasion:Runtime/ProcessInjection.Proc	660
DefenseEvasion:Runtime/ProcessInjection.Ptrace	660
DefenseEvasion:Runtime/ProcessInjection.VirtualMemoryWrite	661
Execution:Runtime/ReverseShell	662
DefenseEvasion:Runtime/FilelessExecution	662
Impact:Runtime/CryptoMinerExecuted	663
Execution:Runtime/NewLibraryLoaded	664
PrivilegeEscalation:Runtime/ContainerMountsHostDirectory	664
PrivilegeEscalation:Runtime/UserfaultfdUsage	665
Execution:Runtime/SuspiciousTool	666
Execution:Runtime/SuspiciousCommand	667

DefenseEvasion:Runtime/SuspiciousCommand	667
DefenseEvasion:Runtime/PtraceAntiDebugging	668
Execution:Runtime/MaliciousFileExecuted	669
Execution:Runtime/SuspiciousShellCreated	670
PrivilegeEscalation:Runtime/ElevationToRoot	670
Discovery:Runtime/SuspiciousCommand	671
Persistence:Runtime/SuspiciousCommand	672
PrivilegeEscalation:Runtime/SuspiciousCommand	673
Perlindungan Malware untuk EC2 menemukan jenis	674
Execution:EC2/MaliciousFile	675
Execution:ECS/MaliciousFile	675
Execution:Kubernetes/MaliciousFile	675
Execution:Container/MaliciousFile	676
Execution:EC2/SuspiciousFile	676
Execution:ECS/SuspiciousFile	677
Execution:Kubernetes/SuspiciousFile	678
Execution:Container/SuspiciousFile	679
Perlindungan Malware untuk tipe pencarian S3	679
Object:S3/MaliciousFile	680
Jenis temuan Perlindungan RDS	680
CredentialAccess:RDS/AnomalousBehavior.SuccessfulLogin	681
CredentialAccess:RDS/AnomalousBehavior.FailedLogin	682
CredentialAccess:RDS/AnomalousBehavior.SuccessfulBruteForce	683
CredentialAccess:RDS/MaliciousIPCaller.SuccessfulLogin	684
CredentialAccess:RDS/MaliciousIPCaller.FailedLogin	684
Discovery:RDS/MaliciousIPCaller	685
CredentialAccess:RDS/TorIPCaller.SuccessfulLogin	686
CredentialAccess:RDS/TorIPCaller.FailedLogin	686
Discovery:RDS/TorIPCaller	687
Jenis temuan Perlindungan Lambda	688
Backdoor:Lambda/C&CActivity.B	688
CryptoCurrency:Lambda/BitcoinTool.B	689
Trojan:Lambda/BlackholeTraffic	690
Trojan:Lambda/DropPoint	690
UnauthorizedAccess:Lambda/MaliciousIPCaller.Custom	691
UnauthorizedAccess:Lambda/TorClient	691

UnauthorizedAccess:Lambda/TorRelay	692
Tipe temuan yang sudah dihentikan	692
Exfiltration:S3/ObjectRead.Unusual	693
Impact:S3/PermissionsModification.Unusual	694
Impact:S3/ObjectDelete.Unusual	695
Discovery:S3/BucketEnumeration.Unusual	695
Persistence:IAMUser/NetworkPermissions	696
Persistence:IAMUser/ResourcePermissions	697
Persistence:IAMUser/UserPermissions	697
PrivilegeEscalation:IAMUser/AdministrativePermissions	698
Recon:IAMUser/NetworkPermissions	699
Recon:IAMUser/ResourcePermissions	700
Recon:IAMUser/UserPermissions	701
ResourceConsumption:IAMUser/ComputeResources	701
Stealth:IAMUser/LoggingConfigurationModified	702
UnauthorizedAccess:IAMUser/ConsoleLogin	703
UnauthorizedAccess:EC2/TorIPCaller	704
Backdoor:EC2/XORDDOS	704
Behavior:IAMUser/InstanceLaunchUnusual	704
CryptoCurrency:EC2/BitcoinTool.A	705
UnauthorizedAccess:IAMUser/UnusualASNCaller	705
GuardDuty menemukan jenis dengan sumber daya yang berpotensi terkena dampak	706
GuardDuty jenis temuan aktif	706
Memahami dan menghasilkan temuan	728
GuardDuty menemukan format	729
Tujuan Ancaman	730
GuardDuty mesin pemindai deteksi malware	734
Sampel temuan	734
Menghasilkan temuan sampel melalui GuardDuty konsol atau API	735
GuardDuty Temuan uji	736
Pertimbangan	736
GuardDuty temuan skrip tester dapat menghasilkan	738
Langkah 1 - Prasyarat	740
Langkah 2 - Menyebarkan sumber daya AWS	741
Langkah 3 - Jalankan skrip pengujian	743
Langkah 4 - Bersihkan sumber daya AWS tes	745

Memecahkan masalah umum	745
Halaman temuan di GuardDuty konsol	747
Menavigasi halaman Temuan	748
Temuan tingkat keparahan	750
Tingkat keparahan kritis	750
Tingkat keparahan tinggi	750
Tingkat keparahan sedang	751
Tingkat keparahan rendah	752
Detail temuan	752
Menemukan ikhtisar	753
Sumber Daya	754
Detail pencarian urutan serangan	760
Rincian pengguna database RDS (DB)	767
Detail penemuan Runtime Monitoring	768
Detail pemindaian volume EBS	770
Perlindungan Malware untuk EC2 menemukan detail	771
Perlindungan Malware untuk detail penemuan S3	772
Tindakan	773
Aktor atau Target	774
Detail geolokasi	775
Informasi tambahan	775
Bukti	776
Perilaku anomali	776
GuardDuty menemukan agregasi	781
Mengelola GuardDuty temuan	783
GuardDuty Dasbor ringkasan	784
Gambaran Umum	785
Temuan	786
Jenis temuan yang paling umum	787
Temuan berdasarkan tingkat keparahan	787
Akun dengan sebagian besar temuan	788
Sumber daya dengan temuan	788
Temuan yang paling tidak terjadi	789
Cakupan rencana perlindungan	789
Penyaringan temuan GuardDuty	790
Membuat dan menyimpan set filter di GuardDuty konsol	791

Membuat dan menyimpan set filter dengan menggunakan GuardDuty API dan CLI	793
Filter properti di GuardDuty	795
Aturan penekanan	802
.....	802
Menggunakan aturan penekanan dengan Extended Threat Detection	803
Kasus penggunaan umum untuk aturan penekanan dan contoh	803
Membuat aturan penekanan	807
Menghapus aturan penekanan	810
.....	808
Daftar IP terpercaya dan daftar ancaman	811
Format daftar	812
Izin yang diperlukan untuk mengunggah daftar IP terpercaya dan daftar ancaman	815
Menggunakan enkripsi sisi server untuk daftar IP terpercaya dan daftar ancaman	816
Menambahkan dan mengaktifkan daftar IP terpercaya atau daftar IP ancaman	817
Memperbarui daftar IP terpercaya dan daftar ancaman	819
Menonaktifkan atau menghapus daftar IP terpercaya atau daftar ancaman	820
Mengekspor temuan yang dihasilkan ke Amazon S3	822
Pertimbangan	822
Langkah 1 - Izin diperlukan untuk mengekspor temuan	823
Langkah 2 - Melampirkan kebijakan ke kunci KMS Anda	824
Langkah 3 - Melampirkan kebijakan ke bucket Amazon S3	826
Langkah 4 - Mengekspor temuan ke bucket S3 (Konsol)	829
Langkah 5 - Frekuensi untuk mengekspor temuan	831
Memproses temuan dengan EventBridge	831
EventBridge Frekuensi pemberitahuan di GuardDuty	832
Siapkan topik dan titik akhir Amazon SNS	833
Menggunakan EventBridge dengan GuardDuty	834
Membuat EventBridge aturan	836
EventBridge aturan untuk lingkungan multi-akun	843
Memahami CloudWatch Log dan alasan melewatkan sumber daya	844
Mengaudit CloudWatch Log dalam Perlindungan GuardDuty Malware untuk EC2	844
GuardDuty Perlindungan Malware untuk retensi EC2 log	846
Alasan melewatkan sumber daya	846
Melaporkan hasil pemindaian EC2 malware positif palsu	853
Melaporkan hasil pemindaian objek S3 positif palsu	854
Mengatasi temuan	856

Memperbaiki instans Amazon yang berpotensi dikompromikan EC2	856
Memperbaiki bucket S3 yang berpotensi dikompromikan	858
Rekomendasi berdasarkan kebutuhan akses bucket S3 tertentu	860
Memperbaiki objek S3 yang berpotensi berbahaya	861
Memulihkan cluster ECS yang berpotensi dikompromikan	861
Memulihkan kredensi yang berpotensi dikompromikan AWS	862
Memulihkan wadah mandiri yang berpotensi dikompromikan	864
Remediasi temuan Perlindungan EKS	865
Potensi masalah konfigurasi	866
Memulihkan pengguna Kubernetes yang berpotensi dikompromikan	866
Remediasi pod Kubernetes yang berpotensi dikompromikan	869
Memulihkan gambar kontainer yang berpotensi dikompromikan	870
Remediasi node Kubernetes yang berpotensi dikompromikan	871
Remediasi temuan Runtime Monitoring	872
Memulihkan gambar kontainer yang dikompromikan	873
Memulihkan database yang berpotensi dikompromikan	874
Memulihkan database yang berpotensi dikompromikan dengan peristiwa login yang berhasil	875
Memulihkan database yang berpotensi dikompromikan dengan peristiwa login yang gagal ..	876
Memulihkan kredensi yang berpotensi dikompromikan	877
Batasi akses jaringan	877
Memperbaiki fungsi Lambda yang berpotensi dikompromikan	878
Memperkirakan biaya penggunaan	880
Memahami cara GuardDuty menghitung biaya penggunaan	881
.....	881
Runtime Monitoring - Bagaimana log aliran VPC EC2 dari instans memengaruhi biaya penggunaan	882
Bagaimana GuardDuty memperkirakan biaya penggunaan untuk CloudTrail acara	882
Meninjau perkiraan biaya penggunaan	882
Nama fitur untuk paket perlindungan di API	885
Ubah dari sumber data ke fitur	885
GuardDuty Perubahan API	885
Fitur dibandingkan dengan sumber data	886
Memahami cara APIs kerja fitur	886
Menggabungkan perubahan fitur di APIs	887
Fitur yang dipetakan GuardDuty	888

Keamanan	891
Perlindungan data	892
Enkripsi diam	893
Enkripsi bergerak	893
Memilih untuk tidak menggunakan data Anda untuk perbaikan layanan	893
Logging dengan CloudTrail	895
GuardDuty informasi di CloudTrail	895
GuardDuty peristiwa pesawat kontrol di CloudTrail	896
GuardDuty peristiwa data di CloudTrail	896
Contoh: entri file GuardDuty log	898
Identity and Access Management	900
Audiens	901
Mengautentikasi dengan identitas	901
Mengelola akses menggunakan kebijakan	905
Bagaimana Amazon GuardDuty bekerja dengan IAM	908
Contoh kebijakan berbasis identitas	915
Menggunakan peran terkait layanan	924
AWS kebijakan terkelola	944
Pemecahan Masalah	957
Validasi kepatuhan	959
Ketahanan	961
Keamanan infrastruktur	961
Titik akhir VPC (AWS PrivateLink)	962
Pertimbangan untuk titik akhir GuardDuty VPC	962
Buat VPC endpoint antarmuka untuk GuardDuty	962
Membuat kebijakan titik akhir VPC untuk GuardDuty	963
Subnet bersama	963
Integrasi dengan layanan AWS keamanan	965
Integrasi dengan GuardDuty AWS Security Hub	965
Integrasi GuardDuty dengan Amazon Detective	965
AWS Security Hub integrasi	965
Bagaimana Amazon GuardDuty mengirimkan temuan ke AWS Security Hub	966
Melihat GuardDuty temuan di AWS Security Hub	967
Mengaktifkan dan mengonfigurasi integrasi	986
Menggunakan GuardDuty kontrol di Security Hub	986
Menghentikan publikasi temuan ke Security Hub	986

Integrasi Amazon Detective	986
Mengaktifkan integrasi	987
Berputar ke Detektif Amazon dari sebuah temuan GuardDuty	987
Menggunakan integrasi dengan lingkungan GuardDuty multi-akun	988
Menangguhkan atau menonaktifkan	989
GuardDuty pengumuman	991
Format pesan Amazon SNS	997
GuardDuty kuota	1002
Pemecahan Masalah	1007
Mengekspor temuan ke Amazon S3 - kesalahan akses	1007
Perlindungan Malware untuk EC2 masalah	1008
Tidak ada izin AWS Organizations manajemen yang diperlukan saat mengaktifkan pemindaian GuardDuty malware yang dimulai	1008
Saya memulai pemindaian malware On-Demand tetapi menghasilkan kesalahan izin yang diperlukan hilang.	1008
Saya menerima iam:GetRole kesalahan saat bekerja dengan Perlindungan Malware untuk EC2.	1008
Saya adalah akun GuardDuty administrator yang perlu mengaktifkan GuardDuty pemindaian malware yang dimulai tetapi tidak menggunakan kebijakan AWS terkelola: AmazonGuardDutyFullAccess untuk mengelola. GuardDuty	1009
Masalah Runtime Monitoring	1009
Masalah cakupan runtime	1009
Memecahkan masalah kesalahan memori	1009
AWS Step Functions Alur kerja saya gagal secara tak terduga	1010
Masalah pemecahan masalah lainnya	1011
Wilayah dan titik akhir	1012
Ketersediaan fitur khusus wilayah	1012
Tindakan dan parameter lama	1014
Riwayat dokumen	1016
Pembaruan lebih awal	1097
.....	mxcviii

Apa itu Amazon GuardDuty?

Amazon GuardDuty adalah layanan deteksi ancaman yang terus memantau, menganalisis, dan memproses sumber AWS data dan log di AWS lingkungan Anda. GuardDuty Menggunakan feed intelijen ancaman, seperti daftar alamat IP berbahaya dan domain, hash file, dan model machine learning (ML) untuk mengidentifikasi aktivitas yang mencurigakan dan berpotensi berbahaya di lingkungan Anda. AWS Daftar berikut memberikan ikhtisar skenario ancaman potensial yang GuardDuty dapat membantu Anda mendeteksi:

- Kredensi yang dikompromikan dan diekstraksi. AWS
- Eksfiltrasi dan penghancuran data yang dapat menyebabkan peristiwa ransomware. Pola peristiwa login yang tidak biasa dalam versi mesin yang didukung dari database Amazon Aurora dan Amazon RDS, yang menunjukkan perilaku anomali.
- Aktivitas cryptomining yang tidak sah di instans Amazon Elastic Compute Cloud (Amazon EC2) dan beban kerja container Anda.
- Kehadiran malware di EC2 instans Amazon dan beban kerja penampung, serta file yang baru diunggah di bucket Amazon Simple Storage Service (Amazon S3).
- Tingkat sistem operasi, jaringan, dan peristiwa file yang menunjukkan perilaku tidak sah pada kluster Amazon Elastic Kubernetes Service (Amazon EKS), Amazon Elastic Container Service (Amazon ECS) - tugas, dan instans Amazon serta beban kerja AWS Fargate container. EC2

Video berikut memberikan ikhtisar tentang bagaimana GuardDuty membantu Anda mendeteksi ancaman di AWS lingkungan Anda.

[Apa itu Amazon GuardDuty](#)

Daftar Isi

- [Fitur dari GuardDuty](#)
- [Kepatuhan PCI DSS](#)
- [Harga di GuardDuty](#)
- [Mengakses GuardDuty](#)

Fitur dari GuardDuty

Berikut adalah beberapa cara utama Amazon GuardDuty dapat membantu Anda memantau, mendeteksi, dan mengelola potensi ancaman di AWS lingkungan Anda.

Terus memantau sumber data tertentu dan log peristiwa

- **Deteksi ancaman dasar** — Ketika Anda mengaktifkan GuardDuty Akun AWS, GuardDuty secara otomatis mulai menelan sumber data dasar yang terkait dengan akun itu. Sumber data ini mencakup peristiwa AWS CloudTrail manajemen, log aliran VPC (dari EC2 instans Amazon), dan log DNS. Anda tidak perlu mengaktifkan hal lain GuardDuty untuk mulai menganalisis dan memproses sumber data ini untuk menghasilkan temuan keamanan terkait. Untuk informasi selengkapnya, lihat [GuardDuty sumber data dasar](#).
- **Extended Threat Detection** — Kemampuan ini mendeteksi serangan multi-tahap yang menjangkau sumber data dasar, berbagai jenis sumber AWS daya, dan waktu, dalam file. Akun AWS Mungkin ada beberapa peristiwa di akun Anda yang, secara individual, tidak menampilkan diri sebagai ancaman yang jelas. Namun, ketika peristiwa ini diamati dalam urutan yang menunjukkan aktivitas yang mencurigakan, GuardDuty mengidentifikasinya sebagai urutan serangan. GuardDuty memberi tahu Anda dengan membuat jenis pencarian urutan serangan terkait untuk memberikan detail tentang urutan serangan yang diamati.

Tanpa biaya tambahan yang terkait dengannya, Extended Threat Detection diaktifkan secara otomatis untuk masing-masing Akun AWS saat diaktifkan GuardDuty. Kemampuan ini tidak mengharuskan Anda untuk mengaktifkan rencana perlindungan yang berfokus pada kasus penggunaan apa pun. Namun, untuk meningkatkan luasnya keamanan ke sumber daya Amazon S3 Anda GuardDuty , rekomendasikan untuk mengaktifkan Perlindungan S3 di akun Anda. Ini akan membantu Extended Threat Detection untuk mengidentifikasi serangan multi-tahap yang berpotensi memengaruhi sumber daya Amazon S3 Anda.

Untuk informasi selengkapnya tentang cara kerja kemampuan ini dan skenario ancaman apa yang dicakupnya, lihat [GuardDuty Deteksi Ancaman Diperpanjang](#).

- **Paket GuardDuty perlindungan yang berfokus pada kasus penggunaan** — Untuk meningkatkan visibilitas deteksi ancaman ke dalam keamanan AWS lingkungan Anda, GuardDuty menawarkan paket perlindungan khusus yang dapat Anda pilih untuk diaktifkan. Paket perlindungan membantu Anda memantau log dan peristiwa dari AWS layanan lain. Sumber-sumber ini termasuk log audit EKS, aktivitas login RDS, peristiwa data Amazon S3 CloudTrail di, volume EBS, Pemantauan Runtime di Amazon EKS, Amazon, EC2 dan Amazon ECS-Fargate, dan log aktivitas jaringan Lambda. GuardDuty mengkonsolidasikan sumber log

dan peristiwa ini di bawah istilah - [Fitur](#). Anda dapat mengaktifkan satu atau lebih paket perlindungan khusus di dukungan Wilayah AWS kapan saja. GuardDuty akan mulai memantau, memproses, dan menganalisis aktivitas berdasarkan rencana perlindungan yang Anda aktifkan. Untuk informasi selengkapnya tentang setiap rencana perlindungan dan cara kerjanya, lihat dokumen rencana perlindungan yang sesuai.

Rencana perlindungan	Deskripsi
Perlindungan S3	Mengidentifikasi potensi risiko keamanan seperti eksfiltrasi data dan upaya penghancuran di bucket Amazon S3 Anda.
Perlindungan EKS	EKS Audit Log Monitoring menganalisis log audit Kubernetes dari kluster Amazon EKS Anda untuk aktivitas yang berpotensi mencurigakan dan berbahaya.
Pemantauan Runtime	Memantau dan menganalisis peristiwa tingkat sistem operasi di Amazon EKS, Amazon, EC2 dan Amazon ECS Anda (termasuk AWS Fargate), untuk mendeteksi potensi ancaman runtime.
Perlindungan Malware untuk EC2	Mendeteksi potensi keberadaan malware dengan memindai volume Amazon EBS yang terkait dengan instans Amazon EC2 Anda. Ada opsi untuk menggunakan fitur ini sesuai permintaan.
Perlindungan Malware untuk S3	Mendeteksi potensi keberadaan malware di objek yang baru diunggah dalam bucket Amazon S3 Anda.
Perlindungan RDS	Menganalisis dan membuat profil aktivitas login RDS Anda untuk potensi ancaman akses ke basis data Amazon Aurora dan Amazon RDS yang didukung.
Perlindungan Lambda	Memantau log aktivitas jaringan Lambda, dimulai dengan log aliran VPC, untuk mendeteksi ancaman terhadap fungsi Anda. AWS Lambda Contoh ancaman potensial ini termasuk cryptomining dan berkomunikasi dengan server jahat.

Aktifkan Perlindungan Malware untuk S3 secara mandiri

GuardDuty menawarkan fleksibilitas untuk menggunakan Perlindungan Malware untuk S3 secara independen, tanpa mengaktifkan layanan Amazon GuardDuty. Untuk informasi selengkapnya tentang memulai hanya dengan Perlindungan Malware untuk S3, lihat [GuardDuty Perlindungan Malware untuk S3](#). Untuk menggunakan semua paket perlindungan lainnya, Anda harus mengaktifkan GuardDuty layanan.

Kelola lingkungan beberapa akun

Anda dapat mengelola AWS lingkungan beberapa akun dengan menggunakan metode undangan AWS Organizations (disarankan) atau lama. Untuk informasi selengkapnya, lihat [Beberapa akun di GuardDuty](#).

Menghasilkan temuan keamanan untuk ancaman yang terdeteksi

Ketika GuardDuty mendeteksi potensi ancaman keamanan yang terkait dengan AWS sumber daya Anda, itu mulai menghasilkan temuan keamanan yang memberikan informasi tentang sumber daya yang berpotensi dikompromikan. Setelah Anda mengaktifkan GuardDuty di akun Anda, buat [Sampel temuan](#) untuk melihat yang terkait [Detail temuan](#). Untuk daftar lengkap temuan keamanan, lihat [GuardDuty menemukan jenis](#).

Dengan GuardDuty, Anda juga dapat menggunakan skrip pengujian yang menghasilkan temuan GuardDuty keamanan khusus untuk memahami cara meninjau dan menanggapi GuardDuty temuan. Untuk informasi selengkapnya, lihat [GuardDuty Temuan uji di akun khusus](#).

Menilai dan mengelola temuan keamanan

GuardDuty menggabungkan temuan keamanan Anda di seluruh akun dan menampilkan hasil di dasbor Ringkasan di GuardDuty konsol. Anda juga dapat mengambil temuan melalui AWS Security Hub API AWS Command Line Interface, atau AWS SDK. Dengan pandangan holistik tentang status keamanan Anda saat ini, Anda dapat mengidentifikasi tren dan potensi masalah, dan mengambil langkah-langkah perbaikan yang diperlukan. Untuk informasi selengkapnya, lihat [Mengelola GuardDuty temuan](#).

Integrasi dengan layanan AWS keamanan terkait

Untuk lebih membantu Anda menganalisis dan menyelidiki tren keamanan di AWS lingkungan Anda, pertimbangkan untuk menggunakan layanan AWS terkait keamanan berikut dalam kombinasi dengan GuardDuty

- **AWS Security Hub**— Layanan ini memberi Anda pandangan komprehensif tentang keadaan keamanan AWS sumber daya Anda dan membantu Anda memeriksa AWS lingkungan Anda terhadap standar industri keamanan dan praktik terbaik. Hal ini dilakukan sebagian dengan mengkonsumsi, menggabungkan, mengatur, dan memprioritaskan temuan keamanan Anda dari berbagai layanan (AWS termasuk Amazon Macie) dan produk Jaringan Mitra (APN) yang didukung AWS . Security Hub membantu Anda menganalisis tren keamanan dan mengidentifikasi masalah keamanan prioritas tertinggi di AWS lingkungan Anda.

Untuk informasi tentang penggunaan GuardDuty dan Security Hub bersama-sama, lihat [Integrasi dengan GuardDuty AWS Security Hub](#). Untuk mempelajari selengkapnya tentang Security Hub, lihat [Panduan Pengguna AWS Security Hub](#).

- **Detektif Amazon** — Layanan ini membantu Anda menganalisis, menyelidiki, dan mengidentifikasi akar penyebab temuan keamanan atau aktivitas mencurigakan dengan cepat. Detective secara otomatis mengumpulkan data log dari sumber daya Anda. AWS Kemudian menggunakan pembelajaran mesin, analisis statistik, dan teori grafik untuk menghasilkan visualisasi yang membantu Anda melakukan penyelidikan keamanan yang lebih cepat dan lebih efisien. Agregasi data Detective prebuilt, ringkasan, dan konteks membantu Anda menganalisis dan menentukan sifat dan tingkat potensi masalah keamanan.

Untuk informasi tentang penggunaan GuardDuty dan Detektif bersama-sama, lihat. [Integrasi GuardDuty dengan Amazon Detective](#) Untuk mempelajari lebih lanjut tentang Detektif, lihat Panduan Pengguna [Detektif](#) Amazon.

- **Amazon EventBridge** — Layanan ini membantu Anda menerima pemberitahuan dan menanggapi temuan GuardDuty keamanan dalam waktu dekat. GuardDuty menciptakan peristiwa ketika ada perubahan dalam temuan. Anda dapat memilih seberapa sering Anda ingin menerima pemberitahuan dari EventBridge. Untuk informasi selengkapnya, lihat [Apa itu Amazon EventBridge](#) di Panduan EventBridge Pengguna Amazon.

Kepatuhan PCI DSS

GuardDuty mendukung pemrosesan, penyimpanan, dan transmisi data kartu kredit oleh pedagang atau penyedia layanan, dan telah divalidasi sesuai dengan Standar Keamanan Data Industri Kartu Pembayaran (PCI) Data Security Standard (DSS). Untuk informasi selengkapnya tentang PCI DSS, termasuk cara meminta salinan PCI AWS Compliance Package, lihat [PCI](#) DSS Level 1.

Untuk informasi selengkapnya, lihat [Penguji pihak ketiga baru membandingkan Amazon GuardDuty dengan sistem deteksi intrusi jaringan di Blog](#) Keamanan.AWS

Harga di GuardDuty

Bagian ini berfokus pada AWS Tingkat Gratis model yang GuardDuty digunakan untuk berbagai rencana perlindungan, dan bagaimana Anda dapat melihat perkiraan dan biaya penggunaan aktual. Jika Anda mencari detail harga yang terkait dengan semua paket perlindungan di seluruh Wilayah yang didukung, lihat [GuardDutyharga](#).

AWS Tingkat Gratis

AWS Tingkat Gratis membantu Anda menjelajahi dan mencoba Layanan AWS gratis hingga batas yang ditentukan untuk setiap layanan. Ada tiga kategori — 12 bulan gratis, selalu gratis, dan uji coba gratis jangka pendek. Amazon GuardDuty termasuk dalam kategori uji coba gratis jangka pendek dan menawarkan uji coba gratis 30 hari. Ketika Anda terus menggunakan GuardDuty setelah uji coba gratis ini berakhir, Anda mulai mengeluarkan biaya berdasarkan cara Anda menggunakan layanan ini.

¹ Pengecualian untuk uji GuardDuty coba gratis 30 hari

Pemindaian malware sesuai permintaan (di bawah Perlindungan Malware untuk EC2) dan Perlindungan Malware untuk S3 tidak termasuk dalam kategori uji coba gratis jangka pendek GuardDuty 30 hari. Perlindungan Malware untuk S3 termasuk dalam kategori gratis 12 bulan AWS Tingkat Gratis sedangkan pemindaian malware On-Demand mengikuti model pay-as-you-use biaya. Tidak ada uji coba gratis 30 hari atau model biaya Tingkat Gratis 12 bulan dengan pemindaian malware sesuai permintaan.

Menggunakan uji GuardDuty coba gratis 30 hari

Saat menggunakan GuardDuty untuk pertama kalinya Wilayah AWS, Anda Akun AWS secara otomatis terdaftar dalam uji coba gratis 30 hari di Wilayah tersebut. Beberapa paket perlindungan juga akan diaktifkan secara otomatis dan termasuk dalam uji coba gratis 30 hari. Karena GuardDuty merupakan layanan regional, ketika Anda mengaktifkannya untuk pertama kalinya di Wilayah yang berbeda, akun Anda akan mendapatkan uji coba gratis 30 hari GuardDuty di Wilayah tersebut. Saat bekerja dengan beberapa akun dalam suatu GuardDuty organisasi, setiap akun mendapatkan uji coba gratis 30 hari sendiri.

Gunakan tabel berikut untuk meninjau paket perlindungan mana yang diaktifkan secara default GuardDuty, dan ketersediaan uji coba gratisnya.

Rencana perlindungan	Diaktifkan secara default dengan GuardDuty	Pisahkan ketersediaan uji coba gratis ²	
Perlindungan EKS	Ya	Ya	
Perlindungan S3	Ya	Ya	
Pemantauan Runtime	Tidak	Ya	
Perlindungan Malware untuk EC2 – GuardDuty-pemindaian malware yang dimulai	Ya	Ya	
Perlindungan Malware untuk EC2 – Pemindaian malware sesuai permintaan di GuardDuty	Tidak	Tidak ¹	
GuardDuty Perlindungan Malware untuk S3	Tidak	Tidak ¹	
Perlindungan RDS	Ya	Ya	
Perlindungan Lambda	Ya	Ya	

² Saat Anda mengaktifkan GuardDuty untuk pertama kalinya, paket perlindungan (kecuali Runtime Monitoring) secara otomatis diaktifkan dan disertakan dalam uji coba gratis 30 hari awal. Ketika GuardDuty akun yang ada memungkinkan rencana perlindungan baru setelah uji coba GuardDuty gratis awal mereka berakhir, maka paket perlindungan itu dilengkapi dengan uji coba gratis 30 hari sendiri. Untuk informasi selengkapnya tentang uji coba gratis untuk paket perlindungan, lihat dokumen yang terkait dengan setiap paket perlindungan.

Lihat perkiraan biaya penggunaan selama uji coba gratis — Selama uji coba gratis 30 hari GuardDuty dan kemungkinan rencana perlindungan, GuardDuty berikan perkiraan biaya penggunaan untuk

akun Anda. Jika Anda adalah akun GuardDuty administrator yang didelegasikan, Anda dapat melihat total perkiraan biaya penggunaan dan rincian tingkat akun untuk semua akun anggota yang telah diaktifkan. GuardDuty Untuk informasi selengkapnya, lihat [Memperkirakan biaya GuardDuty penggunaan](#).

Biaya penggunaan setelah uji coba gratis berakhir — Saat Anda terus menggunakan GuardDuty atau paket perlindungannya setelah uji coba gratis berakhir, Anda akan mulai mengeluarkan biaya penggunaan terkait. Untuk melihat tagihan Anda, navigasikan ke Cost Explorer di <https://console.aws.amazon.com/costmanagement/> konsol. Untuk informasi selengkapnya tentang penagihan AWS akun, lihat [Panduan AWS Billing Pengguna](#).

Menggunakan Perlindungan Malware untuk S3 dengan Tingkat Gratis 12 bulan

Perlindungan Malware untuk S3 menggunakan paket Tingkat Gratis yang terkait dengan Anda Akun AWS yang baru, memiliki tingkat gratis yang berkelanjutan, atau memiliki tingkat gratis 12 bulan yang kedaluwarsa. Untuk informasi selengkapnya, lihat [Harga dan biaya penggunaan untuk Perlindungan Malware untuk S3](#).

Mengakses GuardDuty

Amazon GuardDuty tersedia di sebagian besar Wilayah AWS. Untuk daftar Wilayah yang saat GuardDuty ini tersedia, lihat [Wilayah dan titik akhir](#).

Anda dapat menggunakan GuardDuty salah satu cara berikut:

GuardDuty konsol

<https://console.aws.amazon.com/guardduty/>

Konsol adalah antarmuka berbasis browser untuk mengakses dan menggunakan. GuardDuty GuardDuty Konsol menyediakan akses ke GuardDuty akun, data, dan sumber daya Anda.

AWS Command Line Interface

Dengan AWS Command Line Interface (AWS CLI), Anda dapat mengeluarkan perintah di baris perintah sistem Anda untuk melakukan GuardDuty tugas dan AWS tugas. AWS CLI Perintah berguna jika Anda ingin membangun skrip yang melakukan tugas.

Untuk informasi tentang menginstal dan menggunakan AWS CLI, lihat [Panduan AWS Command Line Interface Pengguna](#). Untuk melihat AWS CLI perintah yang tersedia GuardDuty, lihat [Referensi AWS CLI Perintah](#).

GuardDuty HTTPS API

Anda dapat mengakses GuardDuty dan AWS secara terprogram menggunakan GuardDuty HTTPS API, yang memungkinkan Anda mengeluarkan permintaan HTTPS langsung ke layanan. Untuk informasi selengkapnya, lihat [Referensi Amazon GuardDuty API](#).

AWS SDKs

AWS menyediakan kit pengembangan perangkat lunak (SDKs) yang terdiri dari pustaka dan kode sampel untuk berbagai bahasa dan platform pemrograman (Java, Python, Ruby, .NET, iOS, Android, dan lainnya). SDKs Menyediakan cara mudah untuk membuat akses terprogram ke GuardDuty. Untuk informasi tentang AWS SDKs, termasuk cara mengunduh dan menginstalnya, lihat [Alat untuk Amazon Web Services](#).

Konsep dan istilah kunci di Amazon GuardDuty

Saat Anda memulai dengan Amazon GuardDuty, Anda bisa mendapatkan keuntungan dari mempelajari konsepnya dan istilah kunci terkait.

Akun

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

Anda juga dapat mengundang akun lain untuk mengaktifkan GuardDuty dan menjadi terkait dengan AWS akun Anda di GuardDuty. Jika undangan Anda diterima, akun Anda ditetapkan sebagai akun administrator, dan GuardDuty akun yang ditambahkan menjadi akun anggota Anda. Anda kemudian dapat melihat dan mengelola GuardDuty temuan akun tersebut atas nama mereka.

Pengguna akun administrator dapat mengonfigurasi GuardDuty serta melihat dan mengelola GuardDuty temuan untuk akun mereka sendiri dan semua akun anggota mereka. Untuk informasi tentang jumlah akun anggota yang dapat dikelola oleh akun administrator Anda, lihat [GuardDuty kuota](#).

Pengguna akun anggota dapat mengonfigurasi GuardDuty serta melihat dan mengelola GuardDuty temuan di akun mereka (baik melalui konsol GuardDuty manajemen atau GuardDuty API). Pengguna akun anggota tidak dapat melihat atau mengelola temuan di akun anggota lain.

Tidak Akun AWS dapat menjadi akun GuardDuty administrator dan akun anggota secara bersamaan. An hanya Akun AWS dapat menerima satu undangan keanggotaan. Menerima undangan keanggotaan bersifat opsional.

Untuk informasi selengkapnya, lihat [Beberapa akun di Amazon GuardDuty](#).

Urutan serangan

Urutan serangan adalah korelasi dari beberapa peristiwa yang, seperti yang diamati oleh GuardDuty, terjadi dalam urutan tertentu yang cocok dengan pola aktivitas yang mencurigakan. GuardDuty menggunakan [Deteksi Ancaman Diperpanjang](#) kemampuannya untuk mendeteksi serangan multi-tahap yang mencakup sumber data dasar, sumber AWS daya, dan garis waktu, di akun Anda.

Daftar berikut menjelaskan secara singkat istilah-istilah kunci yang terkait dengan urutan serangan:

- Indikator — Memberikan informasi mengapa urutan peristiwa sejalan dengan potensi aktivitas yang mencurigakan.
- Sinyal — Sinyal adalah aktivitas API yang GuardDuty diamati, atau GuardDuty temuan yang sudah terdeteksi di akun Anda. Dengan mengkorelasikan peristiwa yang diamati dalam urutan tertentu di akun Anda, GuardDuty mengidentifikasi urutan serangan.

Ada peristiwa di akun Anda yang tidak menunjukkan potensi ancaman. GuardDuty menganggapnya sebagai sinyal lemah. Namun, ketika sinyal dan GuardDuty temuan lemah diamati dalam urutan tertentu yang, ketika berkorelasi, sejajar dengan aktivitas yang berpotensi mencurigakan, GuardDuty menghasilkan temuan urutan serangan.

- Endpoints — Informasi tentang titik akhir jaringan yang berpotensi digunakan oleh aktor ancaman dalam urutan serangan.

Detektor

Amazon GuardDuty adalah layanan regional. Saat Anda mengaktifkan GuardDuty secara spesifik Wilayah AWS, Anda Akun AWS akan dikaitkan dengan ID detektor. ID alfanumerik 32 karakter ini unik untuk akun Anda di Wilayah tersebut. Misalnya, ketika Anda mengaktifkan GuardDuty akun yang sama di Wilayah yang berbeda, akun Anda akan dikaitkan dengan ID detektor yang berbeda. Format detectorID adalah. 12abc34d567e8fa901bc2d34e56789f0

Semua GuardDuty temuan, akun, dan tindakan tentang mengelola temuan dan GuardDuty layanan menggunakan ID detektor untuk menjalankan operasi API.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan detectorId [ListDetectors](#)API.

Note

Di lingkungan multi-akun, semua temuan untuk akun anggota digulung ke detektor akun administrator.

Beberapa GuardDuty fungsi dikonfigurasi melalui detektor, seperti mengonfigurasi frekuensi pemberitahuan CloudWatch Acara, dan mengaktifkan atau menonaktifkan rencana perlindungan opsional untuk diproses. GuardDuty

Menggunakan Perlindungan Malware untuk S3 di dalam GuardDuty

Saat Anda mengaktifkan Perlindungan Malware untuk S3 di akun yang GuardDuty diaktifkan, Perlindungan Malware untuk tindakan S3 seperti mengaktifkan, mengedit, dan menonaktifkan sumber daya yang dilindungi tidak terkait dengan ID detektor.

Jika Anda tidak mengaktifkan GuardDuty dan memilih opsi deteksi ancaman Perlindungan Malware untuk S3, tidak ada ID detektor yang dibuat untuk akun Anda.

Sumber data dasar

Asal atau lokasi satu set data. Untuk mendeteksi aktivitas yang tidak sah atau tidak terduga di AWS lingkungan Anda. GuardDuty menganalisis dan memproses data dari log AWS CloudTrail peristiwa, peristiwa AWS CloudTrail manajemen, peristiwa AWS CloudTrail data untuk S3, log aliran VPC, log DNS, lihat. [GuardDuty sumber data dasar](#)

Fitur

Objek fitur yang dikonfigurasi untuk paket GuardDuty perlindungan Anda membantu mendeteksi aktivitas yang tidak sah atau tidak terduga di AWS lingkungan Anda. Setiap rencana GuardDuty perlindungan mengkonfigurasi objek fitur yang sesuai untuk menganalisis dan memproses data. Beberapa objek fitur termasuk log audit EKS, pemantauan aktivitas login RDS, log aktivitas jaringan Lambda, dan volume EBS. Untuk informasi selengkapnya, lihat [Nama fitur untuk paket perlindungan di GuardDuty API](#).

Menemukan

Masalah keamanan potensial ditemukan oleh GuardDuty. Untuk informasi selengkapnya, lihat [Memahami dan menghasilkan GuardDuty temuan Amazon](#).

Temuan ditampilkan di GuardDuty konsol dan berisi deskripsi rinci tentang masalah keamanan. Anda juga dapat mengambil temuan yang dihasilkan dengan menghubungi dan [GetFindingsListFindings](#) Operasi API.

Anda juga dapat melihat GuardDuty temuan Anda melalui CloudWatch acara Amazon. GuardDuty mengirimkan temuan ke Amazon CloudWatch melalui protokol HTTPS. Untuk informasi selengkapnya, lihat [Memproses GuardDuty temuan dengan Amazon EventBridge](#).

Peran IAM

Ini adalah peran IAM dengan izin yang diperlukan untuk memindai objek S3. Saat menandai objek yang dipindai diaktifkan, PassRole izin IAM membantu GuardDuty menambahkan tag ke objek yang dipindai.

Sumber daya paket Perlindungan Malware

Setelah Anda mengaktifkan Perlindungan Malware untuk S3 untuk bucket, GuardDuty buat Perlindungan Malware untuk sumber daya EC2 paket. Sumber daya ini dikaitkan dengan Perlindungan Malware untuk ID EC2 paket, pengenal unik untuk bucket Anda yang dilindungi. Gunakan sumber daya paket Perlindungan Malware untuk melakukan operasi API pada sumber daya yang dilindungi.

Ember yang dilindungi (sumber daya terlindungi)

Bucket Amazon S3 dianggap dilindungi saat Anda mengaktifkan Perlindungan Malware untuk S3 untuk bucket ini dan status perlindungannya berubah menjadi Aktif.

GuardDuty hanya mendukung bucket S3 sebagai sumber daya yang dilindungi.

Status perlindungan

Status yang terkait dengan sumber daya paket Perlindungan Malware Anda. Setelah mengaktifkan Perlindungan Malware untuk S3 untuk bucket, status ini menunjukkan apakah bucket sudah diatur dengan benar atau tidak.

Awalan objek S3

Di bucket Amazon Simple Storage Service (Amazon S3), Anda dapat menggunakan awalan untuk mengatur penyimpanan Anda. Awalan adalah pengelompokan logis objek dalam ember S3. Untuk informasi selengkapnya, lihat [Mengatur dan mencantumkan objek](#) di Panduan Pengguna Amazon S3.

Opsi pemindaian

Saat Perlindungan GuardDuty Malware untuk EC2 diaktifkan, Anda dapat menentukan EC2 instans Amazon dan volume Amazon Elastic Block Store (EBS) mana yang akan dipindai atau dilewati. Fitur ini memungkinkan Anda menambahkan tag yang ada yang terkait dengan EC2 instance dan volume EBS Anda ke daftar tag inklusi atau daftar tag pengecualian. Sumber daya yang terkait dengan tag yang Anda tambahkan ke daftar tag inklusi, dipindai untuk malware, dan yang ditambahkan ke daftar tag pengecualian tidak dipindai. Untuk informasi selengkapnya, lihat [Opsi pindai dengan tag yang ditentukan pengguna](#).

Retensi snapshot

Ketika Perlindungan GuardDuty Malware untuk EC2 diaktifkan, ini menyediakan opsi untuk menyimpan snapshot volume EBS Anda di akun Anda AWS . GuardDuty menghasilkan replika volume EBS berdasarkan snapshot volume EBS Anda. Anda dapat menyimpan snapshot

volume EBS Anda hanya jika Perlindungan Malware untuk EC2 pemindaian mendeteksi malware dalam volume replika EBS. Jika tidak ada malware yang terdeteksi dalam volume replika EBS, GuardDuty secara otomatis menghapus snapshot volume EBS Anda, terlepas dari pengaturan retensi snapshot. Untuk informasi selengkapnya, lihat [Retensi snapshot](#).

Aturan penindasan

Aturan penekanan memungkinkan Anda membuat kombinasi atribut yang sangat spesifik untuk menekan temuan. Misalnya, Anda dapat menentukan aturan melalui GuardDuty filter untuk mengarsipkan otomatis hanya Recon:EC2/Portscan dari instance tersebut di VPC tertentu, menjalankan AMI tertentu, atau dengan tag tertentu. EC2 Aturan ini akan mengakibatkan temuan pemindaian port diarsipkan secara otomatis dari instans yang memenuhi kriteria. Namun, masih memungkinkan peringatan jika GuardDuty mendeteksi instans yang melakukan aktivitas berbahaya lainnya, seperti penambangan mata uang kripto.

Aturan penindasan yang ditentukan dalam akun GuardDuty administrator berlaku untuk akun GuardDuty anggota. GuardDuty akun anggota tidak dapat mengubah aturan penindasan.

Dengan aturan penindasan, GuardDuty masih menghasilkan semua temuan. Aturan penekanan memberikan penekanan pada temuan sekaligus mempertahankan riwayat yang lengkap dan tidak berubah dari semua aktivitas.

Biasanya aturan penindasan digunakan untuk menyembunyikan temuan yang telah Anda tentukan sebagai positif palsu untuk lingkungan Anda, dan mengurangi kebisingan dari temuan bernilai rendah sehingga Anda dapat fokus pada ancaman yang lebih besar. Untuk informasi selengkapnya, lihat [Aturan penindasan di GuardDuty](#).

Daftar IP tepercaya

Daftar alamat IP tepercaya untuk komunikasi yang sangat aman dengan AWS lingkungan Anda. GuardDuty tidak menghasilkan temuan berdasarkan daftar IP tepercaya. Untuk informasi selengkapnya, lihat [Bekerja dengan daftar IP tepercaya dan daftar ancaman](#).

Daftar IP ancaman

Daftar alamat IP berbahaya yang diketahui. Selain menghasilkan temuan karena aktivitas yang berpotensi mencurigakan, GuardDuty juga menghasilkan temuan berdasarkan daftar ancaman ini. Lihat informasi yang lebih lengkap di [Bekerja dengan daftar IP tepercaya dan daftar ancaman](#).

Memulai dengan GuardDuty

Tutorial ini memberikan pengantar langsung untuk GuardDuty Persyaratan minimum untuk mengaktifkan GuardDuty sebagai akun mandiri atau sebagai GuardDuty administrator AWS Organizations tercakup dalam Langkah 1. Langkah 2 hingga 5 mencakup menggunakan fitur tambahan yang direkomendasikan oleh GuardDuty untuk mendapatkan hasil maksimal dari temuan Anda.

Topik

- [Sebelum Anda mulai](#)
- [Langkah 1: Aktifkan Amazon GuardDuty](#)
- [Langkah 2: Menghasilkan temuan sampel dan menjelajahi operasi dasar](#)
- [Langkah 3: Konfigurasi GuardDuty temuan ekspor ke bucket Amazon S3](#)
- [Langkah 4: Siapkan peringatan GuardDuty pencarian melalui SNS](#)
- [Langkah selanjutnya](#)

Sebelum Anda mulai

GuardDuty adalah layanan deteksi ancaman yang memantau [Sumber data dasar](#) seperti peristiwa AWS CloudTrail manajemen, Amazon VPC Flow Logs, dan log kueri Amazon Route 53 Resolver DNS. GuardDuty juga menganalisis fitur yang terkait dengan jenis perlintungannya hanya jika Anda mengaktifkannya secara terpisah. [Fitur](#) termasuk log audit Kubernetes, aktivitas login RDS, peristiwa AWS CloudTrail data untuk Amazon S3, volume Amazon EBS, Pemantauan Runtime, dan log aktivitas jaringan Lambda. Menggunakan sumber dan fitur data ini (jika diaktifkan), GuardDuty menghasilkan temuan keamanan untuk akun Anda.

Setelah Anda mengaktifkan GuardDuty, itu mulai memantau akun Anda untuk potensi ancaman berdasarkan aktivitas di sumber data dasar. Secara default, [Deteksi Ancaman Diperpanjang](#) diaktifkan untuk semua Akun AWS yang telah diaktifkan GuardDuty. Kemampuan ini mendeteksi urutan serangan multi-tahap yang mencakup beberapa sumber data dasar, sumber AWS daya, dan waktu, di akun Anda. Untuk mendeteksi potensi ancaman terhadap AWS sumber daya tertentu, Anda dapat memilih untuk mengaktifkan paket perlindungan yang berfokus pada kasus penggunaan yang GuardDuty menawarkan. Untuk informasi selengkapnya, lihat [Fitur dari GuardDuty](#).

Anda tidak perlu mengaktifkan salah satu sumber data dasar secara eksplisit. Saat mengaktifkan Perlindungan S3, Anda tidak perlu mengaktifkan pencatatan peristiwa data Amazon S3 secara

eksplisit. Demikian pula, saat Anda mengaktifkan Perlindungan EKS, Anda tidak perlu mengaktifkan log audit Amazon EKS secara eksplisit. Amazon GuardDuty menarik aliran data independen langsung dari layanan ini.

Untuk GuardDuty akun baru, beberapa jenis perlindungan yang tersedia yang didukung dalam akun Wilayah AWS diaktifkan dan disertakan dalam periode uji coba gratis 30 hari secara default. Anda dapat memilih keluar dari salah satu atau semua dari mereka. Jika sudah ada Akun AWS dengan GuardDuty diaktifkan, Anda dapat memilih untuk mengaktifkan salah satu atau semua paket perlindungan yang tersedia di Wilayah Anda. Untuk ikhtisar rencana perlindungan dan rencana perlindungan mana yang akan diaktifkan secara default, lihat [Harga di GuardDuty](#).

Saat mengaktifkan GuardDuty, pertimbangkan item berikut:

- GuardDuty adalah layanan Regional, artinya prosedur konfigurasi apa pun yang Anda ikuti di halaman ini harus diulang di setiap Wilayah yang ingin Anda pantau GuardDuty.

Kami sangat menyarankan agar Anda mengaktifkan GuardDuty di semua AWS Wilayah yang didukung. Hal ini memungkinkan GuardDuty untuk menghasilkan temuan tentang aktivitas yang tidak sah atau tidak biasa bahkan di Wilayah yang tidak Anda gunakan secara aktif. Ini juga memungkinkan GuardDuty untuk memantau AWS CloudTrail acara untuk AWS layanan global seperti IAM. Jika tidak GuardDuty diaktifkan di semua Wilayah yang didukung, kemampuannya untuk mendeteksi aktivitas yang melibatkan layanan global berkurang. Untuk daftar lengkap Wilayah yang GuardDuty tersedia, lihat [Wilayah dan titik akhir](#).

- Setiap pengguna dengan hak administrator di AWS akun dapat mengaktifkan GuardDuty, namun, mengikuti praktik keamanan terbaik dengan hak istimewa terkecil, disarankan agar Anda membuat peran, pengguna, atau grup IAM untuk dikelola secara khusus. GuardDuty Untuk informasi tentang izin yang diperlukan untuk mengaktifkan GuardDuty lihat [Izin diperlukan untuk mengaktifkan GuardDuty](#).
- Ketika Anda mengaktifkan GuardDuty untuk pertama kalinya di salah satu Wilayah AWS, secara default, itu juga memungkinkan semua jenis perlindungan yang tersedia yang didukung di Wilayah tersebut, termasuk Perlindungan Malware untuk EC2. GuardDuty membuat peran terkait layanan untuk akun Anda yang dipanggil. `AWSServiceRoleForAmazonGuardDuty` Peran ini mencakup izin dan kebijakan kepercayaan yang memungkinkan GuardDuty untuk mengkonsumsi dan menganalisis peristiwa secara langsung dari [GuardDuty sumber data dasar](#) untuk menghasilkan temuan keamanan. Perlindungan Malware untuk EC2 membuat peran terkait layanan lain untuk akun Anda yang dipanggil. `AWSServiceRoleForAmazonGuardDutyMalwareProtection` Peran ini mencakup izin dan kebijakan kepercayaan yang memungkinkan Perlindungan Malware untuk EC2 melakukan pemindaian tanpa agen untuk mendeteksi malware di akun Anda.

GuardDuty Ini memungkinkan GuardDuty untuk membuat snapshot volume EBS di akun Anda, dan berbagi snapshot itu dengan akun layanan. GuardDuty Untuk informasi selengkapnya, lihat [Izin peran terkait layanan untuk GuardDuty](#). Untuk informasi selengkapnya tentang peran terkait layanan, lihat [Menggunakan peran terkait layanan](#).

- Saat Anda mengaktifkan GuardDuty untuk pertama kalinya di Wilayah mana pun, AWS akun Anda secara otomatis terdaftar dalam uji coba GuardDuty gratis 30 hari untuk Wilayah tersebut.

Video berikut menjelaskan bagaimana akun administrator dapat memulai GuardDuty dan mengaktifkannya di beberapa akun anggota.

[Memulai: Mengaktifkan Amazon GuardDuty untuk lingkungan mandiri atau multi-akun](#)

Langkah 1: Aktifkan Amazon GuardDuty

Langkah pertama yang harus digunakan GuardDuty adalah mengaktifkannya di akun Anda. Setelah diaktifkan, GuardDuty akan segera mulai memantau ancaman keamanan di Wilayah saat ini.

Jika Anda ingin mengelola GuardDuty temuan untuk akun lain dalam organisasi Anda sebagai GuardDuty administrator, Anda harus menambahkan akun anggota dan GuardDuty mengaktifkannya juga.

Note

Jika Anda ingin mengaktifkan Perlindungan GuardDuty Malware untuk S3 tanpa mengaktifkan GuardDuty, maka untuk langkah-langkahnya, lihat. [GuardDuty Perlindungan Malware untuk S3](#)

Standalone account environment

1. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>
2. Pilih opsi Amazon GuardDuty - Semua fitur.
3. Pilih Mulai.
4. Pada GuardDuty halaman Selamat Datang di, lihat persyaratan layanan. Pilih Aktifkan GuardDuty.

Multi-account environment

Important

Sebagai prasyarat untuk proses ini, Anda harus berada di organisasi yang sama dengan semua akun yang ingin Anda kelola, dan memiliki akses ke akun AWS Organizations manajemen untuk mendelegasikan administrator di dalam organisasi Anda. GuardDuty Izin tambahan mungkin diperlukan untuk mendelegasikan administrator, untuk info selengkapnya, lihat [Izin yang diperlukan untuk menunjuk akun administrator yang didelegasikan GuardDuty](#).

Untuk menunjuk akun administrator yang didelegasikan GuardDuty

1. Buka AWS Organizations konsol di <https://console.aws.amazon.com/organizations/>, menggunakan akun manajemen.
2. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.

Apakah GuardDuty sudah diaktifkan di akun Anda?

- Jika belum GuardDuty diaktifkan, Anda dapat memilih Memulai dan kemudian menunjuk administrator yang GuardDuty didelegasikan pada halaman Selamat Datang GuardDuty di.
 - Jika GuardDuty diaktifkan, Anda dapat menunjuk administrator yang GuardDuty didelegasikan pada halaman Pengaturan.
3. Masukkan ID AWS akun dua belas digit dari akun yang ingin Anda tetapkan sebagai administrator yang GuardDuty didelegasikan untuk organisasi dan pilih Delegasi.

Note

Jika belum GuardDuty diaktifkan, menunjuk administrator yang didelegasikan akan mengaktifkan GuardDuty akun tersebut di Wilayah Anda saat ini.

Untuk menambahkan akun anggota

Prosedur ini mencakup penambahan akun anggota ke akun administrator yang GuardDuty didelegasikan melalui AWS Organizations. Ada juga opsi untuk menambahkan anggota melalui

undangan. Untuk mempelajari lebih lanjut tentang kedua metode untuk mengasosiasikan anggota GuardDuty, lihat [Beberapa akun di Amazon GuardDuty](#).

1. Masuk ke akun administrator yang didelegasikan
2. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.
3. Di panel navigasi, pilih Pengaturan, lalu pilih Akun.

Tabel akun menampilkan semua akun dalam organisasi.

4. Pilih akun yang ingin Anda tambahkan sebagai anggota dengan mencentang kotak di samping ID akun. Kemudian dari menu Tindakan, pilih Tambah anggota.

 Tip

Anda dapat mengotomatiskan penambahan akun baru sebagai anggota dengan mengaktifkan fitur Aktifkan otomatis; namun, ini hanya berlaku untuk akun yang bergabung dengan organisasi Anda setelah fitur diaktifkan.

Langkah 2: Menghasilkan temuan sampel dan menjelajahi operasi dasar

Ketika GuardDuty menemukan masalah keamanan, itu menghasilkan temuan. GuardDuty Temuan adalah kumpulan data yang berisi detail yang berkaitan dengan masalah keamanan unik itu. Detail temuan dapat digunakan untuk membantu Anda menyelidiki masalah tersebut.

GuardDuty mendukung menghasilkan temuan sampel dengan nilai placeholder, yang dapat digunakan untuk menguji GuardDuty fungsionalitas dan membiasakan diri dengan temuan sebelum perlu menanggapi masalah keamanan nyata yang ditemukan oleh GuardDuty. Ikuti panduan di bawah ini untuk menghasilkan temuan sampel untuk setiap jenis temuan yang tersedia di GuardDuty, untuk cara tambahan untuk menghasilkan temuan sampel, termasuk menghasilkan peristiwa keamanan simulasi dalam akun Anda, lihat [Sampel temuan](#).

Untuk membuat dan mengeksplorasi temuan sampel

1. Pada panel navigasi, silakan pilih Pengaturan.
2. Di halaman Pengaturan, di bawah Sampel temuan, pilih Buat sampel temuan.

3. Di panel navigasi, pilih Ringkasan untuk melihat wawasan tentang temuan yang dihasilkan di lingkungan Anda AWS . Untuk informasi selengkapnya tentang komponen dasbor Ringkasan, lihat [Dasbor ringkasan di Amazon GuardDuty](#).
4. Di panel navigasi, pilih Temuan. Temuan sampel ditampilkan pada halaman Temuan saat ini dengan prefiks [SAMPEL].
5. Pilih temuan dari daftar untuk menampilkan detail temuan.
 - Anda dapat meninjau bidang informasi yang berbeda yang tersedia di panel detail temuan. Berbagai jenis temuan dapat memiliki bidang yang berbeda. Untuk informasi selengkapnya tentang bidang yang tersedia di semua jenis pencarian, lihat [Detail temuan](#). Dari panel detail, Anda dapat mengambil tindakan berikut:
 - Pilih ID temuan di bagian atas panel untuk membuka detail JSON lengkap untuk temuan. File JSON yang lengkap juga dapat diunduh dari panel ini. JSON berisi beberapa informasi tambahan yang tidak disertakan dalam tampilan konsol dan merupakan format yang dapat digunakan oleh alat dan layanan lainnya.
 - Lihat bagian Sumber daya yang terpengaruh. Dalam temuan nyata, informasi di sini akan membantu Anda mengidentifikasi sumber daya di akun Anda yang harus diselidiki dan akan menyertakan tautan ke sumber daya yang sesuai AWS Management Console untuk ditindaklanjuti.
 - Pilih ikon kaca pembesar dengan + atau - untuk membuat filter inklusif atau eksklusif untuk detail tersebut. Untuk informasi selengkapnya tentang menemukan filter, lihat [Penyaringan temuan di GuardDuty](#).
6. Arsipkan semua temuan sampel Anda
 - a. Pilih semua temuan dengan memilih kotak centang di bagian atas daftar.
 - b. Hapus pilihan temuan apa pun yang ingin Anda simpan.
 - c. Pilih menu Tindakan, lalu pilih Arsip untuk menyembunyikan temuan sampel.

 Note

Untuk melihat temuan yang diarsipkan, pilih Saat ini, lalu pilih Diarsipkan untuk beralih tampilan temuan.

Langkah 3: Konfigurasikan GuardDuty temuan ekspor ke bucket Amazon S3

GuardDuty merekomendasikan konfigurasi pengaturan untuk mengekspor temuan karena memungkinkan Anda untuk mengekspor temuan Anda ke bucket S3 untuk penyimpanan tidak terbatas di luar periode retensi 90 hari. GuardDuty Ini memungkinkan Anda untuk menyimpan catatan temuan atau melacak masalah dalam AWS lingkungan Anda dari waktu ke waktu. GuardDuty mengenkripsi data temuan di bucket S3 Anda dengan menggunakan AWS Key Management Service (AWS KMS) key. Untuk mengkonfigurasi pengaturan, Anda harus memberikan GuardDuty izin kunci KMS. Untuk langkah-langkah lebih rinci, lihat [Mengekspor temuan yang dihasilkan ke Amazon S3](#).

Untuk mengekspor GuardDuty temuan ke ember Amazon S3

1. Lampirkan kebijakan ke kunci KMS

- a. Masuk ke AWS Management Console dan buka konsol AWS Key Management Service (AWS KMS) di <https://console.aws.amazon.com/kms>.
- b. Untuk mengubah Wilayah AWS, gunakan pemilih Wilayah di sudut kanan atas halaman.
- c. Di panel navigasi, pilih Kunci yang dikelola pelanggan.
- d. Pilih kunci KMS yang ada, atau lakukan langkah-langkah untuk [Membuat kunci KMS enkripsi simetris di Panduan Pengembang](#) AWS Key Management Service .

Wilayah kunci KMS dan bucket Amazon S3 Anda harus sama.

Salin kunci ARN ke notepad untuk digunakan di langkah selanjutnya.

- e. Di bagian Kebijakan kunci pada kunci KMS Anda, pilih Edit. Jika Beralih ke tampilan kebijakan ditampilkan, pilih untuk menampilkan Kebijakan kunci, lalu pilih Edit.
- f. Salin blok kebijakan berikut ke kebijakan kunci KMS Anda:

```
{
  "Sid": "AllowGuardDutyKey",
  "Effect": "Allow",
  "Principal": {
    "Service": "guardduty.amazonaws.com"
  },
  "Action": "kms:GenerateDataKey",
  "Resource": "KMS key ARN",
  "Condition": {
```

```
    "StringEquals": {
      "aws:SourceAccount": "123456789012",
      "aws:SourceArn":
"arn:aws:guardduty:Region2:123456789012:detector/SourceDetectorID"
    }
  }
}
```

Edit kebijakan dengan mengganti nilai berikut yang diformat *red* dalam contoh kebijakan:

1. Ganti *KMS key ARN* dengan Nama Sumber Daya Amazon (ARN) dari kunci KMS. Untuk menemukan kunci ARN, lihat [Menemukan ID kunci dan ARN](#) di Panduan Pengembang AWS Key Management Service
2. Ganti *123456789012* dengan Akun AWS ID yang memiliki GuardDuty akun yang mengeksport temuan.
3. Ganti *Region2* dengan Wilayah AWS tempat GuardDuty temuan dihasilkan.
4. Ganti *SourceDetectorID* dengan GuardDuty akun di Wilayah tertentu tempat temuan dihasilkan. detectorID

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/> konsol, atau jalankan `detectorId` [ListDetectorsAPI](#).

2. Lampirkan kebijakan ke bucket Amazon S3

Jika Anda belum memiliki bucket Amazon S3 tempat Anda ingin mengeksport temuan ini, lihat [Membuat bucket](#) di Panduan Pengguna Amazon S3.

- a. Lakukan langkah-langkah di bawah [Untuk membuat atau mengedit kebijakan bucket](#) di Panduan Pengguna Amazon S3, hingga halaman Edit kebijakan bucket muncul.
- b. Kebijakan contoh menunjukkan cara memberikan GuardDuty izin untuk mengeksport temuan ke bucket Amazon S3 Anda. Jika Anda mengubah jalur setelah mengonfigurasi temuan ekspor, Anda harus mengubah kebijakan untuk memberikan izin ke lokasi baru.

Salin contoh kebijakan berikut dan tempelkan ke editor kebijakan Bucket.

Jika Anda menambahkan pernyataan kebijakan sebelum pernyataan akhir, tambahkan koma sebelum menambahkan pernyataan ini. Pastikan bahwa sintaks JSON dari kebijakan kunci KMS Anda valid.

Kebijakan contoh bucket S3

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Allow GetBucketLocation",
      "Effect": "Allow",
      "Principal": {
        "Service": "guardduty.amazonaws.com"
      },
      "Action": "s3:GetBucketLocation",
      "Resource": "Amazon S3 bucket ARN",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "123456789012",
          "aws:SourceArn":
            "arn:aws:guardduty:Region2:123456789012:detector/SourceDetectorID"
        }
      }
    },
    {
      "Sid": "Allow PutObject",
      "Effect": "Allow",
      "Principal": {
        "Service": "guardduty.amazonaws.com"
      },
      "Action": "s3:PutObject",
      "Resource": "Amazon S3 bucket ARN/[optional prefix]/*",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "123456789012",
          "aws:SourceArn":
            "arn:aws:guardduty:Region2:123456789012:detector/SourceDetectorID"
        }
      }
    },
    {
      "Sid": "Deny unencrypted object uploads",
      "Effect": "Deny",
      "Principal": {
```

```

        "Service": "guardduty.amazonaws.com"
    },
    "Action": "s3:PutObject",
    "Resource": "Amazon S3 bucket ARN/[optional prefix]/*",
    "Condition": {
        "StringNotEquals": {
            "s3:x-amz-server-side-encryption": "aws:kms"
        }
    }
},
{
    "Sid": "Deny incorrect encryption header",
    "Effect": "Deny",
    "Principal": {
        "Service": "guardduty.amazonaws.com"
    },
    "Action": "s3:PutObject",
    "Resource": "Amazon S3 bucket ARN/[optional prefix]/*",
    "Condition": {
        "StringNotEquals": {
            "s3:x-amz-server-side-encryption-aws-kms-key-id": "KMS key
ARN"
        }
    }
},
{
    "Sid": "Deny non-HTTPS access",
    "Effect": "Deny",
    "Principal": "*",
    "Action": "s3:*",
    "Resource": "Amazon S3 bucket ARN/[optional prefix]/*",
    "Condition": {
        "Bool": {
            "aws:SecureTransport": "false"
        }
    }
}
]
}

```

- c. Edit kebijakan dengan mengganti nilai berikut yang diformat *red* dalam contoh kebijakan:

1. Ganti *Amazon S3 bucket ARN* dengan Nama Sumber Daya Amazon (ARN) dari bucket Amazon S3. Anda dapat menemukan Bucket ARN di halaman kebijakan Edit bucket di konsol. <https://console.aws.amazon.com/s3/>
2. Ganti *123456789012* dengan Akun AWS ID yang memiliki GuardDuty akun yang mengeksport temuan.
3. Ganti *Region2* dengan Wilayah AWS tempat GuardDuty temuan dihasilkan.
4. Ganti *SourceDetectorID* dengan GuardDuty akun di Wilayah tertentu tempat temuan dihasilkan. detectorID

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/> konsol, atau jalankan `detectorId` [ListDetectorsAPI](#).

5. Ganti *[optional prefix]* bagian dari nilai *S3 bucket ARN/[optional prefix]* placeholder dengan lokasi folder opsional yang ingin Anda ekspor temuannya. Untuk informasi selengkapnya tentang penggunaan awalan, lihat [Mengatur objek menggunakan awalan](#) di Panduan Pengguna Amazon S3.

Bila Anda menyediakan lokasi folder opsional yang belum ada, GuardDuty akan membuat lokasi tersebut hanya jika akun yang terkait dengan bucket S3 sama dengan akun yang mengeksport temuan. Saat Anda mengeksport temuan ke bucket S3 milik akun lain, lokasi folder harus sudah ada.

6. Ganti *KMS key ARN* dengan Nama Sumber Daya Amazon (ARN) dari kunci KMS yang terkait dengan enkripsi temuan yang diekspor ke bucket S3. Untuk menemukan kunci ARN, lihat [Menemukan ID kunci dan ARN](#) di Panduan Pengembang AWS Key Management Service

3. Langkah-langkah di GuardDuty konsol

- a. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.
- b. Pada panel navigasi, silakan pilih Pengaturan.
- c. Pada halaman Pengaturan, di bawah opsi ekspor temuan, untuk bucket S3, pilih Konfigurasi sekarang (atau Edit, sesuai kebutuhan).
- d. Untuk S3 bucket ARN, masukkan **bucket ARN** yang ingin Anda kirim temuannya. Untuk melihat ARN bucket, lihat [Melihat properti untuk bucket S3](#) di Panduan Pengguna Amazon S3.

- e. Untuk ARN kunci KMS, masukkan file. **key ARN** Untuk menemukan kunci ARN, lihat [Temukan ID kunci dan kunci ARN](#) di Panduan Pengembang.AWS Key Management Service
- f. Pilih Simpan.

Langkah 4: Siapkan peringatan GuardDuty pencarian melalui SNS

GuardDuty terintegrasi dengan Amazon EventBridge, yang dapat digunakan untuk mengirim data temuan ke aplikasi dan layanan lain untuk diproses. Dengan EventBridge Anda dapat menggunakan GuardDuty temuan untuk memulai respons otomatis terhadap temuan Anda dengan menghubungkan peristiwa pencarian ke target seperti AWS Lambda fungsi, otomatisasi Amazon EC2 Systems Manager, Amazon Simple Notification Service (SNS) dan banyak lagi.

Dalam contoh ini Anda akan membuat topik SNS untuk menjadi target EventBridge aturan, lalu Anda akan menggunakan EventBridge untuk membuat aturan yang menangkap data temuan dari. GuardDuty Aturan yang dihasilkan akan meneruskan detail temuan ke alamat email. Untuk mempelajari bagaimana Anda dapat mengirim temuan ke Slack atau Amazon Chime, dan juga memodifikasi jenis peringatan temuan yang dikirim, lihat. [Siapkan topik dan titik akhir Amazon SNS](#)

Untuk membuat topik SNS untuk peringatan temuan Anda

1. [Buka konsol Amazon SNS di https://console.aws.amazon.com/sns/v3/home](https://console.aws.amazon.com/sns/v3/home).
2. Di panel navigasi, pilih Pengguna.
3. Pilih Buat Topik.
4. Untuk Jenis, pilih Standar.
5. Untuk Nama, masukkan **GuardDuty**.
6. Pilih Buat Topik. Detail topik untuk topik baru Anda akan terbuka.
7. Di bagian Subscriptions (Berlangganan), pilih Create subscription (Buat langganan).
8. Untuk Protokol, pilih Email.
9. Untuk Endpoint, masukkan alamat email untuk mengirim notifikasi.
10. Pilih Buat langganan.

Setelah Anda membuat langganan, Anda harus mengonfirmasi langganan melalui email.

11. Untuk memeriksa pesan langganan, buka kotak masuk email Anda, dan di pesan berlangganan, pilih Konfirmasi langganan.

 Note

Untuk memeriksa status konfirmasi email, buka konsol SNS dan pilih Langganan.

Untuk membuat EventBridge aturan untuk menangkap GuardDuty temuan dan memformatnya

1. Buka EventBridge konsol di <https://console.aws.amazon.com/events/>.
2. Di panel navigasi, pilih Aturan.
3. Pilih Buat aturan.
4. Masukkan nama dan deskripsi untuk aturan.

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

5. Untuk Bus peristiwa, pilih default.
6. Untuk Tipe aturan, pilih Aturan dengan pola peristiwa.
7. Pilih Selanjutnya.
8. Untuk sumber Acara, pilih AWS acara.
9. Untuk pola Acara, pilih Formulir pola acara.
10. Untuk Sumber peristiwa, pilih Layanan AWS .
11. Untuk Layanan AWS , pilih GuardDuty.
12. Untuk Jenis Acara, pilih GuardDutyMenemukan.
13. Pilih Berikutnya.
14. Untuk Jenis target, pilih Layanan AWS .
15. Untuk Pilih target, pilih topik SNS, dan untuk Topik, pilih nama topik SNS yang Anda buat sebelumnya.
16. Di bagian Pengaturan tambahan, untuk Konfigurasi input target, pilih Transformator input.

Menambahkan transformator input memformat data pencarian JSON yang dikirim dari GuardDuty ke dalam pesan yang dapat dibaca manusia.

17. Pilih Konfigurasi transformator input.
18. Di bagian Transformator input target, untuk jalur Input, tempel kode berikut:

```
{
  "severity": "$.detail.severity",
  "Finding_ID": "$.detail.id",
  "Finding_Type": "$.detail.type",
  "region": "$.region",
  "Finding_description": "$.detail.description"
}
```

19. Untuk memformat email, untuk Template, tempel kode berikut dan pastikan untuk mengganti teks berwarna merah dengan nilai yang sesuai dengan Wilayah Anda:

```
"You have a severity severity GuardDuty finding type Finding_Type in
the Region_Name Region."
"Finding Description:"
"Finding_Description."
"For more details open the GuardDuty console at https://console.aws.amazon.com/
guardduty/home?region=region#/findings?search=id%3DFinding_ID"
```

20. Pilih Konfirmasi.
21. Pilih Berikutnya.
22. (Opsional) Masukkan satu atau lebih tanda untuk aturan. Untuk informasi selengkapnya, lihat [EventBridge tag Amazon](#) di Panduan EventBridge Pengguna Amazon.
23. Pilih Berikutnya.
24. Tinjau detail aturan dan pilih Buat aturan.
25. (Opsional) Uji aturan baru Anda dengan menghasilkan temuan sampel dengan proses di Langkah 2. Anda akan menerima email untuk setiap temuan sampel yang dihasilkan.

Langkah selanjutnya

Saat Anda terus menggunakan GuardDuty, Anda akan memahami jenis temuan yang relevan dengan lingkungan Anda. Setiap kali Anda menerima temuan baru, Anda dapat menemukan informasi, termasuk rekomendasi perbaikan tentang temuan itu, dengan memilih Pelajari lebih lanjut dari deskripsi temuan di panel rincian temuan, atau dengan mencari nama temuan di. [GuardDuty menemukan jenis](#)

Fitur-fitur berikut akan membantu Anda menyetel GuardDuty sehingga dapat memberikan temuan yang paling relevan untuk AWS lingkungan Anda:

- Untuk mengurutkan temuan dengan mudah berdasarkan kriteria tertentu, seperti ID instans, ID akun, nama bucket S3, dan lainnya, Anda dapat membuat dan menyimpan filter di dalamnya GuardDuty. Untuk informasi selengkapnya, lihat [Penyaringan temuan di GuardDuty](#).
- Jika Anda menerima temuan untuk perilaku yang diharapkan di lingkungan Anda, Anda dapat secara otomatis mengarsipkan temuan berdasarkan kriteria yang Anda tentukan dengan [aturan penekanan](#).
- Untuk mencegah temuan dihasilkan dari subset tepercaya IPs, atau memiliki GuardDuty monitor IPs di luar lingkup pemantauan normalnya, Anda dapat menyiapkan [IP Tepercaya dan daftar ancaman](#).

GuardDuty sumber data dasar

GuardDuty menggunakan sumber data dasar untuk mendeteksi komunikasi dengan domain berbahaya dan alamat IP yang diketahui, dan mengidentifikasi perilaku yang berpotensi anomali dan aktivitas yang tidak sah. Saat transit dari sumber-sumber ini ke GuardDuty, semua data log dienkripsi. GuardDuty mengekstrak berbagai bidang dari sumber log ini untuk profil dan deteksi anomali, dan kemudian membuang log ini.

Saat Anda mengaktifkan GuardDuty untuk pertama kalinya di suatu Wilayah, ada uji coba gratis 30 hari yang mencakup deteksi ancaman untuk semua sumber data dasar. Selama uji coba gratis ini, Anda dapat memantau perkiraan penggunaan bulanan yang dirinci oleh setiap sumber data dasar. Sebagai akun GuardDuty administrator yang didelegasikan, Anda dapat melihat perkiraan biaya penggunaan bulanan yang dirinci oleh setiap akun anggota milik organisasi Anda dan telah diaktifkan GuardDuty. Setelah uji coba 30 hari berakhir, Anda dapat menggunakan AWS Billing informasi tentang biaya penggunaan.

Tidak ada biaya tambahan saat GuardDuty mengakses peristiwa dan log dari sumber data dasar ini.

Setelah Anda mengaktifkan GuardDuty di Akun AWS, secara otomatis mulai memantau sumber log yang dijelaskan di bagian berikut. Anda tidak perlu mengaktifkan hal lain GuardDuty untuk mulai menganalisis dan memproses sumber data ini untuk menghasilkan temuan keamanan terkait.

Topik

- [AWS CloudTrail acara manajemen](#)
- [Log Alur VPC](#)
- [Log kueri DNS Route53 Resolver](#)

AWS CloudTrail acara manajemen

AWS CloudTrail memberi Anda riwayat panggilan AWS API untuk akun Anda, termasuk panggilan API yang dilakukan menggunakan AWS Management Console, alat baris perintah, dan AWS layanan tertentu. AWS SDKs CloudTrail juga membantu Anda mengidentifikasi pengguna dan akun mana yang dipanggil AWS APIs untuk layanan yang mendukung CloudTrail, alamat IP sumber dari mana panggilan dipanggil, dan waktu di mana panggilan dipanggil. Untuk informasi selengkapnya, lihat [Apa yang ada AWS CloudTrail](#) di Panduan AWS CloudTrail Pengguna.

GuardDuty Memantau peristiwa CloudTrail manajemen, juga dikenal sebagai peristiwa bidang kontrol. Peristiwa ini memberikan wawasan tentang operasi manajemen yang dilakukan pada sumber daya di Akun AWS.

Berikut ini adalah contoh peristiwa CloudTrail manajemen yang GuardDuty memantau:

- Mengkonfigurasi keamanan (operasi `AttachRolePolicy` API IAM)
- Mengkonfigurasi aturan untuk merutekan data (operasi Amazon EC2 `CreateSubnet` API)
- Menyiapkan logging (operasi AWS CloudTrail `CreateTrail` API)

Ketika Anda mengaktifkan GuardDuty, itu mulai mengkonsumsi peristiwa CloudTrail manajemen langsung dari CloudTrail melalui aliran peristiwa independen dan duplikat dan menganalisis log CloudTrail peristiwa Anda.

GuardDuty tidak mengelola CloudTrail acara Anda atau memengaruhi CloudTrail konfigurasi yang ada. Demikian pula, CloudTrail konfigurasi Anda tidak memengaruhi cara GuardDuty mengkonsumsi dan memproses log peristiwa. Untuk mengelola akses dan retensi CloudTrail acara Anda, gunakan konsol CloudTrail layanan atau API. Untuk informasi selengkapnya, lihat [Melihat peristiwa dengan riwayat CloudTrail acara](#) di Panduan AWS CloudTrail Pengguna.

Bagaimana GuardDuty menangani peristiwa AWS CloudTrail global

Untuk sebagian besar AWS layanan, CloudTrail acara dicatat di Wilayah AWS tempat mereka dibuat. Untuk layanan global seperti AWS Identity and Access Management (IAM), AWS Security Token Service (AWS STS), Amazon Simple Storage Service (Amazon S3), Amazon CloudFront, dan Amazon Route 53 (Route 53), peristiwa hanya dihasilkan di Wilayah tempat kejadian tetapi memiliki signifikansi global.

Saat GuardDuty mengkonsumsi [peristiwa layanan CloudTrail Global](#) (GSE) dengan nilai keamanan seperti konfigurasi jaringan atau izin pengguna, ia mereplikasi peristiwa tersebut dan memprosesnya di setiap Wilayah yang telah Anda aktifkan. GuardDuty Perilaku ini membantu GuardDuty menjaga profil pengguna dan peran di setiap Wilayah, yang sangat penting untuk mendeteksi kejadian anomali.

Note

Untuk temuan yang dihasilkan dari peristiwa layanan global ini, nilai Wilayah dalam temuan mungkin berbeda dari Wilayah tempat GuardDuty membuat deteksi. Misalnya, temuan

mungkin ditampilkan us-east-1 sebagai Wilayah bahkan jika GuardDuty membuat deteksi di Wilayah yang berbeda.

Kami menyarankan Anda mengaktifkan GuardDuty semua yang Wilayah AWS tersedia di Akun AWS. Bahkan jika Anda tidak memiliki sumber daya yang digunakan di Wilayah tertentu, mengaktifkan akan GuardDuty membantu melindungi akun Anda dari potensi ancaman. Aktor ancaman berpotensi meluncurkan serangan melalui layanan global (seperti IAM, AWS STS, atau Amazon CloudFront). Mereka dapat mencoba membuat sumber daya yang tidak sah untuk mengeksploitasi Wilayah di mana Anda memiliki kehadiran terbatas. GuardDuty memproses peristiwa layanan global di semua Wilayah tempat Anda mengaktifkan layanan, termasuk Wilayah default dan keikutsertaan. Ini membantu GuardDuty mendeteksi aktivitas yang berpotensi mencurigakan di seluruh wilayah Anda Akun AWS, termasuk Wilayah di mana Anda tidak menggunakan sumber daya secara aktif.

Log Alur VPC

Fitur VPC Flow Logs dari Amazon VPC menangkap informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan yang dilampirkan ke instans Amazon Elastic Compute Cloud (Amazon EC2) di lingkungan Anda. AWS

Ketika Anda mengaktifkan GuardDuty, itu segera mulai menganalisis log aliran VPC Anda dari EC2 instans Amazon dalam akun Anda. Ini mengkonsumsi peristiwa log aliran VPC langsung dari fitur VPC Flow Logs melalui aliran log aliran independen dan duplikat. Proses ini tidak memengaruhi konfigurasi log aliran apa pun yang ada.

[Perlindungan Lambda](#)

Lambda Protection adalah peningkatan opsional untuk Amazon. GuardDuty Saat ini, Pemantauan Aktivitas Jaringan Lambda menyertakan log aliran VPC Amazon dari semua fungsi Lambda untuk akun Anda, bahkan log yang tidak menggunakan jaringan VPC. Untuk melindungi fungsi Lambda Anda dari potensi ancaman keamanan, Anda perlu mengonfigurasi Perlindungan Lambda di akun Anda. GuardDuty Untuk informasi selengkapnya, lihat [Perlindungan Lambda](#).

[GuardDuty Pemantauan Runtime](#)

Saat Anda mengelola agen keamanan (baik secara manual atau melalui GuardDuty) di EKS Runtime Monitoring atau Runtime Monitoring untuk EC2 instance, dan saat GuardDuty ini digunakan di instans EC2 Amazon dan menerima [Jenis acara runtime yang dikumpulkan](#) dari

instance ini GuardDuty, tidak akan membebankan biaya Akun AWS untuk analisis log aliran VPC dari instans Amazon ini. EC2 Ini membantu GuardDuty menghindari biaya penggunaan ganda di akun.

GuardDuty tidak mengelola log aliran Anda atau membuatnya dapat diakses di akun Anda. Untuk mengelola akses dan retensi log aliran, Anda harus mengonfigurasi fitur VPC Flow Logs.

Log kueri DNS Route53 Resolver

Jika Anda menggunakan resolver AWS DNS untuk EC2 instans Amazon Anda (setelan default), maka GuardDuty dapat mengakses dan memproses log kueri DNS Route53 Resolver permintaan dan respons Anda melalui resolver DNS internal. AWS Jika Anda menggunakan resolver DNS lain, seperti OpenDNS atau Googledns, atau jika Anda menyiapkan resolver DNS Anda sendiri, maka tidak dapat mengakses dan memproses data dari sumber data ini. GuardDuty

Saat Anda mengaktifkan GuardDuty, itu segera mulai menganalisis log kueri DNS Route53 Resolver Anda dari aliran data independen. Aliran data ini terpisah dari data yang disediakan melalui fitur [pencatatan kueri Route 53 Resolver](#). Konfigurasi fitur ini tidak mempengaruhi GuardDuty analisis.

Note

GuardDuty tidak mendukung pemantauan log DNS untuk EC2 instans Amazon yang diluncurkan AWS Outposts karena fitur pencatatan Amazon Route 53 Resolver kueri tidak tersedia di lingkungan tersebut.

GuardDuty Deteksi Ancaman Diperpanjang

GuardDuty Extended Threat Detection secara otomatis mendeteksi serangan multi-tahap yang menjangkau sumber data, berbagai jenis AWS sumber daya, dan waktu, dalam file. Akun AWS Dengan kemampuan ini, GuardDuty berfokus pada urutan beberapa peristiwa yang diamati dengan memantau berbagai jenis sumber data. Extended Threat Detection menghubungkan peristiwa-peristiwa ini untuk mengidentifikasi skenario yang menampilkan diri sebagai ancaman potensial terhadap AWS lingkungan Anda, dan kemudian menghasilkan temuan urutan serangan.

Topik

- [Contoh skenario ancaman urutan serangan](#)
- [Cara kerjanya](#)
- [Mengaktifkan rencana perlindungan untuk memaksimalkan deteksi ancaman](#)
- [Deteksi Ancaman Diperpanjang di GuardDuty konsol](#)
- [Memahami dan mengelola temuan urutan serangan](#)
- [Sumber daya tambahan](#)

Contoh skenario ancaman urutan serangan

Extended Threat Detection mencakup skenario ancaman yang melibatkan kompromi terkait penyalahgunaan AWS kredensial, upaya kompromi data di bucket Amazon S3, dan kompromi sumber daya container dan Kubernetes di kluster Amazon EKS. Sebuah temuan tunggal dapat mencakup seluruh urutan serangan. Misalnya, daftar berikut menjelaskan skenario yang GuardDuty mungkin mendeteksi:

Contoh 1 - AWS kredensi dan kompromi data bucket Amazon S3

- Aktor ancaman mendapatkan akses tidak sah ke beban kerja komputasi.
- Aktor kemudian melakukan serangkaian tindakan seperti eskalasi hak istimewa dan membangun ketekunan.
- Akhirnya, aktor mengeksfiltrasi data dari sumber daya Amazon S3.

Contoh 2 - Kompromi kluster Amazon EKS

- Seorang aktor ancaman mencoba mengeksploitasi aplikasi kontainer dalam cluster Amazon EKS.

- Aktor menggunakan wadah yang disusupi itu untuk mendapatkan token akun layanan istimewa.
- Aktor kemudian memanfaatkan hak istimewa yang ditinggikan ini untuk mengakses rahasia atau AWS sumber daya Kubernetes yang sensitif melalui identitas pod.

Karena sifat skenario ancaman terkait, GuardDuty anggap semua [Jenis pencarian urutan serangan](#) sebagai Kritis.

Video berikut memberikan demonstrasi bagaimana Anda dapat menggunakan Extended Threat Detection.

[Demonstrasi Deteksi Ancaman Amazon GuardDuty Diperpanjang](#)

Cara kerjanya

Saat Anda mengaktifkan Amazon GuardDuty di akun Anda secara spesifik Wilayah AWS, Deteksi Ancaman Diperpanjang juga diaktifkan secara default. Tidak ada biaya tambahan yang terkait dengan penggunaan Extended Threat Detection. Secara default, ini menghubungkan peristiwa di semua. [Sumber data dasar](#) Namun, ketika Anda mengaktifkan lebih banyak rencana GuardDuty perlindungan, seperti Perlindungan S3, Perlindungan EKS, dan Pemantauan Runtime, ini akan membuka jenis deteksi urutan serangan tambahan dengan memperluas jangkauan sumber peristiwa. Ini berpotensi membantu dengan analisis ancaman yang lebih komprehensif dan deteksi urutan serangan yang lebih baik. Untuk informasi selengkapnya, lihat [Mengaktifkan rencana perlindungan untuk memaksimalkan deteksi ancaman](#).

GuardDuty mengkorelasikan beberapa peristiwa, termasuk aktivitas dan GuardDuty temuan API. Peristiwa ini disebut Sinyal. Terkadang, mungkin ada peristiwa di lingkungan Anda yang, dengan sendirinya, tidak menampilkan diri sebagai ancaman potensial yang jelas. GuardDuty menyebutnya sebagai sinyal lemah. Dengan Extended Threat Detection, GuardDuty mengidentifikasi kapan urutan beberapa tindakan sejajar dengan aktivitas yang berpotensi mencurigakan, dan menghasilkan temuan urutan serangan di akun Anda. Berbagai tindakan ini dapat mencakup sinyal lemah dan GuardDuty temuan yang sudah diidentifikasi di akun Anda.

Note

Saat menghubungkan peristiwa untuk urutan serangan, Extended Threat Detection tidak mempertimbangkan temuan yang diarsipkan, termasuk temuan yang diarsipkan secara

otomatis karena. [Aturan penekanan](#) Perilaku ini memastikan bahwa hanya sinyal aktif dan relevan yang berkontribusi pada deteksi urutan serangan. Untuk memastikan bahwa Anda tidak terpengaruh oleh hal ini, tinjau aturan penekanan yang ada di akun Anda. Untuk informasi selengkapnya, lihat [Menggunakan aturan penekanan dengan Extended Threat Detection](#).

GuardDuty juga dirancang untuk mengidentifikasi potensi perilaku serangan yang sedang berlangsung atau baru-baru ini (dalam jangka waktu bergulir 24 jam) di akun Anda. Misalnya, serangan bisa dimulai oleh aktor yang mendapatkan akses yang tidak diinginkan ke beban kerja komputasi. Aktor kemudian akan melakukan serangkaian langkah, termasuk enumerasi, eskalasi hak istimewa, dan eksfiltrasi kredensial. AWS Kredensial ini berpotensi digunakan untuk kompromi lebih lanjut atau akses berbahaya ke data.

Mengaktifkan rencana perlindungan untuk memaksimalkan deteksi ancaman

Untuk GuardDuty akun apa pun di Wilayah, kemampuan Deteksi Ancaman Diperpanjang diaktifkan secara otomatis. Secara default, kemampuan ini mempertimbangkan beberapa peristiwa di semua [Sumber data dasar](#). Untuk memanfaatkan kemampuan ini, Anda tidak perlu mengaktifkan semua rencana [GuardDuty perlindungan yang berfokus pada kasus penggunaan](#). Misalnya, dengan deteksi ancaman dasar, GuardDuty dapat mengidentifikasi urutan serangan potensial mulai dari aktivitas penemuan hak istimewa IAM di Amazon S3 APIs, dan mendeteksi perubahan bidang kontrol S3 berikutnya, seperti perubahan yang membuat kebijakan sumber daya bucket lebih permisif.

Extended Threat Detection dirancang sedemikian rupa sehingga jika Anda mengaktifkan lebih banyak rencana perlindungan, ini membantu GuardDuty menghubungkan sinyal yang lebih beragam di berbagai sumber data. Ini berpotensi meningkatkan luasnya sinyal keamanan untuk analisis ancaman komprehensif dan cakupan urutan serangan. Untuk mengidentifikasi temuan yang berpotensi menjadi salah satu dari beberapa tahap dalam urutan serangan, GuardDuty merekomendasikan untuk mengaktifkan rencana perlindungan khusus - Perlindungan S3, Perlindungan EKS, dan Pemantauan Runtime (dengan add-on EKS).

Topik

- [Mendeteksi urutan serangan di cluster Amazon EKS](#)
- [Mendeteksi urutan serangan di bucket Amazon S3](#)

Mendeteksi urutan serangan di cluster Amazon EKS

GuardDuty mengkorelasikan beberapa sinyal keamanan di seluruh log audit EKS, perilaku proses runtime, dan aktivitas AWS API untuk mendeteksi pola serangan yang canggih. Untuk mendapatkan manfaat dari Extended Threat Detection untuk EKS, Anda harus mengaktifkan setidaknya satu dari fitur ini — Perlindungan EKS atau Runtime Monitoring (dengan add-on EKS). EKS Protection memantau aktivitas pesawat kontrol melalui log audit, sementara Runtime Monitoring mengamati perilaku di dalam kontainer.

Untuk cakupan maksimum dan deteksi ancaman komprehensif, GuardDuty merekomendasikan untuk mengaktifkan kedua rencana perlindungan. Bersama-sama, mereka membuat tampilan lengkap dari kluster EKS Anda, memungkinkan GuardDuty untuk mendeteksi pola serangan yang kompleks. Misalnya, ia dapat mengidentifikasi penerapan anomali dari wadah istimewa (terdeteksi dengan Perlindungan EKS), diikuti oleh upaya persistensi, penambangan kriptografi, dan pembuatan shell terbalik dalam wadah itu (terdeteksi dengan Runtime Monitoring). GuardDuty mewakili peristiwa-peristiwa terkait ini sebagai temuan tunggal yang sangat kritis, yang disebut [AttackSequence:EKS/CompromisedCluster](#). Saat Anda mengaktifkan kedua rencana perlindungan, temuan urutan serangan mencakup skenario ancaman berikut:

- Kompromi kontainer yang menjalankan aplikasi web yang rentan
- Akses tidak sah melalui kredensial yang salah dikonfigurasi
- Upaya untuk meningkatkan hak istimewa
- Permintaan API yang mencurigakan
- Upaya mengakses data dengan jahat

Daftar berikut memberikan detail kapan paket perlindungan khusus ini diaktifkan secara individual:

Perlindungan EKS

Mengaktifkan Perlindungan EKS memberikan GuardDuty kemampuan untuk mendeteksi urutan serangan yang melibatkan aktivitas pesawat kontrol cluster Amazon EKS. Hal ini memungkinkan GuardDuty untuk mengkorelasikan log audit EKS dan aktivitas AWS API. Misalnya, GuardDuty dapat mendeteksi urutan serangan di mana aktor mencoba akses tidak sah ke rahasia kluster, memodifikasi izin kontrol akses berbasis peran (RBAC) Kubernetes, dan membuat pod istimewa. Untuk informasi selengkapnya tentang mengaktifkan rencana perlindungan ini, lihat [Perlindungan EKS](#).

Pemantauan Runtime untuk Amazon EKS

Mengaktifkan Runtime Monitoring untuk kluster Amazon EKS memberikan GuardDuty kemampuan untuk meningkatkan deteksi urutan serangan EKS dengan visibilitas tingkat kontainer. Ini membantu GuardDuty mendeteksi potensi proses berbahaya, perilaku runtime yang mencurigakan, dan potensi eksekusi malware. Misalnya, GuardDuty dapat mendeteksi urutan serangan di mana wadah mulai menunjukkan perilaku mencurigakan, seperti proses cryptomining atau membangun koneksi ke titik akhir berbahaya yang diketahui. Untuk informasi selengkapnya tentang mengaktifkan rencana perlindungan ini, lihat [Pemantauan Runtime](#).

Jika Anda tidak mengaktifkan Perlindungan EKS atau Runtime Monitoring, tidak GuardDuty akan dapat menghasilkan individu [Jenis penemuan Perlindungan EKS](#) atau [Jenis penemuan Runtime Monitoring](#). Oleh karena itu, tidak GuardDuty akan dapat mendeteksi urutan serangan multi-tahap yang melibatkan temuan terkait.

Mendeteksi urutan serangan di bucket Amazon S3

Mengaktifkan Perlindungan S3 memberikan GuardDuty kemampuan untuk mendeteksi urutan serangan yang melibatkan upaya kompromi data di bucket Amazon S3 Anda. Tanpa Perlindungan S3, GuardDuty dapat mendeteksi kapan kebijakan sumber daya bucket S3 Anda menjadi terlalu permisif. Saat Anda mengaktifkan Perlindungan S3, GuardDuty dapatkan kemampuan untuk mendeteksi aktivitas eksfiltrasi data potensial yang mungkin terjadi setelah bucket S3 Anda menjadi terlalu permisif.

Jika Perlindungan S3 tidak diaktifkan, tidak GuardDuty akan dapat menghasilkan individu [Jenis temuan Perlindungan S3](#). Oleh karena itu, tidak GuardDuty akan dapat mendeteksi urutan serangan multi-tahap yang melibatkan temuan terkait. Untuk informasi selengkapnya tentang mengaktifkan rencana perlindungan ini, lihat [Perlindungan S3](#).

Deteksi Ancaman Diperpanjang di GuardDuty konsol

Secara default, halaman Extended Threat Detection di GuardDuty konsol menampilkan Status sebagai Diaktifkan. Dengan deteksi ancaman dasar, status mewakili yang GuardDuty dapat mendeteksi urutan serangan potensial yang melibatkan aktivitas penemuan hak istimewa IAM di Amazon S3 APIs dan mendeteksi perubahan bidang kontrol S3 berikutnya.

Gunakan langkah-langkah berikut untuk mengakses halaman Extended Threat Detection di GuardDuty konsol:

1. Anda dapat membuka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.
2. Di panel navigasi kiri, pilih Extended Threat Detection.

Halaman ini memberikan detail tentang skenario ancaman yang dicakup oleh Extended Threat Detection.

3. Pada halaman Extended Threat Detection, lihat bagian Rencana perlindungan terkait. Jika Anda ingin mengaktifkan paket perlindungan khusus untuk meningkatkan cakupan deteksi ancaman di akun Anda, pilih opsi Konfigurasi untuk paket perlindungan tersebut.

Memahami dan mengelola temuan urutan serangan

Temuan urutan serangan sama seperti GuardDuty temuan lain di akun Anda. Anda dapat melihatnya di halaman Temuan di GuardDuty konsol. Untuk informasi tentang melihat temuan, lihat [Halaman temuan di GuardDuty konsol](#).

Mirip dengan GuardDuty temuan lain, temuan urutan serangan juga secara otomatis dikirim ke Amazon EventBridge. Berdasarkan pengaturan Anda, temuan urutan serangan juga diekspor ke tujuan penerbitan (bucket Amazon S3). Untuk menetapkan tujuan penerbitan baru atau memperbarui yang sudah ada, lihat [Mengekspor temuan yang dihasilkan ke Amazon S3](#).

Sumber daya tambahan

Lihat bagian berikut untuk mendapatkan pemahaman lebih lanjut tentang urutan serangan:

- Setelah mempelajari tentang Extended Threat Detection dan urutan serangan, Anda dapat menghasilkan contoh jenis pencarian urutan serangan dengan mengikuti langkah-langkahnya. [Sampel temuan](#)
- Pelajari tentang [Jenis pencarian urutan serangan](#).
- Tinjau temuan dan jelajahi detail temuan yang terkait dengan [Detail pencarian urutan serangan](#).
- Prioritaskan dan atasi jenis pencarian urutan serangan dengan mengikuti langkah-langkah untuk sumber daya yang terkena dampak terkait di. [Mengatasi temuan](#)

GuardDuty Perlindungan EKS

EKS Protection membantu Anda mendeteksi potensi risiko keamanan di kluster Amazon Elastic Kubernetes Service (Amazon EKS) di lingkungan Anda. AWS Misalnya, ini membantu Anda mendeteksi ketika kluster EKS yang salah dikonfigurasi diakses oleh aktor yang tidak diautentikasi yang mencoba mengumpulkan rahasia atau AWS kredensial dari cluster Anda. EKS Protection menggunakan log audit EKS untuk menganalisis aktivitas pengguna dan aplikasi.

Saat Anda mengaktifkan Perlindungan EKS, GuardDuty secara otomatis mulai memantau kluster Amazon EKS Anda untuk potensi ancaman keamanan. GuardDuty menggunakan aliran independennya sendiri untuk mengumpulkan dan menganalisis [Log audit EKS di Perlindungan EKS](#) — tidak diperlukan konfigurasi tambahan.

Ketika GuardDuty mendeteksi potensi ancaman berdasarkan pemantauan log audit EKS, itu menghasilkan temuan keamanan. Untuk informasi tentang jenis temuan yang GuardDuty mungkin dihasilkan saat Anda mengaktifkan Perlindungan EKS, lihat [Jenis penemuan Perlindungan EKS](#).

Note

Untuk melihat log audit EKS di akun Anda (opsional), Anda dapat mengonfigurasi pencatatan bidang kontrol Amazon EKS untuk mengirim log audit ke CloudWatch Log. Konfigurasi ini terpisah dari Perlindungan EKS dan tidak diperlukan untuk kemampuan pemantauan keamanan di GuardDuty.

Uji coba gratis 30 hari

- Ketika Anda mengaktifkan GuardDuty Akun AWS in an Wilayah AWS untuk pertama kalinya, Anda mendapatkan uji coba gratis 30 hari. Dalam hal ini, juga GuardDuty akan mengaktifkan Perlindungan EKS, yang termasuk dalam uji coba gratis 30 hari.
- Ketika Anda sudah menggunakan GuardDuty dan memutuskan untuk mengaktifkan Perlindungan EKS untuk pertama kalinya, akun Anda di Wilayah ini akan mendapatkan uji coba gratis 30 hari untuk Perlindungan EKS.
- Anda dapat memilih untuk menonaktifkan Perlindungan EKS di Wilayah mana pun kapan saja.
- Selama uji coba gratis 30 hari, Anda bisa mendapatkan perkiraan biaya penggunaan Anda di akun dan Wilayah tersebut. Setelah uji coba gratis 30 hari berakhir, GuardDuty tidak secara otomatis

menonaktifkan Perlindungan EKS. Akun Anda di Wilayah ini akan mulai menimbulkan biaya penggunaan. Untuk informasi selengkapnya, lihat [Memperkirakan biaya penggunaan](#).

Saat Anda menonaktifkan Perlindungan EKS, GuardDuty segera berhenti memantau dan menganalisis log audit EKS untuk sumber daya Amazon EKS Anda.

Perlindungan EKS mungkin tidak tersedia di semua Wilayah AWS tempat GuardDuty yang tersedia. Untuk informasi selengkapnya, lihat [Ketersediaan fitur khusus wilayah](#).

Note

EKS Runtime Monitoring dikelola sebagai bagian dari Runtime Monitoring. Untuk informasi selengkapnya, lihat [GuardDuty Pemantauan Runtime](#).

Log audit EKS di Perlindungan EKS

Log audit EKS menangkap tindakan berurutan dalam kluster Amazon EKS Anda, termasuk aktivitas dari pengguna, aplikasi yang menggunakan Kubernetes API, dan control plane. Audit logging adalah komponen dari semua kluster Kubernetes.

Untuk informasi selengkapnya, lihat [Auditing](#) dalam dokumentasi Kubernetes.

Amazon EKS memungkinkan log audit EKS untuk dicerna sebagai Amazon CloudWatch Logs melalui fitur [logging pesawat kontrol EKS](#). GuardDuty tidak mengelola pencatatan pesawat kontrol Amazon EKS Anda atau membuat log audit EKS dapat diakses di akun Anda jika Anda belum mengaktifkannya untuk Amazon EKS. Untuk mengelola akses dan retensi log audit EKS Anda, Anda harus mengonfigurasi fitur pencatatan bidang kontrol Amazon EKS. Untuk informasi selengkapnya, lihat [Mengaktifkan dan menonaktifkan log bidang kontrol di Panduan](#) Pengguna Amazon EKS.

Mengaktifkan Perlindungan EKS di lingkungan multi-akun

Dalam lingkungan beberapa akun, hanya akun GuardDuty administrator yang didelegasikan yang memiliki opsi untuk mengaktifkan atau menonaktifkan Perlindungan EKS; fitur untuk akun anggota di organisasi mereka. Akun GuardDuty anggota tidak dapat mengubah konfigurasi ini dari akun mereka. Akun GuardDuty administrator yang didelegasikan mengelola akun anggota mereka menggunakan AWS Organizations. Akun GuardDuty administrator yang didelegasikan ini dapat memilih untuk mengaktifkan Perlindungan EKS secara otomatis untuk semua akun baru saat mereka

bergabung dengan organisasi. Untuk informasi selengkapnya tentang lingkungan beberapa akun, lihat [Mengelola beberapa akun di Amazon](#). GuardDuty

Mengkonfigurasi EKS Audit Log Monitoring untuk akun administrator yang didelegasikan GuardDuty

Pilih metode akses pilihan Anda untuk mengonfigurasi Pemantauan Log Audit EKS untuk akun GuardDuty administrator yang didelegasikan.

Console

1. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.
2. Di panel navigasi, pilih Perlindungan EKS.
3. Di bawah tab Konfigurasi, Anda dapat melihat status konfigurasi EKS Audit Log Monitoring saat ini di bagian masing-masing. Untuk memperbarui konfigurasi akun GuardDuty administrator yang didelegasikan, pilih Edit di panel Pemantauan Log Audit EKS.
4. Lakukan salah satu hal berikut ini:

Menggunakan Aktifkan untuk semua akun

- Pilih Aktifkan untuk semua akun. Ini akan memungkinkan rencana perlindungan untuk semua GuardDuty akun aktif di AWS organisasi Anda, termasuk akun baru yang bergabung dengan organisasi.
- Pilih Simpan.

Menggunakan Konfigurasi akun secara manual

- Untuk mengaktifkan paket perlindungan hanya untuk akun GuardDuty administrator yang didelegasikan, pilih Konfigurasi akun secara manual.
- Pilih Aktifkan di bawah bagian akun GuardDuty administrator yang didelegasikan (akun ini).
- Pilih Simpan.

API/CLI

Jalankan [updateDetector](#) Operasi API menggunakan ID detektor regional Anda sendiri dan meneruskan features objek name sebagai EKS_AUDIT_LOGS dan status sebagai ENABLED atau DISABLED.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan `detectorId` [ListDetectors](#) API.

Anda dapat mengaktifkan atau menonaktifkan EKS Audit Log Monitoring dengan menjalankan AWS CLI perintah berikut. Pastikan untuk menggunakan akun GuardDuty administrator yang didelegasikan valid *detector ID*.

 Note

Kode contoh berikut memungkinkan EKS Audit Log Monitoring. Pastikan untuk mengganti *12abc34d567e8fa901bc2d34e56789f0* dengan akun administrator `detector-id` yang didelegasikan dan *5555555555* dengan akun GuardDuty administrator Akun AWS yang didelegasikan GuardDuty .

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan `detectorId` [ListDetectors](#) API.

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --  
features '[{"Name": "EKS_AUDIT_LOGS", "Status": "ENABLED"}]'
```

Untuk menonaktifkan EKS Audit Log Monitoring, ganti `ENABLED` dengan `DISABLED`.

Aktifkan Pemantauan Log Audit EKS secara otomatis untuk semua akun anggota

Pilih metode akses pilihan Anda untuk mengaktifkan Pemantauan Log Audit EKS untuk akun anggota yang ada di organisasi Anda.

Console

1. Masuk ke AWS Management Console dan buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.

Pastikan untuk menggunakan kredensi akun GuardDuty administrator yang didelegasikan.

2. Lakukan salah satu hal berikut ini:

Menggunakan halaman Perlindungan EKS

1. Di panel navigasi, pilih Perlindungan EKS.

2. Di bawah tab Konfigurasi, Anda dapat melihat status Pemantauan Log Audit EKS saat ini untuk akun anggota aktif di organisasi Anda.

Untuk memperbarui konfigurasi EKS Audit Log Monitoring, pilih Edit.

3. Pilih Aktifkan untuk semua akun. Tindakan ini secara otomatis memungkinkan Pemantauan Log Audit EKS untuk akun yang ada dan yang baru di organisasi.
4. Pilih Simpan.

 Note

Mungkin diperlukan waktu hingga 24 jam untuk memperbarui konfigurasi akun anggota.

Menggunakan halaman Akun

1. Di panel navigasi, pilih Akun.
2. Pada halaman Akun, pilih Preferensi Aktifkan otomatis sebelum Tambahkan akun berdasarkan undangan.
3. Di jendela Kelola preferensi aktifkan otomatis, pilih Aktifkan untuk semua akun di bawah Pemantauan Log Audit EKS.
4. Pilih Simpan.

Jika Anda tidak dapat menggunakan opsi Aktifkan untuk semua akun dan ingin menyesuaikan konfigurasi Pemantauan Log Audit EKS untuk akun tertentu di organisasi Anda, lihat [Aktifkan atau nonaktifkan Pemantauan Log Audit EKS secara selektif untuk akun anggota](#).

API/CLI

- Untuk mengaktifkan atau menonaktifkan Pemantauan Log Audit EKS secara selektif untuk akun anggota Anda, jalankan [updateMemberDetectors](#) Operasi API menggunakan milik Anda sendiri *detector ID*.
- Contoh berikut menunjukkan bagaimana Anda dapat mengaktifkan EKS Audit Log Monitoring untuk satu akun anggota. Untuk menonaktifkannya, ganti ENABLED dengan DISABLED.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan `detectorId` [ListDetectors](#) API.

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features ' [{"name": "EKS_AUDIT_LOGS", "status": "ENABLED"} ] '
```

 Note

Anda juga dapat melewati daftar akun yang IDs dipisahkan oleh spasi.

- Ketika kode telah berhasil dijalankan, daftar `UnprocessedAccounts` akan kembali kosong. Jika ada masalah dalam mengubah pengaturan detektor untuk suatu akun, ID akun tersebut akan dicantumkan bersama dengan ringkasan masalahnya.

Aktifkan Pemantauan Log Audit EKS untuk semua akun anggota aktif yang ada

Pilih metode akses pilihan Anda untuk mengaktifkan Pemantauan Log Audit EKS untuk semua akun anggota aktif yang ada di organisasi.

Console

1. Masuk ke AWS Management Console dan buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.

Masuk menggunakan kredensi akun GuardDuty administrator yang didelegasikan.

2. Di panel navigasi, pilih Perlindungan EKS.
3. Pada halaman Perlindungan EKS, Anda dapat melihat status saat ini dari konfigurasi pemindaian malware GuardDuty yang dimulai. Di bawah bagian Akun anggota aktif, pilih Tindakan.
4. Dari menu tarik-turun Tindakan, pilih Aktifkan untuk semua akun anggota aktif yang ada.
5. Pilih Simpan.

API/CLI

- Untuk mengaktifkan atau menonaktifkan Pemantauan Log Audit EKS secara selektif untuk akun anggota Anda, jalankan [updateMemberDetectors](#) Operasi API menggunakan milik Anda sendiri *detector ID*.
- Contoh berikut menunjukkan bagaimana Anda dapat mengaktifkan EKS Audit Log Monitoring untuk satu akun anggota. Untuk menonaktifkannya, ganti ENABLED dengan DISABLED.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan `detectorId` [ListDetectors](#) API.

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"name": "EKS_AUDIT_LOGS", "status": "ENABLED"}]'
```

Note

Anda juga dapat melewati daftar akun yang IDs dipisahkan oleh spasi.

- Ketika kode telah berhasil dijalankan, daftar `UnprocessedAccounts` akan kembali kosong. Jika ada masalah dalam mengubah pengaturan detektor untuk suatu akun, ID akun tersebut akan dicantumkan bersama dengan ringkasan masalahnya.

Aktifkan Pemantauan Log Audit EKS secara otomatis untuk akun anggota baru

Akun anggota yang baru ditambahkan harus Aktifkan GuardDuty sebelum memilih mengkonfigurasi GuardDuty pemindaian malware yang dimulai. Akun anggota yang dikelola oleh undangan dapat mengonfigurasi GuardDuty pemindaian malware yang dimulai secara manual untuk akun mereka. Untuk informasi selengkapnya, lihat [Step 3 - Accept an invitation](#).

Pilih metode akses pilihan Anda untuk mengaktifkan Pemantauan Log Audit EKS untuk akun baru yang bergabung dengan organisasi Anda.

Console

Akun GuardDuty administrator yang didelegasikan dapat mengaktifkan Pemantauan Log Audit EKS untuk akun anggota baru dalam suatu organisasi, baik menggunakan halaman Pemantauan Log Audit EKS atau Akun.

Untuk mengaktifkan Pemantauan Log Audit EKS secara otomatis untuk akun anggota baru

1. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.

Pastikan untuk menggunakan kredensi akun GuardDuty administrator yang didelegasikan.

2. Lakukan salah satu hal berikut ini:
 - Menggunakan halaman Perlindungan EKS:
 1. Di panel navigasi, pilih Perlindungan EKS.
 2. Pada halaman Perlindungan EKS, pilih Edit di Pemantauan Log Audit EKS.
 3. Pilih Konfigurasi akun secara manual.
 4. Pilih Aktifkan secara otomatis untuk akun anggota baru. Langkah ini memastikan bahwa setiap kali akun baru bergabung dengan organisasi Anda, Pemantauan Log Audit EKS akan diaktifkan secara otomatis untuk akun mereka. Hanya akun GuardDuty administrator yang didelegasikan organisasi yang dapat mengubah konfigurasi ini.
 5. Pilih Simpan.
 - Menggunakan halaman Akun:
 1. Di panel navigasi, pilih Akun.
 2. Pada halaman Akun, pilih Preferensi Aktifkan otomatis.
 3. Di jendela Kelola preferensi aktifkan otomatis, pilih Aktifkan untuk akun baru di bawah Pemantauan Log Audit EKS.
 4. Pilih Simpan.

API/CLI

- Untuk mengaktifkan atau menonaktifkan Pemantauan Log Audit EKS secara selektif untuk akun baru Anda, jalankan [UpdateOrganizationConfiguration](#) Operasi API menggunakan milik Anda sendiri *detector ID*.
- Contoh berikut menunjukkan bagaimana Anda dapat mengaktifkan EKS Audit Log Monitoring untuk anggota baru yang bergabung dengan organisasi Anda. Anda juga dapat melewati daftar akun yang IDs dipisahkan oleh spasi.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/> konsol, atau jalankan `detectorId` [ListDetectors](#) API.

```
aws guardduty update-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0 --auto-enable --features '[{"Name": "EKS_AUDIT_LOGS", "AutoEnable": "NEW"}]'
```

Aktifkan atau nonaktifkan Pemantauan Log Audit EKS secara selektif untuk akun anggota

Pilih metode akses pilihan Anda untuk mengaktifkan atau menonaktifkan Pemantauan Log Audit EKS untuk akun anggota selektif di organisasi Anda.

Console

1. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.

Pastikan untuk menggunakan kredensi akun GuardDuty administrator yang didelegasikan.

2. Di panel navigasi, pilih Akun.

Pada halaman Akun, tinjau kolom Pemantauan Log Audit EKS untuk status akun anggota Anda.

3. Untuk mengaktifkan atau menonaktifkan Pemantauan Log Audit EKS

Pilih akun yang ingin Anda konfigurasikan untuk EKS Audit Log Monitoring. Anda dapat memilih beberapa akun sekaligus. Di bawah menu tarik-turun Edit Rencana Perlindungan, pilih Pemantauan Log Audit EKS, lalu pilih opsi yang sesuai.

API/CLI

Untuk mengaktifkan atau menonaktifkan Pemantauan Log Audit EKS secara selektif untuk akun anggota Anda, panggil [updateMemberDetectors](#) Operasi API menggunakan milik Anda sendiri **detector ID**.

Contoh berikut menunjukkan bagaimana Anda dapat mengaktifkan EKS Audit Log Monitoring untuk satu akun anggota. Untuk menonaktifkannya, ganti ENABLED dengan DISABLED. Anda juga dapat melewati daftar akun yang IDs dipisahkan oleh spasi.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/> konsol, atau jalankan [detectorId ListDetectors](#) API.

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
--accountids 111122223333 --features '[{"Name": "EKS_AUDIT_LOGS", "Status":
"ENABLED"}]'
```

Mengaktifkan Perlindungan EKS untuk akun mandiri

Akun mandiri memiliki keputusan untuk mengaktifkan atau menonaktifkan rencana perlindungan di AWS akun mereka di Wilayah tertentu.

Jika akun Anda dikaitkan dengan akun GuardDuty administrator melalui AWS Organizations, atau dengan metode undangan, bagian ini tidak berlaku untuk Anda. Untuk informasi tentang mengelola beberapa akun, lihat [Mengaktifkan Perlindungan EKS di lingkungan multi-akun](#).

Setelah Anda mengaktifkan Perlindungan EKS, GuardDuty akan mulai memantau log audit EKS untuk kluster Amazon EKS di akun Anda.

Pilih metode akses pilihan Anda untuk mengaktifkan Perlindungan EKS di akun mandiri Anda.

Console

1. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.
2. Dari pemilih Wilayah di sudut kanan atas, pilih Wilayah tempat Anda ingin mengaktifkan Perlindungan EKS.
3. Di panel navigasi, pilih Perlindungan EKS.
4. Halaman Perlindungan EKS memberikan status Perlindungan EKS saat ini untuk akun Anda. Pilih Aktifkan untuk mengaktifkan Perlindungan EKS.
5. Pilih Konfirmasi untuk menyimpan pilihan Anda.

API/CLI

- Jalankan [updateDetector](#) Operasi API menggunakan ID detektor regional dari akun GuardDuty administrator yang didelegasikan dan meneruskan nama features objek sebagai EKS_AUDIT_LOGS dan status sebagai ENABLED.

Atau, Anda juga dapat mengaktifkan Perlindungan EKS menjalankan AWS CLI perintah. Jalankan perintah berikut, dan ganti `12abc34d567e8fa901bc2d34e56789f0` dengan

ID detektor akun Anda dan *us-east-1* dengan Wilayah tempat Anda ingin mengaktifkan Perlindungan EKS.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan `detectorId` [ListDetectors](#) API.

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --  
region us-east-1 --features [{"Name" : "EKS_AUDIT_LOGS", "Status" : "ENABLED"}]'
```

GuardDuty Perlindungan S3

S3 Protection membantu Anda mendeteksi potensi risiko keamanan untuk data, seperti eksfiltrasi dan penghancuran data, di bucket Amazon Simple Storage Service (Amazon S3). GuardDuty memantau peristiwa AWS CloudTrail data untuk Amazon S3, yang mencakup operasi API tingkat objek untuk mengidentifikasi risiko ini di semua bucket Amazon S3 di akun Anda.

Ketika GuardDuty mendeteksi potensi ancaman berdasarkan pemantauan peristiwa data S3, itu menghasilkan temuan keamanan. Untuk informasi tentang jenis temuan yang GuardDuty mungkin dihasilkan saat Anda mengaktifkan Perlindungan S3, lihat [GuardDuty Jenis temuan Perlindungan S3](#).

Secara default, deteksi ancaman dasar mencakup pemantauan [AWS CloudTrail acara manajemen](#) untuk mengidentifikasi potensi ancaman di sumber daya Amazon S3 Anda. Sumber data ini berbeda dari peristiwa AWS CloudTrail data untuk S3 karena keduanya memantau berbagai jenis aktivitas di lingkungan Anda.

Anda dapat mengaktifkan Perlindungan S3 di akun di Wilayah mana pun yang GuardDuty [mendukung fitur ini](#). Ini akan membantu Anda memantau peristiwa CloudTrail data untuk S3 di akun dan Wilayah itu. Setelah Anda mengaktifkan Perlindungan S3, Anda GuardDuty akan dapat sepenuhnya memantau bucket Amazon S3 Anda dan menghasilkan temuan untuk akses mencurigakan ke data yang disimpan di bucket S3 Anda.

Untuk menggunakan Perlindungan S3, Anda tidak perlu secara eksplisit mengaktifkan atau mengonfigurasi login peristiwa data S3. AWS CloudTrail

Uji coba gratis 30 hari

Daftar berikut menjelaskan bagaimana uji coba gratis 30 hari akan bekerja untuk akun Anda:

- Saat Anda mengaktifkan GuardDuty di Wilayah baru untuk pertama kalinya, Anda mendapatkan uji coba gratis 30 hari. Akun AWS Dalam hal ini, juga GuardDuty akan mengaktifkan Perlindungan S3, yang termasuk dalam uji coba gratis.
- Ketika Anda sudah menggunakan GuardDuty dan memutuskan untuk mengaktifkan Perlindungan S3 untuk pertama kalinya, akun Anda di Wilayah ini akan mendapatkan uji coba gratis 30 hari untuk Perlindungan S3.
- Anda dapat memilih untuk menonaktifkan Perlindungan S3 di Wilayah mana pun kapan saja.
- Selama uji coba gratis 30 hari, Anda bisa mendapatkan perkiraan biaya penggunaan Anda di akun dan Wilayah tersebut. Setelah uji coba gratis 30 hari berakhir, Perlindungan S3

tidak dinonaktifkan secara otomatis. Akun Anda di Wilayah ini akan mulai menimbulkan biaya penggunaan. Untuk informasi selengkapnya, lihat [Memperkirakan biaya GuardDuty penggunaan](#).

AWS CloudTrail peristiwa data untuk S3

Peristiwa data, juga dikenal sebagai operasi bidang data, memberikan wawasan tentang operasi sumber daya yang dilakukan pada atau di dalam sumber daya. Operasi ini sering kali merupakan aktivitas bervolume tinggi.

Berikut ini adalah contoh peristiwa CloudTrail data untuk S3 yang GuardDuty dapat memantau:

- Operasi API `GetObject`
- Operasi API `PutObject`
- Operasi API `ListObjects`
- Operasi API `DeleteObject`

Untuk informasi selengkapnya tentang ini APIs, lihat [Referensi API Amazon Simple Storage Service](#).

Cara GuardDuty menggunakan peristiwa CloudTrail data untuk S3

Saat Anda mengaktifkan Perlindungan S3, GuardDuty mulailah menganalisis peristiwa CloudTrail data untuk S3 dari semua bucket S3 Anda, dan memantaunya untuk aktivitas berbahaya dan mencurigakan. Untuk informasi selengkapnya, lihat [AWS CloudTrail acara manajemen](#).

Ketika pengguna yang tidak diautentikasi mengakses objek S3, itu berarti bahwa objek S3 dapat diakses publik. Oleh karena itu, GuardDuty tidak memproses permintaan tersebut. GuardDuty memproses permintaan yang dibuat ke objek S3 dengan menggunakan kredensial IAM (AWS Identity and Access Management) atau AWS STS (AWS Security Token Service) yang valid.

Catatan

Setelah mengaktifkan Perlindungan S3, GuardDuty memantau peristiwa data dari bucket Amazon S3 yang berada di Wilayah yang sama tempat Anda mengaktifkan. GuardDuty

Jika Anda menonaktifkan Perlindungan S3 di akun Anda di Wilayah tertentu, GuardDuty menghentikan pemantauan peristiwa data S3 dari data yang disimpan di bucket S3 Anda. GuardDuty tidak akan lagi menghasilkan jenis pencarian Perlindungan S3 untuk akun Anda di Wilayah tersebut.

GuardDuty menggunakan peristiwa CloudTrail data untuk S3 untuk urutan serangan

[GuardDuty Deteksi Ancaman Diperpanjang](#) mendeteksi urutan serangan multi-tahap yang menjangkau sumber data dasar, sumber AWS daya, dan garis waktu, dalam sebuah akun. Saat GuardDuty mengamati urutan peristiwa yang menunjukkan aktivitas mencurigakan baru-baru ini atau sedang berlangsung di akun Anda, buat temuan urutan serangan GuardDuty terkait.

Secara default, saat Anda mengaktifkan GuardDuty, Extended Threat Detection juga diaktifkan di akun Anda. Kemampuan ini mencakup skenario ancaman yang terkait dengan peristiwa CloudTrail manajemen tanpa biaya tambahan. Namun, untuk menggunakan Extended Threat Detection pada potensi penuhnya, GuardDuty merekomendasikan untuk mengaktifkan Perlindungan S3 untuk mencakup skenario ancaman yang terkait dengan peristiwa CloudTrail data untuk S3.

Setelah Anda mengaktifkan Perlindungan S3, secara otomatis GuardDuty akan mencakup skenario ancaman urutan serangan, seperti kompromi atau penghancuran data, di mana sumber daya Amazon S3 Anda mungkin terlibat.

Mengaktifkan Perlindungan S3 di lingkungan beberapa akun

Dalam lingkungan multi-akun, hanya akun GuardDuty administrator yang didelegasikan yang memiliki opsi untuk mengonfigurasi (mengaktifkan atau menonaktifkan) Perlindungan S3 untuk akun anggota di organisasi mereka. AWS Akun GuardDuty anggota tidak dapat mengubah konfigurasi ini dari akun mereka. Akun GuardDuty administrator yang didelegasikan mengelola akun anggota mereka menggunakan AWS Organizations. Akun GuardDuty administrator yang didelegasikan dapat memilih untuk mengaktifkan Perlindungan S3 secara otomatis di semua akun, hanya akun baru, atau tidak ada akun di organisasi. Untuk informasi selengkapnya, lihat [Mengelola akun dengan AWS Organizations](#).

Mengaktifkan Perlindungan S3 untuk akun administrator yang didelegasikan GuardDuty

Pilih metode akses pilihan Anda untuk mengaktifkan Perlindungan S3 untuk akun GuardDuty administrator yang didelegasikan.

Console

1. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.
2. Di panel navigasi, pilih Perlindungan S3.
3. Pada halaman Perlindungan S3, pilih Edit.
4. Lakukan salah satu hal berikut ini:

Menggunakan Aktifkan untuk semua akun

- Pilih Aktifkan untuk semua akun. Ini akan memungkinkan rencana perlindungan untuk semua GuardDuty akun aktif di AWS organisasi Anda, termasuk akun baru yang bergabung dengan organisasi.
- Pilih Simpan.

Menggunakan Konfigurasi akun secara manual

- Untuk mengaktifkan paket perlindungan hanya untuk akun GuardDuty administrator yang didelegasikan, pilih Konfigurasi akun secara manual.
- Pilih Aktifkan di bawah bagian akun GuardDuty administrator yang didelegasikan (akun ini).
- Pilih Simpan.

API/CLI

Jalankan [updateDetector](#) dengan menggunakan ID detektor dari akun GuardDuty administrator yang didelegasikan untuk Wilayah saat ini dan meneruskan features objek name sebagai S3_DATA_EVENTS dan status sebagai ENABLED.

Atau, Anda dapat mengkonfigurasi Perlindungan S3 dengan menggunakan AWS Command Line Interface. Jalankan perintah berikut, dan pastikan untuk mengganti **12abc34d567e8fa901bc2d34e56789f0** dengan ID detektor akun GuardDuty administrator yang didelegasikan untuk Wilayah saat ini.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/> konsol, atau jalankan `detectorId` [ListDetectors](#) API.

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name": "S3_DATA_EVENTS", "Status": "ENABLED"}]'
```

Aktifkan Perlindungan S3 secara otomatis untuk semua akun anggota di organisasi

Pilih metode akses pilihan Anda untuk mengaktifkan Perlindungan S3 untuk akun GuardDuty administrator yang didelegasikan.

Console

1. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.

Masuk menggunakan akun administrator Anda.

2. Lakukan salah satu hal berikut ini:

Menggunakan halaman Perlindungan S3

1. Di panel navigasi, pilih Perlindungan S3.
2. Pilih Aktifkan untuk semua akun. Tindakan ini secara otomatis mengaktifkan Perlindungan S3 untuk akun yang ada dan baru di organisasi.
3. Pilih Simpan.



Note

Mungkin diperlukan waktu hingga 24 jam untuk memperbarui konfigurasi akun anggota.

Menggunakan halaman Akun

1. Di panel navigasi, pilih Akun.
2. Pada halaman Akun, pilih Preferensi Aktifkan otomatis sebelum Tambahkan akun berdasarkan undangan.
3. Di jendela Kelola preferensi aktifkan otomatis, pilih Aktifkan untuk semua akun di bawah Perlindungan S3.
4. Pilih Simpan.

Jika Anda tidak dapat menggunakan opsi Aktifkan untuk semua akun, lihat [Aktifkan Perlindungan S3 secara selektif di akun anggota](#).

API/CLI

- Untuk mengaktifkan Perlindungan S3 secara selektif untuk akun anggota Anda, panggil [updateMemberDetectors](#) Operasi API menggunakan milik Anda sendiri *detector ID*.
- Contoh berikut menunjukkan bagaimana Anda dapat mengaktifkan Perlindungan S3 untuk satu akun anggota. Pastikan untuk mengganti *12abc34d567e8fa901bc2d34e56789f0* dengan akun GuardDuty administrator `detector-id` yang didelegasikan, dan *111122223333*.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan `detectorId` [ListDetectors](#) API.

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"name": "S3_DATA_EVENTS", "status": "ENABLED"}]'
```



Note

Anda juga dapat melewati daftar akun yang IDs dipisahkan oleh spasi.

- Ketika kode telah berhasil dijalankan, daftar `UnprocessedAccounts` akan kembali kosong. Jika ada masalah dalam mengubah pengaturan detektor untuk suatu akun, ID akun tersebut akan dicantumkan bersama dengan ringkasan masalahnya.

Aktifkan Perlindungan S3 untuk semua akun anggota aktif yang ada

Pilih metode akses pilihan Anda untuk mengaktifkan Perlindungan S3 untuk semua akun anggota aktif yang ada di organisasi Anda.

Console

1. Masuk ke AWS Management Console dan buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.

Masuk menggunakan kredensi akun GuardDuty administrator yang didelegasikan.

2. Di panel navigasi, pilih Perlindungan S3.
3. Pada halaman Perlindungan S3, Anda dapat melihat status konfigurasi saat ini. Di bawah bagian Akun anggota aktif, pilih Tindakan.
4. Dari menu tarik-turun Tindakan, pilih Aktifkan untuk semua akun anggota aktif yang ada.

5. Pilih Konfirmasi.

API/CLI

- Untuk mengaktifkan Perlindungan S3 secara selektif untuk akun anggota Anda, panggil [updateMemberDetectors](#) Operasi API menggunakan milik Anda sendiri *detector ID*.
- Contoh berikut menunjukkan bagaimana Anda dapat mengaktifkan Perlindungan S3 untuk satu akun anggota. Pastikan untuk mengganti *12abc34d567e8fa901bc2d34e56789f0* dengan akun GuardDuty administrator detector-id yang didelegasikan, dan *111122223333*.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan `detectorId` [ListDetectors](#) API.

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"name": "S3_DATA_EVENTS", "status": "ENABLED"}]'
```



Note

Anda juga dapat melewati daftar akun yang IDs dipisahkan oleh spasi.

- Ketika kode telah berhasil dijalankan, daftar `UnprocessedAccounts` akan kembali kosong. Jika ada masalah dalam mengubah pengaturan detektor untuk suatu akun, ID akun tersebut akan dicantumkan bersama dengan ringkasan masalahnya.

Aktifkan Perlindungan S3 secara otomatis untuk akun anggota baru

Pilih metode akses pilihan Anda untuk mengaktifkan Perlindungan S3 untuk akun baru yang bergabung dengan organisasi Anda.

Console

Akun GuardDuty administrator yang didelegasikan dapat mengaktifkan akun anggota baru di organisasi melalui konsol, menggunakan halaman Perlindungan S3 atau Akun.

Untuk mengaktifkan Perlindungan S3 secara otomatis untuk akun anggota baru

1. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.

Pastikan untuk menggunakan kredensial akun GuardDuty administrator yang didelegasikan.

2. Lakukan salah satu hal berikut ini:

- Menggunakan halaman Perlindungan S3:
 1. Di panel navigasi, pilih Perlindungan S3.
 2. Pada halaman Perlindungan S3, pilih Edit.
 3. Pilih Konfigurasi akun secara manual.
 4. Pilih Aktifkan secara otomatis untuk akun anggota baru. Langkah ini memastikan bahwa setiap kali akun baru bergabung dengan organisasi Anda, Perlindungan S3 akan diaktifkan secara otomatis untuk akun mereka. Hanya akun GuardDuty administrator yang didelegasikan organisasi yang dapat mengubah konfigurasi ini.
 5. Pilih Simpan.
- Menggunakan halaman Akun:
 1. Di panel navigasi, pilih Akun.
 2. Pada halaman Akun, pilih Preferensi Aktifkan otomatis.
 3. Di jendela Kelola preferensi aktifkan otomatis, pilih Aktifkan untuk akun baru di bawah Perlindungan S3.
 4. Pilih Simpan.

API/CLI

- Untuk mengaktifkan Perlindungan S3 secara selektif untuk akun anggota Anda, panggil [UpdateOrganizationConfiguration](#) Operasi API menggunakan milik Anda sendiri *detector ID*.
- Contoh berikut menunjukkan bagaimana Anda dapat mengaktifkan Perlindungan S3 untuk satu akun anggota. Tetapkan preferensi untuk mengaktifkan atau menonaktifkan paket perlindungan secara otomatis di Wilayah tersebut untuk akun baru (NEW) yang bergabung dengan organisasi, semua akun (ALL), atau tidak ada akun (NONE) di organisasi. Untuk informasi selengkapnya, lihat [autoEnableOrganizationAnggota](#). Berdasarkan preferensi Anda, Anda mungkin perlu mengganti NEW dengan ALL atau NONE.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan `detectorId` [ListDetectors](#) API.

```
aws guardduty update-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0 --auto-enable --features '[{"Name": "S3_DATA_EVENTS", "autoEnable": "NEW"}]'
```

- Ketika kode telah berhasil dijalankan, daftar UnprocessedAccounts akan kembali kosong. Jika ada masalah dalam mengubah pengaturan detektor untuk suatu akun, ID akun tersebut akan dicantumkan bersama dengan ringkasan masalahnya.

Aktifkan Perlindungan S3 secara selektif di akun anggota

Pilih metode akses pilihan Anda untuk mengaktifkan Perlindungan S3 secara selektif untuk akun anggota.

Console

1. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.

Pastikan untuk menggunakan kredensial akun GuardDuty administrator yang didelegasikan.

2. Di panel navigasi, pilih Akun.

Pada halaman Akun, tinjau kolom Perlindungan S3 untuk status akun anggota Anda.

3. Untuk mengaktifkan Perlindungan S3 secara selektif

Pilih akun yang ingin Anda aktifkan Perlindungan S3. Anda dapat memilih beberapa akun sekaligus. Di menu dropdown Edit Protection Plans, pilih S3Pro, lalu pilih opsi yang sesuai.

API/CLI

Untuk mengaktifkan Perlindungan S3 secara selektif untuk akun anggota Anda, jalankan [updateMemberDetectors](#) Operasi API menggunakan ID detektor Anda sendiri. Contoh berikut menunjukkan bagaimana Anda dapat mengaktifkan Perlindungan S3 untuk satu akun anggota. Untuk menonaktifkannya, ganti `true` dengan `false`.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/> konsol, atau jalankan `detectorId` [ListDetectors](#) API.

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 123456789012 --features ' [{"Name" : "S3_DATA_EVENTS", "Status" : "ENABLED"} ] '
```

Note

Anda juga dapat melewati daftar akun yang IDs dipisahkan oleh spasi.

Ketika kode telah berhasil dijalankan, daftar `UnprocessedAccounts` akan kembali kosong. Jika ada masalah dalam mengubah pengaturan detektor untuk suatu akun, ID akun tersebut akan dicantumkan bersama dengan ringkasan masalahnya.

Note

Jika Anda menggunakan skrip untuk memasukkan akun baru dan ingin menonaktifkan Perlindungan S3 di akun baru Anda, Anda dapat memodifikasi [createDetector](#) Operasi API dengan `dataSources` objek opsional seperti yang dijelaskan dalam topik ini.

Mengaktifkan Perlindungan S3 untuk akun mandiri

Akun mandiri memiliki keputusan untuk mengaktifkan atau menonaktifkan rencana perlindungan di akun mereka Akun AWS secara spesifik. Wilayah AWS

Jika akun Anda dikaitkan dengan akun GuardDuty administrator melalui AWS Organizations, atau dengan metode undangan, bagian ini tidak berlaku untuk akun Anda. Untuk informasi selengkapnya, lihat [Mengaktifkan Perlindungan S3 di lingkungan beberapa akun](#).

Setelah Anda mengaktifkan Perlindungan S3, GuardDuty akan mulai memantau peristiwa AWS CloudTrail data untuk bucket S3 di akun Anda.

Pilih metode akses pilihan Anda untuk mengonfigurasi Perlindungan S3 untuk akun mandiri.

Console

1. Masuk ke AWS Management Console dan buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.

2. Dari pemilih Wilayah di sudut kanan atas, pilih Wilayah tempat Anda ingin mengaktifkan Perlindungan S3.
3. Di panel navigasi, pilih Perlindungan S3.
4. Halaman Perlindungan S3 memberikan status Perlindungan S3 saat ini untuk akun Anda. Pilih Aktifkan atau Nonaktifkan untuk mengaktifkan atau menonaktifkan Perlindungan S3 kapan saja.
5. Pilih Konfirmasi untuk mengonfirmasi pilihan Anda.

API/CLI

Jalankan [updateDetector](#) dengan menggunakan ID detektor Anda yang valid untuk Wilayah saat ini dan meneruskan `features` objek `name` yang `S3_DATA_EVENTS` disetel `ENABLED` untuk mengaktifkan Perlindungan S3, masing-masing.

Note

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan `detectorId` [ListDetectors](#) API.

Atau, Anda dapat menggunakan AWS Command Line Interface. Untuk mengaktifkan Perlindungan S3, jalankan perintah berikut, dan ganti `12abc34d567e8fa901bc2d34e56789f0` dengan ID detektor akun Anda dan `us-east-1` dengan Wilayah tempat Anda ingin mengaktifkan Perlindungan S3.

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --  
region us-east-1 --features '[{"Name" : "S3_DATA_EVENTS", "Status" : "ENABLED"}]'
```

GuardDuty Pemantauan Runtime

Runtime Monitoring mengamati dan menganalisis tingkat sistem operasi, jaringan, dan peristiwa file untuk membantu Anda mendeteksi potensi ancaman dalam beban kerja tertentu AWS di lingkungan Anda.

AWS Sumber daya yang didukung dalam Runtime Monitoring — GuardDuty awalnya merilis Runtime Monitoring untuk hanya mendukung sumber daya Amazon Elastic Kubernetes Service (Amazon EKS). Sekarang, Anda dapat menggunakan fitur Runtime Monitoring untuk menyediakan deteksi ancaman untuk Amazon Elastic Container Service (AWS Fargate Amazon ECS) Service Elastic Container (Amazon) dan Amazon Elastic Compute Cloud (Amazon EC2) resource juga.

GuardDuty tidak mendukung kluster Amazon EKS yang berjalan AWS Fargate.

Dalam dokumen ini dan bagian lain yang terkait dengan Runtime Monitoring, GuardDuty menggunakan terminologi jenis sumber daya untuk merujuk ke Amazon EKS, Fargate Amazon ECS, dan sumber daya Amazon. EC2

Runtime Monitoring menggunakan agen GuardDuty keamanan yang menambahkan visibilitas ke dalam perilaku runtime, seperti akses file, eksekusi proses, argumen baris perintah, dan koneksi jaringan. Untuk setiap jenis sumber daya yang ingin Anda pantau untuk potensi ancaman, Anda dapat mengelola agen keamanan untuk jenis sumber daya tertentu baik secara otomatis atau manual (dengan pengecualian untuk Fargate (hanya Amazon ECS)). Mengelola agen keamanan secara otomatis berarti Anda mengizinkan GuardDuty untuk menginstal dan memperbarui agen keamanan atas nama Anda. Di sisi lain, ketika Anda mengelola agen keamanan untuk sumber daya Anda secara manual, Anda bertanggung jawab untuk menginstal dan memperbarui agen keamanan, sesuai kebutuhan.

Dengan kemampuan yang diperluas ini, GuardDuty dapat membantu Anda mengidentifikasi dan merespons potensi ancaman yang dapat menargetkan aplikasi dan data yang berjalan di beban kerja dan instance pribadi Anda. Misalnya, ancaman berpotensi dimulai dengan mengorbankan satu wadah yang menjalankan aplikasi web yang rentan. Aplikasi web ini mungkin memiliki izin akses ke wadah dan beban kerja yang mendasarinya. Dalam skenario ini, kredensial yang tidak dikonfigurasi dengan benar berpotensi menyebabkan akses yang lebih luas ke akun, dan data yang tersimpan di dalamnya.

Dengan menganalisis peristiwa runtime dari setiap container dan beban kerja, GuardDuty berpotensi mengidentifikasi kompromi kontainer dan AWS kredensial terkait pada fase awal, dan mendeteksi

upaya untuk meningkatkan hak istimewa, permintaan API yang mencurigakan, dan akses berbahaya ke data di lingkungan Anda.

Daftar Isi

- [Cara kerjanya](#)
- [Bagaimana cara kerja uji coba gratis 30 hari di Runtime Monitoring](#)
- [Prasyarat untuk mengaktifkan Runtime Monitoring](#)
- [Mengaktifkan GuardDuty Runtime Monitoring](#)
- [Mengelola agen GuardDuty keamanan](#)
- [Meninjau statistik cakupan runtime dan masalah pemecahan masalah](#)
- [Menyiapkan CPU dan pemantauan memori](#)
- [Menggunakan VPC bersama dengan Runtime Monitoring](#)
- [Menggunakan Infrastructure as Code \(IaC\) dengan GuardDuty agen keamanan otomatis](#)
- [Mengumpulkan jenis peristiwa runtime yang menggunakan GuardDuty](#)
- [Agen hosting repositori Amazon ECR GuardDuty](#)
- [Dua agen keamanan pada host dasar yang sama](#)
- [Pemantauan Runtime EKS di GuardDuty](#)
- [GuardDuty versi rilis agen keamanan](#)
- [Menonaktifkan, menghapus instalasi, dan membersihkan sumber daya di Runtime Monitoring](#)

Cara kerjanya

Untuk menggunakan Runtime Monitoring, Anda harus mengaktifkan Runtime Monitoring dan kemudian mengelola agen GuardDuty keamanan. Daftar berikut menjelaskan proses dua langkah ini:

1. Aktifkan Runtime Monitoring untuk akun Anda sehingga GuardDuty dapat menerima peristiwa runtime yang diterimanya dari EC2 instans Amazon, kluster Amazon ECS, dan beban kerja Amazon EKS.
2. Kelola GuardDuty agen untuk sumber daya individual yang ingin Anda pantau perilaku runtime. Berdasarkan jenis sumber daya, Anda dapat memilih untuk:
 - Gunakan konfigurasi agen otomatis, tempat GuardDuty mengelola penyebaran agen dan secara otomatis titik akhir Amazon Virtual Private Cloud (Amazon VPC).

- Instal agen secara manual, yang mengharuskan Anda untuk membuat titik akhir VPC sebagai prasyarat.

Agan keamanan menggunakan titik akhir VPC untuk mengirimkan acara GuardDuty, memastikan bahwa data tetap berada di dalam jaringan. AWS Pendekatan ini meningkatkan keamanan dan memungkinkan GuardDuty untuk memantau dan menganalisis perilaku runtime di seluruh sumber daya Anda (Amazon EKS, Amazon EC2, dan AWS Fargate-Amazon ECS). GuardDuty menggunakan [peran identitas Instance](#) yang mengautentikasi agen keamanan untuk setiap jenis sumber daya untuk mengirim peristiwa runtime terkait ke titik akhir VPC.

Note

GuardDuty tidak membuat acara runtime dapat diakses oleh Anda.

Saat Anda mengelola agen keamanan (baik secara manual atau melalui GuardDuty) di EKS Runtime Monitoring atau Runtime Monitoring untuk EC2 instance, dan saat GuardDuty ini digunakan di instans EC2 Amazon dan menerima [Jenis acara runtime yang dikumpulkan](#) dari instance ini GuardDuty , tidak akan membebankan biaya Akun AWS untuk analisis log aliran VPC dari instans Amazon ini. EC2 Ini membantu GuardDuty menghindari biaya penggunaan ganda di akun.

Topik berikut menjelaskan cara mengaktifkan Runtime Monitoring dan mengelola agen GuardDuty keamanan bekerja secara berbeda untuk setiap jenis sumber daya.

Daftar Isi

- [Cara kerja Runtime Monitoring dengan kluster Amazon EKS](#)
- [Cara kerja Runtime Monitoring dengan instans Amazon EC2](#)
- [Bagaimana Runtime Monitoring bekerja dengan Fargate \(hanya Amazon ECS\)](#)
- [Setelah Anda mengaktifkan Runtime Monitoring](#)

Cara kerja Runtime Monitoring dengan kluster Amazon EKS

Runtime Monitoring menggunakan [add-on EKS aws-guardduty-agent](#), juga disebut sebagai agen GuardDuty keamanan. Setelah agen GuardDuty keamanan diterapkan di kluster EKS Anda, GuardDuty dapat menerima peristiwa runtime untuk kluster EKS ini.

Catatan

Runtime Monitoring mendukung kluster Amazon EKS yang berjalan di EC2 instans Amazon dan Mode Otomatis Amazon EKS.

Runtime Monitoring tidak mendukung kluster Amazon EKS dengan Amazon EKS Hybrid Nodes, dan yang berjalan. AWS Fargate

Untuk informasi tentang fitur Amazon EKS ini, lihat [Apa itu Amazon EKS?](#) di Panduan Pengguna Amazon EKS.

Anda dapat memantau peristiwa runtime kluster Amazon EKS di level akun atau kluster. Anda dapat mengelola agen GuardDuty keamanan hanya untuk kluster Amazon EKS yang ingin Anda pantau untuk deteksi ancaman. Anda dapat mengelola agen GuardDuty keamanan baik secara manual atau dengan mengizinkan GuardDuty untuk mengelolanya atas nama Anda, dengan menggunakan konfigurasi agen Otomatis.

Ketika Anda menggunakan pendekatan konfigurasi agen otomatis GuardDuty untuk memungkinkan mengelola penyebaran agen keamanan atas nama Anda, itu akan secara otomatis membuat titik akhir Amazon Virtual Private Cloud (Amazon VPC). Agen keamanan mengirimkan peristiwa runtime GuardDuty dengan menggunakan titik akhir VPC Amazon ini.

Seiring dengan titik akhir VPC, GuardDuty juga membuat grup keamanan baru. Aturan masuk (ingress) mengontrol lalu lintas yang diizinkan untuk mencapai sumber daya, yang terkait dengan grup keamanan. GuardDuty menambahkan aturan masuk yang cocok dengan rentang CIDR VPC untuk sumber daya Anda, dan juga menyesuaikannya saat rentang CIDR berubah. Untuk informasi selengkapnya, lihat [rentang VPC CIDR di Panduan](#) Pengguna Amazon VPC.

Catatan

- Tidak ada biaya tambahan untuk penggunaan titik akhir VPC.
- Bekerja dengan VPC terpusat dengan agen otomatis — Saat Anda GuardDuty menggunakan konfigurasi agen otomatis untuk jenis sumber daya GuardDuty, akan membuat titik akhir VPC atas nama Anda untuk semua VPCs Ini termasuk VPC terpusat dan bicara. VPCs GuardDuty tidak mendukung pembuatan titik akhir VPC hanya untuk VPC terpusat. Untuk informasi selengkapnya tentang cara kerja VPC terpusat, lihat Endpoint VPC [Antarmuka di Whitepaper - Membangun Infrastruktur Jaringan Multi-VPC AWS](#) yang Dapat Diskalakan dan Aman. AWS

Pendekatan untuk mengelola agen GuardDuty keamanan di kluster Amazon EKS

Sebelum 13 September 2023, Anda dapat mengonfigurasi GuardDuty untuk mengelola agen keamanan di tingkat akun. Perilaku ini menunjukkan bahwa secara default, GuardDuty akan mengelola agen keamanan pada semua kluster EKS milik. Akun AWS Sekarang, GuardDuty menyediakan kemampuan granular untuk membantu Anda memilih kluster EKS di mana Anda GuardDuty ingin mengelola agen keamanan.

Ketika Anda memilih untuk [Kelola agen GuardDuty keamanan secara manual](#), Anda masih dapat memilih kluster EKS yang ingin Anda pantau. Namun, untuk mengelola agen secara manual, membuat titik akhir VPC Amazon untuk Anda Akun AWS adalah prasyarat.

Note

Terlepas dari pendekatan yang Anda gunakan untuk mengelola agen GuardDuty keamanan, EKS Runtime Monitoring selalu diaktifkan di tingkat akun.

Topik

- [Mengelola agen keamanan melalui GuardDuty](#)
- [Kelola agen GuardDuty keamanan secara manual](#)

Mengelola agen keamanan melalui GuardDuty

GuardDuty menyebarkan dan mengelola agen keamanan atas nama Anda. Kapan saja, Anda dapat memantau kluster EKS di akun Anda dengan menggunakan salah satu pendekatan berikut.

Topik

- [Pantau semua kluster EKS](#)
- [Kecualikan kluster EKS selektif](#)
- [Sertakan kluster EKS selektif](#)

Pantau semua kluster EKS

Gunakan pendekatan ini ketika Anda GuardDuty ingin menyebarkan dan mengelola agen keamanan untuk semua kluster EKS di akun Anda. Secara default, juga GuardDuty akan menyebarkan agen keamanan pada kluster EKS yang berpotensi baru yang dibuat di akun Anda.

Dampak menggunakan pendekatan ini

- GuardDuty membuat titik akhir Amazon Virtual Private Cloud (Amazon VPC) tempat agen GuardDuty keamanan mengirimkan peristiwa runtime. GuardDuty Tidak ada biaya tambahan untuk pembuatan titik akhir VPC Amazon saat Anda mengelola agen keamanan melalui GuardDuty
- Diperlukan bahwa node pekerja Anda memiliki jalur jaringan yang valid ke titik akhir guardduty-data VPC yang aktif. GuardDuty menyebarkan agen keamanan di kluster EKS Anda. Amazon Elastic Kubernetes Service (Amazon EKS) akan mengoordinasikan penyebaran agen keamanan pada node dalam cluster EKS.
- Atas dasar ketersediaan IP, GuardDuty pilih subnet untuk membuat titik akhir VPC. Jika Anda menggunakan topologi jaringan tingkat lanjut, Anda harus memvalidasi bahwa konektivitas dimungkinkan.

Kecualikan kluster EKS selektif

Gunakan pendekatan ini ketika Anda ingin mengelola agen keamanan GuardDuty untuk semua kluster EKS di akun Anda tetapi tidak termasuk kluster EKS selektif. Metode ini menggunakan pendekatan berbasis tag ¹ di mana Anda dapat menandai cluster EKS yang Anda tidak ingin menerima peristiwa runtime. Tag yang telah ditentukan harus memiliki GuardDutyManaged - false sebagai pasangan kunci-nilai.

Dampak menggunakan pendekatan ini

Pendekatan ini mengharuskan Anda untuk mengaktifkan manajemen otomatis GuardDuty agen hanya setelah menambahkan tag ke kluster EKS yang ingin Anda kecualikan dari pemantauan.

Oleh karena itu, dampaknya ketika Anda [Mengelola agen keamanan melalui GuardDuty](#) menerapkan pendekatan ini juga. Saat Anda menambahkan tag sebelum mengaktifkan manajemen otomatis GuardDuty agen, tidak GuardDuty akan menyebarkan atau mengelola agen keamanan untuk kluster EKS yang dikecualikan dari pemantauan.

Pertimbangan-pertimbangan

- Anda harus menambahkan pasangan nilai kunci tag sebagai GuardDutyManaged: false untuk kluster EKS selektif sebelum mengaktifkan konfigurasi agen Otomatis jika tidak, agen GuardDuty keamanan akan digunakan di semua kluster EKS sampai Anda menggunakan tag.
- Anda harus mencegah tag diubah, kecuali oleh identitas tepercaya.

 Important

Kelola izin untuk mengubah nilai GuardDutyManaged tag untuk kluster EKS Anda dengan menggunakan kebijakan kontrol layanan atau kebijakan IAM. Untuk informasi selengkapnya, lihat [Kebijakan kontrol layanan \(SCPs\)](#) di Panduan AWS Organizations Pengguna atau [Kontrol akses ke AWS sumber daya](#) di Panduan Pengguna IAM.

- Untuk cluster EKS yang berpotensi baru yang tidak ingin Anda pantau, pastikan untuk menambahkan pasangan GuardDutyManaged - false kunci-nilai pada saat membuat cluster EKS ini.
- Pendekatan ini juga akan memiliki pertimbangan yang sama seperti yang ditentukan untuk [Pantau semua kluster EKS](#).

Sertakan kluster EKS selektif

Gunakan pendekatan ini ketika Anda GuardDuty ingin menyebarkan dan mengelola pembaruan ke agen keamanan hanya untuk kluster EKS selektif di akun Anda. Metode ini menggunakan pendekatan berbasis tag ¹ di mana Anda dapat menandai cluster EKS yang ingin Anda terima peristiwa runtime.

Dampak menggunakan pendekatan ini

- Dengan menggunakan tag inklusi, secara otomatis GuardDuty akan menyebarkan dan mengelola agen keamanan hanya untuk kluster EKS selektif yang ditandai dengan GuardDutyManaged - true sebagai pasangan kunci-nilai.
- Menggunakan pendekatan ini juga akan memiliki dampak yang sama seperti yang ditentukan untuk [Pantau semua kluster EKS](#).

Pertimbangan-pertimbangan

- Jika nilai tag tidak disetel ke true, GuardDutyManaged tag inklusi tidak akan berfungsi seperti yang diharapkan dan ini dapat memengaruhi pemantauan kluster EKS Anda.
- Untuk memastikan bahwa kluster EKS selektif Anda dipantau, Anda perlu mencegah tag diubah, kecuali oleh identitas tepercaya.

 Important

Kelola izin untuk mengubah nilai GuardDutyManaged tag untuk kluster EKS Anda dengan menggunakan kebijakan kontrol layanan atau kebijakan IAM. Untuk informasi selengkapnya, lihat [Kebijakan kontrol layanan \(SCPs\)](#) di Panduan AWS Organizations Pengguna atau [Kontrol akses ke AWS sumber daya](#) di Panduan Pengguna IAM.

- Untuk cluster EKS yang berpotensi baru yang tidak ingin Anda pantau, pastikan untuk menambahkan pasangan GuardDutyManaged - false kunci-nilai pada saat membuat cluster EKS ini.
- Pendekatan ini juga akan memiliki pertimbangan yang sama seperti yang ditentukan untuk [Pantau semua kluster EKS](#).

¹ Untuk informasi selengkapnya tentang menandai kluster EKS selektif, lihat [Menandai sumber daya Amazon EKS Anda](#) di Panduan Pengguna Amazon EKS.

Kelola agen GuardDuty keamanan secara manual

Gunakan pendekatan ini saat Anda ingin menyebarkan dan mengelola agen GuardDuty keamanan di semua kluster EKS Anda secara manual. Pastikan bahwa EKS Runtime Monitoring diaktifkan untuk akun Anda. Agen GuardDuty keamanan mungkin tidak berfungsi seperti yang diharapkan jika Anda tidak mengaktifkan EKS Runtime Monitoring.

Dampak menggunakan pendekatan ini

Anda perlu mengoordinasikan penyebaran agen GuardDuty keamanan dalam kluster EKS Anda di semua akun dan Wilayah AWS di mana fitur ini tersedia. Anda juga perlu memperbarui versi agen saat GuardDuty merilisnya. Untuk informasi selengkapnya tentang versi agen untuk EKS, lihat [GuardDuty versi agen keamanan untuk sumber daya Amazon EKS](#).

Pertimbangan-pertimbangan

Anda harus mendukung aliran data yang aman sambil memantau dan mengatasi kesenjangan cakupan karena kluster dan beban kerja baru terus digunakan.

Cara kerja Runtime Monitoring dengan instans Amazon EC2

EC2 Instans Amazon Anda dapat menjalankan beberapa jenis aplikasi dan beban kerja di lingkungan Anda AWS . Bila Anda mengaktifkan Runtime Monitoring dan mengelola agen GuardDuty keamanan, GuardDuty membantu Anda mendeteksi ancaman dalam EC2 instans Amazon yang ada dan yang berpotensi baru. Fitur ini juga mendukung EC2 instans Amazon yang dikelola Amazon ECS.

Mengaktifkan Runtime Monitoring akan GuardDuty siap untuk mengkonsumsi peristiwa runtime dari proses yang sedang berjalan dan proses baru dalam instans Amazon. EC2 GuardDuty membutuhkan agen keamanan untuk mengirim peristiwa runtime dari EC2 instance Anda ke GuardDuty.

Untuk EC2 instans Amazon, agen GuardDuty keamanan beroperasi pada tingkat instans. Anda dapat memutuskan apakah Anda ingin memantau semua atau EC2 instans Amazon selektif di akun Anda. Jika Anda ingin mengelola instance selektif, agen keamanan hanya diperlukan untuk instance ini.

GuardDuty juga dapat menggunakan peristiwa runtime dari tugas baru dan tugas yang ada yang berjalan di EC2 instans Amazon dalam kluster Amazon ECS.

Untuk menginstal agen GuardDuty keamanan, Runtime Monitoring menyediakan dua opsi berikut:

- [Gunakan konfigurasi agen otomatis \(disarankan\)](#), atau
- [Kelola agen keamanan secara manual](#)

Gunakan konfigurasi agen otomatis melalui GuardDuty (disarankan)

Gunakan konfigurasi agen otomatis yang memungkinkan GuardDuty untuk menginstal agen keamanan di EC2 instans Amazon Anda atas nama Anda. GuardDuty juga mengelola pembaruan ke agen keamanan.

Secara default, GuardDuty instal agen keamanan pada semua instans di akun Anda. Jika Anda GuardDuty ingin menginstal dan mengelola agen keamanan hanya untuk EC2 instance yang dipilih, tambahkan tag penyertaan atau pengecualian ke EC2 instance Anda, sesuai kebutuhan.

Terkadang, Anda mungkin tidak ingin memantau peristiwa runtime untuk semua EC2 instans Amazon milik akun Anda. Untuk kasus ketika Anda ingin memantau peristiwa runtime untuk sejumlah instance terbatas, tambahkan tag inklusi sebagai `GuardDutyManaged: true` ke instance yang dipilih ini. Dimulai dengan ketersediaan konfigurasi agen otomatis untuk Amazon EC2, jika EC2 instans Anda memiliki tag inklusi (`GuardDutyManaged:true`), GuardDuty akan menghormati tag dan mengelola

agen keamanan untuk instans yang dipilih meskipun Anda tidak secara eksplisit mengaktifkan konfigurasi agen otomatis.

Di sisi lain, jika ada sejumlah EC2 instance yang tidak ingin Anda pantau peristiwa runtime, tambahkan tag pengecualian (`GuardDutyManaged:false`) ke instance yang dipilih ini. GuardDuty akan menghormati tag pengecualian dengan tidak menginstal atau mengelola agen keamanan untuk EC2 sumber daya ini.

Dampak

Ketika Anda menggunakan konfigurasi agen otomatis dalam suatu Akun AWS atau organisasi, Anda mengizinkan GuardDuty untuk mengambil langkah-langkah berikut atas nama Anda:

- GuardDuty membuat satu asosiasi SSM untuk semua EC2 instans Amazon Anda yang dikelola SSM dan muncul di bawah Fleet Manager di konsol. <https://console.aws.amazon.com/systems-manager/>
- Menggunakan tag penyertaan dengan konfigurasi agen otomatis dinonaktifkan — Setelah mengaktifkan Runtime Monitoring, ketika Anda tidak mengaktifkan konfigurasi agen otomatis tetapi menambahkan tag inklusi ke EC2 instans Amazon Anda, itu berarti Anda mengizinkan GuardDuty untuk mengelola agen keamanan atas nama Anda. Asosiasi SSM kemudian akan menginstal agen keamanan di setiap instance yang memiliki tag inklusi (`GuardDutyManaged:true`).
- Jika Anda mengaktifkan konfigurasi agen otomatis — Asosiasi SSM kemudian akan menginstal agen keamanan di semua EC2 instance milik akun Anda.
- Menggunakan tag pengecualian dengan konfigurasi agen otomatis — Sebelum Anda mengaktifkan konfigurasi agen otomatis, ketika Anda menambahkan tag pengecualian ke EC2 instans Amazon Anda, itu berarti Anda mengizinkan GuardDuty untuk mencegah menginstal dan mengelola agen keamanan untuk instance yang dipilih ini.

Sekarang, ketika Anda mengaktifkan konfigurasi agen otomatis, asosiasi SSM akan menginstal dan mengelola agen keamanan di semua EC2 instance kecuali yang ditandai dengan tag pengecualian.

- GuardDuty membuat titik akhir VPC di semua VPCs, termasuk bersama VPCs, selama setidaknya ada satu EC2 instance Linux di VPC yang tidak dalam status instance yang dihentikan atau dimatikan. Ini termasuk VPC terpusat dan bicara. VPCs GuardDuty tidak mendukung pembuatan titik akhir VPC hanya untuk VPC terpusat. Untuk informasi selengkapnya tentang cara kerja VPC terpusat, lihat Endpoint VPC [Antarmuka di Whitepaper - Membangun Infrastruktur Jaringan Multi-VPC AWS](#) yang Dapat Diskalakan dan Aman. AWS

Untuk informasi tentang status instans yang berbeda, lihat [Siklus hidup instans](#) di EC2 Panduan Pengguna Amazon.

GuardDuty juga mendukung [Menggunakan VPC bersama dengan Runtime Monitoring](#). Ketika semua prasyarat dipertimbangkan untuk organisasi Anda dan Akun AWS, GuardDuty akan menggunakan VPC bersama untuk menerima acara runtime.

 Note

Tidak ada biaya tambahan untuk penggunaan titik akhir VPC.

- Seiring dengan titik akhir VPC, GuardDuty juga membuat grup keamanan baru. Aturan masuk (ingress) mengontrol lalu lintas yang diizinkan untuk mencapai sumber daya, yang terkait dengan grup keamanan. GuardDuty menambahkan aturan masuk yang cocok dengan rentang CIDR VPC untuk sumber daya Anda, dan juga menyesuaikannya saat rentang CIDR berubah. Untuk informasi selengkapnya, lihat [rentang VPC CIDR di Panduan](#) Pengguna Amazon VPC.

Kelola agen keamanan secara manual

Ada dua cara untuk mengelola agen keamanan untuk Amazon EC2 secara manual:

- Gunakan dokumen GuardDuty terkelola AWS Systems Manager untuk menginstal agen keamanan di EC2 instans Amazon Anda yang sudah dikelola SSM.

Setiap kali Anda meluncurkan EC2 instans Amazon baru, pastikan SSM diaktifkan.

- Gunakan skrip pengelola paket RPM (RPM) untuk menginstal agen keamanan di EC2 instans Amazon Anda, terlepas dari apakah mereka dikelola SSM atau tidak.

Langkah berikutnya

Untuk memulai konfigurasi Runtime Monitoring untuk memantau EC2 instans Amazon Anda, lihat [Prasyarat untuk dukungan instans Amazon EC2](#)

Bagaimana Runtime Monitoring bekerja dengan Fargate (hanya Amazon ECS)

Saat Anda mengaktifkan Runtime Monitoring, GuardDuty menjadi siap untuk mengkonsumsi peristiwa runtime dari tugas. Tugas-tugas ini berjalan dalam kluster Amazon ECS, yang pada gilirannya berjalan pada instance. AWS Fargate GuardDuty Untuk menerima acara runtime ini, Anda harus menggunakan agen keamanan khusus yang dikelola sepenuhnya.

Anda dapat mengizinkan GuardDuty untuk mengelola agen GuardDuty keamanan atas nama Anda, dengan menggunakan konfigurasi agen otomatis untuk AWS akun atau organisasi. GuardDuty akan mulai menyebarkan agen keamanan ke tugas Fargate baru yang diluncurkan di cluster Amazon ECS Anda. Daftar berikut menentukan apa yang diharapkan ketika Anda mengaktifkan agen GuardDuty keamanan.

Dampak memungkinkan agen GuardDuty keamanan

GuardDuty membuat titik akhir dan grup keamanan virtual private cloud (VPC)

- Saat Anda menerapkan agen GuardDuty keamanan, GuardDuty akan membuat titik akhir VPC tempat agen keamanan mengirimkan peristiwa runtime. GuardDuty

Seiring dengan titik akhir VPC, GuardDuty juga membuat grup keamanan baru. Aturan masuk (ingress) mengontrol lalu lintas yang diizinkan untuk mencapai sumber daya, yang terkait dengan grup keamanan. GuardDuty menambahkan aturan masuk yang cocok dengan rentang CIDR VPC untuk sumber daya Anda, dan juga menyesuaikannya saat rentang CIDR berubah. Untuk informasi selengkapnya, lihat [rentang VPC CIDR di Panduan Pengguna Amazon VPC](#).

- Bekerja dengan VPC terpusat dengan agen otomatis — Saat Anda GuardDuty menggunakan konfigurasi agen otomatis untuk jenis sumber daya GuardDuty, akan membuat titik akhir VPC atas nama Anda untuk semua VPCs Ini termasuk VPC terpusat dan bicara. VPCs GuardDuty tidak mendukung pembuatan titik akhir VPC hanya untuk VPC terpusat. Untuk informasi selengkapnya tentang cara kerja VPC terpusat, lihat Endpoint VPC [Antarmuka di Whitepaper - Membangun Infrastruktur Jaringan Multi-VPC AWS](#) yang Dapat Diskalakan dan Aman. AWS
- Tidak ada biaya tambahan untuk penggunaan titik akhir VPC.

GuardDuty menambahkan wadah sespan

Untuk tugas atau layanan Fargate baru yang mulai berjalan, GuardDuty kontainer (sespan) menempel pada setiap kontainer dalam tugas Amazon ECS Fargate. Agen GuardDuty keamanan

berjalan di dalam GuardDuty wadah terlampir. Ini GuardDuty membantu mengumpulkan peristiwa runtime dari setiap kontainer yang berjalan dalam tugas-tugas ini.

Gambar wadah GuardDuty sespan disimpan di Amazon Elastic Container Registry (Amazon ECR) Registry, dengan lapisan gambarnya disimpan di Amazon S3. Saat tugas Anda dimulai, perlu menarik gambar ini dari ECR. Tergantung pada konfigurasi jaringan Anda, ini mungkin memerlukan pengaturan khusus untuk memastikan akses ke ECR dan S3. Misalnya, jika Anda menggunakan grup keamanan dengan akses terbatas, Anda harus mengizinkan akses ke daftar awalan terkelola S3. Untuk informasi lebih lanjut tentang cara melakukan ini, lihat [Prasyarat untuk akses gambar kontainer](#).

Saat Anda memulai tugas Fargate, jika GuardDuty container (sespan) tidak dapat diluncurkan dalam keadaan sehat, Runtime Monitoring dirancang untuk tidak mencegah tugas berjalan.

Secara default, tugas Fargate tidak dapat diubah. GuardDuty tidak akan menyebarkan sespan saat tugas sudah dalam keadaan berjalan. Jika Anda ingin memantau wadah dalam tugas yang sudah berjalan, Anda dapat menghentikan tugas dan memulainya lagi.

Pendekatan untuk mengelola agen GuardDuty keamanan di sumber daya Amazon ECS-Fargate

Runtime Monitoring memberi Anda opsi untuk mendeteksi potensi ancaman keamanan pada semua kluster Amazon ECS (tingkat akun) atau cluster selektif (tingkat klaster) di akun Anda. Saat Anda mengaktifkan konfigurasi agen Otomatis untuk setiap tugas Amazon ECS Fargate yang akan berjalan GuardDuty, akan menambahkan wadah sespan untuk setiap beban kerja kontainer dalam tugas tersebut. Agen GuardDuty keamanan akan dikerahkan ke wadah sespan ini. Beginilah cara GuardDuty mendapatkan visibilitas ke dalam perilaku runtime container di dalam tugas Amazon ECS.

Runtime Monitoring mendukung pengelolaan agen keamanan untuk cluster Amazon ECS (AWS Fargate) Anda hanya melalui GuardDuty. Tidak ada dukungan untuk mengelola agen keamanan secara manual di cluster Amazon ECS.

Sebelum mengonfigurasi akun, periksa apakah Anda ingin memantau perilaku runtime semua container yang termasuk dalam tugas Amazon ECS, atau menyertakan atau mengecualikan sumber daya tertentu. Pertimbangkan pendekatan berikut.

Monitor untuk semua cluster Amazon ECS

Pendekatan ini akan membantu Anda mendeteksi potensi ancaman keamanan di tingkat akun. Gunakan pendekatan ini saat Anda GuardDuty ingin mendeteksi potensi ancaman keamanan untuk semua kluster Amazon ECS milik akun Anda.

Kecualikan cluster Amazon ECS tertentu

Gunakan pendekatan ini saat Anda GuardDuty ingin mendeteksi potensi ancaman keamanan untuk sebagian besar kluster Amazon ECS di AWS lingkungan Anda, tetapi kecualikan beberapa kluster. Pendekatan ini membantu Anda memantau perilaku runtime container dalam tugas Amazon ECS Anda di tingkat cluster. Misalnya, jumlah cluster Amazon ECS milik akun Anda adalah 1000. Namun, Anda hanya ingin memantau 930 cluster Amazon ECS.

Pendekatan ini mengharuskan Anda untuk menambahkan GuardDuty tag yang telah ditentukan sebelumnya ke cluster Amazon ECS yang tidak ingin Anda pantau. Untuk informasi selengkapnya, lihat [Mengelola agen keamanan otomatis untuk Fargate \(hanya Amazon ECS\)](#).

Sertakan kluster Amazon ECS tertentu

Gunakan pendekatan ini saat Anda GuardDuty ingin mendeteksi potensi ancaman keamanan untuk beberapa kluster Amazon ECS. Pendekatan ini membantu Anda memantau perilaku runtime container dalam tugas Amazon ECS Anda di tingkat cluster. Misalnya, jumlah cluster Amazon ECS milik akun Anda adalah 1000. Namun, Anda ingin memantau 230 cluster saja.

Pendekatan ini mengharuskan Anda untuk menambahkan GuardDuty tag yang telah ditentukan sebelumnya ke cluster Amazon ECS yang ingin Anda pantau. Untuk informasi selengkapnya, lihat [Mengelola agen keamanan otomatis untuk Fargate \(hanya Amazon ECS\)](#).

Setelah Anda mengaktifkan Runtime Monitoring

Setelah mengaktifkan Runtime Monitoring dan menginstal agen GuardDuty keamanan di akun mandiri atau beberapa akun anggota, Anda dapat mengambil langkah-langkah berikut untuk memastikan bahwa pengaturan rencana perlindungan berfungsi seperti yang diharapkan, dan memantau berapa banyak memori dan CPU yang digunakan agen GuardDuty keamanan.

Menilai cakupan runtime

GuardDuty merekomendasikan Anda untuk terus menilai status cakupan sumber daya tempat Anda menggunakan agen keamanan. Status cakupan bisa sehat atau tidak sehat. Status cakupan

Sehat menunjukkan GuardDuty bahwa menerima peristiwa runtime dari sumber daya yang sesuai ketika ada aktivitas tingkat sistem operasi.

Ketika status cakupan menjadi Sehat untuk sumber daya, GuardDuty dapat menerima peristiwa runtime dan menganalisisnya untuk deteksi ancaman. Saat GuardDuty mendeteksi potensi ancaman keamanan dalam tugas atau aplikasi yang berjalan di beban kerja dan instance container Anda, hasilkan. GuardDuty [GuardDuty Jenis penemuan Runtime Monitoring](#)

Anda juga dapat mengonfigurasi Amazon EventBridge (EventBridge) untuk menerima pemberitahuan ketika status cakupan berubah dari Tidak Sehat menjadi Sehat dan sebaliknya. Untuk informasi selengkapnya, lihat [Meninjau statistik cakupan runtime dan masalah pemecahan masalah](#).

Mengatur CPU dan pemantauan memori untuk agen GuardDuty keamanan

Setelah Anda menilai bahwa status cakupan ditampilkan sebagai Sehat, Anda dapat mengevaluasi kinerja agen keamanan untuk jenis sumber daya Anda. Untuk kluster Amazon EKS yang memiliki rilis agen keamanan v1.5 atau lebih tinggi, GuardDuty mendukung konfigurasi parameter agen keamanan (add-on). Untuk informasi selengkapnya, lihat [Menyiapkan CPU dan pemantauan memori](#).

GuardDuty Mendeteksi potensi ancaman

Saat GuardDuty mulai menerima peristiwa runtime untuk sumber daya Anda, ia mulai menganalisis peristiwa tersebut. Saat GuardDuty mendeteksi potensi ancaman keamanan di salah satu EC2 instans Amazon Anda, kluster Amazon ECS, atau kluster Amazon EKS, itu menghasilkan satu atau lebih. [GuardDuty Jenis penemuan Runtime Monitoring](#) Anda dapat mengakses detail temuan untuk melihat detail sumber daya yang terkena dampak.

Bagaimana cara kerja uji coba gratis 30 hari di Runtime Monitoring

Periode uji coba gratis 30 hari bekerja secara berbeda untuk GuardDuty akun baru dan akun yang sudah ada yang telah mengaktifkan EKS Runtime Monitoring sebelum kemampuan Runtime Monitoring diperluas ke EC2 instans Amazon dan (hanya AWS Fargate Amazon ECS).

Saya menggunakan masa GuardDuty percobaan atau saya tidak pernah mengaktifkan EKS Runtime Monitoring

Daftar berikut menjelaskan cara kerja periode uji coba gratis 30 hari jika Anda menggunakan periode uji coba GuardDuty 30 hari atau belum pernah mengaktifkan EKS Runtime Monitoring:

- Saat Anda mengaktifkan GuardDuty untuk pertama kalinya, Runtime Monitoring dan EKS Runtime Monitoring tidak akan diaktifkan secara default.

Saat Anda mengaktifkan Runtime Monitoring untuk akun atau organisasi Anda, pastikan juga mengonfigurasi agen GuardDuty keamanan untuk sumber daya yang ingin Anda pantau untuk deteksi ancaman. Misalnya, jika Anda ingin menggunakan Runtime Monitoring untuk EC2 instans Amazon Anda, maka setelah Anda mengaktifkan Runtime Monitoring, Anda juga harus mengonfigurasi agen keamanan untuk Amazon. EC2 Anda dapat memilih untuk melakukan ini baik secara manual atau otomatis melalui GuardDuty.

- Paket perlindungan Runtime Monitoring diaktifkan di tingkat akun. Periode uji coba gratis 30 hari bekerja di tingkat sumber daya. Setelah agen GuardDuty keamanan diterapkan ke jenis sumber daya tertentu, uji coba gratis 30 hari dimulai saat GuardDuty menerima peristiwa runtime pertama yang terkait dengan jenis sumber daya ini. Misalnya, Anda telah menerapkan GuardDuty agen di tingkat sumber daya (untuk EC2 instans Amazon, cluster Amazon ECS, dan kluster Amazon EKS). Saat GuardDuty menerima acara runtime pertama untuk EC2 instans Amazon, uji coba gratis 30 hari hanya akan dimulai untuk Amazon EC2 .
- Bila Anda hanya ingin mengaktifkan EKS Runtime Monitoring — Saat Anda mengaktifkan GuardDuty untuk pertama kalinya, EKS Runtime Monitoring tidak diaktifkan secara default (setelah rilis Runtime Monitoring). Anda harus mengaktifkan EKS Runtime Monitoring. Untuk menggunakannya secara optimal, pastikan Anda mengelola agen GuardDuty keamanan secara manual atau mengaktifkan konfigurasi agen otomatis sehingga GuardDuty mengelola agen atas nama Anda. Periode uji coba gratis 30 hari untuk EKS Runtime Monitoring dimulai saat GuardDuty menerima acara runtime pertamanya untuk sumber daya Amazon EKS.

Saya mengaktifkan EKS Runtime Monitoring sebelum peluncuran Runtime Monitoring

Gunakan bagian ini hanya ketika EKS Runtime Monitoring diaktifkan untuk Anda Akun AWS, dan sekarang Anda ingin bermigrasi ke Runtime Monitoring.

Daftar berikut mencakup skenario yang mungkin berlaku untuk kasus penggunaan Anda untuk mengaktifkan Runtime Monitoring:

- Untuk GuardDuty akun yang sudah ada yang mengaktifkan paket perlindungan Pemantauan Runtime EKS dan menggunakan pengalaman GuardDuty konsol untuk menggunakan paket perlindungan ini — Dengan pengumuman Runtime Monitoring, pengalaman konsol Pemantauan Runtime EKS kini telah dikonsolidasikan ke dalam Runtime Monitoring. Konfigurasi Anda yang ada

untuk EKS Runtime Monitoring tetap sama. Anda dapat terus menggunakan dukungan API/CLI untuk melakukan operasi yang terkait dengan EKS Runtime Monitoring.

- Untuk menggunakan EKS Runtime Monitoring sebagai bagian dari Runtime Monitoring, Anda perlu mengonfigurasi Runtime Monitoring untuk akun atau organisasi Anda. Untuk menjaga konfigurasi yang sama untuk Runtime Monitoring, lihat [Migrasi dari EKS Runtime Monitoring ke Runtime Monitoring](#). Namun, ini tidak akan memengaruhi uji coba gratis 30 hari Anda untuk sumber daya Amazon EKS.
- Paket perlindungan Runtime Monitoring diaktifkan pada tingkat akun per Wilayah. Setelah agen GuardDuty keamanan diterapkan ke salah satu jenis sumber daya yang ditentukan (EC2 instans Amazon dan kluster Amazon ECS), uji coba gratis 30 hari dimulai saat GuardDuty menerima peristiwa runtime pertama yang terkait dengan sumber daya. Ada uji coba gratis 30 hari yang terkait dengan setiap jenis sumber daya.

Misalnya, setelah mengaktifkan Runtime Monitoring, Anda memilih untuk menerapkan GuardDuty agen hanya di EC2 instans Amazon, uji coba gratis 30 hari untuk sumber daya ini hanya akan dimulai saat GuardDuty menerima peristiwa runtime pertamanya untuk instans Amazon. EC2 Kemudian, saat Anda menerapkan GuardDuty agen untuk Fargate (hanya Amazon ECS), uji coba gratis 30 hari untuk sumber daya ini hanya akan dimulai GuardDuty saat menerima acara runtime pertamanya untuk cluster Amazon ECS. Mengingat Anda sudah mengaktifkan EKS Runtime Monitoring untuk akun Anda, GuardDuty tidak mengatur ulang uji coba gratis 30 hari untuk sumber daya Amazon EKS.

Prasyarat untuk mengaktifkan Runtime Monitoring

Untuk mengaktifkan Runtime Monitoring dan mengelola agen GuardDuty keamanan, Anda harus memenuhi prasyarat untuk setiap jenis sumber daya yang ingin Anda pantau untuk deteksi ancaman. Setiap jenis sumber daya memiliki prasyarat yang berbeda. Misalnya, GuardDuty mendukung distribusi OS yang berbeda berdasarkan jenis sumber daya.

Bila Anda hanya ingin memantau EC2 sumber daya Amazon, Anda akan mengikuti prasyarat untuk instans Amazon. EC2 Jika di lain waktu, Anda memilih untuk memantau sumber daya Amazon EKS, Anda harus mengikuti prasyarat khusus untuk kluster Amazon EKS.

Bagian berikut mencakup prasyarat berdasarkan jenis sumber daya.

Daftar Isi

- [Prasyarat untuk dukungan instans Amazon EC2](#)

- [Prasyarat untuk dukungan \(khusus AWS Fargate Amazon ECS\)](#)
- [Prasyarat untuk dukungan cluster Amazon EKS](#)

Prasyarat untuk dukungan instans Amazon EC2

Bagian ini mencakup prasyarat untuk memantau perilaku runtime instans Amazon Anda. EC2 Setelah prasyarat ini terpenuhi, lihat. [Mengaktifkan GuardDuty Runtime Monitoring](#)

Topik

- [Membuat EC2 instans SSM dikelola \(hanya untuk konfigurasi agen otomatis\)](#)
- [Validasi persyaratan arsitektur](#)
- [Memvalidasi kebijakan kontrol layanan organisasi Anda di lingkungan multi-akun](#)
- [Saat menggunakan konfigurasi agen otomatis](#)
- [CPU dan batas memori untuk GuardDuty agen](#)
- [Langkah berikutnya](#)

Membuat EC2 instans SSM dikelola (hanya untuk konfigurasi agen otomatis)

GuardDuty menggunakan AWS Systems Manager (SSM) untuk secara otomatis menyebarkan, menginstal, dan mengelola agen keamanan pada instans Anda. Jika Anda berencana untuk menginstal dan mengelola GuardDuty agen secara manual, SSM tidak diperlukan.

Untuk mengelola EC2 instans Amazon dengan Systems Manager, lihat [Menyiapkan Systems Manager untuk EC2 instans Amazon](#) di AWS Systems Manager Panduan Pengguna.

Validasi persyaratan arsitektur

Arsitektur distribusi OS Anda dapat memengaruhi perilaku agen GuardDuty keamanan. Anda harus memenuhi persyaratan berikut sebelum menggunakan Runtime Monitoring untuk EC2 instans Amazon:

- Dukungan kernel termasuk BPF, Tracepoints dan Kprobe. Untuk arsitektur CPU, Runtime Monitoring mendukung AMD64 (x64) dan ARM64 (Graviton2 dan di atasnya). ¹

Tabel berikut menunjukkan distribusi OS yang telah diverifikasi untuk mendukung agen GuardDuty keamanan untuk EC2 instans Amazon.

Distribusi OS ²	Versi kernel ³
Amazon Linux 2	5.4 ⁴ , 5.10, 5.15 ⁴
Amazon Linux 2023	5.4 ⁴ , 5.10, 5.15 ⁴ , 6.1, 6.5, 6.8, 6.12
Ubuntu 20.04 dan Ubuntu 22.04	5.4 ⁴ , 5.10, 5.15 ⁴ , 6.1, 6.5, 6.8
Ubuntu 24.04	6.8
Debian 11 dan Debian 12	5.4 ⁴ , 5.10, 5.15 ⁴ , 6.1, 6.5, 6.8
RedHat 9.4	5.14
Fedora 34.0	5.11, 5.17
Fedora 40	6.8
Fedora 41	6.12
CentOS Aliran 9	5.14
Oracle Linux 8.9	5.15
Oracle Linux 9.3	5.15
Rocky Linux 9.5	5.14

1. Runtime Monitoring untuk EC2 sumber daya Amazon tidak mendukung instans Graviton generasi pertama seperti jenis instans A1.
2. Support untuk berbagai sistem operasi - GuardDuty telah memverifikasi dukungan Runtime Monitoring untuk distribusi operasi yang tercantum dalam tabel sebelumnya. Sementara agen GuardDuty keamanan dapat berjalan pada sistem operasi yang tidak tercantum dalam tabel sebelumnya, GuardDuty tim tidak dapat menjamin nilai keamanan yang diharapkan.
- 3.

Untuk versi kernel apa pun, Anda harus menyetel `CONFIG_DEBUG_INFO_BTF` flag ke `y` (artinya `true`). Ini diperlukan agar agen GuardDuty keamanan dapat berjalan seperti yang diharapkan.

4. Untuk kernel versi 5.10 dan sebelumnya, agen GuardDuty keamanan menggunakan memori terkunci di RAM (`RLIMIT_MEMLOCK`) berfungsi seperti yang diharapkan. Jika `RLIMIT_MEMLOCK` nilai sistem Anda disetel terlalu rendah, GuardDuty merekomendasikan pengaturan batas keras dan lunak setidaknya 32 MB. Untuk informasi tentang memverifikasi dan memodifikasi `RLIMIT_MEMLOCK` nilai default, lihat [Melihat dan memperbarui `RLIMIT\_MEMLOCK` nilai](#).

- Persyaratan tambahan - Hanya jika Anda memiliki Amazon ECS/Amazon EC2

Untuk Amazon ECS/Amazon EC2, kami menyarankan Anda menggunakan Amazon ECS terbaru yang dioptimalkan AMIs (tertanggal 29 September 2023 atau lebih baru), atau menggunakan agen Amazon ECS versi v1.77.0.

Melihat dan memperbarui **RLIMIT_MEMLOCK** nilai

Ketika `RLIMIT_MEMLOCK` batas sistem Anda ditetapkan terlalu rendah, agen GuardDuty keamanan mungkin tidak berfungsi seperti yang dirancang. GuardDuty merekomendasikan bahwa batas keras dan lunak harus setidaknya 32 MB. Jika Anda tidak memperbarui batas, tidak GuardDuty akan dapat memantau peristiwa runtime untuk sumber daya Anda. Ketika `RLIMIT_MEMLOCK` berada di atas batas minimum yang dinyatakan, itu menjadi opsional bagi Anda untuk memperbarui batas ini.

Anda dapat memodifikasi `RLIMIT_MEMLOCK` nilai default baik sebelum atau setelah menginstal agen GuardDuty keamanan.

Untuk melihat **RLIMIT_MEMLOCK** nilai

1. Jalankan `ps aux | grep guardduty`. Ini akan menampilkan ID proses (`pid`).
2. Salin ID proses (`pid`) dari output dari perintah sebelumnya.
3. Jalankan `grep "Max locked memory" /proc/pid/limits` setelah mengganti `pid` dengan ID proses yang disalin dari langkah sebelumnya.

Ini akan menampilkan memori terkunci maksimum untuk menjalankan agen GuardDuty keamanan.

Untuk memperbarui **RLIMIT_MEMLOCK** nilai

1. Jika `/etc/systemd/system.conf.d/NUMBER-limits.conf` file tersebut ada, maka komentari baris `DefaultLimitMEMLOCK` dari file ini. File ini menetapkan default `RLIMIT_MEMLOCK` dengan prioritas tinggi, yang menimpa pengaturan Anda dalam `/etc/systemd/system.conf` file.
2. Buka `/etc/systemd/system.conf` file dan hapus komentar pada baris yang ada `#DefaultLimitMEMLOCK=`.
3. Perbarui nilai default dengan memberikan `RLIMIT_MEMLOCK` batas keras dan lunak setidaknya 32MB. Pembaruan akan terlihat seperti ini: `DefaultLimitMEMLOCK=32M:32M`. Formatnya adalah `soft-limit:hard-limit`.
4. Jalankan `sudo reboot`.

Memvalidasi kebijakan kontrol layanan organisasi Anda di lingkungan multi-akun

Jika Anda telah menyiapkan kebijakan kontrol layanan (SCP) untuk mengelola izin di organisasi Anda, validasi batas izin yang memungkinkan tindakan tersebut. `guardduty:SendSecurityTelemetry` Hal ini diperlukan GuardDuty untuk mendukung Runtime Monitoring di berbagai jenis sumber daya.

Jika Anda adalah akun anggota, sambungkan dengan administrator yang didelegasikan terkait. Untuk informasi tentang mengelola SCPs organisasi Anda, lihat [Kebijakan kontrol layanan \(SCPs\)](#).

Saat menggunakan konfigurasi agen otomatis

Untuk [Gunakan konfigurasi agen otomatis \(disarankan\)](#), Anda Akun AWS harus memenuhi prasyarat berikut:

- Saat menggunakan tag inklusi dengan konfigurasi agen otomatis, GuardDuty untuk membuat asosiasi SSM untuk instance baru, pastikan instans baru dikelola SSM dan muncul di bawah Fleet Manager di <https://console.aws.amazon.com/systems-manager/konsol>.
- Saat menggunakan tag pengecualian dengan konfigurasi agen otomatis:
 - Tambahkan `false` tag `GuardDutyManaged`: sebelum mengonfigurasi agen GuardDuty otomatis untuk akun Anda.

Pastikan Anda menambahkan tag pengecualian ke EC2 instans Amazon sebelum meluncurkannya. Setelah Anda mengaktifkan konfigurasi agen otomatis untuk Amazon EC2,

EC2 instans apa pun yang diluncurkan tanpa tag pengecualian akan tercakup dalam konfigurasi agen GuardDuty otomatis.

- Aktifkan Izinkan tag dalam pengaturan metadata untuk instance Anda. Pengaturan ini diperlukan karena GuardDuty perlu membaca tag pengecualian dari layanan metadata instance (IMDS) untuk menentukan apakah harus mengecualikan instance dari instalasi agen. Untuk informasi selengkapnya, lihat [Mengaktifkan akses ke tag dalam metadata instans](#) di EC2 Panduan Pengguna Amazon.

CPU dan batas memori untuk GuardDuty agen

Batas CPU

Batas CPU maksimum untuk agen GuardDuty keamanan yang terkait dengan EC2 instans Amazon adalah 10 persen dari total inti vCPU. Misalnya, jika EC2 instans Anda memiliki 4 core vCPU, maka agen keamanan dapat menggunakan maksimum 40 persen dari total 400 persen yang tersedia.

Batas memori

Dari memori yang terkait dengan EC2 instans Amazon Anda, ada memori terbatas yang dapat digunakan agen GuardDuty keamanan.

Tabel berikut menunjukkan batas memori.

Memori EC2 instance Amazon	Memori maksimum untuk GuardDuty agen
Kurang dari 8 GB	128 MB
Kurang dari 32 GB	270 MB
Lebih dari atau sama dengan 32 GB	1 GB

Langkah berikutnya

Langkah selanjutnya adalah mengkonfigurasi Runtime Monitoring dan juga mengelola agen keamanan (secara otomatis atau manual).

Prasyarat untuk dukungan (khusus AWS Fargate Amazon ECS)

Bagian ini mencakup prasyarat untuk memantau perilaku runtime sumber daya Fargate-Amazon ECS Anda. Setelah prasyarat ini terpenuhi, lihat [Mengaktifkan GuardDuty Runtime Monitoring](#)

Topik

- [Memvalidasi persyaratan arsitektur](#)
- [Prasyarat untuk akses gambar kontainer](#)
- [Memvalidasi kebijakan kontrol layanan organisasi Anda di lingkungan multi-akun](#)
- [Memvalidasi izin peran dan batas izin kebijakan](#)
- [Batas CPU dan memori](#)

Memvalidasi persyaratan arsitektur

Platform yang Anda gunakan dapat memengaruhi cara agen GuardDuty keamanan mendukung GuardDuty dalam menerima peristiwa runtime dari kluster Amazon ECS Anda. Anda harus memvalidasi bahwa Anda menggunakan salah satu platform terverifikasi.

Pertimbangan awal:

AWS Fargate Platform untuk cluster Amazon ECS Anda harus Linux. Versi platform yang sesuai harus setidaknya 1.4.0, atau LATEST. Untuk informasi selengkapnya tentang versi platform, lihat [versi platform Linux](#) di Panduan Pengembang Layanan Amazon Elastic Container.

Versi platform Windows belum didukung.

Platform terverifikasi

Distribusi OS dan arsitektur CPU berdampak pada dukungan yang diberikan oleh agen GuardDuty keamanan. Tabel berikut menunjukkan konfigurasi terverifikasi untuk menerapkan agen GuardDuty keamanan dan mengonfigurasi Runtime Monitoring.

Distribusi OS ¹	Dukungan kernel	Arsitektur CPU x64 () AMD64	Arsitektur CPU Graviton () ARM64
Linux	eBPF, Tracepoints, Kprobe	Didukung	Didukung

¹ Support untuk berbagai sistem operasi - GuardDuty telah memverifikasi dukungan Runtime Monitoring untuk distribusi operasi yang tercantum dalam tabel sebelumnya. Sementara agen GuardDuty keamanan dapat berjalan pada sistem operasi yang tidak tercantum dalam tabel sebelumnya, GuardDuty tim tidak dapat menjamin nilai keamanan yang diharapkan.

Prasyarat untuk akses gambar kontainer

Prasyarat berikut membantu Anda mengakses gambar GuardDuty kontainer sespan dari repositori Amazon ECR.

Persyaratan izin

Peran eksekusi tugas memerlukan izin Amazon Elastic Container Registry (Amazon ECR) tertentu untuk mengunduh GuardDuty gambar kontainer agen keamanan:

```
...  
    "ecr:GetAuthorizationToken",  
    "ecr:BatchCheckLayerAvailability",  
    "ecr:GetDownloadUrlForLayer",  
    "ecr:BatchGetImage",  
...
```

Untuk lebih membatasi izin Amazon ECR, Anda dapat menambahkan URI repositori Amazon ECR yang menampung GuardDuty agen keamanan untuk (AWS Fargate hanya Amazon ECS). Untuk informasi selengkapnya, lihat [Agen hosting repositori Amazon ECR GuardDuty](#).

Anda dapat menggunakan kebijakan ECSTask ExecutionRolePolicy terkelola [Amazon](#) atau menambahkan izin di atas ke TaskExecutionRole kebijakan Anda.

Konfigurasi definisi tugas

Saat membuat atau memperbarui layanan Amazon ECS, Anda perlu memberikan informasi subnet dalam definisi tugas Anda:

Menjalankan [CreateService](#) dan [UpdateService](#) APIs di Amazon Elastic Container Service API Reference mengharuskan Anda untuk meneruskan informasi subnet. Untuk informasi selengkapnya, lihat [definisi tugas Amazon ECS](#) di Panduan Pengembang Layanan Kontainer Elastis Amazon.

Persyaratan konektivitas jaringan

Anda harus memastikan konektivitas jaringan untuk mengunduh gambar GuardDuty kontainer dari Amazon ECR. Persyaratan ini khusus untuk GuardDuty karena menggunakan Amazon ECR untuk

meng-host agen keamanannya. Bergantung pada konfigurasi jaringan Anda, Anda perlu menerapkan salah satu opsi berikut:

Opsi 1 - Menggunakan akses jaringan publik (jika tersedia)

Jika tugas Fargate Anda berjalan di subnet dengan akses internet keluar, tidak diperlukan konfigurasi jaringan tambahan.

Opsi 2 - Menggunakan titik akhir Amazon VPC (untuk subnet pribadi)

Jika tugas Fargate Anda berjalan di subnet pribadi tanpa akses internet, Anda harus mengonfigurasi titik akhir VPC untuk ECR guna memastikan bahwa URI repositori ECR yang menampung agen keamanan dapat diakses jaringan. GuardDuty Tanpa titik akhir ini, tugas dalam subnet pribadi tidak dapat mengunduh gambar GuardDuty kontainer.

Untuk petunjuk penyiapan titik akhir VPC, lihat Membuat titik akhir [VPC untuk Amazon ECR di Panduan Pengguna Amazon Elastic Container Registry](#).

Untuk informasi tentang mengaktifkan Fargate mengunduh GuardDuty penampung, lihat [Menggunakan gambar Amazon ECR dengan Amazon ECS di Panduan Pengguna Amazon Elastic Container Registry](#).

Konfigurasi grup keamanan

Gambar GuardDuty kontainer ada di Amazon ECR dan memerlukan akses Amazon S3. Persyaratan ini khusus untuk mengunduh gambar kontainer dari Amazon ECR. Untuk tugas dengan akses jaringan terbatas, Anda harus mengonfigurasi grup keamanan Anda untuk mengizinkan akses ke S3.

Tambahkan aturan keluar di grup keamanan Anda yang memungkinkan lalu lintas ke [daftar awalan terkelola S3 \(p1-xxxxxxx\) pada](#) port 443. Untuk menambahkan aturan keluar, lihat [Mengonfigurasi aturan grup keamanan](#) di Panduan Pengguna Amazon VPC.

Untuk melihat daftar awalan AWS-managed di konsol atau mendeskripsikannya dengan menggunakan AWS Command Line Interface (AWS CLI), lihat daftar [awalan AWS-managed di Panduan Pengguna Amazon VPC](#).

Memvalidasi kebijakan kontrol layanan organisasi Anda di lingkungan multi-akun

Bagian ini menjelaskan cara memvalidasi setelan kebijakan kontrol layanan (SCP) Anda untuk memastikan Runtime Monitoring berfungsi seperti yang diharapkan di seluruh organisasi Anda.

Jika Anda telah menyiapkan satu atau beberapa kebijakan kontrol layanan untuk mengelola izin di organisasi, Anda harus memvalidasi bahwa kebijakan tersebut tidak menolak tindakan tersebut `guardduty:SendSecurityTelemetry`. Untuk informasi tentang cara SCPs kerja, lihat [evaluasi SCP](#) di Panduan AWS Organizations Pengguna.

Jika Anda adalah akun anggota, sambungkan dengan administrator yang didelegasikan terkait. Untuk informasi tentang mengelola SCPs organisasi Anda, lihat [Kebijakan kontrol layanan \(SCPs\)](#) di Panduan AWS Organizations Pengguna.

Lakukan langkah-langkah berikut untuk semua SCPs yang telah Anda atur di lingkungan multi-akun Anda:

Untuk memvalidasi **`guardduty:SendSecurityTelemetry`** tidak ditolak di SCP

1. Masuk ke konsol Organizations di <https://console.aws.amazon.com/organizations/>. Anda harus masuk sebagai peran IAM, atau masuk sebagai pengguna root ([tidak disarankan](#)) di akun manajemen organisasi.
2. Pada panel navigasi sebelah kiri, pilih Kebijakan. Kemudian, di bawah Jenis kebijakan yang didukung, pilih Kebijakan kontrol layanan.
3. Pada halaman Kebijakan kontrol layanan, pilih nama kebijakan yang ingin Anda validasi.
4. Pada halaman detail kebijakan, lihat Konten kebijakan ini. Pastikan bahwa itu tidak menyangkal `guardduty:SendSecurityTelemetry` tindakan.

Kebijakan SCP berikut adalah contoh untuk tidak menyangkal tindakan:
`guardduty:SendSecurityTelemetry`

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        ...,
        ...,
        "guardduty:SendSecurityTelemetry"
      ],
      "Resource": "*"
    }
  ]
}
```

Jika kebijakan Anda menolak tindakan ini, Anda harus memperbarui kebijakan tersebut. Untuk informasi selengkapnya, lihat [Memperbarui kebijakan kontrol layanan \(SCP\)](#) di Panduan AWS Organizations Pengguna.

Memvalidasi izin peran dan batas izin kebijakan

Gunakan langkah-langkah berikut untuk memvalidasi bahwa batas izin yang terkait dengan peran dan kebijakannya tidak membatasi tindakan. `guardduty:SendSecurityTelemetry`

Untuk melihat batas izin untuk peran dan kebijakannya

1. Masuk ke AWS Management Console dan buka konsol IAM di <https://console.aws.amazon.com/iam/>.
2. Di panel navigasi kiri, di bawah Manajemen akses, pilih Peran.
3. Pada halaman Peran, pilih peran *TaskExecutionRole* yang mungkin telah Anda buat.
4. Pada halaman peran yang dipilih, di bawah tab Izin, perluas nama kebijakan yang terkait dengan peran ini. Kemudian, validasi bahwa kebijakan ini tidak membatasi `guardduty:SendSecurityTelemetry`.
5. Jika batas izin ditetapkan, maka perluas bagian ini. Kemudian, perluas setiap kebijakan untuk meninjau bahwa itu tidak membatasi `guardduty:SendSecurityTelemetry` tindakan. Kebijakan harus tampak mirip dengan ini [Example SCP policy](#).

Sesuai kebutuhan, lakukan salah satu tindakan berikut:

- Untuk mengubah kebijakan, pilih Edit. Pada halaman Ubah izin untuk kebijakan ini, perbarui kebijakan di editor Kebijakan. Pastikan bahwa skema JSON tetap valid. Lalu, pilih Selanjutnya. Kemudian, Anda dapat meninjau dan menyimpan perubahan.
- Untuk mengubah batas izin ini dan memilih batas lain, pilih Ubah batas.
- Untuk menghapus batas izin ini, pilih Hapus batas.

Untuk informasi tentang mengelola kebijakan, lihat [Kebijakan dan izin AWS Identity and Access Management di](#) Panduan Pengguna IAM.

Batas CPU dan memori

Dalam definisi tugas Fargate, Anda harus menentukan CPU dan nilai memori di tingkat tugas. Tabel berikut menunjukkan kombinasi yang valid dari CPU tingkat tugas dan nilai memori, dan batas memori maksimum agen GuardDuty keamanan yang sesuai untuk wadah. GuardDuty

Nilai CPU	Nilai memori	GuardDuty batas memori maksimum agen
256 (.25 vCPU)	512 MiB, 1 GB, 2GB	128 MB
512 (.5 vCPU)	1 GB, 2 GB, 3 GB, 4 GB	
1024 (1 vCPU)	2 GB, 3 GB, 4 GB	
	5 GB, 6 GB, 7 GB, 8 GB	
2048 (2 vCPU)	Antara 4 GB dan 16 GB dalam peningkatan 1 GB	
4096 (4 vCPU)	Antara 8 GB dan 20 GB dalam peningkatan 1 GB	
8192 (8 vCPU)	Antara 16 GB dan 28 GB dalam peningkatan 4 GB	270 MB
	Antara 32 GB dan 60 GB dalam peningkatan 4 GB	512 MB
16384 (16 vCPU)	Antara 32 GB dan 120 GB dalam peningkatan 8 GB	1 GB

Setelah mengaktifkan Runtime Monitoring dan menilai bahwa status cakupan kluster Anda Sehat, Anda dapat menyiapkan dan melihat metrik wawasan Container. Untuk informasi selengkapnya, lihat [Menyiapkan pemantauan di Amazon ECS cluster](#).

Langkah selanjutnya adalah mengkonfigurasi Runtime Monitoring dan juga mengkonfigurasi agen keamanan.

Prasyarat untuk dukungan cluster Amazon EKS

Bagian ini mencakup prasyarat untuk memantau perilaku runtime sumber daya Amazon EKS Anda. Prasyarat ini sangat penting bagi GuardDuty agen untuk berfungsi seperti yang diharapkan. Setelah prasyarat ini terpenuhi, lihat [Mengaktifkan GuardDuty Runtime Monitoring](#) untuk mulai memantau sumber daya Anda.

Dukungan untuk fitur Amazon EKS

Runtime Monitoring mendukung kluster Amazon EKS yang berjalan di EC2 instans Amazon dan Mode Otomatis Amazon EKS.

Runtime Monitoring tidak mendukung kluster Amazon EKS dengan Amazon EKS Hybrid Nodes, dan yang berjalan. AWS Fargate

Untuk informasi tentang fitur Amazon EKS ini, lihat [Apa itu Amazon EKS?](#) di Panduan Pengguna Amazon EKS.

Memvalidasi persyaratan arsitektur

Platform yang Anda gunakan dapat memengaruhi cara agen GuardDuty keamanan mendukung GuardDuty dalam menerima peristiwa runtime dari kluster EKS Anda. Anda harus memvalidasi bahwa Anda menggunakan salah satu platform terverifikasi. Jika Anda mengelola GuardDuty agen secara manual, pastikan bahwa versi Kubernetes mendukung versi GuardDuty agen yang sedang digunakan.

Platform terverifikasi

Distribusi OS, versi kernel, dan arsitektur CPU memengaruhi dukungan yang diberikan oleh agen GuardDuty keamanan. Dukungan kernel termasuk BPF, Tracepoints dan Kprobe. Untuk arsitektur CPU, Runtime Monitoring mendukung AMD64 (x64) dan ARM64 (Graviton2 dan di atasnya). ¹

Tabel berikut menunjukkan konfigurasi terverifikasi untuk menerapkan agen GuardDuty keamanan dan mengonfigurasi EKS Runtime Monitoring.

Distribusi OS ²	Versi kernel ³	Versi Kubernetes yang didukung
Bottlerocket	5.4, 5.10, 5.15, 6.1 ⁴	v1.23 - v1.32

Distribusi OS ²	Versi kernel ³	Versi Kubernetes yang didukung
Ubuntu	5.4, 5.10, 5.15, 6.1 ⁴	v1.21 - v1.32
Amazon Linux 2	5.4, 5.10, 5.15, 6.1 ⁴	v1.21 - v1.32
Amazon Linux 2023 ⁵	5.4, 5.10, 5.15, 6.1 ⁴	v1.21 - v1.32
RedHat 9.4	5.14 ⁴	v1.21 - v1.32
Fedora 34.0	5.11, 5,.	v1.21 - v1.32
CentOS Aliran 9	5.14	v1.21 - v1.32

1. Runtime Monitoring untuk kluster Amazon EKS tidak mendukung instans Graviton generasi pertama seperti tipe instans A1.
2. Support untuk berbagai sistem operasi - GuardDuty telah memverifikasi dukungan Runtime Monitoring untuk distribusi operasi yang tercantum dalam tabel sebelumnya. Sementara agen GuardDuty keamanan dapat berjalan pada sistem operasi yang tidak tercantum dalam tabel sebelumnya, GuardDuty tim tidak dapat menjamin nilai keamanan yang diharapkan.
3. Untuk versi kernel apa pun, Anda harus menyetel CONFIG_DEBUG_INFO_BTF flag ke y (artinya true). Ini diperlukan agar agen GuardDuty keamanan dapat berjalan seperti yang diharapkan.
4. Saat ini, dengan versi Kernel 6.1, tidak GuardDuty dapat menghasilkan [GuardDuty Jenis penemuan Runtime Monitoring](#) yang terkait [Acara Sistem Nama Domain \(DNS\)](#) dengan.
5. Runtime Monitoring mendukung AL2 023 dengan rilis agen GuardDuty keamanan v1.6.0 ke atas. Untuk informasi selengkapnya, lihat [GuardDuty versi agen keamanan untuk sumber daya Amazon EKS](#).

Versi Kubernetes didukung oleh agen keamanan GuardDuty

Tabel berikut menunjukkan versi Kubernetes untuk kluster EKS Anda yang didukung oleh agen keamanan. GuardDuty

Amazon EKS versi agen GuardDuty keamanan add-on	Versi Kubernetes
v1.10.0 (terbaru - v1.10.0-eksbuild.2)	
v1.9.0 (terbaru - v1.9.0-eksbuild.2)	1,21 - 1,32
v1.8.1 (terbaru - v1.8.1-eksbuild.2)	
v1.7.0	
v1.6.1	1,21 - 1,31
v1.7.1	
v1.7.0	1,21 - 1,31
v1.6.1	
v1.6.0	
v1.5.0	
v1.4.1	1,21 - 1,29
v1.4.0	
v1.3.1	
v1.3.0	
v1.2.0	1,21 - 1,28
v1.1.0	1,21 - 1,26
v1.0.0	1,21 - 1,25

Beberapa versi agen GuardDuty keamanan akan mencapai akhir dukungan standar.

Untuk informasi tentang versi rilis agen, lihat [GuardDuty versi agen keamanan untuk sumber daya Amazon EKS](#).

Batas CPU dan memori

Tabel berikut menunjukkan batas CPU dan memori untuk add-on Amazon EKS for GuardDuty (aws-guardduty-agent).

Parameter	Batas minimum	Batas maksimum
CPU	200m	1000m
Memori	256 Mi	1024 Mi

Saat Anda menggunakan add-on Amazon EKS versi 1.5.0 atau yang lebih baru, GuardDuty menyediakan kemampuan untuk mengonfigurasi skema add-on untuk nilai CPU dan memori Anda. Untuk informasi tentang rentang yang dapat dikonfigurasi, lihat [Parameter dan nilai yang dapat dikonfigurasi](#).

Setelah mengaktifkan EKS Runtime Monitoring dan menilai status cakupan kluster EKS Anda, Anda dapat mengatur dan melihat metrik wawasan container. Untuk informasi selengkapnya, lihat [Menyiapkan CPU dan pemantauan memori](#).

Memvalidasi kebijakan kontrol layanan organisasi Anda

Jika Anda telah menyiapkan kebijakan kontrol layanan (SCP) untuk mengelola izin di organisasi Anda, validasi bahwa batas izin tidak membatasi. `guardduty:SendSecurityTelemetry` Hal ini diperlukan GuardDuty untuk mendukung Runtime Monitoring di berbagai jenis sumber daya.

Jika Anda adalah akun anggota, sambungkan dengan administrator yang didelegasikan terkait. Untuk informasi tentang mengelola SCPs organisasi Anda, lihat [Kebijakan kontrol layanan \(SCPs\)](#).

Mengaktifkan GuardDuty Runtime Monitoring

Sebelum mengaktifkan Runtime Monitoring di akun Anda, pastikan bahwa jenis sumber daya yang ingin Anda pantau peristiwa runtime, mendukung persyaratan platform. Untuk informasi selengkapnya, lihat [Prasyarat](#).

Jika Anda telah menggunakan EKS Runtime Monitoring sebelum peluncuran Runtime Monitoring, Anda dapat menggunakan APIs untuk memeriksa dan memperbarui konfigurasi yang ada untuk EKS Runtime Monitoring. Anda juga dapat memigrasikan konfigurasi yang ada dari EKS Runtime Monitoring ke Runtime Monitoring. Untuk informasi selengkapnya, lihat [Migrasi dari EKS Runtime Monitoring ke Runtime Monitoring](#).

 Note

Saat ini, dokumentasi ini menyediakan langkah-langkah untuk mengaktifkan Runtime Monitoring untuk akun dan organisasi Anda hanya berdasarkan konsol. Anda juga dapat mengaktifkan Runtime Monitoring dengan menggunakan [API Actions](#) atau [AWS CLI for GuardDuty](#).

Anda dapat mengonfigurasi Runtime Monitoring dengan menggunakan langkah-langkah dalam topik berikut.

Daftar Isi

- [Mengaktifkan Runtime Monitoring untuk lingkungan multi-akun](#)
- [Mengaktifkan Runtime Monitoring untuk akun mandiri](#)

Mengaktifkan Runtime Monitoring untuk lingkungan multi-akun

Di lingkungan beberapa akun, hanya akun GuardDuty administrator yang didelegasikan yang dapat mengaktifkan atau menonaktifkan Runtime Monitoring untuk akun anggota, dan mengelola konfigurasi agen otomatis untuk jenis sumber daya milik akun anggota di organisasinya. Akun GuardDuty anggota tidak dapat mengubah konfigurasi ini dari akun mereka. Akun akun GuardDuty administrator yang didelegasikan mengelola akun anggota mereka menggunakan AWS Organizations. Untuk informasi selengkapnya tentang lingkungan multi-akun, lihat [Mengelola beberapa akun](#).

Untuk akun GuardDuty administrator yang didelegasikan

Untuk mengaktifkan Runtime Monitoring untuk akun administrator yang didelegasikan GuardDuty

1. Masuk ke AWS Management Console dan buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.
2. Di panel navigasi, pilih Runtime Monitoring.

3. Di bawah tab Konfigurasi, pilih Edit di bagian konfigurasi Runtime Monitoring.
4. Menggunakan Aktifkan untuk semua akun

Jika Anda ingin mengaktifkan Runtime Monitoring untuk semua akun milik organisasi, termasuk akun GuardDuty administrator yang didelegasikan, pilih Aktifkan untuk semua akun.

5. Menggunakan Konfigurasi akun secara manual

Jika Anda ingin mengaktifkan Runtime Monitoring untuk setiap akun anggota satu per satu, lalu pilih Konfigurasi akun secara manual.

- Pilih Aktifkan di bawah bagian Administrator Delegasi (akun ini).

6. GuardDuty Untuk menerima peristiwa runtime dari satu atau beberapa jenis sumber daya — EC2 instans Amazon, kluster Amazon ECS, atau kluster Amazon EKS, gunakan opsi berikut untuk mengelola agen keamanan untuk sumber daya ini:

Untuk mengaktifkan agen GuardDuty keamanan

- [Mengaktifkan agen keamanan otomatis untuk instans Amazon EC2](#)
- [Mengelola agen keamanan secara manual untuk EC2 sumber daya Amazon](#)
- [Mengelola agen keamanan otomatis untuk Fargate \(hanya Amazon ECS\)](#)
- [Mengelola agen keamanan secara otomatis untuk sumber daya Amazon EKS](#)
- [Mengelola agen keamanan secara manual untuk kluster Amazon EKS](#)

Untuk semua akun anggota

Untuk mengaktifkan Runtime Monitoring untuk semua akun anggota di organisasi

1. Masuk ke AWS Management Console dan buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.

Masuk menggunakan akun GuardDuty administrator yang didelegasikan.

2. Di panel navigasi, pilih Runtime Monitoring.
3. Pada halaman Runtime Monitoring, di bawah tab Configuration, pilih Edit di bagian konfigurasi Runtime Monitoring.
4. Pilih Aktifkan untuk semua akun.

5. GuardDuty Untuk menerima peristiwa runtime dari satu atau beberapa jenis sumber daya — EC2 instans Amazon, kluster Amazon ECS, atau kluster Amazon EKS, gunakan opsi berikut untuk mengelola agen keamanan untuk sumber daya ini:

Untuk mengaktifkan agen GuardDuty keamanan

- [Mengaktifkan agen keamanan otomatis untuk instans Amazon EC2](#)
- [Mengelola agen keamanan secara manual untuk EC2 sumber daya Amazon](#)
- [Mengelola agen keamanan otomatis untuk Fargate \(hanya Amazon ECS\)](#)
- [Mengelola agen keamanan secara otomatis untuk sumber daya Amazon EKS](#)
- [Mengelola agen keamanan secara manual untuk kluster Amazon EKS](#)

Untuk semua akun anggota aktif yang ada

Untuk mengaktifkan Runtime Monitoring untuk akun anggota yang ada di organisasi

1. Masuk ke AWS Management Console dan buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.

Masuk menggunakan akun GuardDuty administrator yang didelegasikan untuk organisasi.

2. Di panel navigasi, pilih Runtime Monitoring.
3. Pada halaman Runtime Monitoring, di bawah tab Configuration, Anda dapat melihat status konfigurasi Runtime Monitoring saat ini.
4. Dalam panel Runtime Monitoring, di bawah bagian Account anggota aktif, pilih Tindakan.
5. Dari menu tarik-turun Tindakan, pilih Aktifkan untuk semua akun anggota aktif yang ada.
6. Pilih Konfirmasi.
7. GuardDuty Untuk menerima peristiwa runtime dari satu atau beberapa jenis sumber daya — EC2 instans Amazon, kluster Amazon ECS, atau kluster Amazon EKS, gunakan opsi berikut untuk mengelola agen keamanan untuk sumber daya ini:

Untuk mengaktifkan agen GuardDuty keamanan

- [Mengaktifkan agen keamanan otomatis untuk instans Amazon EC2](#)
- [Mengelola agen keamanan secara manual untuk EC2 sumber daya Amazon](#)
- [Mengelola agen keamanan otomatis untuk Fargate \(hanya Amazon ECS\)](#)
- [Mengelola agen keamanan secara otomatis untuk sumber daya Amazon EKS](#)

- [Mengelola agen keamanan secara manual untuk kluster Amazon EKS](#)

 Note

Mungkin diperlukan waktu hingga 24 jam untuk memperbarui konfigurasi akun anggota.

Aktifkan otomatis Runtime Monitoring hanya untuk akun anggota baru

Untuk mengaktifkan Runtime Monitoring untuk akun anggota baru di organisasi Anda

1. Masuk ke AWS Management Console dan buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.

Masuk menggunakan akun GuardDuty administrator organisasi yang didelegasikan yang ditunjuk.

2. Di panel navigasi, pilih Runtime Monitoring
3. Di bawah tab Konfigurasi, pilih Edit di bagian konfigurasi Runtime Monitoring.
4. Pilih Konfigurasikan akun secara manual.
5. Pilih Aktifkan secara otomatis untuk akun anggota baru.
6. GuardDuty Untuk menerima peristiwa runtime dari satu atau beberapa jenis sumber daya — EC2 instans Amazon, kluster Amazon ECS, atau kluster Amazon EKS, gunakan opsi berikut untuk mengelola agen keamanan untuk sumber daya ini:

Untuk mengaktifkan agen GuardDuty keamanan

- [Mengaktifkan agen keamanan otomatis untuk instans Amazon EC2](#)
- [Mengelola agen keamanan secara manual untuk EC2 sumber daya Amazon](#)
- [Mengelola agen keamanan otomatis untuk Fargate \(hanya Amazon ECS\)](#)
- [Mengelola agen keamanan secara otomatis untuk sumber daya Amazon EKS](#)
- [Mengelola agen keamanan secara manual untuk kluster Amazon EKS](#)

Hanya untuk akun anggota aktif selektif

Untuk mengaktifkan Runtime Monitoring untuk akun anggota aktif individu

1. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.

Masuk menggunakan kredensi akun GuardDuty administrator yang didelegasikan.

2. Di panel navigasi, pilih Akun.
3. Pada halaman Akun, tinjau nilai di kolom Runtime Monitoring dan Manage agent secara otomatis. Nilai ini menunjukkan apakah Runtime Monitoring dan manajemen GuardDuty agen Diaktifkan atau Tidak diaktifkan untuk akun terkait.
4. Dari tabel Akun, pilih akun yang ingin Anda aktifkan Runtime Monitoring. Anda dapat memilih beberapa akun sekaligus.
5. Pilih Konfirmasi.
6. Pilih Edit paket perlindungan. Pilih tindakan yang sesuai.
7. Pilih Konfirmasi.
8. GuardDuty Untuk menerima peristiwa runtime dari satu atau beberapa jenis sumber daya — EC2 instans Amazon, klaster Amazon ECS, atau kluster Amazon EKS, gunakan opsi berikut untuk mengelola agen keamanan untuk sumber daya ini:

Untuk mengaktifkan agen GuardDuty keamanan

- [Mengaktifkan agen keamanan otomatis untuk instans Amazon EC2](#)
- [Mengelola agen keamanan secara manual untuk EC2 sumber daya Amazon](#)
- [Mengelola agen keamanan otomatis untuk Fargate \(hanya Amazon ECS\)](#)
- [Mengelola agen keamanan secara otomatis untuk sumber daya Amazon EKS](#)
- [Mengelola agen keamanan secara manual untuk klaster Amazon EKS](#)

Mengaktifkan Runtime Monitoring untuk akun mandiri

Akun mandiri memiliki keputusan untuk mengaktifkan atau menonaktifkan rencana perlindungan di akun mereka Akun AWS secara spesifik. Wilayah AWS

Jika akun Anda dikaitkan dengan akun GuardDuty administrator melalui AWS Organizations, atau dengan metode undangan, bagian ini tidak berlaku untuk akun Anda. Untuk informasi selengkapnya, lihat [Mengaktifkan Runtime Monitoring untuk lingkungan multi-akun](#).

Setelah Anda mengaktifkan Runtime Monitoring, pastikan untuk menginstal agen GuardDuty keamanan melalui konfigurasi otomatis atau penerapan manual. Sebagai bagian dari menyelesaikan semua langkah yang tercantum dalam prosedur berikut, pastikan untuk menginstal agen keamanan.

Untuk mengaktifkan Runtime Monitoring di akun mandiri

1. Masuk ke AWS Management Console dan buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.
2. Di panel navigasi, pilih Runtime Monitoring.
3. Di bawah tab Konfigurasi, pilih Aktifkan untuk mengaktifkan Runtime Monitoring untuk akun Anda.
4. GuardDuty Untuk menerima peristiwa runtime dari satu atau beberapa jenis sumber daya — EC2 instans Amazon, klaster Amazon ECS, atau kluster Amazon EKS, gunakan opsi berikut untuk mengelola agen keamanan untuk sumber daya ini:

Untuk mengaktifkan agen GuardDuty keamanan

- [Mengaktifkan agen keamanan otomatis untuk instans Amazon EC2](#)
- [Mengelola agen keamanan secara manual untuk EC2 sumber daya Amazon](#)
- [Mengelola agen keamanan otomatis untuk Fargate \(hanya Amazon ECS\)](#)
- [Mengelola agen keamanan secara otomatis untuk sumber daya Amazon EKS](#)
- [Mengelola agen keamanan secara manual untuk klaster Amazon EKS](#)

Mengelola agen GuardDuty keamanan

Anda dapat mengelola agen GuardDuty keamanan untuk sumber daya yang ingin Anda pantau. Jika Anda ingin memantau lebih dari satu jenis sumber daya, pastikan untuk mengelola GuardDuty agen untuk sumber daya tersebut.

Topik berikut akan membantu Anda dengan langkah selanjutnya untuk mengelola agen keamanan.

Daftar Isi

- [Mengaktifkan agen keamanan otomatis untuk instans Amazon EC2](#)
- [Mengelola agen keamanan secara manual untuk EC2 sumber daya Amazon](#)
- [Mengelola agen keamanan otomatis untuk Fargate \(hanya Amazon ECS\)](#)
- [Mengelola agen keamanan secara otomatis untuk sumber daya Amazon EKS](#)

- [Mengelola agen keamanan secara manual untuk klaster Amazon EKS](#)
- [Konfigurasi parameter agen GuardDuty keamanan \(add-on\) untuk Amazon EKS](#)
- [Memvalidasi konfigurasi titik akhir VPC](#)

Mengaktifkan agen keamanan otomatis untuk instans Amazon EC2

Bagian ini mencakup langkah-langkah untuk mengaktifkan agen GuardDuty otomatis untuk EC2 sumber daya Amazon Anda di akun mandiri Anda atau lingkungan beberapa akun.

Sebelum Anda melanjutkan, pastikan untuk mengikuti semua [Prasyarat untuk dukungan instans Amazon EC2](#).

Jika Anda bermigrasi dari mengelola GuardDuty agen secara manual ke mengaktifkan agen GuardDuty otomatis, maka sebelum mengikuti langkah-langkah untuk mengaktifkan agen GuardDuty otomatis, lihat. [Migrasi dari agen EC2 manual Amazon ke agen otomatis](#)

Mengaktifkan GuardDuty agen untuk EC2 sumber daya Amazon di lingkungan multi-akun

Dalam lingkungan beberapa akun, hanya akun GuardDuty administrator yang didelegasikan yang dapat mengaktifkan atau menonaktifkan konfigurasi agen otomatis untuk jenis sumber daya milik akun anggota di organisasi mereka. Akun GuardDuty anggota tidak dapat mengubah konfigurasi ini dari akun mereka. Akun akun GuardDuty administrator yang didelegasikan mengelola akun anggota mereka menggunakan AWS Organizations. Untuk informasi selengkapnya tentang lingkungan multi-akun, lihat [Mengelola beberapa akun](#).

Untuk akun GuardDuty administrator yang didelegasikan

Configure for all instances

Jika Anda memilih Aktifkan untuk semua akun untuk Runtime Monitoring, pilih salah satu opsi berikut untuk akun GuardDuty administrator yang didelegasikan:

- Opsi 1

Di bawah Konfigurasi agen otomatis, di EC2 bagian ini, pilih Aktifkan untuk semua akun.

- Opsi 2
 - Di bawah Konfigurasi agen otomatis, di EC2 bagian ini, pilih Konfigurasi akun secara manual.
 - Di bawah Administrator Delegasi (akun ini), pilih Aktifkan.

- Pilih Simpan.

Jika Anda memilih Konfigurasi akun secara manual untuk Runtime Monitoring, lakukan langkah-langkah berikut:

- Di bawah Konfigurasi agen otomatis, di EC2 bagian ini, pilih Konfigurasi akun secara manual.
- Di bawah Administrator Delegasi (akun ini), pilih Aktifkan.
- Pilih Simpan.

Terlepas dari opsi mana yang Anda pilih untuk mengaktifkan konfigurasi agen otomatis untuk akun GuardDuty administrator yang didelegasikan, Anda dapat memverifikasi bahwa asosiasi SSM yang GuardDuty membuat akan menginstal dan mengelola agen keamanan pada semua EC2 sumber daya milik akun ini.

1. Buka AWS Systems Manager konsol di <https://console.aws.amazon.com/systems-manager/>.
2. Buka tab Target untuk asosiasi SSM (GuardDutyRuntimeMonitoring-do-not-delete). Perhatikan bahwa tombol Tag muncul sebagai Instancedata.

Using inclusion tag in selected instances

Untuk mengonfigurasi GuardDuty agen untuk EC2 instans Amazon yang dipilih

1. Masuk ke AWS Management Console dan buka EC2 konsol Amazon di <https://console.aws.amazon.com/ec2/>.
2. Tambahkan true tagGuardDutyManaged: ke instance yang GuardDuty ingin Anda pantau dan deteksi potensi ancaman. Untuk informasi tentang menambahkan tag ini, lihat [Untuk menambahkan tag ke sumber daya individual](#).

Menambahkan tag ini akan memungkinkan GuardDuty untuk menginstal dan mengelola agen keamanan untuk EC2 instance yang dipilih ini. Anda tidak perlu mengaktifkan konfigurasi agen otomatis secara eksplisit.

3. Anda dapat memverifikasi bahwa asosiasi SSM yang GuardDuty membuat akan menginstal dan mengelola agen keamanan hanya pada EC2 sumber daya yang ditandai dengan tag inklusi.

Buka AWS Systems Manager konsol di <https://console.aws.amazon.com/systems-manager/>.

- Buka tab Target untuk asosiasi SSM yang akan dibuat (GuardDutyRuntimeMonitoring-do-not-delete). Tombol Tag muncul sebagai tag: GuardDutyManaged.

Using exclusion tag in selected instances

Note

Pastikan Anda menambahkan tag pengecualian ke EC2 instans Amazon sebelum meluncurkannya. Setelah Anda mengaktifkan konfigurasi agen otomatis untuk Amazon EC2, EC2 instans apa pun yang diluncurkan tanpa tag pengecualian akan tercakup dalam konfigurasi agen GuardDuty otomatis.

Untuk mengonfigurasi GuardDuty agen untuk EC2 instans Amazon yang dipilih

1. Masuk ke AWS Management Console dan buka EC2 konsol Amazon di <https://console.aws.amazon.com/ec2/>.
2. Tambahkan false tagGuardDutyManaged: ke instance yang tidak GuardDuty ingin Anda pantau dan deteksi potensi ancaman. Untuk informasi tentang menambahkan tag ini, lihat [Untuk menambahkan tag ke sumber daya individual](#).
3. Agar [tag pengecualian tersedia](#) dalam metadata instance, lakukan langkah-langkah berikut:
 - a. Di bawah tab Detail instans Anda, lihat status untuk Izinkan tag dalam metadata instance.

Jika saat ini Dinonaktifkan, gunakan langkah-langkah berikut untuk mengubah status menjadi Diaktifkan. Jika tidak, lewati langkah ini.
 - b. Di bawah menu Tindakan, pilih Pengaturan instans.
 - c. Pilih Izinkan tag dalam metadata contoh.
4. Setelah Anda menambahkan tag pengecualian, lakukan langkah yang sama seperti yang ditentukan dalam tab Configure for all instance.

Anda sekarang dapat menilai runtime[Cakupan runtime dan pemecahan masalah untuk instans Amazon EC2](#).

Aktifkan otomatis untuk semua akun anggota

Note

Mungkin diperlukan waktu hingga 24 jam untuk memperbarui konfigurasi akun anggota.

Configure for all instances

Langkah-langkah berikut mengasumsikan bahwa Anda memilih Aktifkan untuk semua akun di bagian Runtime Monitoring:

1. Pilih Aktifkan untuk semua akun di bagian Konfigurasi agen otomatis untuk Amazon EC2.
2. Anda dapat memverifikasi bahwa asosiasi SSM yang GuardDuty membuat (GuardDutyRuntimeMonitoring-do-not-delete) akan menginstal dan mengelola agen keamanan pada semua EC2 sumber daya milik akun ini.
 - a. Buka AWS Systems Manager konsol di <https://console.aws.amazon.com/systems-manager/>.
 - b. Buka tab Target untuk asosiasi SSM. Perhatikan bahwa tombol Tag muncul sebagai InstanceIds.

Using inclusion tag in selected instances

Untuk mengonfigurasi GuardDuty agen untuk EC2 instans Amazon yang dipilih

1. Masuk ke AWS Management Console dan buka EC2 konsol Amazon di <https://console.aws.amazon.com/ec2/>.
2. Tambahkan true tagGuardDutyManaged: ke EC2 instance yang GuardDuty ingin Anda pantau dan deteksi potensi ancaman. Untuk informasi tentang menambahkan tag ini, lihat [Untuk menambahkan tag ke sumber daya individual](#).

Menambahkan tag ini akan memungkinkan GuardDuty untuk menginstal dan mengelola agen keamanan untuk EC2 instance yang dipilih ini. Anda tidak perlu mengaktifkan konfigurasi agen otomatis secara eksplisit.

3. Anda dapat memverifikasi bahwa asosiasi SSM yang GuardDuty membuat akan menginstal dan mengelola agen keamanan pada semua EC2 sumber daya milik akun Anda.

- a. Buka AWS Systems Manager konsol di <https://console.aws.amazon.com/systems-manager/>.
- b. Buka tab Target untuk asosiasi SSM (GuardDutyRuntimeMonitoring-do-not-delete). Perhatikan bahwa tombol Tag muncul sebagai InstanceIds.

Using exclusion tag in selected instances

 Note

Pastikan Anda menambahkan tag pengecualian ke EC2 instans Amazon sebelum meluncurkannya. Setelah Anda mengaktifkan konfigurasi agen otomatis untuk Amazon EC2, EC2 instans apa pun yang diluncurkan tanpa tag pengecualian akan tercakup dalam konfigurasi agen GuardDuty otomatis.

Untuk mengonfigurasi agen GuardDuty keamanan untuk EC2 instans Amazon yang dipilih

1. Masuk ke AWS Management Console dan buka EC2 konsol Amazon di <https://console.aws.amazon.com/ec2/>.
2. Tambahkan `false` tagGuardDutyManaged: ke instance yang tidak GuardDuty ingin Anda pantau dan deteksi potensi ancaman. Untuk informasi tentang menambahkan tag ini, lihat [Untuk menambahkan tag ke sumber daya individual](#).
3. Agar [tag pengecualian tersedia](#) dalam metadata instance, lakukan langkah-langkah berikut:
 - a. Di bawah tab Detail instans Anda, lihat status untuk Izinkan tag dalam metadata instance.

Jika saat ini Dinonaktifkan, gunakan langkah-langkah berikut untuk mengubah status menjadi Diaktifkan. Jika tidak, lewati langkah ini.
 - b. Di bawah menu Tindakan, pilih Pengaturan instans.
 - c. Pilih Izinkan tag dalam metadata contoh.
4. Setelah Anda menambahkan tag pengecualian, lakukan langkah yang sama seperti yang ditentukan dalam tab Configure for all instance.

Anda sekarang dapat menilai runtime [Cakupan runtime dan pemecahan masalah untuk instans Amazon EC2](#).

Aktifkan otomatis hanya untuk akun anggota baru

Akun GuardDuty administrator yang didelegasikan dapat mengatur konfigurasi agen otomatis untuk EC2 sumber daya Amazon agar secara otomatis mengaktifkan akun anggota baru saat mereka bergabung dengan organisasi.

Configure for all instances

Langkah-langkah berikut mengasumsikan bahwa Anda memilih Aktifkan secara otomatis untuk akun anggota baru di bawah bagian Runtime Monitoring:

1. Di panel navigasi, pilih Runtime Monitoring.
2. Pada halaman Runtime Monitoring, pilih Edit.
3. Pilih Aktifkan secara otomatis untuk akun anggota baru. Langkah ini memastikan bahwa setiap kali akun baru bergabung dengan organisasi Anda, konfigurasi agen otomatis untuk Amazon EC2 akan diaktifkan secara otomatis untuk akun mereka. Hanya akun GuardDuty administrator organisasi yang didelegasikan yang dapat mengubah pilihan ini.
4. Pilih Simpan.

Ketika akun anggota baru bergabung dengan organisasi, konfigurasi ini akan diaktifkan untuk mereka secara otomatis. GuardDuty Untuk mengelola agen keamanan untuk EC2 instans Amazon yang termasuk dalam akun anggota baru ini, pastikan semua prasyarat [Sebagai EC2 contoh](#) terpenuhi.

Ketika asosiasi SSM dibuat (GuardDutyRuntimeMonitoring-do-not-delete), Anda dapat memverifikasi bahwa asosiasi SSM akan menginstal dan mengelola agen keamanan pada semua EC2 instance milik akun anggota baru.

- Buka AWS Systems Manager konsol di <https://console.aws.amazon.com/systems-manager/>.
- Buka tab Target untuk asosiasi SSM. Perhatikan bahwa tombol Tag muncul sebagai InstanceIds.

Using inclusion tag in selected instances

Untuk mengonfigurasi agen GuardDuty keamanan untuk instans yang dipilih di akun Anda

1. Masuk ke AWS Management Console dan buka EC2 konsol Amazon di <https://console.aws.amazon.com/ec2/>.

2. Tambahkan `true` tagGuardDutyManaged: ke instance yang GuardDuty ingin Anda pantau dan deteksi potensi ancaman. Untuk informasi tentang menambahkan tag ini, lihat [Untuk menambahkan tag ke sumber daya individual](#).

Menambahkan tag ini akan memungkinkan GuardDuty untuk menginstal dan mengelola agen keamanan untuk instance yang dipilih ini. Anda tidak perlu mengaktifkan konfigurasi agen otomatis secara eksplisit.

3. Anda dapat memverifikasi bahwa asosiasi SSM yang GuardDuty membuat akan menginstal dan mengelola agen keamanan hanya pada EC2 sumber daya yang ditandai dengan tag inklusi.
 - a. Buka AWS Systems Manager konsol di <https://console.aws.amazon.com/systems-manager/>.
 - b. Buka tab Target untuk asosiasi SSM yang akan dibuat. Tombol Tag muncul sebagai tag: GuardDutyManaged.

Using exclusion tag in selected instances

Note

Pastikan Anda menambahkan tag pengecualian ke EC2 instans Amazon sebelum meluncurkannya. Setelah Anda mengaktifkan konfigurasi agen otomatis untuk Amazon EC2, EC2 instans apa pun yang diluncurkan tanpa tag pengecualian akan tercakup dalam konfigurasi agen GuardDuty otomatis.

Untuk mengonfigurasi agen GuardDuty keamanan untuk instans tertentu di akun mandiri Anda

1. Masuk ke AWS Management Console dan buka EC2 konsol Amazon di <https://console.aws.amazon.com/ec2/>.
2. Tambahkan `false` tagGuardDutyManaged: ke instance yang tidak GuardDuty ingin Anda pantau dan deteksi potensi ancaman. Untuk informasi tentang menambahkan tag ini, lihat [Untuk menambahkan tag ke sumber daya individual](#).
3. Agar [tag pengecualian tersedia](#) dalam metadata instance, lakukan langkah-langkah berikut:
 - a. Di bawah tab Detail instans Anda, lihat status untuk Izinkan tag dalam metadata instance.

Jika saat ini Dinonaktifkan, gunakan langkah-langkah berikut untuk mengubah status menjadi Diaktifkan. Jika tidak, lewati langkah ini.

- b. Di bawah menu Tindakan, pilih Pengaturan instans.
 - c. Pilih Izinkan tag dalam metadata contoh.
4. Setelah Anda menambahkan tag pengecualian, lakukan langkah yang sama seperti yang ditentukan dalam tab Configure for all instance.

Anda sekarang dapat menilai runtime [Cakupan runtime dan pemecahan masalah untuk instans Amazon EC2](#).

Hanya akun anggota selektif

Configure for all instances

1. Pada halaman Akun, pilih satu atau beberapa akun yang ingin Anda aktifkan konfigurasi agen Runtime Monitoring-Automated agent (Amazon). EC2 Pastikan akun yang Anda pilih pada langkah ini sudah mengaktifkan Runtime Monitoring.
2. Dari Edit paket perlindungan, pilih opsi yang sesuai untuk mengaktifkan konfigurasi agen Runtime Monitoring-Automated agent (Amazon). EC2
3. Pilih Konfirmasi.

Using inclusion tag in selected instances

Untuk mengonfigurasi agen GuardDuty keamanan untuk instans yang dipilih

1. Masuk ke AWS Management Console dan buka EC2 konsol Amazon di <https://console.aws.amazon.com/ec2/>.
2. Tambahkan true tagGuardDutyManaged: ke instance yang GuardDuty ingin Anda pantau dan deteksi potensi ancaman. Untuk informasi tentang menambahkan tag ini, lihat [Untuk menambahkan tag ke sumber daya individual](#).

Menambahkan tag ini akan memungkinkan GuardDuty untuk mengelola agen keamanan untuk EC2 instans Amazon yang ditandai. Anda tidak perlu secara eksplisit mengaktifkan konfigurasi agen otomatis (Runtime Monitoring - Automated agent configuration). EC2

Using exclusion tag in selected instances

Note

Pastikan Anda menambahkan tag pengecualian ke EC2 instans Amazon sebelum meluncurkannya. Setelah Anda mengaktifkan konfigurasi agen otomatis untuk Amazon EC2, EC2 instans apa pun yang diluncurkan tanpa tag pengecualian akan tercakup dalam konfigurasi agen GuardDuty otomatis.

Untuk mengonfigurasi agen GuardDuty keamanan untuk instans yang dipilih

1. Masuk ke AWS Management Console dan buka EC2 konsol Amazon di <https://console.aws.amazon.com/ec2/>.
2. Tambahkan `false` tagGuardDutyManaged: ke EC2 instance yang tidak GuardDuty ingin Anda pantau atau deteksi potensi ancaman. Untuk informasi tentang menambahkan tag ini, lihat [Untuk menambahkan tag ke sumber daya individual](#).
3. Agar [tag pengecualian tersedia](#) dalam metadata instance, lakukan langkah-langkah berikut:
 - a. Di bawah tab Detail instans Anda, lihat status untuk Izinkan tag dalam metadata instance.

Jika saat ini Dinonaktifkan, gunakan langkah-langkah berikut untuk mengubah status menjadi Diaktifkan. Jika tidak, lewati langkah ini.
 - b. Di bawah menu Tindakan, pilih Pengaturan instans.
 - c. Pilih Izinkan tag dalam metadata contoh.
4. Setelah Anda menambahkan tag pengecualian, lakukan langkah yang sama seperti yang ditentukan dalam tab Configure for all instance.

Anda sekarang dapat menilai [Cakupan runtime dan pemecahan masalah untuk instans Amazon EC2](#).

Mengaktifkan agen GuardDuty otomatis untuk EC2 sumber daya Amazon di akun mandiri

Akun mandiri memiliki keputusan untuk mengaktifkan atau menonaktifkan rencana perlindungan di akun mereka Akun AWS secara spesifik. Wilayah AWS

Jika akun Anda dikaitkan dengan akun GuardDuty administrator melalui AWS Organizations, atau dengan metode undangan, bagian ini tidak berlaku untuk akun Anda. Untuk informasi selengkapnya, lihat [Mengaktifkan Runtime Monitoring untuk lingkungan multi-akun](#).

Setelah Anda mengaktifkan Runtime Monitoring, pastikan untuk menginstal agen GuardDuty keamanan melalui konfigurasi otomatis atau penerapan manual. Sebagai bagian dari menyelesaikan semua langkah yang tercantum dalam prosedur berikut, pastikan untuk menginstal agen keamanan.

Berdasarkan preferensi Anda untuk memantau semua atau EC2 sumber daya Amazon selektif, pilih metode yang disukai dan ikuti langkah-langkah dalam tabel berikut.

Configure for all instances

Untuk mengonfigurasi Runtime Monitoring untuk semua instance di akun mandiri Anda

1. Masuk ke AWS Management Console dan buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.
2. Di panel navigasi, pilih Runtime Monitoring.
3. Di bawah tab Konfigurasi, pilih Edit.
4. Di EC2 bagian ini, pilih Aktifkan.
5. Pilih Simpan.
6. Anda dapat memverifikasi bahwa asosiasi SSM yang GuardDuty membuat akan menginstal dan mengelola agen keamanan pada semua EC2 sumber daya milik akun Anda.
 - a. Buka AWS Systems Manager konsol di <https://console.aws.amazon.com/systems-manager/>.
 - b. Buka tab Target untuk asosiasi SSM (GuardDutyRuntimeMonitoring-do-not-delete). Perhatikan bahwa tombol Tag muncul sebagai InstanceIds.

Using inclusion tag in selected instances

Untuk mengonfigurasi agen GuardDuty keamanan untuk EC2 instans Amazon yang dipilih

1. Masuk ke AWS Management Console dan buka EC2 konsol Amazon di <https://console.aws.amazon.com/ec2/>.
2. Tambahkan true tagGuardDutyManaged: ke instance yang GuardDuty ingin Anda pantau dan deteksi potensi ancaman. Untuk informasi tentang menambahkan tag ini, lihat [Untuk menambahkan tag ke sumber daya individual](#).

3. Anda dapat memverifikasi bahwa asosiasi SSM yang GuardDuty membuat akan menginstal dan mengelola agen keamanan hanya pada EC2 sumber daya yang ditandai dengan tag inklusi.

Buka AWS Systems Manager konsol di <https://console.aws.amazon.com/systems-manager/>.

- Buka tab Target untuk asosiasi SSM yang akan dibuat (GuardDutyRuntimeMonitoring-do-not-delete). Tombol Tag muncul sebagai tag: GuardDutyManaged.

Using exclusion tag in selected instances

Note

Pastikan Anda menambahkan tag pengecualian ke EC2 instans Amazon sebelum meluncurkannya. Setelah Anda mengaktifkan konfigurasi agen otomatis untuk Amazon EC2, EC2 instans apa pun yang diluncurkan tanpa tag pengecualian akan tercakup dalam konfigurasi agen GuardDuty otomatis.

Untuk mengonfigurasi agen GuardDuty keamanan untuk EC2 instans Amazon yang dipilih

1. Masuk ke AWS Management Console dan buka EC2 konsol Amazon di <https://console.aws.amazon.com/ec2/>.
2. Tambahkan `false` tagGuardDutyManaged: ke instance yang tidak GuardDuty ingin Anda pantau dan deteksi potensi ancaman. Untuk informasi tentang menambahkan tag ini, lihat [Untuk menambahkan tag ke sumber daya individual](#).
3. Agar [tag pengecualian tersedia](#) dalam metadata instance, lakukan langkah-langkah berikut:
 - a. Di bawah tab Detail instans Anda, lihat status untuk Izinkan tag dalam metadata instance.

Jika saat ini Dinonaktifkan, gunakan langkah-langkah berikut untuk mengubah status menjadi Diaktifkan. Jika tidak, lewati langkah ini.
 - b. Pilih contoh yang ingin Anda izinkan tag.
 - c. Di bawah menu Tindakan, pilih Pengaturan instans.
 - d. Pilih Izinkan tag dalam metadata contoh.

- e. Di bawah Akses ke tag dalam metadata instance, pilih Izinkan.
 - f. Pilih Simpan.
4. Setelah Anda menambahkan tag pengecualian, lakukan langkah yang sama seperti yang ditentukan di tab Configure for all instance.

Anda sekarang dapat menilai runtime [Cakupan runtime dan pemecahan masalah untuk instans Amazon EC2](#).

Migrasi dari agen EC2 manual Amazon ke agen otomatis

Bagian ini berlaku untuk Anda Akun AWS jika sebelumnya Anda mengelola agen keamanan secara manual dan sekarang ingin menggunakan konfigurasi agen GuardDuty otomatis. Jika ini tidak berlaku untuk Anda, lanjutkan dengan mengonfigurasi agen keamanan untuk akun Anda.

Ketika Anda mengaktifkan agen GuardDuty otomatis, GuardDuty mengelola agen keamanan atas nama Anda. Untuk informasi tentang langkah-langkah apa yang GuardDuty diambil, lihat [Gunakan konfigurasi agen otomatis \(disarankan\)](#).

Pembersihan sumber daya

Hapus asosiasi SSM

- Hapus asosiasi SSM apa pun yang mungkin telah Anda buat saat mengelola agen keamanan untuk Amazon EC2 secara manual. Untuk informasi selengkapnya, lihat [Menghapus asosiasi](#).
- Hal ini dilakukan agar GuardDuty dapat mengambil alih pengelolaan tindakan SSM apakah Anda menggunakan agen otomatis di tingkat akun atau tingkat instans (dengan menggunakan tag inklusi atau pengecualian). Untuk informasi selengkapnya tentang tindakan SSM yang dapat GuardDuty dilakukan, lihat [Izin peran terkait layanan untuk GuardDuty](#).
- Ketika Anda menghapus asosiasi SSM yang sebelumnya dibuat untuk mengelola agen keamanan secara manual, mungkin ada periode singkat tumpang tindih ketika GuardDuty membuat asosiasi SSM untuk mengelola agen keamanan secara otomatis. Selama periode ini, Anda dapat mengalami konflik berdasarkan penjadwalan SSM. Untuk informasi selengkapnya, lihat [penjadwalan Amazon EC2 SSM](#).

Mengelola tag inklusi dan pengecualian untuk instans Amazon EC2 Anda

- Tag penyertaan — Jika Anda tidak mengaktifkan konfigurasi agen GuardDuty otomatis tetapi menandai EC2 instans Amazon Anda dengan tag inklusi (`GuardDutyManaged:true`), GuardDuty buat asosiasi SSM yang akan menginstal dan mengelola agen keamanan pada

instans yang dipilih EC2 . Ini adalah perilaku yang diharapkan yang membantu Anda mengelola agen keamanan hanya pada EC2 instans yang dipilih. Untuk informasi selengkapnya, lihat [Cara kerja Runtime Monitoring dengan instans Amazon EC2](#).

Untuk GuardDuty mencegah menginstal dan mengelola agen keamanan, hapus tag inklusi dari EC2 instance ini. Untuk informasi selengkapnya, lihat [Menambahkan dan menghapus tag](#) di Panduan EC2 Pengguna Amazon.

- Tag pengecualian — Saat Anda ingin mengaktifkan konfigurasi agen GuardDuty otomatis untuk semua EC2 instance di akun Anda, pastikan tidak ada EC2 instance yang ditandai dengan tag pengecualian (:). `GuardDutyManaged false`

Mengelola agen keamanan secara manual untuk EC2 sumber daya Amazon

Bagian ini menyediakan langkah-langkah untuk menginstal dan memperbarui agen keamanan secara manual untuk EC2 sumber daya Amazon Anda.

Setelah Anda mengaktifkan Runtime Monitoring, Anda harus menginstal agen GuardDuty keamanan secara manual. Untuk mengelola agen GuardDuty keamanan secara manual, Anda harus terlebih dahulu membuat endpoint Amazon VPC secara manual. Setelah ini, Anda dapat menginstal agen keamanan sehingga GuardDuty akan mulai menerima peristiwa runtime dari EC2 instans Amazon. Saat GuardDuty merilis versi agen baru untuk sumber daya ini, Anda dapat memperbarui versi agen di akun Anda.

Topik berikut mencakup langkah-langkah untuk terus mengelola agen keamanan untuk EC2 sumber daya Amazon Anda.

Topik

- [Prasyarat - Membuat titik akhir Amazon VPC secara manual](#)
- [Memasang agen keamanan secara manual](#)
- [Memperbarui agen GuardDuty keamanan untuk EC2 instans Amazon secara manual](#)

Prasyarat - Membuat titik akhir Amazon VPC secara manual

Sebelum Anda dapat menginstal agen GuardDuty keamanan, Anda harus membuat titik akhir Amazon Virtual Private Cloud (Amazon VPC). Ini akan membantu GuardDuty menerima peristiwa runtime dari EC2 instans Amazon Anda.

 Note

Tidak ada biaya tambahan untuk penggunaan titik akhir VPC.

Untuk membuat titik akhir VPC Amazon

1. Masuk ke AWS Management Console dan buka konsol VPC Amazon di. <https://console.aws.amazon.com/vpc/>
2. Di panel navigasi, di bawah VPC private cloud, pilih Endpoints.
3. Pilih Buat Titik Akhir.
4. Pada halaman Buat titik akhir, untuk kategori Layanan, pilih Layanan titik akhir lainnya.
5. Untuk nama Layanan, masukkan **com.amazonaws.us-east-1.guardduty-data**.

Pastikan untuk mengganti **us-east-1** dengan Anda Wilayah AWS. Ini harus Wilayah yang sama dengan EC2 instans Amazon yang termasuk dalam ID AWS akun Anda.

6. Pilih Verifikasi layanan.
7. Setelah nama layanan berhasil diverifikasi, pilih VPC tempat instans Anda berada. Tambahkan kebijakan berikut untuk membatasi penggunaan titik akhir VPC Amazon hanya ke akun yang ditentukan. Dengan organisasi yang Condition disediakan di bawah kebijakan ini, Anda dapat memperbarui kebijakan berikut untuk membatasi akses ke titik akhir Anda. Untuk memberikan dukungan endpoint Amazon VPC ke akun tertentu IDs di organisasi Anda, lihat. [Organization condition to restrict access to your endpoint](#)

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": "*",
      "Resource": "*",
      "Effect": "Allow",
      "Principal": "*"
    },
    {
      "Condition": {
        "StringNotEquals": {
          "aws:PrincipalAccount": "111122223333"
        }
      }
    }
  ]
}
```



```

    },
    "Action": "*",
    "Resource": "*",
    "Effect": "Deny",
    "Principal": "*"
  }
]
}

```

ID `aws:PrincipalAccount` akun harus cocok dengan akun yang berisi titik akhir VPC dan VPC. Daftar berikut menunjukkan cara berbagi titik akhir VPC dengan akun lain: AWS IDs

- Untuk menentukan beberapa akun untuk mengakses titik akhir VPC, ganti `"aws:PrincipalAccount: "` **`111122223333`** dengan blok berikut:

```

"aws:PrincipalAccount": [
    "666666666666",
    "555555555555"
]

```

Pastikan untuk mengganti AWS akun IDs dengan akun akun IDs yang perlu mengakses titik akhir VPC.

- Untuk mengizinkan semua anggota dari organisasi mengakses titik akhir VPC, ganti `"aws:PrincipalAccount: "` **`111122223333`** dengan baris berikut:

```

"aws:PrincipalOrgID": "o-abcdef0123"

```

Pastikan untuk mengganti organisasi **`o-abcdef0123`** dengan ID organisasi Anda.

- Untuk membatasi akses sumber daya berdasarkan ID organisasi, tambahkan `ResourceOrgID` ke kebijakan. Untuk informasi lebih lanjut, lihat [aws:ResourceOrgID](#) dalam Panduan Pengguna IAM.

```

"aws:ResourceOrgID": "o-abcdef0123"

```

8. Di bawah Pengaturan tambahan, pilih Aktifkan nama DNS.
9. Di bawah Subnet, pilih subnet tempat instance Anda berada.
10. Di bawah Grup keamanan, pilih grup keamanan yang mengaktifkan port 443 dalam terikat dari VPC Anda (atau instans Amazon Anda). EC2 Jika Anda belum memiliki grup keamanan yang

mengaktifkan port 443 dalam ikatan, lihat [Membuat grup keamanan untuk VPC Anda di Panduan Pengguna Amazon VPC](#).

Jika ada masalah saat membatasi izin masuk ke VPC (atau instance), Anda dapat menggunakan port 443 yang di-bound dari alamat IP apa pun. (0.0.0.0/0) Namun, GuardDuty merekomendasikan untuk menggunakan alamat IP yang cocok dengan blok CIDR untuk VPC Anda. Untuk informasi selengkapnya, lihat [blok CIDR VPC di Panduan Pengguna Amazon VPC](#).

Setelah Anda mengikuti langkah-langkahnya, lihat [Memvalidasi konfigurasi titik akhir VPC](#) untuk memastikan bahwa titik akhir VPC telah diatur dengan benar.

Memasang agen keamanan secara manual

GuardDuty menyediakan dua metode berikut untuk menginstal agen GuardDuty keamanan di EC2 instans Amazon Anda. Sebelum melanjutkan, pastikan untuk mengikuti langkah-langkah di bawah [Prasyarat - Membuat titik akhir Amazon VPC secara manual](#) ini.

Pilih metode akses yang disukai untuk menginstal agen keamanan di EC2 sumber daya Amazon Anda.

- [Metode 1 - Menggunakan AWS Systems Manager](#)— Metode ini mengharuskan EC2 instans Amazon Anda AWS Systems Manager dikelola.
- [Metode 2 - Menggunakan Linux Package Manager](#)— Anda dapat menggunakan metode ini apakah EC2 instans Amazon Anda AWS Systems Manager dikelola atau tidak. Berdasarkan [distribusi OS](#) Anda, Anda dapat memilih metode yang sesuai untuk menginstal skrip RPM atau skrip Debian. Jika Anda menggunakan platform Fedora, maka Anda harus menggunakan metode ini untuk menginstal agen.

Metode 1 - Menggunakan AWS Systems Manager

Untuk menggunakan metode ini, pastikan EC2 instans Amazon Anda AWS Systems Manager dikelola dan kemudian instal agen.

AWS Systems Manager EC2 instans Amazon yang dikelola

Gunakan langkah-langkah berikut untuk membuat EC2 instans Amazon Anda AWS Systems Manager dikelola.

- [AWS Systems Manager](#) membantu Anda mengelola AWS aplikasi end-to-end dan sumber daya serta mengaktifkan operasi yang aman dalam skala besar.

Untuk mengelola EC2 instans Amazon Anda AWS Systems Manager, lihat [Menyiapkan Systems Manager untuk EC2 instans Amazon](#) di AWS Systems Manager Panduan Pengguna.

- Tabel berikut menunjukkan AWS Systems Manager dokumen GuardDuty terkelola baru:

Nama dokumen	Jenis dokumen	Tujuan
AmazonGuardDuty-RunTimeMonitoringSsmPlugin	Distributor	Untuk mengemas agen GuardDuty keamanan.
AmazonGuardDuty-ConfigureRuntimeMonitoringSsmPlugin	Perintah	Untuk menjalankan skrip instalasi/penghapusan instalasi untuk menginstal agen keamanan. GuardDuty

Untuk informasi selengkapnya AWS Systems Manager, lihat [Dokumen Amazon EC2 Systems Manager](#) di Panduan AWS Systems Manager Pengguna.

Untuk Server Debian

Amazon Machine Images (AMIs) untuk Server Debian yang disediakan oleh AWS mengharuskan Anda untuk menginstal AWS Systems Manager agen (agen SSM). Anda perlu melakukan langkah tambahan untuk menginstal agen SSM untuk membuat instans Amazon EC2 Debian Server SSM dikelola. Untuk informasi tentang langkah-langkah yang perlu Anda ambil, lihat [Menginstal agen SSM secara manual pada instance Server Debian di Panduan Pengguna.AWS Systems Manager](#)

Untuk menginstal GuardDuty agen untuk EC2 instans Amazon dengan menggunakan AWS Systems Manager

1. Buka AWS Systems Manager konsol di <https://console.aws.amazon.com/systems-manager/>.
2. Di panel navigasi, pilih Dokumen

3. Di Dimiliki oleh Amazon, pilih `AmazonGuardDuty-ConfigureRuntimeMonitoringSsmPlugin`.
4. Pilih Run Command.
5. Masukkan parameter Run Command berikut
 - Tindakan: Pilih Instal.
 - Jenis Instalasi: Pilih Instal atau Hapus Instalasi.
 - Nama: `AmazonGuardDuty-RuntimeMonitoringSsmPlugin`
 - Versi: Jika ini tetap kosong, Anda akan mendapatkan versi terbaru dari agen GuardDuty keamanan. Untuk informasi lebih lanjut tentang versi rilis, [GuardDuty versi agen keamanan untuk EC2 instans Amazon](#).
6. Pilih EC2 instans Amazon yang ditargetkan. Anda dapat memilih satu atau beberapa EC2 instans Amazon. Untuk informasi selengkapnya, lihat [AWS Systems Manager Menjalankan perintah dari konsol](#) di Panduan AWS Systems Manager Pengguna
7. Validasi jika instalasi GuardDuty agen sehat. Untuk informasi selengkapnya, lihat [Memvalidasi status instalasi agen GuardDuty keamanan](#).

Metode 2 - Menggunakan Linux Package Manager

Dengan metode ini, Anda dapat menginstal agen GuardDuty keamanan dengan menjalankan skrip RPM atau skrip Debian. Berdasarkan sistem operasi, Anda dapat memilih metode yang disukai:

- Gunakan skrip RPM untuk menginstal agen keamanan pada distribusi OS AL2, AL2 023,, RedHat CentOS, atau Fedora.
- Gunakan skrip Debian untuk menginstal agen keamanan pada distribusi OS Ubuntu atau Debian. Untuk informasi tentang distribusi Ubuntu dan Debian OS yang didukung, lihat. [Validasi persyaratan arsitektur](#)

RPM installation

Important

Sebaiknya verifikasi tanda tangan RPM agen GuardDuty keamanan sebelum menginstalnya di mesin Anda.

1. Verifikasi tanda tangan RPM agen GuardDuty keamanan

a. Siapkan template

Siapkan perintah dengan kunci publik yang sesuai, tanda tangan x86_64 RPM, tanda tangan arm64 RPM, dan tautan akses yang sesuai ke skrip RPM yang dihosting di bucket Amazon S3. Ganti nilai Wilayah AWS, ID AWS akun, dan versi GuardDuty agen untuk mengakses skrip RPM.

- Kunci publik:

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.7.1/publickey.pem
```

- GuardDuty tanda tangan agen keamanan RPM:

Tanda tangan dari x86_64 RPM

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.7.1/x86_64/amazon-guardduty-agent-1.7.1.x86_64.sig
```

Tanda tangan arm64 RPM

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.7.1/arm64/amazon-guardduty-agent-1.7.1.arm64.sig
```

- Akses tautan ke skrip RPM di bucket Amazon S3:

Tautan akses untuk x86_64 RPM

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.7.1/x86_64/amazon-guardduty-agent-1.7.1.x86_64.rpm
```

Tautan akses untuk arm64 RPM

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.7.1/arm64/amazon-guardduty-agent-1.7.1.arm64.rpm
```

Wilayah AWS	Nama wilayah	AWS ID akun

eu-west-1	Eropa (Irlandia)	694911143906
us-east-1	AS Timur (Virginia Utara)	593207742271
us-west-2	AS Barat (Oregon)	733349766148
eu-west-3	Eropa (Paris)	665651866788
us-east-2	AS Timur (Ohio)	307168627858
eu-central-1	Eropa (Frankfurt)	323658145986
ap-northeast-2	Asia Pasifik (Seoul)	914738172881
eu-north-1	Eropa (Stockholm)	591436053604
ap-east-1	Asia Pasifik (Hong Kong)	258348409381
me-south-1	Timur Tengah (Bahrain)	536382113932
eu-west-2	Eropa (London)	892757235363
ap-northeast-1	Asia Pasifik (Tokyo)	533107202818
ap-southeast-1	Asia Pasifik (Singapura)	174946120834
ap-south-1	Asia Pasifik (Mumbai)	251508486986
ap-southeast-3	Asia Pasifik (Jakarta)	510637619217
sa-east-1	Amerika Selatan (Sao Paulo)	758426053663
ap-northeast-3	Asia Pasifik (Osaka)	273192626886
eu-south-1	Eropa (Milan)	266869475730
af-south-1	Afrika (Cape Town)	197869348890
ap-southeast-2	Asia Pasifik (Sydney)	005257825471
me-central-1	Timur Tengah (UEA)	000014521398

us-west-1	AS Barat (California Utara)	684579721401
ca-central-1	Kanada (Pusat)	354763396469
ca-west-1	Kanada Barat (Calgary)	339712888787
ap-south-2	Asia Pasifik (Hyderabad)	950823858135
eu-south-2	Eropa (Spanyol)	919611009337
eu-central-2	Eropa (Zürich)	529164026651
ap-southeast-4	Asia Pasifik (Melbourne)	251357961535
ap-southeast-7	Asia Pasifik (Thailand)	054037130133
il-central-1	Israel (Tel Aviv)	870907303882
mx-central-1	Meksiko (Tengah)	982081086614

b. Unduh templatnya

Dalam perintah berikut untuk mengunduh kunci publik yang sesuai, tanda tangan x86_64 RPM, tanda tangan arm64 RPM, dan tautan akses yang sesuai ke skrip RPM yang dihosting di bucket Amazon S3, pastikan untuk mengganti ID akun dengan ID yang sesuai Akun AWS dan Wilayah dengan Wilayah Anda saat ini.

```
aws s3 cp s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.7.1/
x86_64/amazon-guardduty-agent-1.7.1.x86_64.rpm ./amazon-guardduty-
agent-1.7.1.x86_64.rpm
aws s3 cp s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.7.1/
x86_64/amazon-guardduty-agent-1.7.1.x86_64.sig ./amazon-guardduty-
agent-1.7.1.x86_64.sig
aws s3 cp s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.7.1/
publickey.pem ./publickey.pem
```

c. Impor kunci publik

Gunakan perintah berikut untuk mengimpor kunci publik ke database:

```
gpg --import publickey.pem
```

gpg menunjukkan impor berhasil

```
gpg: key 093FF49D: public key "AwsGuardDuty" imported
gpg: Total number processed: 1
gpg:             imported: 1 (RSA: 1)
```

d. Verifikasi tanda tangan

Gunakan perintah berikut untuk memverifikasi tanda tangan

```
gpg --verify amazon-guardduty-agent-1.7.1.x86_64.sig amazon-guardduty-agent-1.7.1.x86_64.rpm
```

Jika verifikasi berlalu, Anda akan melihat pesan yang mirip dengan hasil di bawah ini. Anda sekarang dapat melanjutkan untuk menginstal agen GuardDuty keamanan menggunakan RPM.

Contoh output:

```
gpg: Signature made Fri 17 Nov 2023 07:58:11 PM UTC using ? key ID 093FF49D
gpg: Good signature from "AwsGuardDuty"
gpg: WARNING: This key is not certified with a trusted signature!
gpg:             There is no indication that the signature belongs to the
owner.
Primary key fingerprint: 7478 91EF 5378 1334 4456 7603 06C9 06A7 093F F49D
```

Jika verifikasi gagal, itu berarti tanda tangan pada RPM berpotensi dirusak. Anda harus menghapus kunci publik dari database dan mencoba lagi proses verifikasi.

Contoh:

```
gpg: Signature made Fri 17 Nov 2023 07:58:11 PM UTC using ? key ID 093FF49D
gpg: BAD signature from "AwsGuardDuty"
```

Gunakan perintah berikut untuk menghapus kunci publik dari database:


```
gpg --delete-keys AwsGuardDuty
```

Sekarang, coba proses verifikasi lagi.

2. [Connect dengan SSH dari Linux atau macOS.](#)
3. Instal agen GuardDuty keamanan dengan menggunakan perintah berikut:

```
sudo rpm -ivh amazon-guardduty-agent-1.7.1.x86_64.rpm
```

4. Validasi jika instalasi GuardDuty agen sehat. Untuk informasi selengkapnya tentang langkah-langkahnya, lihat [Memvalidasi status instalasi agen GuardDuty keamanan.](#)

Debian installation

Important

Sebaiknya verifikasi tanda tangan agen GuardDuty keamanan Debian sebelum menginstalnya di mesin Anda.

1. Verifikasi tanda GuardDuty tangan agen keamanan Debian
 - a. Siapkan template untuk kunci publik yang sesuai, tanda tangan paket Debian amd64, tanda tangan paket Debian arm64, dan tautan akses terkait ke skrip Debian yang dihosting di bucket Amazon S3

Dalam template berikut, ganti nilai, ID AWS akun Wilayah AWS, dan versi GuardDuty agen untuk mengakses skrip paket Debian.

- Kunci publik:

```
s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.7.1/publickey.pem
```

- GuardDuty tanda tangan agen keamanan Debian:

Tanda tangan amd64

```
s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.7.1/amd64/
amazon-guardduty-agent-1.7.1.amd64.sig
```

Tanda tangan arm64

```
s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.7.1/arm64/
amazon-guardduty-agent-1.7.1.arm64.sig
```

- Akses tautan ke skrip Debian di bucket Amazon S3:

Tautan akses untuk amd64

```
s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.7.1/amd64/
amazon-guardduty-agent-1.7.1.amd64.deb
```

Tautan akses untuk arm64

```
s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.7.1/arm64/
amazon-guardduty-agent-1.7.1.arm64.deb
```

Wilayah AWS	Nama wilayah	AWS ID akun
eu-west-1	Eropa (Irlandia)	694911143906
us-east-1	AS Timur (Virginia Utara)	593207742271
us-west-2	AS Barat (Oregon)	733349766148
eu-west-3	Eropa (Paris)	665651866788
us-east-2	AS Timur (Ohio)	307168627858
eu-central-1	Eropa (Frankfurt)	323658145986
ap-northeast-2	Asia Pasifik (Seoul)	914738172881
eu-north-1	Eropa (Stockholm)	591436053604

ap-east-1	Asia Pasifik (Hong Kong)	258348409381
me-south-1	Timur Tengah (Bahrain)	536382113932
eu-west-2	Eropa (London)	892757235363
ap-northeast-1	Asia Pasifik (Tokyo)	533107202818
ap-southeast-1	Asia Pasifik (Singapura)	174946120834
ap-south-1	Asia Pasifik (Mumbai)	251508486986
ap-southeast-3	Asia Pasifik (Jakarta)	510637619217
sa-east-1	Amerika Selatan (Sao Paulo)	758426053663
ap-northeast-3	Asia Pasifik (Osaka)	273192626886
eu-south-1	Eropa (Milan)	266869475730
af-south-1	Afrika (Cape Town)	197869348890
ap-southeast-2	Asia Pasifik (Sydney)	005257825471
me-central-1	Timur Tengah (UEA)	000014521398
us-west-1	AS Barat (California Utara)	684579721401
ca-central-1	Kanada (Pusat)	354763396469
ca-west-1	Kanada Barat (Calgary)	339712888787
ap-south-2	Asia Pasifik (Hyderabad)	950823858135
eu-south-2	Eropa (Spanyol)	919611009337
eu-central-2	Eropa (Zürich)	529164026651
ap-southeast-4	Asia Pasifik (Melbourne)	251357961535

il-central-1	Israel (Tel Aviv)	870907303882
mx-central-1	Meksiko (Tengah)	982081086614

- b. Unduh kunci publik yang sesuai, tanda tangan amd64, tanda tangan arm64, dan tautan akses yang sesuai ke skrip Debian yang dihosting di bucket Amazon S3

Dalam perintah berikut, ganti ID akun dengan ID yang sesuai Akun AWS , dan Wilayah dengan Wilayah Anda saat ini.

```
aws s3 cp s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.7.1/
amd64/amazon-guardduty-agent-1.7.1.amd64.deb ./amazon-guardduty-
agent-1.7.1.amd64.deb
aws s3 cp s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.7.1/
amd64/amazon-guardduty-agent-1.7.1.amd64.sig ./amazon-guardduty-
agent-1.7.1.amd64.sig
aws s3 cp s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.7.1/
publickey.pem ./publickey.pem
```

- c. Impor kunci publik ke database

```
gpg --import publickey.pem
```

gpg menunjukkan impor berhasil

```
gpg: key 093FF49D: public key "AwsGuardDuty" imported
gpg: Total number processed: 1
gpg:          imported: 1 (RSA: 1)
```

- d. Verifikasi tanda tangan

```
gpg --verify amazon-guardduty-agent-1.7.1.amd64.sig amazon-guardduty-
agent-1.7.1.amd64.deb
```

Setelah verifikasi berhasil, Anda akan melihat pesan yang mirip dengan hasil berikut:

Contoh output:

```
gpg: Signature made Fri 17 Nov 2023 07:58:11 PM UTC using ? key ID 093FF49D
gpg: Good signature from "AwsGuardDuty"
gpg: WARNING: This key is not certified with a trusted signature!
```

```
gpg:          There is no indication that the signature belongs to the
owner.
Primary key fingerprint: 7478 91EF 5378 1334 4456  7603 06C9 06A7 093F F49D
```

Anda sekarang dapat melanjutkan untuk menginstal agen GuardDuty keamanan menggunakan Debian.

Namun, jika verifikasi gagal, itu berarti tanda tangan dalam paket Debian berpotensi dirusak.

Contoh:

```
gpg: Signature made Fri 17 Nov 2023 07:58:11 PM UTC using ? key ID 093FF49D
gpg: BAD signature from "AwsGuardDuty"
```

Gunakan perintah berikut untuk menghapus kunci publik dari database:

```
gpg --delete-keys AwsGuardDuty
```

Sekarang, coba lagi proses verifikasi.

2. [Connect dengan SSH dari Linux atau macOS.](#)
3. Instal agen GuardDuty keamanan dengan menggunakan perintah berikut:

```
sudo dpkg -i amazon-guardduty-agent-1.7.1.amd64.deb
```

4. Validasi jika instalasi GuardDuty agen sehat. Untuk informasi selengkapnya tentang langkah-langkahnya, lihat [Memvalidasi status instalasi agen GuardDuty keamanan](#).

Kesalahan kehabisan memori

Jika Anda mengalami out-of-memory kesalahan saat menginstal atau memperbarui agen GuardDuty keamanan untuk Amazon EC2 secara manual, lihat [Memecahkan masalah kesalahan memori](#).

Memvalidasi status instalasi agen GuardDuty keamanan

Setelah Anda melakukan langkah-langkah untuk menginstal agen GuardDuty keamanan, gunakan langkah-langkah berikut untuk memvalidasi status agen:

Untuk memvalidasi jika agen GuardDuty keamanan sehat

1. [Connect dengan SSH dari Linux atau macOS](#).
2. Jalankan perintah berikut untuk memeriksa status agen GuardDuty keamanan:

```
sudo systemctl status amazon-guardduty-agent
```

Jika Anda ingin melihat log instalasi agen keamanan, mereka tersedia di bawah `/var/log/amzn-guardduty-agent/`.

Untuk melihat log, lakukan `sudo journalctl -u amazon-guardduty-agent`.

Memperbarui agen GuardDuty keamanan untuk EC2 instans Amazon secara manual

GuardDuty merilis pembaruan ke versi agen keamanan. Saat mengelola agen keamanan secara manual, Anda bertanggung jawab untuk memperbarui agen untuk EC2 instans Amazon Anda. Untuk informasi tentang versi agen baru, lihat [GuardDuty versi rilis agen keamanan](#) EC2 instans Amazon. Untuk menerima pemberitahuan tentang rilis versi agen baru, lihat [Berlangganan pengumuman Amazon GuardDuty SNS](#).

Untuk memperbarui agen keamanan untuk EC2 instans Amazon secara manual

Proses untuk memperbarui agen keamanan sama dengan menginstal agen keamanan. Bergantung pada metode yang Anda gunakan untuk menginstal agen, Anda dapat melakukan langkah-langkah [Memasang agen keamanan secara manual](#) untuk EC2 instans Amazon.

Jika Anda menggunakan [Metode 1 - Dengan menggunakan AWS Systems Manager](#), maka Anda dapat memperbarui agen keamanan dengan menggunakan perintah Run. Gunakan versi agen yang ingin Anda perbarui.

Jika Anda menggunakan [Metode 2 - Dengan menggunakan Linux Package Managers](#), Anda dapat menggunakan skrip seperti yang ditentukan di [Memasang agen keamanan secara manual](#) bagian. Skrip sudah menyertakan versi rilis agen terbaru. Untuk informasi tentang versi agen yang baru dirilis, lihat [GuardDuty versi agen keamanan untuk EC2 instans Amazon](#).

Setelah Anda memperbarui agen keamanan, Anda dapat memeriksa status instalasi dengan melihat log. Untuk informasi selengkapnya, lihat [Memvalidasi status instalasi agen GuardDuty keamanan](#).

Mengelola agen keamanan otomatis untuk Fargate (hanya Amazon ECS)

Runtime Monitoring mendukung pengelolaan agen keamanan untuk cluster Amazon ECS (AWS Fargate) Anda hanya melalui GuardDuty. Tidak ada dukungan untuk mengelola agen keamanan secara manual di cluster Amazon ECS.

Sebelum melanjutkan dengan langkah-langkah di bagian ini, pastikan untuk mengikuti [Prasyarat untuk dukungan \(khusus AWS Fargate Amazon ECS\)](#).

Berdasarkan [Pendekatan untuk mengelola agen GuardDuty keamanan di sumber daya Amazon ECS-Fargate](#), pilih metode yang disukai untuk mengaktifkan agen GuardDuty otomatis untuk sumber daya Anda.

Mengkonfigurasi GuardDuty agen untuk lingkungan multi-akun

Dalam lingkungan beberapa akun, hanya akun GuardDuty administrator yang didelegasikan yang dapat mengaktifkan atau menonaktifkan konfigurasi agen otomatis untuk akun anggota, dan mengelola konfigurasi agen otomatis untuk kluster Amazon ECS milik akun anggota di organisasinya. Akun GuardDuty anggota tidak dapat mengubah konfigurasi ini. Akun GuardDuty administrator yang didelegasikan mengelola akun anggota mereka menggunakan AWS Organizations. Untuk informasi selengkapnya tentang lingkungan multi-akun, lihat [Mengelola beberapa akun di GuardDuty](#).

Mengaktifkan konfigurasi agen otomatis untuk akun administrator yang didelegasikan GuardDuty

Manage for all Amazon ECS clusters (account level)

Jika Anda memilih Aktifkan untuk semua akun untuk Runtime Monitoring, maka Anda memiliki opsi berikut:

- Pilih Aktifkan untuk semua akun di bagian Konfigurasi agen otomatis. GuardDuty akan menyebarkan dan mengelola agen keamanan untuk semua tugas Amazon ECS yang diluncurkan.
- Pilih Konfigurasikan akun secara manual.

Jika Anda memilih Konfigurasi akun secara manual di bagian Runtime Monitoring, lakukan hal berikut:

1. Pilih Konfigurasi akun secara manual di bagian Konfigurasi agen otomatis.
2. Pilih Aktifkan di bagian akun GuardDuty administrator yang didelegasikan (akun ini).

Pilih Simpan.

Ketika Anda GuardDuty ingin memantau tugas yang merupakan bagian dari layanan, itu memerlukan penerapan layanan baru setelah Anda mengaktifkan Runtime Monitoring. Jika penerapan terakhir untuk layanan ECS tertentu dimulai sebelum Anda mengaktifkan Runtime Monitoring, Anda dapat memulai ulang layanan, atau memperbarui layanan dengan menggunakan `forceNewDeployment`

Untuk langkah-langkah memperbarui layanan, lihat sumber daya berikut:

- [Memperbarui layanan Amazon ECS menggunakan konsol](#) di Panduan Pengembang Layanan Amazon Elastic Container.
- [UpdateService](#) di Referensi API Layanan Amazon Elastic Container.
- [update-service](#) di Command Reference.AWS CLI

Manage for all Amazon ECS clusters but exclude some of the clusters (cluster level)

1. Tambahkan tag ke cluster Amazon ECS ini dengan pasangan nilai kunci sebagai `- GuardDutyManaged false`
2. Mencegah modifikasi tag, kecuali oleh entitas tepercaya. Kebijakan yang disediakan dalam [Mencegah tag diubah kecuali oleh prinsip-prinsip resmi](#) dalam Panduan AWS Organizations Pengguna telah dimodifikasi agar dapat diterapkan di sini.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
      "Effect": "Deny",
      "Action": [
        "ecs:TagResource",
        "ecs:UntagResource"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringNotEquals": {
          "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}"
        }
      }
    }
  ]
}
```



```

        "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
    },
    "Null": {
        "ecs:ResourceTag/GuardDutyManaged": false
    }
},
{
    "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
    "Effect": "Deny",
    "Action": [
        "ecs:TagResource",
        "ecs:UntagResource"
    ],
    "Resource": [
        "*"
    ],
    "Condition": {
        "StringNotEquals": {
            "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
            "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
        },
        "ForAnyValue:StringEquals": {
            "aws:TagKeys": [
                "GuardDutyManaged"
            ]
        }
    }
},
{
    "Sid": "DenyModifyTagsIfPrinTagNotExists",
    "Effect": "Deny",
    "Action": [
        "ecs:TagResource",
        "ecs:UntagResource"
    ],
    "Resource": [
        "*"
    ],
    "Condition": {
        "StringNotEquals": {

```

```

        "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
      },
      "Null": {
        "aws:PrincipalTag/GuardDutyManaged": true
      }
    }
  ]
}

```

3. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.
4. Di panel navigasi, pilih Runtime Monitoring.
- 5.

 Note

Selalu tambahkan tag pengecualian ke kluster Amazon ECS Anda sebelum mengaktifkan konfigurasi agen otomatis untuk akun Anda; jika tidak, wadah GuardDuty sespan akan dilampirkan ke semua kontainer dalam tugas Amazon ECS yang diluncurkan.

Di bawah tab Konfigurasi, pilih Aktifkan dalam konfigurasi agen otomatis.

Untuk cluster Amazon ECS yang belum dikecualikan, GuardDuty akan mengelola penyebaran agen keamanan di wadah sespan.

6. Pilih Simpan.
7. Ketika Anda GuardDuty ingin memantau tugas yang merupakan bagian dari layanan, itu memerlukan penerapan layanan baru setelah Anda mengaktifkan Runtime Monitoring. Jika penerapan terakhir untuk layanan ECS tertentu dimulai sebelum Anda mengaktifkan Runtime Monitoring, Anda dapat memulai ulang layanan, atau memperbarui layanan dengan menggunakan `forceNewDeployment`

Untuk langkah-langkah memperbarui layanan, lihat sumber daya berikut:

- [Memperbarui layanan Amazon ECS menggunakan konsol](#) di Panduan Pengembang Layanan Amazon Elastic Container.
- [UpdateService](#) di Referensi API Layanan Amazon Elastic Container.
- [update-service](#) di Command Reference.AWS CLI

Manage for selective (inclusion only) Amazon ECS clusters (cluster level)

1. Tambahkan tag ke cluster Amazon ECS yang ingin Anda sertakan semua tugasnya. Pasangan kunci-nilai harus GuardDutyManaged -. true
2. Mencegah modifikasi tag ini, kecuali oleh entitas tepercaya. Kebijakan yang disediakan dalam [Mencegah tag diubah kecuali oleh prinsip-prinsip resmi](#) dalam Panduan AWS Organizations Pengguna telah dimodifikasi agar dapat diterapkan di sini.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
      "Effect": "Deny",
      "Action": [
        "ecs:TagResource",
        "ecs:UntagResource"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringNotEquals": {
          "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
          "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
        },
        "Null": {
          "ecs:ResourceTag/GuardDutyManaged": false
        }
      }
    },
    {
      "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
      "Effect": "Deny",
      "Action": [
        "ecs:TagResource",
        "ecs:UntagResource"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

```

    ],
    "Condition": {
      "StringNotEquals": {
        "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
        "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
      },
      "ForAnyValue:StringEquals": {
        "aws:TagKeys": [
          "GuardDutyManaged"
        ]
      }
    }
  },
  {
    "Sid": "DenyModifyTagsIfPrinTagNotExists",
    "Effect": "Deny",
    "Action": [
      "ecs:TagResource",
      "ecs:UntagResource"
    ],
    "Resource": [
      "*"
    ],
    "Condition": {
      "StringNotEquals": {
        "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
      },
      "Null": {
        "aws:PrincipalTag/GuardDutyManaged": true
      }
    }
  }
]
}

```

Note

Saat menggunakan tag inklusi untuk kluster Amazon ECS, Anda tidak perlu mengaktifkan GuardDuty agen melalui konfigurasi agen otomatis secara eksplisit.

3. Ketika Anda GuardDuty ingin memantau tugas yang merupakan bagian dari layanan, itu memerlukan penerapan layanan baru setelah Anda mengaktifkan Runtime Monitoring. Jika penerapan terakhir untuk layanan ECS tertentu dimulai sebelum Anda mengaktifkan Runtime Monitoring, Anda dapat memulai ulang layanan, atau memperbarui layanan dengan menggunakan `forceNewDeployment`

Untuk langkah-langkah memperbarui layanan, lihat sumber daya berikut:

- [Memperbarui layanan Amazon ECS menggunakan konsol](#) di Panduan Pengembang Layanan Amazon Elastic Container.
- [UpdateService](#) di Referensi API Layanan Amazon Elastic Container.
- [update-service](#) di Command Reference.AWS CLI

Aktifkan otomatis untuk semua akun anggota

Manage for all Amazon ECS clusters (account level)

Langkah-langkah berikut mengasumsikan bahwa Anda memilih Aktifkan untuk semua akun di bagian Runtime Monitoring.

1. Pilih Aktifkan untuk semua akun di bagian Konfigurasi agen otomatis. GuardDuty akan menyebarkan dan mengelola agen keamanan untuk semua tugas Amazon ECS yang diluncurkan.
2. Pilih Simpan.
3. Ketika Anda GuardDuty ingin memantau tugas yang merupakan bagian dari layanan, itu memerlukan penerapan layanan baru setelah Anda mengaktifkan Runtime Monitoring. Jika penerapan terakhir untuk layanan ECS tertentu dimulai sebelum Anda mengaktifkan Runtime Monitoring, Anda dapat memulai ulang layanan, atau memperbarui layanan dengan menggunakan `forceNewDeployment`

Untuk langkah-langkah memperbarui layanan, lihat sumber daya berikut:

- [Memperbarui layanan Amazon ECS menggunakan konsol](#) di Panduan Pengembang Layanan Amazon Elastic Container.
- [UpdateService](#) di Referensi API Layanan Amazon Elastic Container.
- [update-service](#) di Command Reference.AWS CLI

Manage for all Amazon ECS clusters but exclude some of the clusters (cluster level)

1. Tambahkan tag ke cluster Amazon ECS ini dengan pasangan nilai kunci sebagai -.
GuardDutyManaged false
2. Mencegah modifikasi tag, kecuali oleh entitas tepercaya. Kebijakan yang disediakan dalam [Mencegah tag diubah kecuali oleh prinsip-prinsip resmi](#) dalam Panduan AWS Organizations Pengguna telah dimodifikasi agar dapat diterapkan di sini.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
      "Effect": "Deny",
      "Action": [
        "ecs:TagResource",
        "ecs:UntagResource"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringNotEquals": {
          "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
          "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
        },
        "Null": {
          "ecs:ResourceTag/GuardDutyManaged": false
        }
      }
    },
    {
      "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
      "Effect": "Deny",
      "Action": [
        "ecs:TagResource",
        "ecs:UntagResource"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

```

    ],
    "Condition": {
      "StringNotEquals": {
        "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
        "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
      },
      "ForAnyValue:StringEquals": {
        "aws:TagKeys": [
          "GuardDutyManaged"
        ]
      }
    }
  },
  {
    "Sid": "DenyModifyTagsIfPrinTagNotExists",
    "Effect": "Deny",
    "Action": [
      "ecs:TagResource",
      "ecs:UntagResource"
    ],
    "Resource": [
      "*"
    ],
    "Condition": {
      "StringNotEquals": {
        "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
      },
      "Null": {
        "aws:PrincipalTag/GuardDutyManaged": true
      }
    }
  }
]
}

```

3. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.
4. Di panel navigasi, pilih Runtime Monitoring.

5.

 Note

Selalu tambahkan tag pengecualian ke kluster Amazon ECS Anda sebelum mengaktifkan konfigurasi agen otomatis untuk akun Anda; jika tidak, wadah GuardDuty sespan akan dilampirkan ke semua kontainer dalam tugas Amazon ECS yang diluncurkan.

Di bawah tab Konfigurasi, pilih Edit.

6. Pilih Aktifkan untuk semua akun di bagian Konfigurasi agen otomatis

Untuk cluster Amazon ECS yang belum dikecualikan, GuardDuty akan mengelola penyebaran agen keamanan di wadah sespan.

7. Pilih Simpan.

8. Ketika Anda GuardDuty ingin memantau tugas yang merupakan bagian dari layanan, itu memerlukan penerapan layanan baru setelah Anda mengaktifkan Runtime Monitoring. Jika penerapan terakhir untuk layanan ECS tertentu dimulai sebelum Anda mengaktifkan Runtime Monitoring, Anda dapat memulai ulang layanan, atau memperbarui layanan dengan menggunakan `forceNewDeployment`

Untuk langkah-langkah memperbarui layanan, lihat sumber daya berikut:

- [Memperbarui layanan Amazon ECS menggunakan konsol](#) di Panduan Pengembang Layanan Amazon Elastic Container.
- [UpdateService](#) di Referensi API Layanan Amazon Elastic Container.
- [update-service](#) di Command Reference.AWS CLI

Manage for selective (inclusion-only) Amazon ECS clusters (cluster level)

Terlepas dari cara Anda memilih untuk mengaktifkan Runtime Monitoring, langkah-langkah berikut akan membantu Anda memantau tugas Amazon ECS Fargate selektif untuk semua akun anggota di organisasi Anda.

1. Jangan aktifkan konfigurasi apa pun di bagian Konfigurasi agen otomatis. Pertahankan konfigurasi Runtime Monitoring sama seperti yang Anda pilih pada langkah sebelumnya.
2. Pilih Simpan.

3. Mencegah modifikasi tag ini, kecuali oleh entitas tepercaya. Kebijakan yang disediakan dalam [Mencegah tag diubah kecuali oleh prinsip-prinsip resmi](#) dalam Panduan AWS Organizations Pengguna telah dimodifikasi agar dapat diterapkan di sini.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
      "Effect": "Deny",
      "Action": [
        "ecs:TagResource",
        "ecs:UntagResource"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringNotEquals": {
          "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
          "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
        },
        "Null": {
          "ecs:ResourceTag/GuardDutyManaged": false
        }
      }
    },
    {
      "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
      "Effect": "Deny",
      "Action": [
        "ecs:TagResource",
        "ecs:UntagResource"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringNotEquals": {
          "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}"
        }
      }
    }
  ]
}
```

```

        "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
    },
    "ForAnyValue:StringEquals": {
        "aws:TagKeys": [
            "GuardDutyManaged"
        ]
    }
},
{
    "Sid": "DenyModifyTagsIfPrinTagNotExists",
    "Effect": "Deny",
    "Action": [
        "ecs:TagResource",
        "ecs:UntagResource"
    ],
    "Resource": [
        "*"
    ],
    "Condition": {
        "StringNotEquals": {
            "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
        },
        "Null": {
            "aws:PrincipalTag/GuardDutyManaged": true
        }
    }
}
]
}

```

Note

Saat menggunakan tag inklusi untuk kluster Amazon ECS, Anda tidak perlu mengaktifkan manajemen otomatis GuardDuty agen secara eksplisit.

4. Ketika Anda GuardDuty ingin memantau tugas yang merupakan bagian dari layanan, itu memerlukan penerapan layanan baru setelah Anda mengaktifkan Runtime Monitoring. Jika penerapan terakhir untuk layanan ECS tertentu dimulai sebelum Anda mengaktifkan

Runtime Monitoring, Anda dapat memulai ulang layanan, atau memperbarui layanan dengan menggunakan `forceNewDeployment`

Untuk langkah-langkah memperbarui layanan, lihat sumber daya berikut:

- [Memperbarui layanan Amazon ECS menggunakan konsol](#) di Panduan Pengembang Layanan Amazon Elastic Container.
- [UpdateService](#) di Referensi API Layanan Amazon Elastic Container.
- [update-service](#) di Command Reference.AWS CLI

Mengaktifkan konfigurasi agen otomatis untuk akun anggota aktif yang ada

Manage for all Amazon ECS clusters (account level)

1. Pada halaman Runtime Monitoring, di bawah tab Konfigurasi, Anda dapat melihat status konfigurasi agen Otomatis saat ini.
2. Dalam panel konfigurasi agen otomatis, di bawah bagian Akun anggota aktif, pilih Tindakan.
3. Dari Tindakan, pilih Aktifkan untuk semua akun anggota aktif yang ada.
4. Pilih Konfirmasi.
5. Ketika Anda GuardDuty ingin memantau tugas yang merupakan bagian dari layanan, itu memerlukan penerapan layanan baru setelah Anda mengaktifkan Runtime Monitoring. Jika penerapan terakhir untuk layanan ECS tertentu dimulai sebelum Anda mengaktifkan Runtime Monitoring, Anda dapat memulai ulang layanan, atau memperbarui layanan dengan menggunakan `forceNewDeployment`

Untuk langkah-langkah memperbarui layanan, lihat sumber daya berikut:

- [Memperbarui layanan Amazon ECS menggunakan konsol](#) di Panduan Pengembang Layanan Amazon Elastic Container.
- [UpdateService](#) di Referensi API Layanan Amazon Elastic Container.
- [update-service](#) di Command Reference.AWS CLI

Manage for all Amazon ECS clusters but exclude some of the clusters (cluster level)

1. Tambahkan tag ke cluster Amazon ECS ini dengan pasangan nilai kunci sebagai `- GuardDutyManaged false`

2. Mencegah modifikasi tag, kecuali oleh entitas tepercaya. Kebijakan yang disediakan dalam [Mencegah tag diubah kecuali oleh prinsip-prinsip resmi](#) dalam Panduan AWS Organizations Pengguna telah dimodifikasi agar dapat diterapkan di sini.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
      "Effect": "Deny",
      "Action": [
        "ecs:TagResource",
        "ecs:UntagResource"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringNotEquals": {
          "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
          "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
        },
        "Null": {
          "ecs:ResourceTag/GuardDutyManaged": false
        }
      }
    },
    {
      "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
      "Effect": "Deny",
      "Action": [
        "ecs:TagResource",
        "ecs:UntagResource"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringNotEquals": {
          "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}"
        }
      }
    }
  ]
}
```

```

        "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
      },
      "ForAnyValue:StringEquals": {
        "aws:TagKeys": [
          "GuardDutyManaged"
        ]
      }
    },
    {
      "Sid": "DenyModifyTagsIfPrinTagNotExists",
      "Effect": "Deny",
      "Action": [
        "ecs:TagResource",
        "ecs:UntagResource"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringNotEquals": {
          "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
        },
        "Null": {
          "aws:PrincipalTag/GuardDutyManaged": true
        }
      }
    }
  ]
}

```

3. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.
4. Di panel navigasi, pilih Runtime Monitoring.
- 5.

 Note

Selalu tambahkan tag pengecualian ke kluster Amazon ECS Anda sebelum mengaktifkan konfigurasi agen otomatis untuk akun Anda; jika tidak, wadah GuardDuty sespan akan dilampirkan ke semua kontainer dalam tugas Amazon ECS yang diluncurkan.

Di bawah tab Konfigurasi, di bagian Konfigurasi agen otomatis, di bawah Akun anggota aktif, pilih Tindakan.

6. Dari Tindakan, pilih Aktifkan untuk semua akun anggota aktif.

Untuk cluster Amazon ECS yang belum dikecualikan, GuardDuty akan mengelola penyebaran agen keamanan di wadah sespan.

7. Pilih Konfirmasi.
8. Ketika Anda GuardDuty ingin memantau tugas yang merupakan bagian dari layanan, itu memerlukan penerapan layanan baru setelah Anda mengaktifkan Runtime Monitoring. Jika penerapan terakhir untuk layanan ECS tertentu dimulai sebelum Anda mengaktifkan Runtime Monitoring, Anda dapat memulai ulang layanan, atau memperbarui layanan dengan menggunakan `forceNewDeployment`

Untuk langkah-langkah memperbarui layanan, lihat sumber daya berikut:

- [Memperbarui layanan Amazon ECS menggunakan konsol](#) di Panduan Pengembang Layanan Amazon Elastic Container.
- [UpdateService](#) di Referensi API Layanan Amazon Elastic Container.
- [update-service](#) di Command Reference.AWS CLI

Manage for selective (inclusion only) Amazon ECS clusters (cluster level)

1. Tambahkan tag ke cluster Amazon ECS yang ingin Anda sertakan semua tugasnya. Pasangan kunci-nilai harus `GuardDutyManaged - true`
2. Mencegah modifikasi tag ini, kecuali oleh entitas tepercaya. Kebijakan yang disediakan dalam [Mencegah tag diubah kecuali oleh prinsip-prinsip resmi](#) dalam Panduan AWS Organizations Pengguna telah dimodifikasi agar dapat diterapkan di sini.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
      "Effect": "Deny",
      "Action": [
        "ecs:TagResource",
```

```

        "ecs:UntagResource"
    ],
    "Resource": [
        "*"
    ],
    "Condition": {
        "StringNotEquals": {
            "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
            "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
        },
        "Null": {
            "ecs:ResourceTag/GuardDutyManaged": false
        }
    }
},
{
    "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
    "Effect": "Deny",
    "Action": [
        "ecs:TagResource",
        "ecs:UntagResource"
    ],
    "Resource": [
        "*"
    ],
    "Condition": {
        "StringNotEquals": {
            "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
            "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
        },
        "ForAnyValue:StringEquals": {
            "aws:TagKeys": [
                "GuardDutyManaged"
            ]
        }
    }
},
{
    "Sid": "DenyModifyTagsIfPrinTagNotExists",
    "Effect": "Deny",

```

```
    "Action": [
      "ecs:TagResource",
      "ecs:UntagResource"
    ],
    "Resource": [
      "*"
    ],
    "Condition": {
      "StringNotEquals": {
        "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-admins/iam-admin"
      },
      "Null": {
        "aws:PrincipalTag/GuardDutyManaged": true
      }
    }
  }
]
```

 Note

Saat menggunakan tag inklusi untuk kluster Amazon ECS, Anda tidak perlu mengaktifkan konfigurasi agen otomatis secara eksplisit.

3. Ketika Anda GuardDuty ingin memantau tugas yang merupakan bagian dari layanan, itu memerlukan penerapan layanan baru setelah Anda mengaktifkan Runtime Monitoring. Jika penerapan terakhir untuk layanan ECS tertentu dimulai sebelum Anda mengaktifkan Runtime Monitoring, Anda dapat memulai ulang layanan, atau memperbarui layanan dengan menggunakan `forceNewDeployment`

Untuk langkah-langkah memperbarui layanan, lihat sumber daya berikut:

- [Memperbarui layanan Amazon ECS menggunakan konsol](#) di Panduan Pengembang Layanan Amazon Elastic Container.
- [UpdateService](#) di Referensi API Layanan Amazon Elastic Container.
- [update-service](#) di Command Reference.AWS CLI

Aktifkan otomatis konfigurasi agen otomatis untuk anggota baru

Manage for all Amazon ECS clusters (account level)

1. Pada halaman Runtime Monitoring, pilih Edit untuk memperbarui konfigurasi yang ada.
2. Di bagian Konfigurasi agen otomatis, pilih Aktifkan secara otomatis untuk akun anggota baru.
3. Pilih Simpan.
4. Ketika Anda GuardDuty ingin memantau tugas yang merupakan bagian dari layanan, itu memerlukan penerapan layanan baru setelah Anda mengaktifkan Runtime Monitoring. Jika penerapan terakhir untuk layanan ECS tertentu dimulai sebelum Anda mengaktifkan Runtime Monitoring, Anda dapat memulai ulang layanan, atau memperbarui layanan dengan menggunakan `forceNewDeployment`

Untuk langkah-langkah memperbarui layanan, lihat sumber daya berikut:

- [Memperbarui layanan Amazon ECS menggunakan konsol](#) di Panduan Pengembang Layanan Amazon Elastic Container.
- [UpdateService](#) di Referensi API Layanan Amazon Elastic Container.
- [update-service](#) di Command Reference.AWS CLI

Manage for all Amazon ECS clusters but exclude some of the clusters (cluster level)

1. Tambahkan tag ke cluster Amazon ECS ini dengan pasangan nilai kunci sebagai `-GuardDutyManaged false`
2. Mencegah modifikasi tag, kecuali oleh entitas tepercaya. Kebijakan yang disediakan dalam [Mencegah tag diubah kecuali oleh prinsip-prinsip resmi](#) dalam Panduan AWS Organizations Pengguna telah dimodifikasi agar dapat diterapkan di sini.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
      "Effect": "Deny",
      "Action": [
        "ecs:TagResource",
        "ecs:UntagResource"
      ],
    }
  ],
}
```

```

        "Resource": [
            "*"
        ],
        "Condition": {
            "StringNotEquals": {
                "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
            },
            "Null": {
                "ecs:ResourceTag/GuardDutyManaged": false
            }
        }
    },
    {
        "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
        "Effect": "Deny",
        "Action": [
            "ecs:TagResource",
            "ecs:UntagResource"
        ],
        "Resource": [
            "*"
        ],
        "Condition": {
            "StringNotEquals": {
                "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
            },
            "ForAnyValue:StringEquals": {
                "aws:TagKeys": [
                    "GuardDutyManaged"
                ]
            }
        }
    },
    {
        "Sid": "DenyModifyTagsIfPrinTagNotExists",
        "Effect": "Deny",
        "Action": [
            "ecs:TagResource",

```

```
        "ecs:UntagResource"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringNotEquals": {
          "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-admins/iam-admin"
        },
        "Null": {
          "aws:PrincipalTag/GuardDutyManaged": true
        }
      }
    }
  ]
}
```

3. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.
4. Di panel navigasi, pilih Runtime Monitoring.
- 5.

 Note

Selalu tambahkan tag pengecualian ke kluster Amazon ECS Anda sebelum mengaktifkan konfigurasi agen otomatis untuk akun Anda; jika tidak, wadah GuardDuty sespan akan dilampirkan ke semua kontainer dalam tugas Amazon ECS yang diluncurkan.

Di bawah tab Konfigurasi, pilih Aktifkan secara otomatis untuk akun anggota baru di bagian Konfigurasi agen otomatis.

Untuk cluster Amazon ECS yang belum dikecualikan, GuardDuty akan mengelola penyebaran agen keamanan di wadah sespan.

6. Pilih Simpan.
7. Ketika Anda GuardDuty ingin memantau tugas yang merupakan bagian dari layanan, itu memerlukan penerapan layanan baru setelah Anda mengaktifkan Runtime Monitoring. Jika penerapan terakhir untuk layanan ECS tertentu dimulai sebelum Anda mengaktifkan Runtime Monitoring, Anda dapat memulai ulang layanan, atau memperbarui layanan dengan menggunakan `forceNewDeployment`

Untuk langkah-langkah memperbarui layanan, lihat sumber daya berikut:

- [Memperbarui layanan Amazon ECS menggunakan konsol](#) di Panduan Pengembang Layanan Amazon Elastic Container.
- [UpdateService](#) di Referensi API Layanan Amazon Elastic Container.
- [update-service](#) di Command Reference.AWS CLI

Manage for selective (inclusion only) Amazon ECS clusters (cluster level)

1. Tambahkan tag ke cluster Amazon ECS yang ingin Anda sertakan semua tugasnya. Pasangan kunci-nilai harus GuardDutyManaged -. true
2. Mencegah modifikasi tag ini, kecuali oleh entitas tepercaya. Kebijakan yang disediakan dalam [Mencegah tag diubah kecuali oleh prinsip-prinsip resmi](#) dalam Panduan AWS Organizations Pengguna telah dimodifikasi agar dapat diterapkan di sini.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
      "Effect": "Deny",
      "Action": [
        "ecs:TagResource",
        "ecs:UntagResource"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringNotEquals": {
          "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
          "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
        },
        "Null": {
          "ecs:ResourceTag/GuardDutyManaged": false
        }
      }
    }
  ],
}
```

```

    {
      "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
      "Effect": "Deny",
      "Action": [
        "ecs:TagResource",
        "ecs:UntagResource"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringNotEquals": {
          "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
          "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
        },
        "ForAnyValue:StringEquals": {
          "aws:TagKeys": [
            "GuardDutyManaged"
          ]
        }
      }
    },
    {
      "Sid": "DenyModifyTagsIfPrinTagNotExists",
      "Effect": "Deny",
      "Action": [
        "ecs:TagResource",
        "ecs:UntagResource"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringNotEquals": {
          "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
        },
        "Null": {
          "aws:PrincipalTag/GuardDutyManaged": true
        }
      }
    }
  }

```

```
]
}
```

Note

Saat menggunakan tag inklusi untuk kluster Amazon ECS, Anda tidak perlu mengaktifkan konfigurasi agen otomatis secara eksplisit.

3. Ketika Anda GuardDuty ingin memantau tugas yang merupakan bagian dari layanan, itu memerlukan penerapan layanan baru setelah Anda mengaktifkan Runtime Monitoring. Jika penerapan terakhir untuk layanan ECS tertentu dimulai sebelum Anda mengaktifkan Runtime Monitoring, Anda dapat memulai ulang layanan, atau memperbarui layanan dengan menggunakan `forceNewDeployment`

Untuk langkah-langkah memperbarui layanan, lihat sumber daya berikut:

- [Memperbarui layanan Amazon ECS menggunakan konsol](#) di Panduan Pengembang Layanan Amazon Elastic Container.
- [UpdateService](#) di Referensi API Layanan Amazon Elastic Container.
- [update-service](#) di Command Reference.AWS CLI

Mengaktifkan konfigurasi agen otomatis untuk akun anggota aktif secara selektif

Manage for all Amazon ECS (account level)

1. Pada halaman Akun, pilih akun yang ingin Anda aktifkan konfigurasi agen Runtime Monitoring-Automated agent (ECS-Fargate). Anda dapat memilih beberapa akun. Pastikan akun yang Anda pilih pada langkah ini sudah diaktifkan dengan Runtime Monitoring.
2. Dari Edit paket perlindungan, pilih opsi yang sesuai untuk mengaktifkan konfigurasi agen Runtime Monitoring-Automated agent (ECS-Fargate).
3. Pilih Konfirmasi.
4. Ketika Anda GuardDuty ingin memantau tugas yang merupakan bagian dari layanan, itu memerlukan penerapan layanan baru setelah Anda mengaktifkan Runtime Monitoring. Jika penerapan terakhir untuk layanan ECS tertentu dimulai sebelum Anda mengaktifkan Runtime Monitoring, Anda dapat memulai ulang layanan, atau memperbarui layanan dengan menggunakan `forceNewDeployment`

Untuk langkah-langkah memperbarui layanan, lihat sumber daya berikut:

- [Memperbarui layanan Amazon ECS menggunakan konsol](#) di Panduan Pengembang Layanan Amazon Elastic Container.
- [UpdateService](#) di Referensi API Layanan Amazon Elastic Container.
- [update-service](#) di Command Reference.AWS CLI

Manage for all Amazon ECS clusters but exclude some of the clusters (cluster level)

1. Tambahkan tag ke cluster Amazon ECS ini dengan pasangan nilai kunci sebagai -. GuardDutyManaged false
2. Mencegah modifikasi tag, kecuali oleh entitas tepercaya. Kebijakan yang disediakan dalam [Mencegah tag diubah kecuali oleh prinsip-prinsip resmi](#) dalam Panduan AWS Organizations Pengguna telah dimodifikasi agar dapat diterapkan di sini.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
      "Effect": "Deny",
      "Action": [
        "ecs:TagResource",
        "ecs:UntagResource"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringNotEquals": {
          "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
          "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
        },
        "Null": {
          "ecs:ResourceTag/GuardDutyManaged": false
        }
      }
    }
  ],
}
```

```

    {
      "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
      "Effect": "Deny",
      "Action": [
        "ecs:TagResource",
        "ecs:UntagResource"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringNotEquals": {
          "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
          "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
        },
        "ForAnyValue:StringEquals": {
          "aws:TagKeys": [
            "GuardDutyManaged"
          ]
        }
      }
    },
    {
      "Sid": "DenyModifyTagsIfPrinTagNotExists",
      "Effect": "Deny",
      "Action": [
        "ecs:TagResource",
        "ecs:UntagResource"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringNotEquals": {
          "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
        },
        "Null": {
          "aws:PrincipalTag/GuardDutyManaged": true
        }
      }
    }
  }

```



```
]
}
```

3. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.
4. Di panel navigasi, pilih Runtime Monitoring.
- 5.

 Note

Selalu tambahkan tag pengecualian ke kluster Amazon ECS Anda sebelum mengaktifkan manajemen otomatis GuardDuty agen untuk akun Anda; jika tidak, wadah GuardDuty sespan akan dilampirkan ke semua kontainer dalam tugas Amazon ECS yang diluncurkan.

Pada halaman Akun, pilih akun yang ingin Anda aktifkan konfigurasi agen Runtime Monitoring-Automated agent (ECS-Fargate). Anda dapat memilih beberapa akun. Pastikan akun yang Anda pilih pada langkah ini sudah diaktifkan dengan Runtime Monitoring.

Untuk cluster Amazon ECS yang belum dikecualikan, GuardDuty akan mengelola penyebaran agen keamanan di wadah sespan.

6. Dari Edit paket perlindungan, pilih opsi yang sesuai untuk mengaktifkan konfigurasi agen Runtime Monitoring-Automated agent (ECS-Fargate).
7. Pilih Simpan.
8. Ketika Anda GuardDuty ingin memantau tugas yang merupakan bagian dari layanan, itu memerlukan penerapan layanan baru setelah Anda mengaktifkan Runtime Monitoring. Jika penerapan terakhir untuk layanan ECS tertentu dimulai sebelum Anda mengaktifkan Runtime Monitoring, Anda dapat memulai ulang layanan, atau memperbarui layanan dengan menggunakan `forceNewDeployment`

Untuk langkah-langkah memperbarui layanan, lihat sumber daya berikut:

- [Memperbarui layanan Amazon ECS menggunakan konsol](#) di Panduan Pengembang Layanan Amazon Elastic Container.
- [UpdateService](#) di Referensi API Layanan Amazon Elastic Container.
- [update-service](#) di Command Reference.AWS CLI

Manage for selective (inclusion only) Amazon ECS clusters (cluster level)

1. Pastikan Anda tidak mengaktifkan konfigurasi agen Otomatis (atau konfigurasi agen Runtime Monitoring-Automated agent (ECS-Fargate)) untuk akun terpilih yang memiliki cluster Amazon ECS yang ingin Anda pantau.
2. Tambahkan tag ke cluster Amazon ECS yang ingin Anda sertakan semua tugasnya. Pasangan kunci-nilai harus GuardDutyManaged -. true
3. Mencegah modifikasi tag ini, kecuali oleh entitas tepercaya. Kebijakan yang disediakan dalam [Mencegah tag diubah kecuali oleh prinsip-prinsip resmi](#) dalam Panduan AWS Organizations Pengguna telah dimodifikasi agar dapat diterapkan di sini.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
      "Effect": "Deny",
      "Action": [
        "ecs:TagResource",
        "ecs:UntagResource"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringNotEquals": {
          "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
          "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
        },
        "Null": {
          "ecs:ResourceTag/GuardDutyManaged": false
        }
      }
    },
    {
      "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
      "Effect": "Deny",
      "Action": [
        "ecs:TagResource",
        "ecs:UntagResource"
      ]
    }
  ]
}
```

```

    ],
    "Resource": [
        "*"
    ],
    "Condition": {
        "StringNotEquals": {
            "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
            "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
        },
        "ForAnyValue:StringEquals": {
            "aws:TagKeys": [
                "GuardDutyManaged"
            ]
        }
    }
},
{
    "Sid": "DenyModifyTagsIfPrinTagNotExists",
    "Effect": "Deny",
    "Action": [
        "ecs:TagResource",
        "ecs:UntagResource"
    ],
    "Resource": [
        "*"
    ],
    "Condition": {
        "StringNotEquals": {
            "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
        },
        "Null": {
            "aws:PrincipalTag/GuardDutyManaged": true
        }
    }
}
]
}

```

 Note

Saat menggunakan tag inklusi untuk kluster Amazon ECS, Anda tidak perlu mengaktifkan konfigurasi agen otomatis secara eksplisit.

4. Ketika Anda GuardDuty ingin memantau tugas yang merupakan bagian dari layanan, itu memerlukan penerapan layanan baru setelah Anda mengaktifkan Runtime Monitoring. Jika penerapan terakhir untuk layanan ECS tertentu dimulai sebelum Anda mengaktifkan Runtime Monitoring, Anda dapat memulai ulang layanan, atau memperbarui layanan dengan menggunakan `forceNewDeployment`

Untuk langkah-langkah memperbarui layanan, lihat sumber daya berikut:

- [Memperbarui layanan Amazon ECS menggunakan konsol](#) di Panduan Pengembang Layanan Amazon Elastic Container.
- [UpdateService](#) di Referensi API Layanan Amazon Elastic Container.
- [update-service](#) di Command Reference.AWS CLI

Mengkonfigurasi GuardDuty agen untuk akun mandiri

1. Masuk ke AWS Management Console dan buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.
2. Di panel navigasi, pilih Runtime Monitoring.
3. Di bawah tab Konfigurasi:
 - a. Untuk mengelola konfigurasi agen otomatis untuk semua kluster Amazon ECS (tingkat akun)

Pilih Aktifkan di bagian Konfigurasi agen otomatis untuk AWS Fargate (khusus ECS). Ketika tugas Fargate Amazon ECS baru diluncurkan, GuardDuty akan mengelola penyebaran agen keamanan.

 - Pilih Simpan.
 - b. Untuk mengelola konfigurasi agen otomatis dengan mengecualikan beberapa cluster Amazon ECS (tingkat cluster)
 - i. Tambahkan tag ke cluster Amazon ECS yang ingin Anda kecualikan semua tugasnya. Pasang kunci-nilai harus `GuardDutyManaged - false`

- ii. Mencegah modifikasi tag ini, kecuali oleh entitas tepercaya. Kebijakan yang disediakan dalam [Mencegah tag diubah kecuali oleh prinsip-prinsip resmi](#) dalam Panduan AWS Organizations Pengguna telah dimodifikasi agar dapat diterapkan di sini.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
      "Effect": "Deny",
      "Action": [
        "ecs:TagResource",
        "ecs:UntagResource"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringNotEquals": {
          "ecs:ResourceTag/GuardDutyManaged":
            "${aws:PrincipalTag/GuardDutyManaged}",
          "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
        },
        "Null": {
          "ecs:ResourceTag/GuardDutyManaged": false
        }
      }
    },
    {
      "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
      "Effect": "Deny",
      "Action": [
        "ecs:TagResource",
        "ecs:UntagResource"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringNotEquals": {
          "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",

```

```

        "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
    },
    "ForAnyValue:StringEquals": {
        "aws:TagKeys": [
            "GuardDutyManaged"
        ]
    }
},
{
    "Sid": "DenyModifyTagsIfPrinTagNotExists",
    "Effect": "Deny",
    "Action": [
        "ecs:TagResource",
        "ecs:UntagResource"
    ],
    "Resource": [
        "*"
    ],
    "Condition": {
        "StringNotEquals": {
            "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
        },
        "Null": {
            "aws:PrincipalTag/GuardDutyManaged": true
        }
    }
}
]
}

```

- iii. Di bawah tab Konfigurasi, pilih Aktifkan di bagian Konfigurasi agen otomatis.

Note

Selalu tambahkan tag pengecualian ke cluster Amazon ECS Anda sebelum mengaktifkan manajemen otomatis GuardDuty agen untuk akun Anda; jika tidak, agen keamanan akan digunakan di semua tugas yang diluncurkan dalam cluster Amazon ECS yang sesuai.

Untuk cluster Amazon ECS yang belum dikecualikan, GuardDuty akan mengelola penyebaran agen keamanan di wadah sespan.

- iv. Pilih Simpan.
- c. Untuk mengelola konfigurasi agen otomatis dengan menyertakan beberapa cluster Amazon ECS (tingkat cluster)
 - i. Tambahkan tag ke cluster Amazon ECS yang ingin Anda sertakan semua tugasnya. Pasangan kunci-nilai harus GuardDutyManaged -. true
 - ii. Mencegah modifikasi tag ini, kecuali oleh entitas tepercaya. Kebijakan yang disediakan dalam [Mencegah tag diubah kecuali oleh prinsip-prinsip resmi](#) dalam Panduan AWS Organizations Pengguna telah dimodifikasi agar dapat diterapkan di sini.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
      "Effect": "Deny",
      "Action": [
        "ecs:TagResource",
        "ecs:UntagResource"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringNotEquals": {
          "ecs:ResourceTag/GuardDutyManaged":
            "${aws:PrincipalTag/GuardDutyManaged}",
          "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
        },
        "Null": {
          "ecs:ResourceTag/GuardDutyManaged": false
        }
      }
    },
    {
      "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
      "Effect": "Deny",
```

```

        "Action": [
            "ecs:TagResource",
            "ecs:UntagResource"
        ],
        "Resource": [
            "*"
        ],
        "Condition": {
            "StringNotEquals": {
                "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
            },
            "ForAnyValue:StringEquals": {
                "aws:TagKeys": [
                    "GuardDutyManaged"
                ]
            }
        }
    },
    {
        "Sid": "DenyModifyTagsIfPrinTagNotExists",
        "Effect": "Deny",
        "Action": [
            "ecs:TagResource",
            "ecs:UntagResource"
        ],
        "Resource": [
            "*"
        ],
        "Condition": {
            "StringNotEquals": {
                "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
            },
            "Null": {
                "aws:PrincipalTag/GuardDutyManaged": true
            }
        }
    }
]
}

```


4. Ketika Anda GuardDuty ingin memantau tugas yang merupakan bagian dari layanan, itu memerlukan penerapan layanan baru setelah Anda mengaktifkan Runtime Monitoring. Jika penerapan terakhir untuk layanan ECS tertentu dimulai sebelum Anda mengaktifkan Runtime Monitoring, Anda dapat memulai ulang layanan, atau memperbarui layanan dengan menggunakan `forceNewDeployment`

Untuk langkah-langkah memperbarui layanan, lihat sumber daya berikut:

- [Memperbarui layanan Amazon ECS menggunakan konsol](#) di Panduan Pengembang Layanan Amazon Elastic Container.
- [UpdateService](#) di Referensi API Layanan Amazon Elastic Container.
- [update-service](#) di Command Reference.AWS CLI

Mengelola agen keamanan secara otomatis untuk sumber daya Amazon EKS

Runtime Monitoring mendukung pengaktifan agen keamanan melalui konfigurasi GuardDuty otomatis dan secara manual. Bagian ini menyediakan langkah-langkah untuk mengaktifkan konfigurasi agen otomatis untuk kluster Amazon EKS.

Sebelum melanjutkan, pastikan Anda telah mengikuti [Prasyarat untuk dukungan cluster Amazon EKS](#)

Berdasarkan pendekatan pilihan Anda tentang cara melakukannya [Mengelola agen keamanan melalui GuardDuty](#), pilih langkah-langkah di bagian berikut yang sesuai.

Mengkonfigurasi agen otomatis untuk lingkungan multi-akun

Dalam lingkungan beberapa akun, hanya akun GuardDuty administrator yang didelegasikan yang dapat mengaktifkan atau menonaktifkan konfigurasi agen otomatis untuk akun anggota, dan mengelola Agen otomatis untuk kluster EKS milik akun anggota di organisasi mereka. Akun GuardDuty anggota tidak dapat mengubah konfigurasi ini dari akun mereka. Akun akun GuardDuty administrator yang didelegasikan mengelola akun anggota mereka menggunakan AWS Organizations. Untuk informasi selengkapnya tentang lingkungan multi-akun, lihat [Mengelola beberapa akun](#).

Mengkonfigurasi konfigurasi agen otomatis untuk akun administrator yang didelegasikan GuardDuty

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-Langkah
Mengelola agen keamanan melalui GuardDuty (Pantau semua kluster EKS)	Jika Anda memilih Aktifkan untuk semua akun di bagian Runtime Monitoring, maka Anda memiliki opsi berikut: • Pilih Aktifkan untuk semua akun di bagian Konfigurasi agen otomatis. GuardDuty akan menyebarkan dan mengelola agen keamanan untuk semua kluster EKS yang termasuk dalam akun akun GuardDuty administrator yang didelegasikan dan juga untuk semua kluster EKS yang termasuk dalam semua akun anggota yang ada dan berpotensi baru di organisasi. • Pilih Konfigurasikan akun secara manual. Jika Anda memilih Konfigurasi akun secara manual di bagian Runtime Monitoring, lakukan hal berikut: 1. Pilih Konfigurasi akun secara manual di bagian Konfigurasi agen otomatis. 2. Pilih Aktifkan di bagian akun GuardDuty administrator yang didelegasikan (akun ini). Pilih Simpan.
Pantau semua cluster EKS tetapi kecualikan beberapa di antaranya (menggunakan tag pengecualian)	Dari prosedur berikut, pilih salah satu skenario yang berlaku untuk Anda. Untuk mengecualikan klaster EKS dari pemantauan saat agen GuardDuty keamanan belum digunakan di cluster ini 1. Tambahkan tag ke cluster EKS ini dengan kunci as GuardDuty Managed dan nilainya sebagaifalse.

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-Langkah
	Untuk informasi selengkapnya tentang menandai kluster Amazon EKS Anda, lihat Bekerja dengan tag menggunakan konsol di Panduan Pengguna Amazon EKS. 2. Untuk mencegah modifikasi tag, kecuali oleh entitas tepercaya, gunakan kebijakan yang disediakan dalam Mencegah tag agar tidak dimodifikasi kecuali oleh prinsipal resmi dalam Panduan Pengguna AWS Organizations. Dalam kebijakan ini, ganti detail berikut: • Ganti <code>ec2:CreateTags</code> dengan <code>eks:TagResource</code>. • Ganti <code>ec2:DeleteTags</code> dengan <code>eks:UntagResource</code>. • Ganti <code>access-project</code> dengan <code>GuardDutyManaged</code>. • Ganti <code>123456789012</code> dengan Akun AWS ID entitas tepercaya. Jika Anda memiliki lebih dari satu entitas tepercaya, gunakan contoh berikut untuk menambahkan beberapa Principal Arn : <pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre> 3. Buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/. 4. Di panel navigasi, pilih Runtime Monitoring.  Note Selalu tambahkan tag pengecualian ke kluster EKS Anda sebelum mengaktifkan manajemen otomatis GuardDuty agen untuk akun Anda; jika tidak, agen GuardDuty

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-Langkah
	keamanan akan digunakan di semua kluster EKS di akun Anda. 5. Di bawah tab Konfigurasi, pilih Aktifkan di bagian manajemen GuardDuty agen. Untuk kluster EKS yang belum dikecualikan dari pemantauan, GuardDuty akan mengelola penyebaran dan pembaruan ke agen GuardDuty keamanan. 6. Pilih Simpan. Untuk mengecualikan kluster EKS dari pemantauan saat agen GuardDuty keamanan telah digunakan di cluster ini 1. Tambahkan tag ke cluster EKS ini dengan kunci <code>as GuardDuty Managed</code> dan nilainya sebagai <code>false</code>. Untuk informasi selengkapnya tentang menandai kluster Amazon EKS Anda, lihat Bekerja dengan tag menggunakan konsol di Panduan Pengguna Amazon EKS. 2. Untuk mencegah modifikasi tag, kecuali oleh entitas tepercaya, gunakan kebijakan yang disediakan dalam Mencegah tag agar tidak dimodifikasi kecuali oleh prinsipal resmi dalam Panduan Pengguna AWS Organizations. Dalam kebijakan ini, ganti detail berikut: • Ganti <code>ec2:CreateTags</code> dengan <code>eks:TagResource</code> . • Ganti <code>ec2:DeleteTags</code> dengan <code>eks:UntagResource</code> . • Ganti <code>access-project</code> dengan <code>GuardDutyManaged</code> • Ganti <code>123456789012</code> dengan Akun AWS ID entitas tepercaya.

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-Langkah
	Jika Anda memiliki lebih dari satu entitas tepercaya, gunakan contoh berikut untuk menambahkan beberapa <code>PrincipalArn</code> : <pre data-bbox="618 474 1507 674">"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre> 3. Jika Anda mengaktifkan agen otomatis untuk kluster EKS ini, maka setelah langkah ini, tidak GuardDuty akan memperbarui agen keamanan untuk cluster ini. Namun, agen keamanan akan tetap digunakan dan GuardDuty akan terus menerima peristiwa runtime dari cluster EKS ini. Ini dapat memengaruhi statistik penggunaan Anda. - Untuk berhenti menerima peristiwa runtime dari cluster ini, Anda harus menghapus agen keamanan yang digunakan dari kluster EKS ini. Untuk informasi selengkapnya tentang menghapus agen keamanan yang digunakan, lihat Menonaktifkan, menghapus instalasi, dan membersihkan sumber daya di Runtime Monitoring 4. Jika Anda mengelola agen GuardDuty keamanan untuk cluster EKS ini secara manual, lihat Menonaktifkan, menghapus instalasi, dan membersihkan sumber daya di Runtime Monitoring.

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-Langkah
Pantau kluster EKS selektif menggunakan tag inklusi	Terlepas dari bagaimana Anda memilih untuk mengaktifkan Runtime Monitoring, langkah-langkah berikut akan membantu Anda memantau kluster EKS selektif di akun Anda: 1. Pastikan untuk memilih Nonaktifkan untuk akun GuardDuty administrator yang didelegasikan (akun ini) di bagian Konfigurasi agen otomatis. Pertahankan konfigurasi Runtime Monitoring sama seperti yang dikonfigurasi pada langkah sebelumnya. 2. Pilih Simpan. 3. Tambahkan tag ke kluster EKS Anda dengan kunci <code>asGuardDutyManaged</code> dan nilainya sebagai <code>true</code>. Untuk informasi selengkapnya tentang menandai kluster Amazon EKS Anda, lihat Bekerja dengan tag menggunakan konsol di Panduan Pengguna Amazon EKS. GuardDuty akan mengelola penyebaran dan pembaruan ke agen keamanan untuk kluster EKS selektif yang ingin Anda pantau. 4. Untuk mencegah modifikasi tag, kecuali oleh entitas tepercaya, gunakan kebijakan yang disediakan dalam Mencegah tag agar tidak dimodifikasi kecuali oleh prinsipal resmi dalam Panduan Pengguna AWS Organizations. Dalam kebijakan ini, ganti detail berikut: • Ganti <code>ec2:CreateTags</code> dengan <code>eks:TagResource</code>. • Ganti <code>ec2:DeleteTags</code> dengan <code>eks:UntagResource</code>. • Ganti <code>access-project</code> dengan <code>GuardDutyManaged</code>. • Ganti <code>123456789012</code> dengan Akun AWS ID entitas tepercaya. Jika Anda memiliki lebih dari satu entitas tepercaya, gunakan contoh berikut untuk menambahkan beberapa <code>PrincipalArn</code>:

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-Langkah
	<pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre>
Mengelola agen GuardDuty keamanan secara manual	Terlepas dari bagaimana Anda memilih untuk mengaktifkan Runtime Monitoring, Anda dapat mengelola agen keamanan secara manual untuk kluster EKS Anda. 1. Pastikan untuk memilih Nonaktifkan untuk akun GuardDuty administrator yang didelegasikan (akun ini) di bagian Konfigurasi agen otomatis. Pertahankan konfigurasi Runtime Monitoring sama seperti yang dikonfigurasi pada langkah sebelumnya. 2. Pilih Simpan. 3. Untuk mengelola agen keamanan, lihat Mengelola agen keamanan secara manual untuk kluster Amazon EKS.

Aktifkan otomatis Agen otomatis untuk semua akun anggota

 Note

Mungkin diperlukan waktu hingga 24 jam untuk memperbarui konfigurasi akun anggota.

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-Langkah
Mengelola agen keamanan melalui GuardDuty	Topik ini adalah untuk mengaktifkan Runtime Monitoring untuk semua akun anggota dan oleh karena itu, langkah-langkah berikut mengasumsikan bahwa Anda harus memilih Aktifkan untuk semua akun di bagian Runtime Monitoring.

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-Langkah
(Pantau semua kluster EKS)	1. Pilih Aktifkan untuk semua akun di bagian Konfigurasi agen otomatis. GuardDuty akan menyebarkan dan mengelola agen keamanan untuk semua kluster EKS yang termasuk dalam akun akun GuardDuty administrator yang didelegasikan dan juga untuk semua kluster EKS yang termasuk dalam semua akun anggota yang ada dan berpotensi baru di organisasi. 2. Pilih Simpan.

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-Langkah
Pantau semua cluster EKS tetapi kecualikan beberapa di antaranya (menggunakan tag pengecualian)	Dari prosedur berikut, pilih salah satu skenario yang berlaku untuk Anda. Untuk mengecualikan kluster EKS dari pemantauan saat agen GuardDuty keamanan belum digunakan di cluster ini 1. Tambahkan tag ke cluster EKS ini dengan kunci <code>as GuardDutyManaged</code> dan nilainya sebagai <code>false</code>. Untuk informasi selengkapnya tentang menandai kluster Amazon EKS Anda, lihat Bekerja dengan tag menggunakan konsol di Panduan Pengguna Amazon EKS. 2. Untuk mencegah modifikasi tag, kecuali oleh entitas tepercaya, gunakan kebijakan yang disediakan dalam Mencegah tag agar tidak dimodifikasi kecuali oleh prinsipal resmi dalam Panduan Pengguna AWS Organizations. Dalam kebijakan ini, ganti detail berikut: • Ganti <code>ec2:CreateTags</code> dengan <code>eks:TagResource</code>. • Ganti <code>ec2:DeleteTags</code> dengan <code>eks:UntagResource</code>. • Ganti <code>access-project</code> dengan <code>GuardDutyManaged</code> • Ganti <code>123456789012</code> dengan Akun AWS ID entitas tepercaya. Jika Anda memiliki lebih dari satu entitas tepercaya, gunakan contoh berikut untuk menambahkan beberapa <code>PrincipalArn</code>: <pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre>

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-Langkah
	3. Buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/. 4. Di panel navigasi, pilih Runtime Monitoring.  Note Selalu tambahkan tag pengecualian ke kluster EKS Anda sebelum mengaktifkan Agen otomatis untuk akun Anda; jika tidak, agen GuardDuty keamanan akan digunakan di semua kluster EKS di akun Anda. 5. Di bawah tab Konfigurasi, pilih Edit di bagian konfigurasi Runtime Monitoring. 6. Pilih Aktifkan untuk semua akun di bagian Konfigurasi agen otomatis. Untuk kluster EKS yang belum dikecualikan dari pemantauan, GuardDuty akan mengelola penyebaran dan pembaruan ke agen GuardDuty keamanan. 7. Pilih Simpan. Untuk mengecualikan kluster EKS dari pemantauan saat agen GuardDuty keamanan telah digunakan di cluster ini 1. Tambahkan tag ke cluster EKS ini dengan kunci <code>as GuardDuty Managed</code> dan nilainya sebagai <code>false</code>. Untuk informasi selengkapnya tentang menandai kluster Amazon EKS Anda, lihat Bekerja dengan tag menggunakan konsol di Panduan Pengguna Amazon EKS. 2. Jika Anda mengaktifkan konfigurasi agen otomatis untuk kluster EKS ini, maka setelah langkah ini, tidak GuardDuty akan memperbarui agen keamanan untuk cluster ini. Namun, agen keamanan akan tetap digunakan dan GuardDuty akan

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-Langkah
	terus menerima peristiwa runtime dari cluster EKS ini. Ini dapat memengaruhi statistik penggunaan Anda. Untuk berhenti menerima peristiwa runtime dari cluster ini, Anda harus menghapus agen keamanan yang digunakan dari klaster EKS ini. Untuk informasi selengkapnya tentang menghapus agen keamanan yang digunakan, lihat Menonaktifkan, menghapus instalasi, dan membersihkan sumber daya di Runtime Monitoring 3. Untuk mencegah modifikasi tag, kecuali oleh entitas tepercaya, gunakan kebijakan yang disediakan dalam Mencegah tag agar tidak dimodifikasi kecuali oleh prinsipal resmi dalam Panduan Pengguna AWS Organizations. Dalam kebijakan ini, ganti detail berikut: • Ganti <code>ec2:CreateTags</code> dengan <code>eks:TagResource</code>. • Ganti <code>ec2:DeleteTags</code> dengan <code>eks:UntagResource</code>. • Ganti <code>access-project</code> dengan <code>GuardDutyManaged</code>. • Ganti <code>123456789012</code> dengan Akun AWS ID entitas tepercaya. Jika Anda memiliki lebih dari satu entitas tepercaya, gunakan contoh berikut untuk menambahkan beberapa Principal Arn : <pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre> 4. Jika Anda mengelola agen GuardDuty keamanan untuk cluster EKS ini secara manual, lihat Menonaktifkan, menghapus instalasi, dan membersihkan sumber daya di Runtime Monitoring.

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-Langkah
Pantau kluster EKS selektif menggunakan tag inklusi	Terlepas dari bagaimana Anda memilih untuk mengaktifkan Runtime Monitoring, langkah-langkah berikut akan membantu Anda memantau kluster EKS selektif untuk semua akun anggota di organisasi Anda: 1. Jangan aktifkan konfigurasi apa pun di bagian Konfigurasi agen otomatis. Pertahankan konfigurasi Runtime Monitoring sama seperti yang dikonfigurasi pada langkah sebelumnya. 2. Pilih Simpan. 3. Tambahkan tag ke kluster EKS Anda dengan kunci <code>asGuardDutyManaged</code> dan nilainya sebagai <code>true</code>. Untuk informasi selengkapnya tentang menandai kluster Amazon EKS Anda, lihat Bekerja dengan tag menggunakan konsol di Panduan Pengguna Amazon EKS. GuardDuty akan mengelola penyebaran dan pembaruan ke agen keamanan untuk kluster EKS selektif yang ingin Anda pantau. 4. Untuk mencegah modifikasi tag, kecuali oleh entitas tepercaya, gunakan kebijakan yang disediakan dalam Mencegah tag agar tidak dimodifikasi kecuali oleh prinsipal resmi dalam Panduan Pengguna AWS Organizations. Dalam kebijakan ini, ganti detail berikut: • Ganti <code>ec2:CreateTags</code> dengan <code>eks:TagResource</code>. • Ganti <code>ec2:DeleteTags</code> dengan <code>eks:UntagResource</code>. • Ganti <code>access-project</code> dengan <code>GuardDutyManaged</code>. • Ganti <code>123456789012</code> dengan Akun AWS ID entitas tepercaya. Jika Anda memiliki lebih dari satu entitas tepercaya, gunakan contoh berikut untuk menambahkan beberapa <code>PrincipalArn</code>:

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-Langkah
	<pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre>
Mengelola agen GuardDuty keamanan secara manual	Terlepas dari bagaimana Anda memilih untuk mengaktifkan Runtime Monitoring, Anda dapat mengelola agen keamanan secara manual untuk kluster EKS Anda. 1. Jangan aktifkan konfigurasi apa pun di bagian Konfigurasi agen otomatis. Pertahankan konfigurasi Runtime Monitoring sama seperti yang dikonfigurasi pada langkah sebelumnya. 2. Pilih Simpan. 3. Untuk mengelola agen keamanan, lihat Mengelola agen keamanan secara manual untuk kluster Amazon EKS.

Mengaktifkan agen otomatis untuk semua akun anggota aktif yang ada

 Note

Mungkin diperlukan waktu hingga 24 jam untuk memperbarui konfigurasi akun anggota.

Untuk mengelola agen GuardDuty keamanan untuk akun anggota aktif yang ada di organisasi Anda

- GuardDuty Untuk menerima acara runtime dari kluster EKS yang termasuk dalam akun anggota aktif yang ada di organisasi, Anda harus memilih pendekatan yang disukai untuk mengelola agen GuardDuty keamanan untuk kluster EKS ini. Untuk informasi lebih lanjut tentang masing-masing pendekatan ini, lihat [Pendekatan untuk mengelola agen GuardDuty keamanan di kluster Amazon EKS](#).

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-Langkah
Mengelola agen keamanan melalui GuardDuty (Pantau semua kluster EKS)	Untuk memantau semua kluster EKS untuk semua akun anggota aktif yang ada 1. Pada halaman Runtime Monitoring, di bawah tab Konfigurasi, Anda dapat melihat status konfigurasi agen Otomatis saat ini. 2. Dalam panel konfigurasi agen otomatis, di bawah bagian Akun anggota aktif, pilih Tindakan. 3. Dari Tindakan, pilih Aktifkan untuk semua akun anggota aktif yang ada. 4. Pilih Konfirmasi.

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-Langkah
Pantau semua cluster EKS tetapi kecualikan beberapa di antaranya (menggunakan tag pengecualian)	Dari prosedur berikut, pilih salah satu skenario yang berlaku untuk Anda. Untuk mengecualikan klaster EKS dari pemantauan saat agen GuardDuty keamanan belum digunakan di cluster ini 1. Tambahkan tag ke cluster EKS ini dengan kunci as GuardDutyManaged dan nilainya sebagaifalse. Untuk informasi selengkapnya tentang menandai klaster Amazon EKS Anda, lihat Bekerja dengan tag menggunakan konsol di Panduan Pengguna Amazon EKS. 2. Untuk mencegah modifikasi tag, kecuali oleh entitas terpercaya, gunakan kebijakan yang disediakan dalam Mencegah tag agar tidak dimodifikasi kecuali oleh prinsipal resmi dalam Panduan Pengguna. AWS Organizations Dalam kebijakan ini, ganti detail berikut: • Ganti <i>ec2:CreateTags</i> dengan <code>eks:TagResource</code>. • Ganti <i>ec2:DeleteTags</i> dengan <code>eks:UntagResource</code>. • Ganti <i>access-project</i> dengan GuardDuty Managed • Ganti <i>123456789012</i> dengan Akun AWS ID entitas terpercaya. Jika Anda memiliki lebih dari satu entitas terpercaya, gunakan contoh berikut untuk menambahkan beberapaPrincipalArn :

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-Langkah
	<pre data-bbox="803 325 1396 556">"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre> 3. Buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/. 4. Di panel navigasi, pilih Runtime Monitoring.  Note Selalu tambahkan tag pengecualian ke kluster EKS Anda sebelum mengaktifkan konfigurasi agen otomatis untuk akun Anda; jika tidak, agen GuardDuty keamanan akan digunakan di semua kluster EKS di akun Anda. 5. Di bawah tab Konfigurasi, di panel Konfigurasi agen otomatis, di bawah Akun anggota aktif, pilih Tindakan. 6. Dari Tindakan, pilih Aktifkan untuk semua akun anggota yang aktif. 7. Pilih Konfirmasi. Untuk mengecualikan cluster EKS dari pemantauan setelah agen GuardDuty keamanan telah digunakan di cluster ini 1. Tambahkan tag ke cluster EKS ini dengan kunci as GuardDutyManaged dan nilainya sebagaifalse.

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-Langkah
	Untuk informasi selengkapnya tentang menandai klaster Amazon EKS Anda, lihat Bekerja dengan tag menggunakan konsol di Panduan Pengguna Amazon EKS. Setelah langkah ini, tidak GuardDuty akan memperbarui agen keamanan untuk cluster ini. Namun, agen keamanan akan tetap digunakan dan GuardDuty akan terus menerima peristiwa runtime dari cluster EKS ini. Ini dapat memengaruhi statistik penggunaan Anda. 2. Untuk mencegah modifikasi tag, kecuali oleh entitas terpercaya, gunakan kebijakan yang disediakan dalam Mencegah tag agar tidak dimodifikasi kecuali oleh prinsipal resmi dalam Panduan Pengguna. AWS Organizations Dalam kebijakan ini, ganti detail berikut: • Ganti <i>ec2:CreateTags</i> dengan <code>eks:TagResource</code>. • Ganti <i>ec2:DeleteTags</i> dengan <code>eks:UntagResource</code>. • Ganti <i>access-project</i> dengan GuardDuty Managed • Ganti <i>123456789012</i> dengan Akun AWS ID entitas terpercaya. Jika Anda memiliki lebih dari satu entitas terpercaya, gunakan contoh berikut untuk menambahkan beberapaPrincipalArn : <pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-</pre>

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-Langkah
	<pre data-bbox="805 306 1396 478">admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre> 3. Terlepas dari bagaimana Anda mengelola agen keamanan (melalui GuardDuty atau secara manual), untuk berhenti menerima peristiwa runtime dari cluster ini, Anda harus menghapus agen keamanan yang digunakan dari cluster EKS ini. Untuk informasi selengkapnya tentang menghapus agen keamanan yang digunakan, lihat Menonaktifkan, menghapus instalasi, dan membersihkan sumber daya di Runtime Monitoring.

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-Langkah
Pantau kluster EKS selektif menggunakan tag inklusi	1. Pada halaman Akun, setelah Anda mengaktifkan Runtime Monitoring, jangan aktifkan Runtime Monitoring - Konfigurasi agen otomatis. 2. Tambahkan tag ke kluster EKS milik akun yang dipilih yang ingin Anda pantau. Pasangan kunci-nilai tag harus GuardDutyManaged - . true Untuk informasi selengkapnya tentang menandai kluster Amazon EKS Anda, lihat Bekerja dengan tag menggunakan konsol di Panduan Pengguna Amazon EKS. GuardDuty akan mengelola penyebaran dan pembaruan ke agen keamanan untuk kluster EKS selektif yang ingin Anda pantau. 3. Untuk mencegah modifikasi tag, kecuali oleh entitas tepercaya, gunakan kebijakan yang disediakan dalam Mencegah tag agar tidak dimodifikasi kecuali oleh prinsipal resmi dalam Panduan Pengguna AWS Organizations. Dalam kebijakan ini, ganti detail berikut: • Ganti <i>ec2:CreateTags</i> dengan eks:TagResource . • Ganti <i>ec2:DeleteTags</i> dengan eks:UntagResource . • Ganti <i>access-project</i> dengan GuardDuty Managed • Ganti <i>123456789012</i> dengan Akun AWS ID entitas tepercaya.

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-Langkah
	Jika Anda memiliki lebih dari satu entitas tepercaya, gunakan contoh berikut untuk menambahkan beberapaPrincipalArn : <pre data-bbox="803 493 1396 724">"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre>
Mengelola agen GuardDuty keamanan secara manual	1. Pastikan Anda tidak memilih Aktifkan di bagian Konfigurasi agen otomatis. Tetap aktifkan Runtime Monitoring. 2. Pilih Simpan. 3. Untuk mengelola agen keamanan, lihatMengelola agen keamanan secara manual untuk kluster Amazon EKS.

Aktifkan otomatis konfigurasi agen otomatis untuk anggota baru

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-Langkah
Mengelola agen keamanan melalui GuardDuty (Pantau semua kluster EKS)	1. Pada halaman Runtime Monitoring, pilih Edit untuk memperbarui konfigurasi yang ada. 2. Di bagian Konfigurasi agen otomatis, pilih Aktifkan secara otomatis untuk akun anggota baru. 3. Pilih Simpan.

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-Langkah
Pantau semua cluster EKS tetapi kecualikan beberapa di antaranya (menggunakan tag pengecualian)	Dari prosedur berikut, pilih salah satu skenario yang berlaku untuk Anda. Untuk mengecualikan klaster EKS dari pemantauan saat agen GuardDuty keamanan belum digunakan di cluster ini 1. Tambahkan tag ke cluster EKS ini dengan kunci as GuardDutyManaged dan nilainya sebagaifalse. Untuk informasi selengkapnya tentang menandai klaster Amazon EKS Anda, lihat Bekerja dengan tag menggunakan konsol di Panduan Pengguna Amazon EKS. 2. Untuk mencegah modifikasi tag, kecuali oleh entitas tepercaya, gunakan kebijakan yang disediakan dalam Mencegah tag agar tidak dimodifikasi kecuali oleh prinsipal resmi dalam Panduan Pengguna.AWS Organizations Dalam kebijakan ini, ganti detail berikut: • Ganti <i>ec2:CreateTags</i> dengan eks:TagResource . • Ganti <i>ec2:DeleteTags</i> dengan eks:UntagResource . • Ganti <i>access-project</i> dengan GuardDuty Managed • Ganti <i>123456789012</i> dengan Akun AWS ID entitas tepercaya. Jika Anda memiliki lebih dari satu entitas tepercaya , gunakan contoh berikut untuk menambahkan beberapaPrincipalArn : <pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin</pre>

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-Langkah
	<pre data-bbox="747 300 1507 436">", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre> 3. Buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/. 4. Di panel navigasi, pilih Runtime Monitoring.  Note Selalu tambahkan tag pengecualian ke kluster EKS Anda sebelum mengaktifkan konfigurasi agen otomatis untuk akun Anda; jika tidak, agen GuardDuty keamanan akan digunakan di semua kluster EKS di akun Anda. 5. Di bawah tab Konfigurasi, pilih Aktifkan secara otomatis untuk akun anggota baru di bagian manajemen GuardDuty agen. Untuk kluster EKS yang belum dikecualikan dari pemantauan, GuardDuty akan mengelola penyebaran dan pembaruan ke agen GuardDuty keamanan. 6. Pilih Simpan. Untuk mengecualikan kluster EKS dari pemantauan saat agen GuardDuty keamanan telah digunakan di cluster ini 1. Terlepas dari apakah Anda mengelola agen GuardDuty keamanan melalui GuardDuty atau secara manual, tambahkan tag ke cluster EKS ini dengan kunci <code>asGuardDutyManaged</code> dan nilainya <code>sebagaifalse</code>.

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-Langkah
	Untuk informasi selengkapnya tentang menandai kluster Amazon EKS Anda, lihat Bekerja dengan tag menggunakan konsol di Panduan Pengguna Amazon EKS. Jika Anda mengaktifkan agen otomatis untuk kluster EKS ini, maka setelah langkah ini, tidak GuardDuty akan memperbarui agen keamanan untuk cluster ini. Namun, agen keamanan akan tetap digunakan dan GuardDuty akan terus menerima peristiwa runtime dari cluster EKS ini. Ini dapat memengaruhi statistik penggunaan Anda. Untuk berhenti menerima peristiwa runtime dari cluster ini, Anda harus menghapus agen keamanan yang digunakan dari kluster EKS ini. Untuk informasi selengkapnya tentang menghapus agen keamanan yang digunakan, lihat Menonaktifkan, menghapus instalasi, dan membersihkan sumber daya di Runtime Monitoring 2. Untuk mencegah modifikasi tag, kecuali oleh entitas tepercaya, gunakan kebijakan yang disediakan dalam Mencegah tag agar tidak dimodifikasi kecuali oleh prinsipal resmi dalam Panduan Pengguna AWS Organizations Dalam kebijakan ini, ganti detail berikut: • Ganti <i>ec2:CreateTags</i> dengan <i>eks:TagResource</i> . • Ganti <i>ec2:DeleteTags</i> dengan <i>eks:UntagResource</i> . • Ganti <i>access-project</i> dengan GuardDuty Managed

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-Langkah
	• Ganti 123456789012 dengan Akun AWS ID entitas tepercaya. Jika Anda memiliki lebih dari satu entitas tepercaya , gunakan contoh berikut untuk menambahkan beberapaPrincipalArn : <pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre> 3. Jika Anda mengelola agen GuardDuty keamanan untuk cluster EKS ini secara manual, lihatMenonaktifkan, menghapus instalasi, dan membersihkan sumber daya di Runtime Monitoring.

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-Langkah
Pantau kluster EKS selektif menggunakan tag inklusi	Terlepas dari bagaimana Anda memilih untuk mengaktifkan Runtime Monitoring, langkah-langkah berikut akan membantu Anda memantau kluster EKS selektif untuk akun anggota baru di organisasi Anda. 1. Pastikan untuk menghapus Aktifkan secara otomatis untuk akun anggota baru di bagian Konfigurasi agen otomatis. Pertahankan konfigurasi Runtime Monitoring sama seperti yang dikonfigurasi pada langkah sebelumnya. 2. Pilih Simpan. 3. Tambahkan tag ke kluster EKS Anda dengan kunci <code>asGuardDutyManaged</code> dan nilainya sebagai <code>true</code>. Untuk informasi selengkapnya tentang menandai kluster Amazon EKS Anda, lihat Bekerja dengan tag menggunakan konsol di Panduan Pengguna Amazon EKS. GuardDuty akan mengelola penyebaran dan pembaruan ke agen keamanan untuk kluster EKS selektif yang ingin Anda pantau. 4. Untuk mencegah modifikasi tag, kecuali oleh entitas tepercaya, gunakan kebijakan yang disediakan dalam Mencegah tag agar tidak dimodifikasi kecuali oleh prinsipal resmi dalam Panduan Pengguna AWS Organizations. Dalam kebijakan ini, ganti detail berikut: • Ganti <code>ec2:CreateTags</code> dengan <code>eks:TagResource</code>. • Ganti <code>ec2:DeleteTags</code> dengan <code>eks:UntagResource</code>.

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-Langkah
	• Ganti <i>access-project</i> dengan GuardDuty Managed • Ganti <i>123456789012</i> dengan Akun AWS ID entitas tepercaya. Jika Anda memiliki lebih dari satu entitas tepercaya, gunakan contoh berikut untuk menambahkan beberapaPrincipalArn : <pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre>
Mengelola agen GuardDuty keamanan secara manual	Terlepas dari bagaimana Anda memilih untuk mengaktifkan Runtime Monitoring, Anda dapat mengelola agen keamanan secara manual untuk kluster EKS Anda. 1. Pastikan kosongkan kotak centang Secara otomatis mengaktifkan akun anggota baru di bagian Konfigurasi agen otomatis. Pertahankan konfigurasi Runtime Monitoring sama seperti yang dikonfigurasi pada langkah sebelumnya. 2. Pilih Simpan. 3. Untuk mengelola agen keamanan, lihatMengelola agen keamanan secara manual untuk kluster Amazon EKS.

Mengkonfigurasi agen otomatis untuk akun anggota aktif secara selektif

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-Langkah
Mengelola agen keamanan melalui GuardDuty (Pantau semua kluster EKS)	1. Pada halaman Akun, pilih akun yang ingin Anda aktifkan Konfigurasi agen otomatis. Anda dapat memilih lebih dari satu akun sekaligus. Pastikan akun yang Anda pilih pada langkah ini sudah mengaktifkan EKS Runtime Monitoring. 2. Dari paket Edit Protection pilih opsi yang sesuai untuk mengaktifkan Runtime Monitoring - Konfigurasi agen otomatis. 3. Pilih Konfirmasi.
Pantau semua cluster EKS tetapi kecualikan beberapa di antaranya (menggunakan tag pengecualian)	Dari prosedur berikut, pilih salah satu skenario yang berlaku untuk Anda. Untuk mengecualikan kluster EKS dari pemantauan saat agen GuardDuty keamanan belum digunakan di cluster ini 1. Tambahkan tag ke cluster EKS ini dengan kunci <code>as GuardDuty Managed</code> dan nilainya sebagai <code>false</code>. Untuk informasi selengkapnya tentang menandai kluster Amazon EKS Anda, lihat Bekerja dengan tag menggunakan konsol di Panduan Pengguna Amazon EKS. 2. Untuk mencegah modifikasi tag, kecuali oleh entitas tepercaya, gunakan kebijakan yang disediakan dalam Mencegah tag agar tidak dimodifikasi kecuali oleh prinsipal resmi dalam Panduan Pengguna AWS Organizations. Dalam kebijakan ini, ganti detail berikut: • Ganti <code>ec2:CreateTags</code> dengan <code>eks:TagResource</code>. • Ganti <code>ec2:DeleteTags</code> dengan <code>eks:UntagResource</code>. • Ganti <code>access-project</code> dengan <code>GuardDutyManaged</code> • Ganti <code>123456789012</code> dengan Akun AWS ID entitas tepercaya.

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-Langkah
	Jika Anda memiliki lebih dari satu entitas tepercaya, gunakan contoh berikut untuk menambahkan beberapa <code>Principal Arn</code> : <pre data-bbox="621 474 1507 674">"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre> 3. Buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.  Note Selalu tambahkan tag pengecualian ke kluster EKS Anda sebelum mengaktifkan konfigurasi agen otomatis untuk akun Anda; jika tidak, agen GuardDuty keamanan akan digunakan di semua kluster EKS di akun Anda. 4. Pada halaman Akun, pilih akun yang ingin Anda aktifkan Kelola agen secara otomatis. Anda dapat memilih lebih dari satu akun sekaligus. 5. Dari Edit paket perlindungan, pilih opsi yang sesuai untuk mengaktifkan konfigurasi agen Runtime Monitoring-Automated untuk akun yang dipilih. Untuk kluster EKS yang belum dikecualikan dari pemantauan, GuardDuty akan mengelola penyebaran dan pembaruan ke agen GuardDuty keamanan. 6. Pilih Simpan.

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-Langkah
	Untuk mengecualikan kluster EKS dari pemantauan saat agen GuardDuty keamanan telah digunakan di cluster ini 1. Tambahkan tag ke cluster EKS ini dengan kunci <code>as GuardDuty Managed</code> dan nilainya sebagai <code>false</code>. Untuk informasi selengkapnya tentang menandai kluster Amazon EKS Anda, lihat Bekerja dengan tag menggunakan konsol di Panduan Pengguna Amazon EKS. Jika sebelumnya Anda mengaktifkan konfigurasi agen otomatis untuk kluster EKS ini, maka setelah langkah ini, tidak GuardDuty akan memperbarui agen keamanan untuk kluster ini. Namun, agen keamanan akan tetap digunakan dan GuardDuty akan terus menerima peristiwa runtime dari cluster EKS ini. Ini dapat memengaruhi statistik penggunaan Anda. Untuk berhenti menerima peristiwa runtime dari cluster ini, Anda harus menghapus agen keamanan yang digunakan dari kluster EKS ini. Untuk informasi selengkapnya tentang menghapus agen keamanan yang digunakan, lihat Menonaktifkan, menghapus instalasi, dan membersihkan sumber daya di Runtime Monitoring 2. Untuk mencegah modifikasi tag, kecuali oleh entitas tepercaya, gunakan kebijakan yang disediakan dalam Mencegah tag agar tidak dimodifikasi kecuali oleh prinsipal resmi dalam Panduan Pengguna AWS Organizations. Dalam kebijakan ini, ganti detail berikut: • Ganti <code>ec2:CreateTags</code> dengan <code>eks:TagResource</code> . • Ganti <code>ec2:DeleteTags</code> dengan <code>eks:UntagResource</code> . • Ganti <code>access-project</code> dengan <code>GuardDutyManaged</code> • Ganti <code>123456789012</code> dengan Akun AWS ID entitas tepercaya.

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-Langkah
	Jika Anda memiliki lebih dari satu entitas tepercaya, gunakan contoh berikut untuk menambahkan beberapaPrincipal Arn : <pre data-bbox="618 474 1507 674">"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre> 3. Jika Anda mengelola agen GuardDuty keamanan untuk cluster EKS ini secara manual, Anda harus menghapusnya. Untuk informasi selengkapnya, lihat Menonaktifkan, menghapus instalasi, dan membersihkan sumber daya di Runtime Monitoring.

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-Langkah
Pantau kluster EKS selektif menggunakan tag inklusi	Terlepas dari cara Anda memilih untuk mengaktifkan Runtime Monitoring, langkah-langkah berikut akan membantu Anda memantau kluster EKS selektif yang termasuk dalam akun yang dipilih: 1. Pastikan Anda tidak mengaktifkan konfigurasi agen Runtime Monitoring-Automated untuk akun terpilih yang memiliki kluster EKS yang ingin Anda pantau. 2. Tambahkan tag ke kluster EKS Anda dengan kunci <code>asGuardDutyManaged</code> dan nilainya sebagai <code>true</code>. Untuk informasi selengkapnya tentang menandai kluster Amazon EKS Anda, lihat Bekerja dengan tag menggunakan konsol di Panduan Pengguna Amazon EKS. Setelah menambahkan tag, GuardDuty akan mengelola penyebaran dan pembaruan ke agen keamanan untuk kluster EKS selektif yang ingin Anda pantau. 3. Untuk mencegah modifikasi tag, kecuali oleh entitas tepercaya, gunakan kebijakan yang disediakan dalam Mencegah tag agar tidak dimodifikasi kecuali oleh prinsipal resmi dalam Panduan Pengguna AWS Organizations. Dalam kebijakan ini, ganti detail berikut: • Ganti <code>ec2:CreateTags</code> dengan <code>eks:TagResource</code>. • Ganti <code>ec2:DeleteTags</code> dengan <code>eks:UntagResource</code>. • Ganti <code>access-project</code> dengan <code>GuardDutyManaged</code> • Ganti <code>123456789012</code> dengan Akun AWS ID entitas tepercaya. Jika Anda memiliki lebih dari satu entitas tepercaya, gunakan contoh berikut untuk menambahkan beberapa <code>Principal</code> <code>Arn</code> :

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-Langkah
	<pre data-bbox="639 325 1406 478">"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre>
Mengelola agen GuardDuty keamanan secara manual	1. Pertahankan konfigurasi Runtime Monitoring sama seperti yang dikonfigurasi pada langkah sebelumnya. Pastikan Anda tidak mengaktifkan Runtime Monitoring- Konfigurasi agen otomatis untuk salah satu akun yang dipilih. 2. Pilih Konfirmasi. 3. Untuk mengelola agen keamanan, lihat Mengelola agen keamanan secara manual untuk kluster Amazon EKS.

Mengkonfigurasi agen otomatis untuk akun mandiri

Akun mandiri memiliki keputusan untuk mengaktifkan atau menonaktifkan rencana perlindungan di akun mereka Akun AWS secara spesifik. Wilayah AWS

Jika akun Anda dikaitkan dengan akun GuardDuty administrator melalui AWS Organizations, atau dengan metode undangan, bagian ini tidak berlaku untuk akun Anda. Untuk informasi selengkapnya, lihat [Mengaktifkan Runtime Monitoring untuk lingkungan multi-akun](#).

Setelah Anda mengaktifkan Runtime Monitoring, pastikan untuk menginstal agen GuardDuty keamanan melalui konfigurasi otomatis atau penerapan manual. Sebagai bagian dari menyelesaikan semua langkah yang tercantum dalam prosedur berikut, pastikan untuk menginstal agen keamanan.

Berdasarkan preferensi Anda untuk memantau semua atau sumber daya Amazon EKS selektif, pilih metode yang disukai dan ikuti langkah-langkah dalam tabel berikut.

1. Masuk ke AWS Management Console dan buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.
2. Di panel navigasi, pilih Runtime Monitoring.

3. Di bawah tab Konfigurasi, pilih Aktifkan untuk mengaktifkan konfigurasi agen otomatis untuk akun Anda.

Pendekatan yang disukai untuk menyebarkan agen GuardDuty keamanan	Langkah-Langkah
Mengelola agen keamanan melalui GuardDuty (Pantau semua kluster EKS)	1. Pilih Aktifkan di bagian Konfigurasi agen otomatis. GuardDuty akan mengelola penyebaran dan pembaruan ke agen keamanan untuk semua kluster EKS yang ada dan berpotensi baru di akun Anda. 2. Pilih Simpan.

Pendekatan yang disukai untuk menyebarkan agen GuardDuty keamanan	Langkah-Langkah
Pantau semua cluster EKS tetapi kecualikan beberapa di antaranya (menggunakan tag pengecualian)	Dari prosedur berikut, pilih salah satu skenario yang berlaku untuk Anda. Untuk mengecualikan kluster EKS dari pemantauan saat agen GuardDuty keamanan belum digunakan di cluster ini 1. Tambahkan tag ke cluster EKS ini dengan kunci as GuardDutyManaged dan nilainya sebagaifalse. Untuk informasi selengkapnya tentang menandai kluster Amazon EKS Anda, lihat Bekerja dengan tag menggunakan konsol di Panduan Pengguna Amazon EKS. 2. Untuk mencegah modifikasi tag, kecuali oleh entitas terpercaya, gunakan kebijakan yang disediakan dalam Mencegah tag agar tidak dimodifikasi kecuali oleh prinsipal resmi dalam Panduan Pengguna. AWS Organizations Dalam kebijakan ini, ganti detail berikut: • Ganti <i>ec2:CreateTags</i> dengan <code>eks:TagResource</code>. • Ganti <i>ec2:DeleteTags</i> dengan <code>eks:UntagResource</code>. • Ganti <i>access-project</i> dengan GuardDuty Managed • Ganti <i>123456789012</i> dengan Akun AWS ID entitas terpercaya. Jika Anda memiliki lebih dari satu entitas terpercaya, gunakan contoh berikut untuk menambahkan beberapaPrincipalArn :

Pendekatan yang disukai untuk menyebarkan agen GuardDuty keamanan	Langkah-Langkah
	<pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre> 3. Buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/. 4. Di panel navigasi, pilih Runtime Monitoring.  Note Selalu tambahkan tag pengecualian ke kluster EKS Anda sebelum mengaktifkan manajemen otomatis GuardDuty agen untuk akun Anda; jika tidak, agen GuardDuty keamanan akan digunakan di semua kluster EKS di akun Anda. 5. Di bawah tab Konfigurasi, pilih Aktifkan di bagian manajemen GuardDuty agen. Untuk kluster EKS yang belum dikecualikan dari pemantauan, GuardDuty akan mengelola penyebaran dan pembaruan ke agen GuardDuty keamanan. 6. Pilih Simpan.

Pendekatan yang disukai untuk menyebarkan agen GuardDuty keamanan	Langkah-Langkah
	Untuk mengecualikan cluster EKS dari pemantauan setelah agen GuardDuty keamanan telah digunakan di cluster ini 1. Tambahkan tag ke cluster EKS ini dengan kunci as GuardDutyManaged dan nilainya sebagaifalse. Untuk informasi selengkapnya tentang menandai klaster Amazon EKS Anda, lihat Bekerja dengan tag menggunakan konsol di Panduan Pengguna Amazon EKS. Setelah langkah ini, tidak GuardDuty akan memperbarui agen keamanan untuk cluster ini. Namun, agen keamanan akan tetap digunakan dan GuardDuty akan terus menerima peristiwa runtime dari cluster EKS ini. Ini dapat memengaruhi statistik penggunaan Anda. 2. Untuk mencegah modifikasi tag, kecuali oleh entitas tepercaya, gunakan kebijakan yang disediakan dalam Mencegah tag agar tidak dimodifikasi kecuali oleh prinsipal resmi dalam Panduan Pengguna. AWS Organizations Dalam kebijakan ini, ganti detail berikut: • Ganti <i>ec2:CreateTags</i> dengan <i>eks:TagResource</i> . • Ganti <i>ec2:DeleteTags</i> dengan <i>eks:UntagResource</i> . • Ganti <i>access-project</i> dengan GuardDuty Managed

Pendekatan yang disukai untuk menyebarkan agen GuardDuty keamanan	Langkah-Langkah
	• Ganti 123456789012 dengan Akun AWS ID entitas tepercaya. Jika Anda memiliki lebih dari satu entitas tepercaya, gunakan contoh berikut untuk menambahkan beberapaPrincipalArn : <pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre> 3. Untuk berhenti menerima peristiwa runtime dari cluster ini, Anda harus menghapus agen keamanan yang digunakan dari klaster EKS ini. Untuk informasi selengkapnya tentang menghapus agen keamanan yang digunakan, lihatMenonaktifkan, menghapus instalasi, dan membersihkan sumber daya di Runtime Monitoring.

Pendekatan yang disukai untuk menyebarkan agen GuardDuty keamanan	Langkah-Langkah
Pantau kluster EKS selektif menggunakan tag inklusi	1. Pastikan untuk memilih Nonaktifkan di bagian Konfigurasi agen otomatis. Tetap aktifkan Runtime Monitoring. 2. Pilih Simpan. 3. Tambahkan tag ke cluster EKS ini dengan kunci <code>asGuardDutyManaged</code> dan nilainya sebagai <code>true</code>. Untuk informasi selengkapnya tentang menandai kluster Amazon EKS Anda, lihat Bekerja dengan tag menggunakan konsol di Panduan Pengguna Amazon EKS. GuardDuty akan mengelola penyebaran dan pembaruan ke agen keamanan untuk kluster EKS selektif yang ingin Anda pantau. 4. Untuk mencegah modifikasi tag, kecuali oleh entitas tepercaya, gunakan kebijakan yang disediakan dalam Mencegah tag agar tidak dimodifikasi kecuali oleh prinsipal resmi dalam Panduan Pengguna AWS Organizations. Dalam kebijakan ini, ganti detail berikut: • Ganti <code>ec2:CreateTags</code> dengan <code>eks:TagResource</code>. • Ganti <code>ec2:DeleteTags</code> dengan <code>eks:UntagResource</code>. • Ganti <code>access-project</code> dengan <code>GuardDutyManaged</code> • Ganti <code>123456789012</code> dengan Akun AWS ID entitas tepercaya.

Pendekatan yang disukai untuk menyebarkan agen GuardDuty keamanan	Langkah-Langkah
	Jika Anda memiliki lebih dari satu entitas terpercaya, gunakan contoh berikut untuk menambahkan beberapaPrincipalArn : <pre data-bbox="803 493 1396 724">"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre>
Kelola agen secara manual	1. Pastikan untuk memilih Nonaktifkan di bagian Konfigurasi agen otomatis. Tetap aktifkan Runtime Monitoring. 2. Pilih Simpan. 3. Untuk mengelola agen keamanan, lihatMengelola agen keamanan secara manual untuk kluster Amazon EKS.

Mengelola agen keamanan secara manual untuk kluster Amazon EKS

Bagian ini menjelaskan bagaimana Anda dapat mengelola agen add-on Amazon EKS (GuardDuty agen) setelah Anda mengaktifkan Runtime Monitoring (atau EKS Runtime Monitoring).

Untuk menggunakan Runtime Monitoring, Anda harus mengaktifkan Runtime Monitoring dan mengonfigurasi add-on Amazon EKS,. `aws-guardduty-agent` Anda perlu melakukan kedua langkah GuardDuty untuk mendeteksi potensi ancaman dan menghasilkan[GuardDuty Jenis penemuan Runtime Monitoring](#).

Untuk mengelola agen secara manual, Anda perlu membuat titik akhir VPC sebagai prasyarat. Ini membantu GuardDuty menerima acara runtime. Setelah ini, Anda dapat menginstal agen keamanan sehingga GuardDuty akan mulai menerima peristiwa runtime dari sumber daya Amazon EKS. Saat

GuardDuty merilis versi agen baru untuk sumber daya ini, Anda dapat memperbarui versi agen di akun Anda.

Topik

- [Prasyarat - Membuat titik akhir VPC Amazon](#)
- [Menginstal agen GuardDuty keamanan secara manual di sumber daya Amazon EKS](#)
- [Memperbarui agen keamanan secara manual untuk sumber daya Amazon EKS](#)

Prasyarat - Membuat titik akhir VPC Amazon

Sebelum Anda dapat menginstal agen GuardDuty keamanan, Anda harus membuat titik akhir Amazon Virtual Private Cloud (Amazon VPC). Ini akan membantu GuardDuty menerima peristiwa runtime dari sumber daya Amazon EKS Anda.

Note

Tidak ada biaya tambahan untuk penggunaan titik akhir VPC.

Pilih metode akses yang disukai untuk membuat titik akhir VPC Amazon.

Console

Untuk membuat titik akhir VPC

1. Buka konsol VPC Amazon di <https://console.aws.amazon.com/vpc/>
2. Di panel navigasi, di bawah Virtual private cloud, pilih Endpoints.
3. Pilih Buat Titik Akhir.
4. Pada halaman Buat titik akhir, untuk kategori Layanan, pilih Layanan titik akhir lainnya.
5. Untuk nama Layanan, masukkan **com.amazonaws.us-east-1.guardduty-data**.

Pastikan untuk mengganti **us-east-1** dengan Region yang benar. Ini harus Region yang sama dengan cluster EKS milik Akun AWS ID Anda.

6. Pilih Verifikasi layanan.
7. Setelah nama layanan berhasil diverifikasi, pilih VPC tempat kluster Anda berada. Tambahkan kebijakan berikut untuk membatasi penggunaan titik akhir VPC hanya ke akun tertentu. Dengan organisasi yang Condition disediakan di bawah kebijakan ini,

Anda dapat memperbarui kebijakan berikut untuk membatasi akses ke titik akhir Anda. Untuk memberikan dukungan titik akhir VPC ke akun tertentu IDs di organisasi Anda, lihat. [Organization condition to restrict access to your endpoint](#)

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": "*",
      "Resource": "*",
      "Effect": "Allow",
      "Principal": "*"
    },
    {
      "Condition": {
        "StringNotEquals": {
          "aws:PrincipalAccount": "111122223333"
        }
      },
      "Action": "*",
      "Resource": "*",
      "Effect": "Deny",
      "Principal": "*"
    }
  ]
}
```

ID `aws:PrincipalAccount` akun harus cocok dengan akun yang berisi titik akhir VPC dan VPC. Daftar berikut menunjukkan cara berbagi titik akhir VPC dengan yang lain: Akun AWS IDs

Kondisi organisasi untuk membatasi akses ke titik akhir Anda

- Untuk menentukan beberapa akun untuk mengakses titik akhir VPC, ganti `"aws:PrincipalAccount": "111122223333"` dengan yang berikut:

```
"aws:PrincipalAccount": [
  "666666666666",
  "555555555555"
]
```

- Untuk mengizinkan semua anggota dari organisasi mengakses titik akhir VPC, ganti "aws:PrincipalAccount": "**111122223333**" dengan yang berikut ini:

```
"aws:PrincipalOrgID": "o-abcdef0123"
```

- Untuk membatasi akses sumber daya ke ID organisasi, tambahkan ResourceOrgID ke kebijakan.

Untuk informasi selengkapnya, lihat [ResourceOrgID](#).

```
"aws:ResourceOrgID": "o-abcdef0123"
```

8. Di bawah Pengaturan tambahan, pilih Aktifkan nama DNS.
9. Di bawah Subnet, pilih subnet tempat kluster Anda berada.
10. Di bawah Grup keamanan, pilih grup keamanan yang mengaktifkan port 443 in-bound dari VPC Anda (atau kluster EKS Anda). Jika Anda belum memiliki grup keamanan yang mengaktifkan port 443 dalam terikat, [Buat grup keamanan](#).

Jika ada masalah saat membatasi izin masuk ke VPC (atau instance), Anda dapat menggunakan port 443 yang di-bound dari alamat IP apa pun. (0.0.0.0/0) Namun, GuardDuty merekomendasikan untuk menggunakan alamat IP yang cocok dengan blok CIDR untuk VPC Anda. Untuk informasi selengkapnya, lihat [blok CIDR VPC di Panduan Pengguna Amazon VPC](#).

API/CLI

Untuk membuat titik akhir VPC

- Memohon. [CreateVpcEndpoint](#)
- Gunakan nilai berikut untuk parameter:
 - Untuk nama Layanan, masukkan **com.amazonaws.us-east-1.guardduty-data**.

Pastikan untuk mengganti **us-east-1** dengan Region yang benar. Ini harus Region yang sama dengan cluster EKS milik Akun AWS ID Anda.

- Untuk [DNSOptions](#), aktifkan opsi DNS pribadi dengan menyetelnya ke `true`.
- Untuk AWS Command Line Interface, lihat [create-vpc-endpoint](#).

Setelah Anda mengikuti langkah-langkahnya, lihat [Memvalidasi konfigurasi titik akhir VPC](#) untuk memastikan bahwa titik akhir VPC telah diatur dengan benar.

Menginstal agen GuardDuty keamanan secara manual di sumber daya Amazon EKS

Bagian ini menjelaskan bagaimana Anda dapat menyebarkan agen GuardDuty keamanan untuk pertama kalinya untuk kluster EKS tertentu. Sebelum Anda melanjutkan dengan bagian ini, pastikan Anda telah menyiapkan prasyarat dan mengaktifkan Runtime Monitoring untuk akun Anda. Agen GuardDuty keamanan (add-on EKS) tidak akan berfungsi jika Anda tidak mengaktifkan Runtime Monitoring.

Pilih metode akses pilihan Anda untuk menyebarkan agen GuardDuty keamanan untuk pertama kalinya.

Console

1. Buka konsol Amazon EKS di <https://console.aws.amazon.com/eks/rumah#/cluster>.
2. Pilih nama Cluster Anda.
3. Pilih tab Add-ons.
4. Pilih Get more add-ons
5. Pada halaman Pilih add-on, pilih Amazon GuardDuty EKS Runtime Monitoring.
6. GuardDuty merekomendasikan memilih Versi agen terbaru dan default.
7. Pada halaman Konfigurasi pengaturan add-on yang dipilih, gunakan pengaturan default. Jika Status add-on EKS Anda Memerlukan aktivasi, pilih Aktifkan GuardDuty. Tindakan ini akan membuka GuardDuty konsol untuk mengonfigurasi Runtime Monitoring untuk akun Anda.
8. Setelah mengonfigurasi Runtime Monitoring untuk akun Anda, beralih kembali ke konsol Amazon EKS. Status add-on EKS Anda seharusnya telah berubah menjadi Siap untuk menginstal.
9. (Opsional) Menyediakan skema konfigurasi add-on EKS

Untuk Versi add-on, jika Anda memilih v1.5.0 atau lebih tinggi, Runtime Monitoring mendukung konfigurasi parameter spesifik agen. GuardDuty Untuk informasi tentang rentang parameter, lihat [Konfigurasi parameter add-on EKS](#).

- a. Perluas Pengaturan konfigurasi opsional untuk melihat parameter yang dapat dikonfigurasi serta nilai serta format yang diharapkan.

- b. Atur parameternya. Nilai-nilai harus dalam kisaran yang disediakan di [Konfigurasikan parameter add-on EKS](#).
 - c. Pilih Simpan perubahan untuk membuat add-on berdasarkan konfigurasi lanjutan.
 - d. Untuk metode Resolusi konflik, opsi yang Anda pilih akan digunakan untuk menyelesaikan konflik saat Anda memperbarui nilai parameter ke nilai non-default. Untuk informasi selengkapnya tentang opsi yang tercantum, lihat [ResolveConflicts di Referensi API Amazon EKS](#).
10. Pilih Berikutnya.
 11. Pada halaman Tinjau dan buat, verifikasi semua detail, dan pilih Buat.
 12. Arahkan kembali ke detail cluster dan pilih tab Resources.
 13. Anda dapat melihat pod baru dengan awalan aws-guardduty-agent.

API/CLI

Anda dapat mengonfigurasi agen add-on Amazon EKS (aws-guardduty-agent) menggunakan salah satu opsi berikut:

- Jalankan [CreateAddon](#) untuk akun Anda.

-



Note

Untuk add-on `version`, jika Anda memilih v1.5.0 atau lebih tinggi, Runtime Monitoring mendukung konfigurasi parameter spesifik agen. GuardDuty Untuk informasi selengkapnya, lihat [Konfigurasikan parameter add-on EKS](#).

Gunakan nilai berikut untuk parameter permintaan:

- Untuk `addonName`, masukkan `aws-guardduty-agent`.

Anda dapat menggunakan AWS CLI contoh berikut saat menggunakan nilai yang dapat dikonfigurasi yang didukung untuk versi add-on v1.5.0 atau yang lebih baru. Pastikan untuk mengganti nilai placeholder yang disorot dengan warna merah dan yang terkait `Example.json` dengan nilai yang dikonfigurasi.

```
aws eks create-addon --region us-east-1 --cluster-name myClusterName --addon-name aws-guardduty-agent --addon-version v1.10.0-eksbuild.2 --configuration-values 'file://example.json'
```

Example Contoh.json

```
{
  "priorityClassName": "aws-guardduty-agent.priorityclass-high",
  "dnsPolicy": "Default",
  "resources": {
    "requests": {
      "cpu": "237m",
      "memory": "512Mi"
    },
    "limits": {
      "cpu": "2000m",
      "memory": "2048Mi"
    }
  }
}
```

- Untuk informasi tentang didukungaddonVersion, Lihat [Versi Kubernetes didukung oleh agen keamanan GuardDuty](#).
- Atau, Anda dapat menggunakan AWS CLI. Untuk informasi selengkapnya, lihat [create-addon](#).

Nama DNS pribadi untuk titik akhir VPC

Secara default, agen keamanan menyelesaikan dan menghubungkan ke nama DNS pribadi dari titik akhir VPC. Untuk endpoint non-FIPS, DNS pribadi Anda akan muncul dalam format berikut:

Titik akhir non-FIPS — guardduty-data.*us-east-1*.amazonaws.com

Itu Wilayah AWS,*us-east-1*, akan berubah berdasarkan Wilayah Anda.

Memperbarui agen keamanan secara manual untuk sumber daya Amazon EKS

Ketika Anda mengelola agen GuardDuty keamanan secara manual, Anda bertanggung jawab untuk memperbaruinya untuk akun Anda. Untuk pemberitahuan tentang versi agen baru, Anda dapat berlangganan umpan RSS. [GuardDuty versi rilis agen keamanan](#)

Anda dapat memperbarui agen keamanan ke versi terbaru untuk mendapatkan manfaat dari dukungan dan peningkatan yang ditambahkan. Jika versi agen Anda saat ini mencapai akhir dukungan standar, maka untuk terus menggunakan Runtime Monitoring (atau EKS Runtime Monitoring), Anda harus memperbarui ke versi agen berikutnya yang tersedia atau terbaru.

Prasyarat

Sebelum Anda memperbarui versi agen keamanan, pastikan bahwa versi agen yang Anda rencanakan untuk digunakan sekarang, kompatibel dengan versi Kubernetes Anda. Untuk informasi selengkapnya, lihat [Versi Kubernetes didukung oleh agen keamanan GuardDuty](#).

Console

1. Buka konsol Amazon EKS di <https://console.aws.amazon.com/eks/rumah#/cluster>.
2. Pilih nama Cluster Anda.
3. Di bawah Info cluster, pilih tab Add-ons.
4. Di bawah tab Add-ons, pilih GuardDutyEKS Runtime Monitoring.
5. Pilih Edit untuk memperbarui detail agen.
6. Pada halaman Configure GuardDuty EKS Runtime Monitoring, perbarui detailnya.
7. (Opsional) Memperbarui pengaturan konfigurasi opsional

Jika versi add-on EKS Anda 1.5.0 atau lebih tinggi, Anda juga dapat memperbarui skema konfigurasi add-on.

- a. Perluas pengaturan konfigurasi opsional untuk melihat skema konfigurasi.
- b. Perbarui nilai parameter berdasarkan rentang yang disediakan di [Konfigurasikan parameter add-on EKS](#).
- c. Pilih Simpan perubahan untuk memulai pembaruan.
- d. Untuk metode Resolusi konflik, opsi yang Anda pilih akan digunakan untuk menyelesaikan konflik saat Anda memperbarui nilai parameter ke nilai non-default. Untuk informasi selengkapnya tentang opsi yang tercantum, lihat [ResolveConflicts di Referensi API Amazon EKS](#).

API/CLI

Untuk memperbarui agen GuardDuty keamanan untuk kluster Amazon EKS Anda, lihat [Memperbarui add-on](#).

Note

Untuk `add-on-version`, jika Anda memilih 1.5.0 atau lebih tinggi, Runtime Monitoring mendukung konfigurasi parameter spesifik agen. GuardDuty Untuk informasi tentang rentang parameter, lihat [Konfigurasi parameter add-on EKS](#).

Anda dapat menggunakan AWS CLI contoh berikut saat menggunakan nilai yang dapat dikonfigurasi yang didukung untuk versi add-on 1.5.0 dan yang lebih baru. Pastikan untuk mengganti nilai placeholder yang disorot dengan warna merah dan yang terkait `Example.json` dengan nilai yang dikonfigurasi.

```
aws eks update-addon --region us-east-1 --cluster-name myClusterName --addon-name aws-guardduty-agent --addon-version v1.9.0-eksbuild.2 --configuration-values 'file://example.json'
```

Example Contoh.json

```
{
  "priorityClassName": "aws-guardduty-agent.priorityclass-high",
  "dnsPolicy": "Default",
  "resources": {
    "requests": {
      "cpu": "237m",
      "memory": "512Mi"
    },
    "limits": {
      "cpu": "2000m",
      "memory": "2048Mi"
    }
  }
}
```

Jika versi add-on Amazon EKS Anda adalah 1.5.0 atau lebih tinggi, dan Anda telah mengonfigurasi skema add-on, Anda dapat memverifikasi apakah nilai muncul dengan benar untuk kluster Anda atau tidak. Untuk informasi selengkapnya, lihat [Memverifikasi pembaruan skema konfigurasi](#).

Konfigurasikan parameter agen GuardDuty keamanan (add-on) untuk Amazon EKS

Anda dapat mengonfigurasi parameter spesifik agen GuardDuty keamanan Anda untuk Amazon EKS. Dukungan ini tersedia untuk agen GuardDuty keamanan versi 1.5.0 dan di atasnya. Untuk informasi tentang versi add-on terbaru, lihat [GuardDuty versi agen keamanan untuk sumber daya Amazon EKS](#).

Mengapa saya harus memperbarui skema konfigurasi agen keamanan

Skema konfigurasi untuk agen GuardDuty keamanan sama di semua kontainer dalam kluster Amazon EKS Anda. Jika nilai default tidak sejajar dengan beban kerja dan ukuran instans terkait, pertimbangkan untuk mengonfigurasi pengaturan CPU, pengaturan memori, dan pengaturan. `PriorityClass` `dnsPolicy` Terlepas dari bagaimana Anda mengelola GuardDuty agen untuk kluster Amazon EKS Anda, Anda dapat mengonfigurasi atau memperbarui konfigurasi parameter ini yang ada.

Perilaku konfigurasi agen otomatis dengan parameter yang dikonfigurasi

Ketika GuardDuty mengelola agen keamanan (EKS add-on) atas nama Anda, itu memperbarui add-on, sesuai kebutuhan. GuardDuty akan mengatur nilai parameter yang dapat dikonfigurasi ke nilai default. Namun, Anda masih dapat memperbarui parameter ke nilai yang diinginkan. Jika ini mengarah ke konflik, opsi default untuk [ResolveConflicts](#) adalah. `None`

Parameter dan nilai yang dapat dikonfigurasi

Untuk informasi tentang langkah-langkah untuk mengkonfigurasi parameter add-on, lihat:

- [Menginstal agen GuardDuty keamanan secara manual di sumber daya Amazon EKS](#) atau
- [Memperbarui agen keamanan secara manual untuk sumber daya Amazon EKS](#)

Tabel berikut menyediakan rentang dan nilai yang dapat Anda gunakan untuk menerapkan add-on Amazon EKS secara manual atau memperbarui pengaturan add-on yang ada.

Pengaturan CPU

Parameter	Nilai default	Rentang yang dapat dikonfigurasi
Permintaan	200m	Antara 200m dan 10000m, keduanya inklusif
Batas	1000m	

Pengaturan memori

Parameter	Nilai default	Rentang yang dapat dikonfigurasi
Permintaan	256Mi	Antara 256Mi dan 20000Mi, keduanya inklusif
Batas	1024Mi	

PriorityClass pengaturan

Saat GuardDuty membuat add-on Amazon EKS untuk Anda, yang ditetapkan `PriorityClass` adalah `aws-guardduty-agent.priorityclass`. Ini berarti bahwa tidak ada tindakan yang akan diambil berdasarkan prioritas pod agen. Anda dapat mengonfigurasi parameter add-on ini dengan memilih salah satu `PriorityClass` opsi berikut:

Dapat dikonfigurasi PriorityClass	Nilai preemptio nPolicy	preemptio nPolicy deskripsi	Nilai pod
<code>aws-guardduty-agent.priorityclass</code>	Never	Tidak ada tindakan	1000000
<code>aws-guardduty-agent.priorityclass-high</code>	PreemptLowerPriority	Menetapkan nilai ini akan mendahului sebuah pod yang berjalan dengan nilai prioritas lebih rendah dari nilai pod agen.	100000000

Dapat dikonfigurasi PriorityClass	Nilai preemptio nPolicy	preemptio nPolicy deskripsi	Nilai pod
system-cluster-critical ¹	PreemptLowerPriority		2000000000
system-node-critical ¹	PreemptLowerPriority		2000001000

¹ Kubernetes menyediakan dua PriorityClass opsi ini — dan. `system-cluster-critical` dan `system-node-critical`. Untuk informasi selengkapnya, lihat [PriorityClass](#) di dokumentasi Kubernetes.

dnsPolicy pengaturan

Pilih salah satu opsi kebijakan DNS berikut yang didukung Kubernetes. Ketika tidak ada konfigurasi yang `ClusterFirst` ditentukan, digunakan sebagai nilai default.

- `ClusterFirst`
- `ClusterFirstWithHostNet`
- `Default`

Untuk informasi tentang kebijakan ini, lihat [Kebijakan DNS Pod di dokumentasi](#) Kubernetes.

Memverifikasi pembaruan skema konfigurasi

Setelah Anda mengonfigurasi parameter, lakukan langkah-langkah berikut untuk memverifikasi bahwa skema konfigurasi telah diperbarui:

1. Buka konsol Amazon EKS di <https://console.aws.amazon.com/eks/rumah#/cluster>.
2. Pada panel navigasi, silakan pilih Klaster.
3. Pada halaman Clusters, pilih nama Cluster yang ingin Anda verifikasi pembaruannya.
4. Pilih tab Sumber Daya.

5. Dari panel Jenis sumber daya, di bawah Beban kerja, pilih. DaemonSets
6. Pilih aws-guardduty-agent.
7. Pada aws-guardduty-agent halaman, pilih Tampilan mentah untuk melihat respons JSON yang tidak diformat. Verifikasi bahwa parameter yang dapat dikonfigurasi menampilkan nilai yang Anda berikan.

Setelah Anda memverifikasi, beralih ke GuardDuty konsol. Pilih yang sesuai Wilayah AWS dan lihat status cakupan untuk kluster Amazon EKS Anda. Untuk informasi selengkapnya, lihat [Cakupan runtime dan pemecahan masalah untuk kluster Amazon EKS](#).

Memvalidasi konfigurasi titik akhir VPC

Setelah Anda menginstal agen keamanan secara manual atau melalui konfigurasi GuardDuty otomatis, Anda dapat menggunakan dokumen ini untuk memvalidasi konfigurasi titik akhir VPC. Anda juga dapat menggunakan langkah-langkah ini setelah memecahkan [masalah cakupan runtime](#) untuk jenis sumber daya. Anda dapat memastikan bahwa langkah-langkah tersebut bekerja seperti yang diharapkan dan status cakupan berpotensi muncul sebagai Sehat.

Gunakan langkah-langkah berikut untuk memvalidasi bahwa konfigurasi titik akhir VPC untuk jenis sumber daya Anda diatur dengan benar di akun pemilik VPC:

1. Masuk ke AWS Management Console dan buka konsol VPC Amazon di <https://console.aws.amazon.com/vpc/>
2. Di panel navigasi, di bawah Virtual Private Cloud, pilih Your VPCs.
3. Di VPCs halaman Anda, pilih IPv4 CIDR yang terkait dengan ID VPC Anda.
4. Di panel navigasi, di bawah Virtual private cloud, pilih Endpoints.
5. Dalam tabel Endpoints, pilih baris yang memiliki nama Service mirip dengan com.amazonaws.
us-east-1.guardduty-data. Region (us-east-1) mungkin berbeda untuk titik akhir Anda.
6. Panel untuk detail titik akhir akan muncul. Di bawah tab Grup Keamanan, pilih tautan ID Grup terkait untuk detail selengkapnya.
7. Dalam tabel Grup Keamanan, pilih baris dengan ID grup Keamanan terkait untuk melihat detailnya.
8. Di bawah tab Aturan masuk, pastikan bahwa ada kebijakan masuk dengan rentang Port sebagai 443 dan Sumber sebagai nilai yang disalin dari CIDR. IPv4 Aturan masuk mengontrol lalu lintas masuk yang diizinkan untuk mencapai instance. Gambar berikut menunjukkan aturan

masuk untuk grup keamanan yang terkait dengan VPC yang digunakan oleh GuardDuty agen keamanan.

Jika Anda belum memiliki grup keamanan yang mengaktifkan port 443 dalam terikat, [Buat grup keamanan](#) di EC2 Panduan Pengguna Amazon.

Jika ada masalah saat membatasi izin masuk ke VPC (atau cluster) Anda, berikan dukungan ke port 443 yang di-bound dari alamat IP apa pun (0.0.0.0/0).

Daftar berikut mencakup item yang baik untuk diketahui setelah Anda menginstal atau memperbarui agen keamanan.

Menilai cakupan runtime

Langkah selanjutnya setelah menginstal atau memperbarui agen keamanan Anda adalah menilai cakupan runtime sumber daya Anda. Jika status cakupan runtime tidak sehat, maka Anda harus memecahkan masalah. Untuk informasi selengkapnya, lihat [Masalah cakupan runtime dan pemecahan masalah](#).

Jika status cakupan runtime ditampilkan sebagai Sehat, ini menunjukkan bahwa Runtime Monitoring dapat mengumpulkan dan menerima peristiwa runtime. Untuk daftar acara ini, lihat [Jenis acara runtime yang dikumpulkan](#).

Nama DNS pribadi untuk titik akhir

Setelah Anda menginstal agen GuardDuty keamanan untuk sumber daya Anda, secara default, itu akan menyelesaikan dan terhubung ke nama DNS pribadi dari titik akhir VPC. Untuk endpoint non-FIPS, DNS pribadi akan muncul dalam format berikut:

```
guardduty-data.us-east-1.amazonaws.com
```

Itu Wilayah AWS, *us-east-1*, akan berubah berdasarkan Wilayah Anda.

Host dapat diinstal dengan dua agen keamanan

Saat bekerja dengan agen GuardDuty keamanan untuk EC2 instans Amazon, Anda dapat menginstal dan menggunakan agen pada host yang mendasari dalam kluster Amazon EKS. Jika Anda telah menggunakan agen keamanan di cluster EKS itu, host yang sama dapat memiliki dua agen keamanan yang berjalan di dalamnya pada saat yang bersamaan. Untuk informasi tentang cara GuardDuty kerja dalam skenario ini, lihat [Agen keamanan di host yang sama](#).

Meninjau statistik cakupan runtime dan masalah pemecahan masalah

Setelah Anda mengaktifkan Runtime Monitoring dan agen GuardDuty keamanan disebarkan ke sumber daya Anda, GuardDuty berikan statistik cakupan untuk jenis sumber daya yang sesuai dan status cakupan individual untuk sumber daya milik akun Anda. Status cakupan ditentukan dengan memastikan bahwa Anda telah mengaktifkan Runtime Monitoring, titik akhir VPC Amazon Anda telah dibuat, dan GuardDuty agen keamanan untuk sumber daya terkait telah digunakan. Status cakupan Sehat menunjukkan bahwa ketika ada peristiwa runtime yang terkait dengan sumber daya Anda, GuardDuty dapat menerima peristiwa runtime tersebut melalui titik akhir VPC Amazon, dan memantau perilakunya. Jika ada masalah pada saat mengonfigurasi Runtime Monitoring, membuat endpoint Amazon VPC, atau menerapkan agen GuardDuty keamanan, status cakupan akan muncul sebagai Tidak Sehat. Jika status cakupan tidak sehat, tidak GuardDuty akan dapat menerima atau memantau perilaku runtime sumber daya yang sesuai, atau menghasilkan temuan Runtime Monitoring.

Topik berikut akan membantu Anda meninjau statistik cakupan, mengonfigurasi EventBridge pemberitahuan, dan memecahkan masalah cakupan untuk jenis sumber daya tertentu.

Daftar Isi

- [Cakupan runtime dan pemecahan masalah untuk instans Amazon EC2](#)
- [Cakupan runtime dan pemecahan masalah untuk klaster Amazon ECS](#)
- [Cakupan runtime dan pemecahan masalah untuk klaster Amazon EKS](#)

Cakupan runtime dan pemecahan masalah untuk instans Amazon EC2

Untuk EC2 sumber daya Amazon, cakupan runtime dievaluasi pada tingkat instans. EC2Instans Amazon Anda dapat menjalankan beberapa jenis aplikasi dan beban kerja antara lain di lingkungan Anda. AWS Fitur ini juga mendukung EC2 instans Amazon yang dikelola Amazon ECS dan jika Anda memiliki kluster Amazon ECS yang berjalan di EC2 instans Amazon, masalah cakupan pada tingkat instans akan muncul di bawah cakupan runtime Amazon. EC2

Topik

- [Meninjau statistik cakupan](#)
- [Perubahan status cakupan dengan EventBridge notifikasi](#)

- [Memecahkan masalah cakupan EC2 runtime Amazon](#)

Meninjau statistik cakupan

Statistik cakupan untuk EC2 instans Amazon yang terkait dengan akun Anda sendiri atau akun anggota Anda adalah persentase EC2 contoh sehat di semua EC2 instance yang dipilih. Wilayah AWS Persamaan berikut mewakili ini sebagai:

$(\text{instances/All Contoh sehat}) * 100$

Jika Anda juga telah menerapkan agen GuardDuty keamanan untuk kluster Amazon ECS Anda, maka masalah cakupan tingkat instans apa pun yang terkait dengan kluster Amazon ECS yang berjalan di EC2 instans Amazon akan muncul sebagai masalah cakupan runtime instans Amazon EC2 .

Pilih salah satu metode akses untuk meninjau statistik cakupan akun Anda.

Console

- Masuk ke AWS Management Console dan buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.
- Di panel navigasi, pilih Runtime Monitoring.
- Pilih tab cakupan Runtime.
- Di bawah tab cakupan runtime EC2 instance, Anda dapat melihat statistik cakupan yang dikumpulkan berdasarkan status cakupan setiap EC2 instans Amazon yang tersedia di tabel daftar Instans.
 - Anda dapat memfilter tabel daftar Instance dengan kolom berikut:
 - ID Akun
 - Jenis manajemen agen
 - Versi agen
 - Status cakupan
 - ID Instance
 - Kluster ARN
 - Jika salah satu EC2 instans Anda memiliki status Cakupan sebagai Tidak Sehat, kolom Masalah menyertakan informasi tambahan tentang alasan status Tidak Sehat.

API/CLI

- Jalankan [ListCoverage](#) API dengan ID detektor valid Anda sendiri, Wilayah saat ini, dan titik akhir layanan. Anda dapat memfilter dan mengurutkan daftar instance menggunakan API ini.
- Anda dapat mengubah contoh filter-criteria dengan salah satu opsi berikut untuk CriterionKey:
 - ACCOUNT_ID
 - RESOURCE_TYPE
 - COVERAGE_STATUS
 - AGENT_VERSION
 - MANAGEMENT_TYPE
 - INSTANCE_ID
 - CLUSTER_ARN
- Saat filter-criteria termasuk RESOURCE_TYPE sebagai EC2, Runtime Monitoring tidak mendukung penggunaan ISSUE sebagai AttributeName. Jika Anda menggunakannya, respons API akan menghasilkan InvalidInputException.

Anda dapat mengubah contoh AttributeName sort-criteria dengan opsi berikut:

- ACCOUNT_ID
- COVERAGE_STATUS
- INSTANCE_ID
- UPDATED_AT
- Anda dapat mengubah *max-results* (hingga 50).
- Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan [ListDetectors](#) API. detectorId

```
aws guardduty --region us-east-1 list-coverage --detector-id 12abc34d567e8fa901bc2d34e56789f0 --sort-criteria '{"AttributeName": "EKS_CLUSTER_NAME", "OrderBy": "DESC"}' --filter-criteria '{"FilterCriterion": [{"CriterionKey": "ACCOUNT_ID", "FilterCondition": {"EqualsValue": "111122223333"} } ]}' --max-results 5
```

- Jalankan [GetCoverageStatistics](#) API untuk mengambil statistik agregat cakupan berdasarkan statisticsType

- **COUNT_BY_COVERAGE_STATUS**— Merupakan statistik cakupan untuk kluster EKS yang dikumpulkan berdasarkan status cakupan.
- **COUNT_BY_RESOURCE_TYPE**— Statistik cakupan dikumpulkan berdasarkan jenis AWS sumber daya dalam daftar.
- Anda dapat mengubah contoh `filter-criteria` dalam perintah. Anda dapat menggunakan opsi berikut untuk `CriterionKey`:
 - **ACCOUNT_ID**
 - **RESOURCE_TYPE**
 - **COVERAGE_STATUS**
 - **AGENT_VERSION**
 - **MANAGEMENT_TYPE**
 - **INSTANCE_ID**
 - **CLUSTER_ARN**
- Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan `ListDetectors` API. `detectorId`

```
aws guardduty --region us-east-1 get-coverage-statistics --detector-id 12abc34d567e8fa901bc2d34e56789f0 --statistics-type COUNT_BY_COVERAGE_STATUS --filter-criteria '{"FilterCriterion":[{"CriterionKey": "ACCOUNT_ID", "FilterCondition": {"EqualsValue": "123456789012"}}] }'
```

Jika status cakupan EC2 instans Anda tidak sehat, lihat [Memecahkan masalah cakupan EC2 runtime Amazon](#).

Perubahan status cakupan dengan EventBridge notifikasi

Status cakupan EC2 instans Amazon Anda mungkin tampak tidak sehat. Untuk mengetahui kapan status pertanggung jawaban berubah, kami sarankan Anda untuk memantau status pertanggung jawaban secara berkala, dan memecahkan masalah jika status menjadi tidak sehat. Atau, Anda dapat membuat EventBridge aturan Amazon untuk menerima pemberitahuan saat status cakupan berubah dari Tidak Sehat menjadi Sehat atau lainnya. Secara default, GuardDuty publikasikan ini di [EventBridge bus](#) untuk akun Anda.

Contoh skema pemberitahuan

Dalam EventBridge aturan, Anda dapat menggunakan contoh peristiwa dan pola peristiwa yang telah ditentukan sebelumnya untuk menerima pemberitahuan status cakupan. Untuk informasi selengkapnya tentang membuat EventBridge aturan, lihat [Membuat aturan](#) di Panduan EventBridge Pengguna Amazon.

Selain itu, Anda dapat membuat pola acara khusus dengan menggunakan skema pemberitahuan contoh berikut. Pastikan untuk mengganti nilai untuk akun Anda. Untuk mendapatkan pemberitahuan ketika status cakupan EC2 instans Amazon Anda berubah dari Healthy keUnhealthy, detail-type seharusnya*GuardDuty Runtime Protection Unhealthy*. Untuk mendapatkan pemberitahuan ketika status cakupan berubah dari Unhealthy keHealthy, ganti nilai detail-type dengan*GuardDuty Runtime Protection Healthy*.

```
{
  "version": "0",
  "id": "event ID",
  "detail-type": "GuardDuty Runtime Protection Unhealthy",
  "source": "aws.guardduty",
  "account": "Akun AWS ID",
  "time": "event timestamp (string)",
  "region": "Wilayah AWS",
  "resources": [
    ],
  "detail": {
    "schemaVersion": "1.0",
    "resourceAccountId": "string",
    "currentStatus": "string",
    "previousStatus": "string",
    "resourceDetails": {
      "resourceType": "EC2",
      "ec2InstanceDetails": {
        "instanceId": "",
        "instanceType": "",
        "clusterArn": "",
        "agentDetails": {
          "version": ""
        },
        "managementType": ""
      }
    },
    "issue": "string",
```

```

    "lastUpdatedAt": "timestamp"
  }
}

```

Memecahkan masalah cakupan EC2 runtime Amazon

Jika status cakupan EC2 instans Amazon Anda tidak sehat, Anda dapat melihat alasannya di bawah kolom Masalah.

Jika EC2 instans Anda dikaitkan dengan kluster EKS dan agen keamanan untuk EKS diinstal baik secara manual atau melalui konfigurasi agen otomatis, maka untuk memecahkan masalah cakupan, lihat. [Cakupan runtime dan pemecahan masalah untuk kluster Amazon EKS](#)

Tabel berikut mencantumkan jenis masalah dan langkah pemecahan masalah yang sesuai.

Jenis masalah	Pesan masalah	Langkah pemecahan masalah
Tidak Ada Pelaporan Agen	Menunggu pemberitahuan SSM	Menerima pemberitahuan SSM mungkin memakan waktu beberapa menit. Pastikan EC2 instans Amazon dikelola SSM. Untuk informasi selengkapnya, lihat langkah-langkah di bawah Metode 1 - Dengan menggunakan AWS Systems Manager di Memasang agen keamanan secara manual.
	(Kosong dengan sengaja)	Jika Anda mengelola agen GuardDuty keamanan secara manual, pastikan Anda mengikuti langkah-langkah di bawah ini Mengelola agen keamanan secara manual untuk EC2 sumber daya Amazon.

Jenis masalah	Pesan masalah	Langkah pemecahan masalah
		Jika Anda telah mengaktifkan konfigurasi agen otomatis: • EC2 Instans Anda dikelola SSM. • Lihat status agen keamanan Anda secara berkala. Untuk informasi selengkapnya, lihat Memvalidasi status instalasi agen GuardDuty keamanan. Validasi bahwa titik akhir VPC untuk instans EC2 Amazon Anda telah dikonfigurasi dengan benar. Untuk informasi selengkapnya, lihat Memvalidasi konfigurasi titik akhir VPC. Jika organisasi Anda memiliki kebijakan kontrol layanan (SCP), validasi bahwa batas izin tidak membatasi izin. <code>guardduty:SendSecurityTelemetry</code> Untuk informasi selengkapnya, lihat Memvalidasi kebijakan kontrol layanan organisasi Anda di lingkungan multi-akun.

Jenis masalah	Pesan masalah	Langkah pemecahan masalah
	Agen terputus	• Lihat status agen keamanan Anda. Untuk informasi selengkapnya, lihat Memvalidasi status instalasi agen GuardDuty keamanan. • Lihat log agen keamanan untuk mengidentifikasi akar penyebab potensial. Log memberikan kesalahan terperinci yang dapat Anda gunakan untuk memecahkan masalah sendiri. File log tersedia di bawah <code>/var/log/amzn-guardduty-agent/</code>. Lakukansudo journalctl -u amazon-guardduty-agent .
Agen Tidak Disediakan	Instance dengan tag pengecualian dikecualikan dari Runtime Monitoring.	GuardDuty tidak menerima peristiwa runtime dari EC2 instans Amazon yang diluncurkan dengan tag pengecualian:. GuardDuty Managed false Untuk menerima peristiwa runtime dari EC2 instance Amazon ini, hapus tag pengecualian.

Jenis masalah	Pesan masalah	Langkah pemecahan masalah
	Versi kernel lebih rendah dari versi yang didukung.	Untuk informasi tentang versi kernel yang didukung di seluruh distribusi OS, lihat Validasi persyaratan arsitektur EC2 instans Amazon.
	Versi kernel lebih tinggi dari versi yang didukung.	Untuk informasi tentang versi kernel yang didukung di seluruh distribusi OS, lihat Validasi persyaratan arsitektur EC2 instans Amazon.

Jenis masalah	Pesan masalah	Langkah pemecahan masalah
	Tidak dapat mengambil dokumen identitas instance.	Ikuti langkah-langkah ini: 1. Konfirmasikan bahwa sumber daya Anda adalah EC2 instans Amazon, dan bukan EC2 non-instance hybrid. 2. Konfirmasikan bahwa Layanan Metadata Instans (IMDS) diaktifkan. Untuk melakukannya, lihat Mengonfigurasi opsi Layanan Metadata Instance di EC2 Panduan Pengguna Amazon. 3. Verifikasi bahwa dokumen identitas instance ada. Untuk melakukannya, lihat Mengambil dokumen identitas instance di Panduan EC2 Pengguna Amazon. 4. Jika dokumen identitas instance masih belum ada, maka restart instance. Dokumen identitas instans dibuat saat instans dihentikan dan dimulai, dimulai ulang, atau diluncurkan.

Jenis masalah	Pesan masalah	Langkah pemecahan masalah
Pembuatan Asosiasi SSM Gagal	GuardDuty Asosiasi SSM sudah ada di akun Anda	1. Hapus asosiasi yang ada secara manual. Untuk informasi selengkapnya, lihat Menghapus asosiasi di Panduan AWS Systems Manager Pengguna. 2. Setelah Anda menghapus asosiasi, nonaktifkan lalu aktifkan kembali konfigurasi agen GuardDuty otomatis untuk Amazon EC2.
	Akun Anda memiliki terlalu banyak asosiasi SSM	Pilih salah satu dari dua opsi berikut: • Hapus semua asosiasi SSM yang tidak digunakan. Untuk informasi selengkapnya, lihat Menghapus asosiasi di Panduan AWS Systems Manager Pengguna. • Periksa apakah akun Anda memenuhi syarat untuk kenaikan kuota. Untuk informasi selengkapnya, lihat kuota Layanan Systems Manager di bagian. Referensi Umum AWS
Pembaruan Asosiasi SSM Gagal	GuardDuty Asosiasi SSM tidak ada di akun Anda	GuardDuty Asosiasi SSM tidak ada di akun Anda. Nonaktifkan dan kemudian aktifkan kembali Runtime Monitoring.

Jenis masalah	Pesan masalah	Langkah pemecahan masalah
Penghapusan Asosiasi SSM Gagal	GuardDuty Asosiasi SSM tidak ada di akun Anda	Asosiasi SSM tidak ada di akun Anda. Jika asosiasi SSM dihapus dengan sengaja, maka tidak ada tindakan yang diperlukan.

Jenis masalah	Pesan masalah	Langkah pemecahan masalah
Eksekusi Asosiasi Instans SSM Gagal	Persyaratan arsitektur atau prasyarat lainnya tidak terpenuhi.	Untuk informasi tentang distribusi sistem operasi terverifikasi, lihat Prasyarat untuk dukungan instans Amazon EC2. Jika Anda masih mengalami masalah ini, langkah-langkah berikut akan membantu Anda mengidentifikasi dan berpotensi menyelesaikan masalah: 1. Buka AWS Systems Manager konsol di https://console.aws.amazon.com/systems-manager/. 2. Di panel navigasi, di bawah Manajemen node, pilih Manajer Negara. 3. Filter berdasarkan properti Nama Dokumen dan masukkan AmazonGuardDuty-ConfigureRuntimeMonitoringSsmPlugin. 4. Pilih ID asosiasi yang sesuai dan lihat riwayat Eksekusi. 5. Menggunakan riwayat eksekusi, melihat kegagalan, mengidentifikasi akar penyebab

Jenis masalah	Pesan masalah	Langkah pemecahan masalah
		potensial, dan mencoba untuk menyelesaikannya.
Pembuatan Titik Akhir VPC Gagal	Pembuatan titik akhir VPC tidak didukung untuk VPC bersama <i>vpcId</i>	Runtime Monitoring mendukung penggunaa n VPC bersama dalam suatu organisasi. Untuk informasi selengkapnya, lihat Menggunakan VPC bersama dengan Runtime Monitoring .
	Hanya saat menggunak an VPC bersama dengan konfigurasi agen otomatis ID akun pemilik <i>11112222333</i> untuk VPC bersama <i>vpcId</i> tidak mengaktif kan Runtime Monitoring, konfigurasi agen otomatis, atau keduanya	Akun pemilik VPC bersama harus mengaktifkan Runtime Monitoring dan konfigurasi agen otomatis untuk setidaknya satu jenis sumber daya (Amazon EKS atau Amazon ECS ()).AWS Fargate Untuk informasi selengkap nya, lihat Prasyarat khusus untuk Runtime Monitoring GuardDuty .

Jenis masalah	Pesan masalah	Langkah pemecahan masalah
	Mengaktifkan DNS pribadi memerlukan atribut keduanya dan <code>enableDnsSupport</code> dan <code>enableDnsHostnames</code> VPC disetel ke <code>true</code> for <i>vpcId</i> (Layanan: Ec2, Kode Status: 400, ID Permintaan:). <i>a1b2c3d4-5678-90ab-cdef-EXAMPLE11111</i>	Pastikan atribut VPC berikut disetel ke <code>true</code> — <code>enableDnsSupport</code> dan <code>enableDnsHostnames</code> Untuk informasi selengkapnya, lihat atribut DNS di VPC Anda. Jika Anda menggunakan Konsol VPC Amazon di https://console.aws.amazon.com/vpc/ untuk membuat VPC Amazon, pastikan untuk memilih Aktifkan nama host DNS dan Aktifkan resolusi DNS. Untuk informasi selengkapnya, lihat opsi konfigurasi VPC.

Jenis masalah	Pesan masalah	Langkah pemecahan masalah
Penghapusan Titik Akhir VPC Bersama Gagal	Penghapusan titik akhir VPC bersama tidak diizinkan untuk ID akun, VPC 111122223333 bersama, ID akun pemilik. vpcId 555555555555	Langkah-langkah potensial: • Menonaktifkan status Runtime Monitoring akun peserta VPC bersama tidak memengaruhi kebijakan titik akhir VPC bersama dan grup keamanan yang ada di akun pemilik. Untuk menghapus titik akhir VPC bersama dan grup keamanan, Anda harus menonaktifkan Pemantauan Waktu Proses atau status konfigurasi agen otomatis di akun pemilik VPC bersama. • Akun peserta VPC bersama tidak dapat menghapus titik akhir VPC bersama dan grup keamanan yang dihosting di akun pemilik VPC bersama.

Jenis masalah	Pesan masalah	Langkah pemecahan masalah
Agan tidak melaporkan	(Kosong dengan sengaja)	Jenis masalah telah mencapai akhir dukungan. Jika Anda terus mengalami masalah ini dan belum melakukannya, aktifkan agen GuardDuty otomatis untuk Amazon EC2. Jika masalah masih berlanjut, pertimbangkan untuk menonaktifkan Runtime Monitoring selama beberapa menit dan kemudian aktifkan lagi.

Cakupan runtime dan pemecahan masalah untuk kluster Amazon ECS

Cakupan runtime untuk kluster Amazon ECS mencakup tugas yang sedang berjalan dan instans penampung AWS Fargate Amazon ECS. ¹

Untuk kluster Amazon ECS yang berjalan di Fargate, cakupan runtime dinilai pada tingkat tugas. Cakupan runtime cluster ECS mencakup tugas-tugas Fargate yang sudah mulai berjalan setelah Anda mengaktifkan Runtime Monitoring dan konfigurasi agen otomatis untuk Fargate (hanya ECS). Secara default, tugas Fargate tidak dapat diubah. GuardDuty tidak akan dapat menginstal agen keamanan untuk memantau kontainer pada tugas yang sudah berjalan. Untuk memasukkan tugas Fargate seperti itu, Anda harus berhenti dan memulai tugas lagi. Pastikan untuk memeriksa apakah layanan terkait didukung.

Untuk informasi tentang wadah Amazon ECS, lihat [Pembuatan kapasitas](#).

Daftar Isi

- [Meninjau statistik cakupan](#)
- [Perubahan status cakupan dengan EventBridge notifikasi](#)
- [Memecahkan masalah cakupan runtime Amazon ECS-Fargate](#)

Meninjau statistik cakupan

Statistik cakupan untuk sumber daya Amazon ECS yang terkait dengan akun Anda sendiri atau akun anggota Anda adalah persentase kluster Amazon ECS yang sehat di semua cluster Amazon ECS yang dipilih. Wilayah AWS Ini termasuk cakupan untuk kluster Amazon ECS yang terkait dengan instans Fargate dan Amazon. EC2 Persamaan berikut mewakili ini sebagai:

$$(\text{clusters/All Cluster sehat}) * 100$$

Pertimbangan

- Statistik cakupan untuk cluster ECS mencakup status cakupan tugas Fargate atau instance kontainer ECS yang terkait dengan cluster ECS tersebut. Status cakupan tugas Fargate mencakup tugas yang sedang berjalan atau baru saja selesai berjalan.
- Di tab cakupan runtime cluster ECS, bidang yang dicakup instance Container menunjukkan status cakupan instance container yang terkait dengan cluster Amazon ECS Anda.

Jika kluster Amazon ECS Anda hanya berisi tugas Fargate, hitungannya muncul sebagai 0/0.

- Jika kluster Amazon ECS Anda dikaitkan dengan EC2 instans Amazon yang tidak memiliki agen keamanan, kluster Amazon ECS juga akan memiliki status cakupan Tidak Sehat.

Untuk mengidentifikasi dan memecahkan masalah cakupan untuk EC2 instans Amazon terkait, lihat instans [Memecahkan masalah cakupan EC2 runtime Amazon](#) Amazon EC2.

Pilih salah satu metode akses untuk meninjau statistik cakupan akun Anda.

Console

- Masuk ke AWS Management Console dan buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.
- Di panel navigasi, pilih Runtime Monitoring.
- Pilih tab cakupan Runtime.
- Di bawah tab cakupan runtime cluster ECS, Anda dapat melihat statistik cakupan yang dikumpulkan berdasarkan status cakupan setiap kluster Amazon ECS yang tersedia di tabel daftar Clusters.
 - Anda dapat memfilter tabel daftar Cluster dengan kolom berikut:
 - ID Akun

- Nama Cluster
- Jenis manajemen agen
- Status cakupan
- Jika salah satu kluster Amazon ECS Anda memiliki status Cakupan sebagai Tidak Sehat, kolom Masalah menyertakan informasi tambahan tentang alasan status Tidak Sehat.

Jika kluster Amazon ECS dikaitkan dengan EC2 instans Amazon, navigasikan ke tab cakupan waktu proses EC2 instans dan filter menurut bidang nama Cluster untuk melihat Masalah terkait.

API/CLI

- Jalankan [ListCoverage](#) API dengan ID detektor valid Anda sendiri, Wilayah saat ini, dan titik akhir layanan. Anda dapat memfilter dan mengurutkan daftar instance menggunakan API ini.
- Anda dapat mengubah contoh `filter-criteria` dengan salah satu opsi berikut untuk `CriterionKey`:
 - `ACCOUNT_ID`
 - `ECS_CLUSTER_NAME`
 - `COVERAGE_STATUS`
 - `MANAGEMENT_TYPE`
- Anda dapat mengubah contoh `AttributeName sort-criteria` dengan opsi berikut:
 - `ACCOUNT_ID`
 - `COVERAGE_STATUS`
 - `ISSUE`
 - `ECS_CLUSTER_NAME`
 - `UPDATED_AT`

Bidang akan diperbarui hanya jika tugas baru dibuat di kluster Amazon ECS terkait atau ada perubahan dalam status cakupan yang sesuai.

- Anda dapat mengubah *max-results* (hingga 50).
- Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan [ListDetectors](#) API. `detectorId`

```
aws guardduty --region us-east-1 list-coverage --detector-id 12abc34d567e8fa901bc2d34e56789f0 --sort-criteria '{"AttributeName": "ECS_CLUSTER_NAME", "OrderBy": "DESC"}' --filter-criteria '{"FilterCriterion": [{"CriterionKey": "ACCOUNT_ID", "FilterCondition": {"EqualsValue": "111122223333"}}] }' --max-results 5
```

- Jalankan [GetCoverageStatistics](#) API untuk mengambil statistik agregat cakupan berdasarkan `statisticsType`
- Anda dapat mengubah contoh `statisticsType` ke salah satu opsi berikut:
 - `COUNT_BY_COVERAGE_STATUS`— Merupakan statistik cakupan untuk cluster ECS yang dikumpulkan berdasarkan status cakupan.
 - `COUNT_BY_RESOURCE_TYPE`— Statistik cakupan dikumpulkan berdasarkan jenis AWS sumber daya dalam daftar.
- Anda dapat mengubah contoh `filter-criteria` dalam perintah. Anda dapat menggunakan opsi berikut untuk `CriterionKey`:
 - `ACCOUNT_ID`
 - `ECS_CLUSTER_NAME`
 - `COVERAGE_STATUS`
 - `MANAGEMENT_TYPE`
 - `INSTANCE_ID`
- Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan [ListDetectors](#) API. `detectorId`

```
aws guardduty --region us-east-1 get-coverage-statistics --detector-id 12abc34d567e8fa901bc2d34e56789f0 --statistics-type COUNT_BY_COVERAGE_STATUS --filter-criteria '{"FilterCriterion": [{"CriterionKey": "ACCOUNT_ID", "FilterCondition": {"EqualsValue": "123456789012"}}] }'
```

Untuk informasi selengkapnya tentang masalah cakupan, lihat [Memecahkan masalah cakupan runtime Amazon ECS-Fargate](#).

Perubahan status cakupan dengan EventBridge notifikasi

Status cakupan cluster Amazon ECS Anda mungkin tampak tidak sehat. Untuk mengetahui kapan status pertanggungungan berubah, kami sarankan Anda untuk memantau status pertanggungungan secara

berkala, dan memecahkan masalah jika status menjadi tidak sehat. Atau, Anda dapat membuat EventBridge aturan Amazon untuk menerima pemberitahuan saat status cakupan berubah dari Tidak Sehat menjadi Sehat atau lainnya. Secara default, GuardDuty publikasikan ini di [EventBridge bus](#) untuk akun Anda.

Contoh skema pemberitahuan

Dalam EventBridge aturan, Anda dapat menggunakan contoh peristiwa dan pola peristiwa yang telah ditentukan sebelumnya untuk menerima pemberitahuan status cakupan. Untuk informasi selengkapnya tentang membuat EventBridge aturan, lihat [Membuat aturan](#) di Panduan EventBridge Pengguna Amazon.

Selain itu, Anda dapat membuat pola acara khusus dengan menggunakan skema pemberitahuan contoh berikut. Pastikan untuk mengganti nilai untuk akun Anda. Untuk mendapatkan pemberitahuan saat status cakupan kluster Amazon ECS Anda berubah dari Healthy keUnhealthy, detail-type seharusnya begitu. *GuardDuty Runtime Protection Unhealthy* Untuk mendapatkan pemberitahuan ketika status cakupan berubah dari Unhealthy keHealthy, ganti nilai detail-type dengan*GuardDuty Runtime Protection Healthy*.

```
{
  "version": "0",
  "id": "event ID",
  "detail-type": "GuardDuty Runtime Protection Unhealthy",
  "source": "aws.guardduty",
  "account": "Akun AWS ID",
  "time": "event timestamp (string)",
  "region": "Wilayah AWS",
  "resources": [
  ],
  "detail": {
    "schemaVersion": "1.0",
    "resourceAccountId": "string",
    "currentStatus": "string",
    "previousStatus": "string",
    "resourceDetails": {
      "resourceType": "ECS",
      "ecsClusterDetails": {
        "clusterName": "",
        "fargateDetails": {
          "issues": [],
          "managementType": ""
        }
      }
    }
  }
}
```

```

        "containerInstanceDetails":{
            "coveredContainerInstances":int,
            "compatibleContainerInstances":int
        }
    },
    "issue": "string",
    "lastUpdatedAt": "timestamp"
}

```

Memecahkan masalah cakupan runtime Amazon ECS-Fargate

Jika status cakupan klaster Amazon ECS Anda tidak sehat, Anda dapat melihat alasannya di bawah kolom Masalah.

Tabel berikut menyediakan langkah-langkah pemecahan masalah yang disarankan untuk masalah Fargate (hanya Amazon ECS). Untuk informasi tentang masalah cakupan EC2 instans Amazon, lihat [Memecahkan masalah cakupan EC2 runtime Amazon](#) EC2 instans Amazon.

Jenis masalah	Informasi tambahan	Langkah pemecahan masalah yang disarankan
Agan tidak melaporkan	Agan tidak melaporkan tugas di TaskDefinition - 'TASK_DEFINITION'	Validasi bahwa titik akhir VPC untuk tugas klaster Amazon ECS Anda telah dikonfigurasi dengan benar. Untuk informasi selengkapnya, lihat Memvalidasi konfigurasi titik akhir VPC. Jika organisasi Anda memiliki kebijakan kontrol layanan (SCP), validasi bahwa batas izin tidak membatasi izin. <code>guardduty:SendSecurityTelemetry</code> Untuk informasi selengkapnya, lihat Memvalidasi kebijakan kontrol

Jenis masalah	Informasi tambahan	Langkah pemecahan masalah yang disarankan
		layanan organisasi Anda di lingkungan multi-akun.
Agen keluar	<code>VPC_ISSUE ; for task in TaskDefinition - 'TASK_DEFINITION '</code>	Lihat detail masalah VPC di informasi tambahan.
	ExitCode: EXIT_CODE untuk tugas-tugas di TaskDefinition - 'TASK_DEFINITION '	Lihat detail masalah di informasi tambahan.
	Alasan: REASON untuk tugas-tugas di TaskDefinition - 'TASK_DEFINITION '	
	ExitCode: EXIT_CODE dengan alasan: 'EXIT_CODE ' untuk tugas di TaskDefinition - 'TASK_DEFINITION '	

Jenis masalah	Informasi tambahan	Langkah pemecahan masalah yang disarankan
	Agan keluar: Alasan:CannotPullContainerError : tarik manifes gambar telah dicoba lagi...	Dalam skenario GuardDuty ini, berpotensi tidak dapat menarik gambar wadah sespan. Tugas Anda akan terus berjalan tetapi tidak GuardDuty dapat mendeteksi potensi ancaman. Lakukan langkah pemecahan masalah berikut satu per satu untuk memeriksa apakah itu membantu menyelesaikan masalah cakupan: • Izin: Pastikan peran eksekusi tugas Anda memiliki izin ECR yang diperlukan yang tercantum di dalamnya. Persyaratan izin • Konektivitas jaringan: Verifikasi bahwa tugas Fargate Anda dapat mencapai ECR baik melalui akses internet publik atau titik akhir VPC yang dikonfigurasi dengan benar seperti yang dijelaskan dalam. Persyaratan konektivitas jaringan • Konfigurasi grup keamanan: Periksa apakah grup keamanan Anda mengizinkan akses keluar ke daftar awalan terkelola S3 pada

Jenis masalah	Informasi tambahan	Langkah pemecahan masalah yang disarankan
		port 443 seperti yang dijelaskan di Konfigurasi grup keamanan • Jalankan AWS Support TroubleshootingECSTaskFailedToStart runbook di Wilayah klaster Anda untuk mengidentifikasi masalah tertentu. • Lihat log tugas untuk pesan kesalahan. Untuk informasi tentang cara melakukannya, lihat Melihat log agen kontainer Amazon ECS di Panduan Pengembang Layanan Kontainer Elastis Amazon. Untuk kesalahan umum dan pemecahan masalah, lihat Pemecahan masalah Amazon ECS di Panduan Pengembang Layanan Amazon Elastic Container. Ketiga komponen ini (izin, konektivitas jaringan, dan konfigurasi grup keamanan) bersifat independen tetapi semuanya diperlukan untuk berhasil mengunduh gambar GuardDuty kontainer dari Amazon ECR.

Jenis masalah	Informasi tambahan	Langkah pemecahan masalah yang disarankan
Pembuatan Titik Akhir VPC Gagal	Mengaktifkan DNS pribadi memerlukan atribut keduanya <code>enableDnsSupport</code> dan <code>enableDnsHostnames</code> VPC disetel ke <code>true</code> for <i>vpcId</i> (Layanan: EC2, Kode Status: 400, ID Permintaan: <i>a1b2c3d4-5678-90ab-cdef-EXAMPLE11111</i>).	Jika masalah berlanjut, lihat AWS Step Functions Alur kerja saya gagal secara tak terduga. Pastikan atribut VPC berikut disetel ke <code>true</code> — <code>enableDnsSupport</code> dan <code>enableDnsHostnames</code>. Untuk informasi selengkapnya, lihat atribut DNS di VPC Anda. Jika Anda menggunakan Konsol VPC Amazon di https://console.aws.amazon.com/vpc/ untuk membuat VPC Amazon, pastikan untuk memilih Aktifkan nama host DNS dan Aktifkan resolusi DNS. Untuk informasi selengkapnya, lihat opsi konfigurasi VPC.
Agan tidak disediakan	Pemanggilan yang tidak didukung oleh <i>SERVICE</i> untuk tugas di TaskDefinition - <i>'TASK_DEFINITION'</i> Arsitektur CPU yang tidak didukung <i>TYPE</i> " untuk tugas di TaskDefinition - <i>'TASK_DEFINITION'</i>	Tugas ini dipanggil oleh a <i>SERVICE</i> yang tidak didukung. Tugas ini berjalan pada arsitektur CPU yang tidak didukung. Untuk informasi tentang arsitektur CPU yang didukung, lihat Memvalidasi persyaratan arsitektur.

Jenis masalah	Informasi tambahan	Langkah pemecahan masalah yang disarankan
	TaskExecutionRole Hilang dari TaskDefinition - <code>'TASK_DEFINITION'</code>	Peran eksekusi tugas ECS tidak ada. Untuk informasi tentang menyediakan peran eksekusi tugas dan izin yang diperlukan, lihat Prasyarat untuk akses gambar kontainer .
	Konfigurasi jaringan <code>'CONFIGURATION_DETAILS'</code> tidak ada untuk tugas di TaskDefinition - <code>'TASK_DEFINITION'</code>	Masalah konfigurasi jaringan mungkin muncul karena konfigurasi VPC yang hilang, atau subnet yang hilang atau kosong. Validasi bahwa konfigurasi jaringan Anda benar. Untuk informasi selengkapnya, lihat Prasyarat untuk akses gambar kontainer. Untuk informasi selengkapnya, lihat parameter definisi tugas Amazon ECS di Panduan Pengembang Layanan Kontainer Elastis Amazon.

Jenis masalah	Informasi tambahan	Langkah pemecahan masalah yang disarankan
	Tugas dimulai ketika cluster memiliki tag pengecualian dikecualikan dari Runtime Monitoring. ID tugas yang terkena dampak: '<i>TASK_ID</i>'	Bila Anda mengubah GuardDuty tag yang telah ditentukan dari GuardDuty Managed - true ke GuardDutyManaged -false, tidak GuardDuty akan menerima peristiwa runtime untuk cluster Amazon ECS ini. Perbarui tag ke GuardDuty Managed - true dan kemudian luncurkan kembali tugas.
	Layanan yang diterapkan saat klaster memiliki tag pengecualian dikecualikan dari Runtime Monitoring. Nama layanan yang terkena dampak: "<i>SERVICE_NAME</i>"	Ketika layanan diterapkan dengan tag pengecualian GuardDutyManaged -false, tidak GuardDuty akan menerima peristiwa runtime untuk klaster Amazon ECS ini. Perbarui tag ke GuardDuty Managed - true dan kemudian gunakan kembali layanan.

Jenis masalah	Informasi tambahan	Langkah pemecahan masalah yang disarankan
	Tugas yang dimulai sebelum mengaktifkan Konfigurasi Agen Otomatis tidak tercakup. ID tugas yang terkena dampak: " <i>TASK_ID</i> "	Ketika cluster berisi tugas yang diluncurkan sebelum mengaktifkan konfigurasi agen Otomatis untuk Amazon ECS, maka tidak GuardDuty akan dapat melindungi ini. Luncurkan kembali tugas untuk dipantau oleh GuardDuty
	Layanan yang digunakan sebelum mengaktifkan Konfigurasi Agen Otomatis tidak tercakup. Nama layanan yang terkena dampak: " <i>SERVICE_NAME</i> "	Ketika layanan diterapkan sebelum mengaktifkan konfigurasi agen Otomatis untuk Amazon ECS, tidak GuardDuty akan menerima peristiwa runtime untuk kluster ECS.

Jenis masalah	Informasi tambahan	Langkah pemecahan masalah yang disarankan
	Layanan '<i>SERVICE_NAME</i>' memerlukan penerapan baru untuk memperbaiki/memecahkan masalah. Referensi dokumentasi, Nama layanan yang terkena dampak: "<i>SERVICE_NAME</i>" Tugas yang dimulai sebelum mengaktifkan Runtime Monitoring memerlukan peluncuran ulang. ID tugas yang terkena dampak: "<i>TASK_ID_1</i>"	Layanan yang dimulai sebelum mengaktifkan Runtime Monitoring tidak didukung. Anda dapat memulai ulang layanan atau memperbarui layanan dengan forceNewDeployment opsi dengan mengikuti langkah-langkah di bawah Memperbarui layanan Amazon ECS menggunakan konsol di Panduan Pengembang Layanan Amazon Elastic Container. Atau, Anda juga dapat menggunakan langkah-langkah UpdateService di bawah Referensi API Amazon Elastic Container Service. Di Amazon ECS, tugasnya tidak dapat diubah. Untuk menilai perilaku runtime atau AWS Fargate tugas yang sedang berjalan, pastikan Runtime Monitoring sudah diaktifkan, lalu restart tugas GuardDuty untuk menambahkan sespan container.

Jenis masalah	Informasi tambahan	Langkah pemecahan masalah yang disarankan
Lainnya	Masalah tak dikenal, untuk tugas di TaskDefinition - '<i>TASK_DEFINITION</i>'	Gunakan pertanyaan-pertanyaan berikut untuk mengidentifikasi akar penyebab masalah: • Apakah tugas dimulai sebelum Anda mengaktifkan Runtime Monitoring? Di Amazon ECS, tugasnya tidak dapat diubah. Untuk menilai perilaku runtime dari tugas Fargate yang sedang berjalan, pastikan Runtime Monitoring sudah diaktifkan, lalu restart tugas GuardDuty untuk menambahkan sespan container. • Apakah tugas ini bagian dari penerapan layanan yang dimulai sebelum Anda mengaktifkan Runtime Monitoring? Jika ya, Anda dapat memulai ulang layanan atau memperbarui layanan <code>forceNewDeployment</code> dengan menggunakan langkah-langkah dalam Memperbarui layanan. Anda juga dapat menggunakan UpdateService atau AWS CLI.

Jenis masalah	Informasi tambahan	Langkah pemecahan masalah yang disarankan
		• Apakah tugas diluncurkan setelah mengecualikan cluster ECS dari Runtime Monitoring? Saat Anda mengubah GuardDuty tag yang telah ditentukan sebelumnya dari GuardDutyManaged - true ke GuardDutyManaged -false, tidak GuardDuty akan menerima peristiwa runtime untuk cluster ECS. • Apakah layanan Anda berisi tugas yang memiliki format lamataskArn? GuardDuty Runtime Monitoring tidak mendukung cakupan untuk tugas yang memiliki format lama. taskArn Untuk informasi tentang Nama Sumber Daya Amazon (ARNs) untuk sumber daya Amazon ECS, lihat Nama Sumber Daya Amazon (ARNs) dan IDs.

Cakupan runtime dan pemecahan masalah untuk kluster Amazon EKS

Setelah Anda mengaktifkan Runtime Monitoring dan menginstal agen GuardDuty keamanan (addon) untuk EKS baik secara manual atau melalui konfigurasi agen otomatis, Anda dapat mulai menilai cakupan untuk kluster EKS Anda.

Daftar Isi

- [Meninjau statistik cakupan](#)
- [Perubahan status cakupan dengan EventBridge notifikasi](#)
- [Memecahkan masalah cakupan runtime Amazon EKS](#)

Meninjau statistik cakupan

Statistik cakupan untuk kluster EKS yang terkait dengan akun Anda sendiri atau akun anggota Anda adalah persentase kluster EKS yang sehat di semua kluster EKS yang dipilih. Wilayah AWS Persamaan berikut mewakili ini sebagai:

$(\text{clusters}/\text{All Cluster sehat}) * 100$

Pilih salah satu metode akses untuk meninjau statistik cakupan akun Anda.

Console

- Masuk ke AWS Management Console dan buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.
- Di panel navigasi, pilih Runtime Monitoring.
- Pilih tab cakupan runtime kluster EKS.
- Di bawah tab cakupan runtime kluster EKS, Anda dapat melihat statistik cakupan yang dikumpulkan berdasarkan status cakupan yang tersedia di tabel daftar Clusters.
 - Anda dapat memfilter tabel daftar Clusters dengan kolom berikut:
 - Nama cluster
 - ID Akun
 - Jenis manajemen agen
 - Status cakupan
 - Versi pengaya

- Jika salah satu kluster EKS Anda memiliki status Cakupan sebagai Tidak Sehat, kolom Masalah dapat menyertakan informasi tambahan tentang alasan status Tidak Sehat.

API/CLI

- Jalankan [ListCoverage](#) API dengan ID detektor, Wilayah, dan titik akhir layanan Anda yang valid. Anda dapat memfilter dan mengurutkan daftar cluster menggunakan API ini.
- Anda dapat mengubah contoh `filter-criteria` dengan salah satu opsi berikut untuk `CriterionKey`:
 - `ACCOUNT_ID`
 - `CLUSTER_NAME`
 - `RESOURCE_TYPE`
 - `COVERAGE_STATUS`
 - `ADDON_VERSION`
 - `MANAGEMENT_TYPE`
- Anda dapat mengubah contoh `AttributeName sort-criteria` dengan opsi berikut:
 - `ACCOUNT_ID`
 - `CLUSTER_NAME`
 - `COVERAGE_STATUS`
 - `ISSUE`
 - `ADDON_VERSION`
 - `UPDATED_AT`
- Anda dapat mengubah *max-results* (hingga 50).
- Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan [ListDetectors](#) API. `detectorId`

```
aws guardduty --region us-east-1 list-coverage --detector-id 12abc34d567e8fa901bc2d34e56789f0 --sort-criteria '{"AttributeName": "EKS_CLUSTER_NAME", "OrderBy": "DESC"}' --filter-criteria '{"FilterCriterion": [{"CriterionKey": "ACCOUNT_ID", "FilterCondition": {"EqualsValue": "111122223333"}}] }' --max-results 5
```

- Jalankan [GetCoverageStatistics](#) API untuk mengambil statistik agregat cakupan berdasarkan.

statisticsType

- Anda dapat mengubah contoh `statisticsType` ke salah satu opsi berikut:
 - `COUNT_BY_COVERAGE_STATUS`— Merupakan statistik cakupan untuk kluster EKS yang dikumpulkan berdasarkan status cakupan.
 - `COUNT_BY_RESOURCE_TYPE`— Statistik cakupan dikumpulkan berdasarkan jenis AWS sumber daya dalam daftar.
- Anda dapat mengubah contoh `filter-criteria` dalam perintah. Anda dapat menggunakan opsi berikut untuk `CriterionKey`:
 - `ACCOUNT_ID`
 - `CLUSTER_NAME`
 - `RESOURCE_TYPE`
 - `COVERAGE_STATUS`
 - `ADDON_VERSION`
 - `MANAGEMENT_TYPE`
- Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan `ListDetectors` API. `detectorId`

```
aws guardduty --region us-east-1 get-coverage-statistics --detector-id 12abc34d567e8fa901bc2d34e56789f0 --statistics-type COUNT_BY_COVERAGE_STATUS --filter-criteria '{"FilterCriterion":[{"CriterionKey": "ACCOUNT_ID", "FilterCondition": {"EqualsValue": "123456789012"}}] }'
```

Jika status cakupan cluster EKS Anda tidak sehat, lihat [Memecahkan masalah cakupan runtime Amazon EKS](#).

Perubahan status cakupan dengan EventBridge notifikasi

Status cakupan kluster EKS di akun Anda mungkin muncul sebagai Tidak Sehat. Untuk mendeteksi kapan status pertanggung jawaban menjadi tidak sehat, kami sarankan Anda memantau status pertanggung jawaban secara berkala dan memecahkan masalah, jika statusnya tidak sehat. Atau, Anda dapat membuat EventBridge aturan Amazon untuk memberi tahu Anda ketika status cakupan berubah dari salah satu `Unhealthy` ke `Healthy` atau sebaliknya. Secara default, GuardDuty publikasikan ini di [EventBridge bus](#) untuk akun Anda.

Contoh skema pemberitahuan

Dalam EventBridge aturan, Anda dapat menggunakan contoh peristiwa dan pola peristiwa yang telah ditentukan sebelumnya untuk menerima pemberitahuan status cakupan. Untuk informasi selengkapnya tentang membuat EventBridge aturan, lihat [Membuat aturan](#) di Panduan EventBridge Pengguna Amazon.

Selain itu, Anda dapat membuat pola acara khusus dengan menggunakan skema pemberitahuan contoh berikut. Pastikan untuk mengganti nilai untuk akun Anda. Untuk mendapatkan pemberitahuan saat status cakupan kluster Amazon EKS Anda berubah dari Healthy keUnhealthy, detail-type seharusnya *GuardDuty Runtime Protection Unhealthy* begitu. Untuk mendapatkan pemberitahuan ketika status cakupan berubah dari Unhealthy keHealthy, ganti nilai detail-type dengan*GuardDuty Runtime Protection Healthy*.

```
{
  "version": "0",
  "id": "event ID",
  "detail-type": "GuardDuty Runtime Protection Unhealthy",
  "source": "aws.guardduty",
  "account": "Akun AWS ID",
  "time": "event timestamp (string)",
  "region": "Wilayah AWS",
  "resources": [
    ],
  "detail": {
    "schemaVersion": "1.0",
    "resourceAccountId": "string",
    "currentStatus": "string",
    "previousStatus": "string",
    "resourceDetails": {
      "resourceType": "EKS",
      "eksClusterDetails": {
        "clusterName": "string",
        "availableNodes": "string",
        "desiredNodes": "string",
        "addonVersion": "string"
      }
    },
    "issue": "string",
    "lastUpdatedAt": "timestamp"
  }
}
```


Memecahkan masalah cakupan runtime Amazon EKS

Jika status cakupan untuk kluster EKS Anda `Unhealthy`, Anda dapat melihat kesalahan terkait baik di bawah kolom Masalah di GuardDuty konsol, atau dengan menggunakan tipe [CoverageResource](#) data.

Saat bekerja dengan tag inklusi atau pengecualian untuk memantau kluster EKS Anda secara selektif, mungkin perlu beberapa waktu bagi tag untuk disinkronkan. Ini dapat memengaruhi status cakupan cluster EKS terkait. Anda dapat mencoba menghapus dan menambahkan tag yang sesuai (penyertaan atau pengecualian) lagi. Untuk informasi selengkapnya, lihat [Menandai sumber daya Amazon EKS Anda](#) di Panduan Pengguna Amazon EKS.

Struktur masalah cakupan adalah `Issue type:Extra information`. Biasanya, masalah akan memiliki informasi Tambahan opsional yang mungkin mencakup pengecualian atau deskripsi sisi klien tertentu tentang masalah tersebut. Berdasarkan informasi tambahan, tabel berikut memberikan langkah-langkah yang disarankan untuk memecahkan masalah cakupan untuk kluster EKS Anda.

Jenis masalah (awalan)	Informasi tambahan	Langkah pemecahan masalah yang disarankan
Pembuatan Addon Gagal	Addon tidak <code>aws-guard-duty-agent</code> kompatibel dengan versi cluster saat ini. <i>ClusterName</i> Addon ditentukan tidak didukung.	Pastikan Anda menggunakan salah satu versi Kubernetes yang mendukung penerapan add-on EKS. <code>aws-guard-duty-agent</code> Untuk informasi selengkapnya, lihat Versi Kubernetes didukung oleh agen keamanan GuardDuty . Untuk informasi tentang memperbarui versi Kubernetes Anda, lihat Memperbarui versi Kubernetes kluster Amazon EKS .
Pembuatan Addon Gagal Update Addon Gagal Addon Status Tidak Sehat	Masalah EKS Addon -AddonIssueCode : AddonIssueMessage	Untuk informasi tentang langkah-langkah yang disarankan untuk kode masalah add-on tertentu,

Jenis masalah (awalan)	Informasi tambahan	Langkah pemecahan masalah yang disarankan
		lihat Troubleshooting steps for Addon creation/updatation error with Addon issue code. Untuk daftar kode masalah addon yang mungkin Anda alami dalam masalah ini, lihat AddonIssue.
Pembuatan Titik Akhir VPC Gagal	Pembuatan titik akhir VPC tidak didukung untuk VPC bersama <i>vpcId</i> Hanya saat menggunakan VPC bersama dengan konfigurasi agen otomatis ID akun pemilik <i>11112222333</i> untuk VPC bersama <i>vpcId</i> tidak mengaktifkan Runtime Monitoring, konfigurasi agen otomatis, atau keduanya.	Runtime Monitoring sekarang mendukung penggunaan VPC bersama dalam suatu organisasi. Pastikan akun Anda memenuhi semua prasyarat. Untuk informasi selengkapnya, lihat Prasyarat untuk menggunakan VPC bersama. Akun pemilik VPC bersama harus mengaktifkan Runtime Monitoring dan konfigurasi agen otomatis untuk setidaknya satu jenis sumber daya (Amazon EKS atau Amazon ECS ()).AWS Fargate Untuk informasi selengkapnya, lihat Prasyarat khusus untuk Runtime Monitoring GuardDuty.

Jenis masalah (awalan)	Informasi tambahan	Langkah pemecahan masalah yang disarankan
	Mengaktifkan DNS pribadi memerlukan atribut keduanya <code>enableDnsSupport</code> dan <code>enableDnsHostnames</code> VPC disetel ke <code>true</code> for <i>vpcId</i> (Layanan: Ec2, Kode Status: 400, ID Permintaan: <i>a1b2c3d4-5678-90ab-cdef-EXAMPLE11111</i>)	Pastikan atribut VPC berikut disetel ke <code>true</code> — <code>enableDnsSupport</code> dan <code>enableDnsHostnames</code> Untuk informasi selengkapnya, lihat atribut DNS di VPC Anda. Jika Anda menggunakan Konsol VPC Amazon di https://console.aws.amazon.com/vpc/ untuk membuat VPC Amazon, pastikan untuk memilih Aktifkan nama host DNS dan Aktifkan resolusi DNS. Untuk informasi selengkapnya, lihat opsi konfigurasi VPC.

Jenis masalah (awalan)	Informasi tambahan	Langkah pemecahan masalah yang disarankan
Penghapusan Titik Akhir VPC Bersama Gagal	Penghapusan titik akhir VPC bersama tidak diizinkan untuk ID akun, VPC 111122223333 bersama, ID akun pemilik. vpcId 555555555555	Langkah-langkah potensial: • Menonaktifkan status Runtime Monitoring akun peserta VPC bersama tidak memengaruhi kebijakan titik akhir VPC bersama dan grup keamanan yang ada di akun pemilik. Untuk menghapus titik akhir VPC bersama dan grup keamanan, Anda harus menonaktifkan Pemantauan Waktu Proses atau status konfigurasi agen otomatis di akun pemilik VPC bersama. • Akun peserta VPC bersama tidak dapat menghapus titik akhir VPC bersama dan grup keamanan yang dihosting di akun pemilik VPC bersama.
Cluster EKS lokal	Addon EKS tidak didukung pada kluster pos terdepan lokal.	Tidak bisa ditindaklanjuti. Untuk informasi lebih lanjut, lihat Amazon EKS di AWS pos terdepan.

Jenis masalah (awalan)	Informasi tambahan	Langkah pemecahan masalah yang disarankan
Izin pengaktifan Pemantauan Runtime EKS tidak diberikan	(mungkin atau mungkin tidak menampilkan informasi tambahan)	1. Jika informasi tambahan tersedia untuk masalah ini, perbaiki akar penyebabnya dan ikuti langkah berikutnya. 2. Alihkan EKS Runtime Monitoring untuk memaatikannya dan kemudian menyalakannya kembali. Pastikan GuardDuty agen juga dikerahkan, baik secara otomatis melalui GuardDuty atau manual.
EKS Runtime Monitoring pemberdayaan penyedia sumber daya sedang berlangsung	(mungkin atau mungkin tidak menampilkan informasi tambahan)	Tidak bisa ditindaklanjuti. Setelah Anda mengaktifkan EKS Runtime Monitoring, status cakupan mungkin tetap ada Unhealthy hingga langkah penyediaan sumber daya selesai. Status cakupan dipantau dan diperbarui secara berkala.
Lainnya (masalah lainnya)	Kesalahan karena kegagalan otorisasi	Alihkan EKS Runtime Monitoring untuk mematikan dan kemudian menyalakannya kembali. Pastikan bahwa GuardDuty agen juga dikerahkan, baik secara otomatis melalui GuardDuty atau manual.

Langkah-langkah pemecahan masalah untuk creation/updation kesalahan Addon dengan kode masalah Addon

Kesalahan pembuatan atau pembaruan addon	Langkah pemecahan masalah
EKS Addon Issue -InsufficientNumber OfReplicas : Add-on tidak sehat karena tidak memiliki jumlah replika yang diinginkan.	- Dengan menggunakan pesan masalah, Anda dapat mengidentifikasi dan memperbaiki akar masalahnya. Anda bisa mulai dengan mendeskripsikan cluster Anda. Misalnya, gunakan kubectl describe pods untuk mengidentifikasi akar penyebab kegagalan pod. Setelah Anda memperbaiki akar penyebabnya, coba lagi langkahnya (pembuatan atau pembaruan add-on). - Jika masalah berlanjut, validasi bahwa titik akhir VPC untuk kluster Amazon EKS Anda telah dikonfigurasi dengan benar. Untuk informasi selengkapnya, lihat Memvalidasi konfigurasi titik akhir VPC.
EKS Addon Issue -InsufficientNumber OfReplicas : Add-on tidak sehat karena satu atau lebih pod tidak dijadwalkan 0/x node tersedia: x Insufficient cpu. preemption: not eligible due to preemptionPolicy=Never EKS Addon Issue -InsufficientNumber OfReplicas : Add-on tidak sehat karena satu atau lebih pod tidak dijadwalkan 0/x node tersedia: x Too many pods. preemptio n: not eligible due to preemptio nPolicy=Never	Untuk mengatasi masalah ini, Anda dapat melakukan salah satu dari yang berikut: - Perbarui prioritas pod GuardDuty agen: Parameter dan nilai yang dapat dikonfigurasi dengan menyetel PriorityClass ke salah satu opsi yang mendukung preemptionPolicy nilai sebagaiPreemptLowerPriority . Untuk informasi tentang prioritas pod, lihat Prioritas Pod dan Preemption di Dokumentasi Kubernetes. - Tingkatkan instans: Untuk mengelola sumber daya dan membuat pemilihan instans

Kesalahan pembuatan atau pembaruan addon	Langkah pemecahan masalah
EKS Addon Issue -InsufficientNumber OfReplicas : Add-on tidak sehat karena satu atau lebih pod tidak dijadwalkan 0/x node tersedia: 1 Insufficient memory. preemption: not eligible due to preemptionPolicy=Never	yang optimal, lihat Mengelola sumber daya komputasi menggunakan node dan Pilih jenis instans EC2 node Amazon yang optimal di Panduan Pengguna Amazon EKS.  Note Pesan ditampilkan o/x karena hanya GuardDuty melaporkan kesalahan pertama yang ditemukan. Jumlah sebenarnya dari pod yang berjalan di GuardDuty daemonset mungkin lebih besar dari 0.

Kesalahan pembuatan atau pembaruan addon	Langkah pemecahan masalah
Masalah EKS Addon -InsufficientNumberOfReplicas : Add-on tidak sehat karena satu atau lebih pod memiliki wadah yang menunggu CrashLoop BackOff: Completed	Anda dapat melihat log yang terkait dengan pod dan mengidentifikasi masalahnya. Untuk informasi tentang cara melakukannya, lihat Debug Running Pods di Dokumentasi Kubernetes. Gunakan daftar periksa berikut untuk memecahkan masalah add-on ini: • Validasi bahwa Runtime Monitoring diaktifkan. • Validasi bahwa Prasyarat untuk dukungan cluster Amazon EKS, seperti distribusi OS terverifikasi dan versi Kubernetes yang didukung, terpenuhi. • Saat Anda mengelola agen keamanan secara manual, konfirmasikan bahwa Anda membuat titik akhir VPC untuk semua VPCs. Saat Anda mengaktifkan konfigurasi GuardDuty otomatis, Anda tetap harus memvalidasi bahwa titik akhir VPC dibuat. Misalnya, saat menggunakan VPC bersama dalam konfigurasi otomatis. Untuk memvalidasi ini, lihat Memvalidasi konfigurasi titik akhir VPC. • Konfirmasikan bahwa agen GuardDuty keamanan dapat menyelesaikan DNS GuardDuty pribadi titik akhir VPC. Untuk mengetahui titik akhir, lihat Nama DNS pribadi untuk titik akhir di Mengelola agen GuardDuty keamanan

Kesalahan pembuatan atau pembaruan addon	Langkah pemecahan masalah
	Untuk melakukan ini, Anda dapat menggunakan <code>nslookup</code> alat di Windows atau Mac, atau <code>dig</code> alat di Linux. Saat menggunakan <code>nslookup</code>, Anda dapat menggunakan perintah berikut setelah mengganti Wilayah <code>us-west-2</code> dengan Wilayah Anda: <pre>nslookup guardduty-data. <i>us-west-2</i> .amazonaws.com</pre> Validasi bahwa kebijakan titik akhir GuardDuty VPC Anda atau kebijakan kontrol layanan tidak memengaruhi tindakan. <code>guardduty:SendSecurityTelemetry</code>

Kesalahan pembuatan atau pembaruan addon	Langkah pemecahan masalah
Masalah EKS Addon -InsufficientNumberOfReplicas : Add-on tidak sehat karena satu atau lebih pod memiliki wadah yang menunggu CrashLoop BackOff: Error	Anda dapat melihat log yang terkait dengan pod dan mengidentifikasi masalahnya. Untuk informasi tentang cara melakukannya, lihat Debug Running Pods di Dokumentasi Kubernetes. Setelah Anda mengidentifikasi masalah, gunakan daftar periksa berikut untuk memecahkan masalah ini: • Validasi bahwa Runtime Monitoring diaktifkan. • Validasi bahwa Prasyarat untuk dukungan cluster Amazon EKS, seperti distribusi OS terverifikasi dan versi Kubernetes yang didukung, terpenuhi. • Agen GuardDuty keamanan dapat menyelesaikan DNS pribadi titik akhir GuardDuty VPC. Untuk mengetahui titik akhir, lihat Nama DNS pribadi untuk titik akhir di Mengelola agen GuardDuty keamanan
EKS Addon Issue -AdmissionRequestDenied : webhook penerimaan "validate.kyverno.svc-fail" menolak permintaan: kebijakan DaemonSet/amazon-guardduty/aws-guardduty-agent untuk pelanggaran sumber daya:: restrict-image-registries:autogen-validate-registries ...	1. Cluster Amazon EKS atau administrator keamanan harus meninjau kebijakan keamanan yang memblokir pembaruan Addon. 2. Anda harus menonaktifkan controller (webhook) atau meminta controller menerima permintaan dari Amazon EKS.

Kesalahan pembuatan atau pembaruan addon	Langkah pemecahan masalah
EKS Addon Issue -ConfigurationConflict : Konflik ditemukan saat mencoba menerapkan. Tidak akan berlanjut karena menyelesaikan mode konflik. Conflicts: DaemonSet.apps aws-guardduty-agent - .spec.template.spec.containers[name="aws-guardduty-agent"].image	Saat membuat atau memperbarui Addon, berikan bendera OVERWRITE konflik penyelesaian. Ini berpotensi menimpa setiap perubahan yang telah dibuat langsung ke sumber daya terkait di Kubernetes dengan menggunakan API Kubernetes. Anda dapat terlebih dahulu Menghapus addon Amazon EKS dari cluster dan kemudian menginstal ulang.

Kesalahan pembuatan atau pembaruan addon	Langkah pemecahan masalah
Masalah EKS Addon - AccessDenied: priorityclasses.scheduling.k8s.io "aws-guardduty-agent.priorityclass" is forbidden: User "eks:addon-manager" cannot patch resource "priorityclasses" in API group "scheduling.k8s.io" at the cluster scope AddonUpdationFailed: EKSAaddon Masalah - AccessDenied: namespaces\"amazon-guardduty\"isforbidden:User\"eks:addon-manager\"cannotpatchresource\"namespaces\"inAPIgroup\"\"inthenamespace\"amazon-guardduty\"	Anda harus menambahkan izin yang hilang ke eks:addon-cluster-admin ClusterRoleBinding manual. Tambahkan yang berikut ini yam1 keeks:addon-cluster-admin : <pre>--- kind: ClusterRoleBinding apiVersion: rbac.authorization .k8s.io/v1 metadata: name: eks:addon-cluster-admin subjects: - kind: User name: eks:addon-manager apiGroup: rbac.authorization.k8s.io roleRef: kind: ClusterRole name: cluster-admin apiGroup: rbac.authorization.k8s.io ---</pre> Anda sekarang dapat menerapkan ini yam1 ke cluster Amazon EKS Anda dengan menggunakan perintah berikut: <pre>kubectl apply -f eks-addon-cluster-admin.yam1</pre>

Kesalahan pembuatan atau pembaruan addon	Langkah pemecahan masalah
Masalah EKS Addon - AccessDenied: admission webhook "validation.gatekeeper.sh" denied the request: [all-namespace-must-have-label-owner] All namespaces must have an `owner` label	Anda harus menonaktifkan pengontrol atau meminta pengontrol menerima permintaan dari kluster Amazon EKS. Sebelum membuat atau memperbarui add-on, Anda juga dapat membuat GuardDuty namespace dan memberi label sebagai. owner
Masalah EKS Addon - AccessDenied: admission webhook "validation.gatekeeper.sh" denied the request: [all-namespace-must-have-label-owner] All namespaces must have an `owner` label	Anda harus menonaktifkan pengontrol atau meminta pengontrol menerima permintaan dari kluster Amazon EKS. Sebelum membuat atau memperbarui add-on, Anda juga dapat membuat GuardDuty namespace dan memberi label sebagai. owner
Masalah EKS Addon - AccessDenied: admission webhook "validation.gatekeeper.sh" denied the request: [allowed-container-registries] container <aws-guardduty-agent> has an invalid image registry	Tambahkan registri gambar GuardDuty ke allowed-container-registries dalam pengontrol penerimaan Anda. Untuk informasi lebih lanjut, lihat repositori ECR untuk EKS v1.8.1-eks-build.2 di. Agen hosting repositori Amazon ECR GuardDuty

Menyiapkan CPU dan pemantauan memori

Setelah mengaktifkan Runtime Monitoring dan menilai bahwa status cakupan kluster Anda Sehat, Anda dapat menyiapkan dan melihat metrik wawasan.

Topik berikut dapat membantu Anda mengevaluasi kinerja agen yang digunakan terhadap CPU dan batas memori untuk GuardDuty agen.

Menyiapkan pemantauan di Amazon ECS cluster

Langkah-langkah berikut dari Panduan CloudWatch Pengguna Amazon dapat membantu Anda mengevaluasi kinerja agen yang digunakan terhadap batas CPU dan memori GuardDuty agen:

1. [Menyiapkan Wawasan Kontainer di Amazon ECS untuk metrik tingkat kluster dan layanan](#)
2. [Metrik Wawasan Kontainer Amazon ECS](#)

Menyiapkan pemantauan di klaster Amazon EKS

Setelah agen GuardDuty keamanan diterapkan dan Anda menilai bahwa status cakupan klaster Anda Sehat, Anda dapat mengatur dan melihat metrik wawasan Container.

Mengevaluasi kinerja agen keamanan

1. [Menyiapkan Wawasan Kontainer di Amazon EKS dan Kubernetes di Panduan Pengguna Amazon CloudWatch](#)
2. [Metrik Amazon EKS dan Kubernetes Container Insights di Panduan Pengguna Amazon CloudWatch](#)

Mengelola kinerja dengan agen keamanan v1.5.0 ke atas

Dengan agen keamanan [v1.5.0 dan](#) yang lebih baru, ketika wawasan menunjukkan bahwa GuardDuty agen terkait mencapai batas yang ditetapkan, Anda dapat mengonfigurasi parameter tertentu. Untuk informasi selengkapnya, lihat [Konfigurasi parameter add-on EKS](#).

Menggunakan VPC bersama dengan Runtime Monitoring

GuardDuty Runtime Monitoring mendukung penggunaan Amazon Virtual Private Cloud bersama (Amazon VPC) untuk Akun AWS Anda yang termasuk dalam organisasi yang sama di AWS Organizations Anda dapat menggunakan VPC bersama dengan dua cara:

- Konfigurasi agen otomatis (Disarankan) — Saat mengelola agen keamanan GuardDuty secara otomatis, itu juga akan mengonfigurasi kebijakan titik akhir VPC Amazon. Kebijakan ini didasarkan pada setelan VPC bersama organisasi Anda.

Anda harus mengaktifkan konfigurasi agen otomatis di akun pemilik VPC bersama dan semua akun yang berpartisipasi yang akan membagikan VPC ini.

- Agen yang dikelola secara manual — Saat Anda mengelola agen keamanan secara manual dengan VPC bersama, Anda harus memperbarui kebijakan titik akhir VPC untuk mengizinkan akun terkait mengakses VPC bersama. Untuk melakukan ini, Anda dapat menggunakan kebijakan contoh yang dibagikan di [Cara kerjanya](#) bagian berikut.

Untuk skenario manajemen manual yang melibatkan akun yang berpartisipasi untuk VPC bersama, status pertanggunggunaan mungkin tidak akurat. Untuk memastikan up-to-date perlindungan dan status cakupan sumber daya Anda, GuardDuty merekomendasikan untuk mengaktifkan konfigurasi agen otomatis untuk semua akun yang akan menggunakan VPC bersama.

Topik

- [Cara kerjanya](#)
- [Prasyarat untuk menggunakan VPC bersama](#)

Cara kerjanya

Yang Akun AWS termasuk dalam organisasi yang sama dengan akun pemilik VPC Amazon bersama juga dapat berbagi titik akhir VPC Amazon yang sama. Setiap akun yang menggunakan kebijakan titik akhir VPC Amazon yang sama disebut sebagai AWS akun peserta dari VPC Amazon bersama yang terkait.

Contoh berikut menunjukkan kebijakan titik akhir VPC default dari akun pemilik VPC bersama dan akun peserta. Ini `aws:PrincipalOrgID` akan menampilkan ID organisasi yang terkait dengan sumber daya VPC bersama. Penggunaan kebijakan ini terbatas pada akun peserta yang ada dalam organisasi akun pemilik.

Example Contoh kebijakan titik akhir VPC bersama

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Action": "*",
    "Resource": "*",
    "Effect": "Allow",
    "Principal": "*"
  },
  {
    "Condition": {
```

```
        "StringNotEquals": {
            "aws:PrincipalOrgID": "o-abcdef0123"
        },
        "Action": "*",
        "Resource": "*",
        "Effect": "Deny",
        "Principal": "*"
    }
}
```

Dengan konfigurasi agen GuardDuty otomatis

Saat akun pemilik VPC bersama mengaktifkan Pemantauan Waktu Proses dan konfigurasi agen otomatis untuk sumber daya apa pun (Amazon EKS atau (hanya Amazon ECS)), semua yang dibagikan VPCs memenuhi syarat untuk penginstalan otomatis titik akhir VPC Amazon bersama dan grup keamanan terkait di akun pemilik VPC bersama. AWS Fargate GuardDuty mengambil ID organisasi yang terkait dengan VPC Amazon bersama.

GuardDuty membuat titik akhir VPC Amazon saat akun pemilik VPC bersama atau akun yang berpartisipasi membutuhkannya. Contoh membutuhkan endpoint VPC Amazon termasuk GuardDuty mengaktifkan, Runtime Monitoring, EKS Runtime Monitoring, atau meluncurkan tugas Amazon ECS-Fargate baru. Jika akun ini mengaktifkan Pemantauan Waktu Proses dan konfigurasi agen otomatis untuk semua jenis sumber daya, GuardDuty buat titik akhir VPC Amazon dan tetapkan kebijakan titik akhir dengan ID organisasi yang sama dengan akun pemilik VPC bersama. GuardDuty menambahkan GuardDutyManaged tag dan menyetelnya `true` untuk titik akhir VPC Amazon yang dibuat. GuardDuty Jika akun pemilik VPC Amazon bersama belum mengaktifkan Pemantauan Waktu Proses atau konfigurasi agen otomatis untuk salah satu sumber daya, tidak GuardDuty akan menetapkan kebijakan titik akhir VPC Amazon. Untuk informasi tentang mengonfigurasi Runtime Monitoring dan mengelola agen keamanan secara otomatis di akun pemilik VPC bersama, lihat.

[Mengaktifkan GuardDuty Runtime Monitoring](#)

Menggunakan dengan agen yang dikelola secara manual

Saat Anda menggunakan VPC bersama dengan agen yang dikelola secara manual, validasi bahwa tidak ada kebijakan Deny titik akhir eksplisit yang memblokir akun apa pun yang perlu menggunakan VPC bersama. Ini akan mencegah agen keamanan mengirim telemetri ke GuardDuty, menghasilkan status `Unhealthy` cakupan. Untuk menyiapkan kebijakan titik akhir, lihat [Example shared VPC endpoint policy](#).

Cakupan runtime mungkin tidak akurat dalam skenario seperti izin yang hilang ke VPC bersama. Anda dapat terus memantau cakupan sumber daya dengan mengikuti langkah-langkah untuk jenis sumber daya Anda [Meninjau statistik cakupan runtime dan masalah pemecahan masalah](#).

Untuk memastikan perlindungan Runtime Monitoring berkelanjutan dari sumber daya komputasi Anda, GuardDuty merekomendasikan untuk mengaktifkan konfigurasi agen otomatis untuk akun pemilik VPC bersama dan semua akun yang berpartisipasi untuk sumber daya Anda.

Prasyarat untuk menggunakan VPC bersama

Sebagai bagian dari pengaturan awal, lakukan langkah-langkah berikut di Akun AWS mana Anda ingin menjadi pemilik VPC bersama:

1. Membuat organisasi — Membuat organisasi dengan mengikuti langkah-langkah dalam [Membuat dan mengelola organisasi](#) dalam Panduan AWS Organizations Pengguna.

Untuk informasi tentang menambahkan atau menghapus akun anggota, lihat [Mengelola Akun AWS di organisasi Anda](#).

2. Membuat sumber daya VPC bersama — Anda dapat membuat sumber daya VPC bersama dari akun pemilik. Untuk informasi selengkapnya, lihat [Berbagi subnet VPC Anda dengan akun lain di Panduan](#) Pengguna Amazon VPC.

Prasyarat khusus untuk Runtime Monitoring GuardDuty

Daftar berikut memberikan prasyarat yang khusus untuk: GuardDuty

- Akun pemilik VPC bersama dan akun yang berpartisipasi dapat berasal dari berbagai organisasi di GuardDuty. Namun, mereka harus menjadi anggota organisasi yang sama di AWS Organizations. Ini diperlukan GuardDuty untuk membuat titik akhir VPC Amazon dan grup keamanan untuk VPC bersama. Untuk informasi tentang cara VPCs kerja bersama, lihat [Membagikan VPC Anda dengan akun lain di Panduan](#) Pengguna Amazon VPC.
- Aktifkan Runtime Monitoring atau EKS Runtime Monitoring, dan konfigurasi agen GuardDuty otomatis untuk sumber daya apa pun di akun pemilik VPC bersama dan akun peserta. Untuk informasi selengkapnya, lihat [Mengaktifkan Runtime Monitoring](#).

Jika Anda telah menyelesaikan konfigurasi ini, lanjutkan dengan langkah berikutnya.

- Saat bekerja dengan Amazon EKS atau tugas Amazon ECS (AWS Fargate hanya), pastikan untuk memilih sumber daya VPC bersama yang terkait dengan akun pemilik dan pilih subnetnya.

Menggunakan Infrastructure as Code (IAC) dengan GuardDuty agen keamanan otomatis

Gunakan bagian ini hanya jika daftar berikut berlaku untuk kasus penggunaan Anda:

- Anda menggunakan alat Infrastructure as Code (IAC), seperti AWS Cloud Development Kit (AWS CDK) dan Terraform, untuk mengelola sumber daya Anda AWS, dan
- Anda perlu mengaktifkan konfigurasi agen GuardDuty otomatis untuk satu atau beberapa jenis sumber daya - Amazon EKS, Amazon EC2, atau Amazon ECS-Fargate.

Ikhtisar grafik ketergantungan sumber daya IAC

Saat Anda mengaktifkan konfigurasi agen GuardDuty otomatis untuk jenis sumber daya, GuardDuty secara otomatis membuat titik akhir VPC dan grup keamanan yang terkait dengan titik akhir VPC ini, dan menginstal agen keamanan untuk jenis sumber daya ini. Secara default, GuardDuty akan menghapus titik akhir VPC dan grup keamanan terkait hanya setelah Anda menonaktifkan Runtime Monitoring. Untuk informasi selengkapnya, lihat [Menonaktifkan, menghapus instalasi, dan membersihkan sumber daya di Runtime Monitoring](#).

Ketika Anda menggunakan alat IAC, ia mempertahankan grafik ketergantungan sumber daya. Pada saat penghapusan sumber daya menggunakan alat IAC, itu hanya menghapus sumber daya yang dapat dilacak sebagai bagian dari grafik ketergantungan sumber daya. Alat IAC mungkin tidak tahu tentang sumber daya yang dibuat di luar konfigurasi yang ditentukan. Misalnya, Anda membuat VPC dengan alat IAC dan kemudian menambahkan grup keamanan ke VPC ini dengan menggunakan AWS konsol atau operasi API. Dalam grafik ketergantungan sumber daya, sumber daya VPC yang Anda buat bergantung pada grup keamanan terkait. Jika Anda menghapus sumber daya VPC ini dengan menggunakan alat IAC, maka Anda akan mendapatkan kesalahan. Cara untuk mengatasi kesalahan ini adalah dengan menghapus grup keamanan terkait secara manual atau memperbarui konfigurasi IAC untuk memasukkan sumber daya tambahan ini.

Masalah umum - Menghapus sumber daya di IAC

Saat menggunakan konfigurasi agen GuardDuty otomatis, Anda mungkin ingin menghapus sumber daya (Amazon EKS, Amazon EC2, atau Amazon ECS-Fargate) yang Anda buat menggunakan alat IAC. Namun, sumber daya ini bergantung pada titik akhir VPC yang dibuat. GuardDuty ini mencegah alat IAC untuk menghapus sumber daya dengan sendirinya dan mengharuskan Anda

untuk menonaktifkan Runtime Monitoring, yang selanjutnya menghapus titik akhir VPC secara otomatis.

Misalnya, ketika Anda mencoba menghapus titik akhir VPC yang GuardDuty dibuat atas nama Anda, Anda akan mendapatkan kesalahan yang mirip dengan contoh berikut.

Example

Contoh kesalahan saat menggunakan CDK

```
The following resource(s) failed to delete:
[mycdkvpcapplicationpublicsubnet1Subnet1SubnetEXAMPLE1, mycdkvpcapplicationprivatesubnet1Subne
Resource handler returned message: "The subnet 'subnet-APKAEIVFHP46CEXAMPLE' has
dependencies and cannot be deleted. (Service: Ec2, Status Code: 400, Request
ID: e071c3c5-7442-4489-838c-0dfc6EXAMPLE)" (RequestToken: 4381cff8-6240-208a-8357-5557b7EXAMPL
HandlerErrorCode: InvalidRequest)
```

Example

Contoh kesalahan saat menggunakan Terraform

```
module.vpc.aws_subnet.private[1]: Still destroying... [id=subnet-APKAEIVFHP46CEXAMPLE,
19m50s elapsed]
module.vpc.aws_subnet.private[1]: Still destroying... [id=subnet-APKAEIVFHP46CEXAMPLE,
20m0s elapsed]

Error: deleting EC2 Subnet (subnet-APKAEIBAERJR2EXAMPLE): DependencyViolation: The
subnet 'subnet-APKAEIBAERJR2EXAMPLE' has dependencies and cannot be deleted.
status code: 400, request id: e071c3c5-7442-4489-838c-0dfc6EXAMPLE
```

Solusi - Mencegah masalah penghapusan sumber daya

Bagian ini membantu Anda mengelola titik akhir VPC dan grup keamanan secara independen. GuardDuty

Untuk mendapatkan kepemilikan penuh atas sumber daya yang dikonfigurasi dengan menggunakan alat IAc, lakukan langkah-langkah berikut dalam urutan yang tercantum:

1. Buat sebuah VPC. Untuk mengizinkan izin masuk, kaitkan titik akhir GuardDuty VPC dengan grup keamanan, ke VPC ini.
2. Aktifkan konfigurasi agen GuardDuty otomatis untuk jenis sumber daya Anda

Setelah Anda menyelesaikan langkah-langkah sebelumnya, tidak GuardDuty akan membuat titik akhir VPC sendiri dan akan menggunakan kembali salah satu yang Anda buat dengan menggunakan alat IAC.

Untuk informasi tentang membuat VPC Anda sendiri, lihat [Membuat VPC hanya di Gateway Transit VPC](#) Amazon. Untuk informasi tentang membuat titik akhir VPC, lihat bagian berikut untuk jenis sumber daya Anda:

- Untuk Amazon EC2, lihat [Prasyarat - Membuat titik akhir Amazon VPC secara manual](#).
- Untuk Amazon EKS, lihat [Prasyarat - Membuat titik akhir VPC Amazon](#).

Mengumpulkan jenis peristiwa runtime yang menggunakan GuardDuty

Agen GuardDuty keamanan mengumpulkan jenis peristiwa berikut dan mengirimkannya ke GuardDuty backend untuk deteksi dan analisis ancaman. GuardDuty tidak membuat acara ini dapat diakses oleh Anda. Jika GuardDuty mendeteksi potensi ancaman dan menghasilkan [Jenis penemuan Runtime Monitoring](#), Anda dapat melihat detail temuan yang sesuai.

Untuk informasi tentang cara GuardDuty menggunakan jenis peristiwa yang dikumpulkan di Runtime Monitoring, lihat [Memilih untuk tidak menggunakan data Anda untuk perbaikan layanan](#).

Proses acara

Peristiwa proses mewakili informasi yang terkait dengan proses yang berjalan di EC2 instans Amazon dan beban kerja kontainer. Tabel berikut mencakup nama bidang dan deskripsi peristiwa proses yang dikumpulkan oleh Runtime Monitoring untuk mendeteksi potensi ancaman.

Nama bidang	Deskripsi
Nama proses	Nama proses yang diamati.
Jalur Proses	Jalur absolut dari proses yang dapat dieksekusi.
ID Proses	ID yang ditetapkan untuk proses oleh sistem operasi.

Nama bidang	Deskripsi
Namespace PID	ID proses proses dalam namespace PID sekunder selain namespace PID tingkat host. Untuk proses di dalam wadah, itu adalah ID proses yang diamati di dalam wadah.
Memproses ID Pengguna	ID unik pengguna yang mengeksekusi proses.
Proses UUID	ID unik yang ditetapkan untuk proses oleh GuardDuty.
Proses GID	ID proses dari grup proses.
Proses EGID	ID grup yang efektif dari grup proses.
Proses EUID	ID pengguna yang efektif dari proses tersebut.
Nama Pengguna Proses	Nama pengguna yang menjalankan proses.
Waktu Mulai Proses	Waktu ketika proses itu dibuat. Bidang ini dalam format string tanggal UTC (2023-03-22T19:37:20.168Z).
Proses yang Dapat Dieksekusi SHA-256	SHA256Hash dari proses yang dapat dieksekusi.
Jalur Skrip Proses	Jalur file skrip yang dieksekusi.
Variabel Lingkungan Proses	Variabel lingkungan tersedia untuk proses. Hanya LD_PRELOAD dan LD_LIBRARY_PATH dikumpulkan.
Proses Direktori Kerja Saat Ini (PWD)	Presentasikan direktori kerja proses.
Proses orang tua	Rincian proses proses induk. Proses induk adalah proses yang menciptakan proses yang diamati.

Nama bidang	Deskripsi
Argumen Baris Perintah Saat ini, bidang ini terbatas pada versi agen tertentu yang sesuai dengan jenis sumber daya: - Fargate (hanya Amazon ECS) dengan agen GuardDuty keamanan v1.0.0 ke atas. - EC2 Instans Amazon dengan agen GuardDuty keamanan v1.0.0 dan yang lebih baru. - Amazon EKS cluster dengan agen keamanan v1.4.0 dan di atasnya. Untuk informasi selengkapnya, lihat GuardDuty versi rilis agen keamanan.	Argumen baris perintah disediakan pada saat eksekusi proses. Bidang ini mungkin berisi data pelanggan yang sensitif.

Acara kontainer

Peristiwa kontainer mewakili informasi yang terkait dengan aktivitas beban kerja kontainer. Tabel berikut mencakup nama bidang dan deskripsi peristiwa beban kerja kontainer yang dikumpulkan Runtime Monitoring untuk mendeteksi potensi ancaman.

Nama bidang	Deskripsi
Nama Kontainer	Nama wadahnya. Bila tersedia, bidang ini menampilkan nilai <code>labelio.kubernetes.container.name</code>.
Kontainer UID	ID unik dari container yang ditetapkan oleh runtime container.
Runtime Kontainer	Runtime kontainer (seperti <code>docker</code> atau <code>containerd</code>) digunakan untuk menjalankan kontainer.

Nama bidang	Deskripsi
ID Gambar Kontainer	ID dari gambar kontainer.
Nama Gambar Kontainer	Nama gambar kontainer.

AWS Fargate (Hanya Amazon ECS) peristiwa tugas

Peristiwa tugas Fargate-Amazon ECS mewakili aktivitas yang terkait dengan tugas Amazon ECS yang berjalan pada komputasi Fargate. Tabel berikut mencakup nama bidang dan deskripsi peristiwa tugas Amazon ECS-Fargate yang dikumpulkan oleh Runtime Monitoring untuk mendeteksi potensi ancaman.

Nama bidang	Deskripsi
Nama Sumber Daya Tugas Amazon (ARN)	ARN dari tugas tersebut.
Nama Klaster	Nama cluster Amazon ECS.
Nama Keluarga	Nama keluarga definisi tugas. <code>family</code> ini digunakan sebagai nama untuk definisi tugas yang digunakan untuk meluncurkan tugas.
Nama Layanan	Nama layanan Amazon ECS, jika tugas diluncurkan sebagai bagian dari layanan.
Jenis Peluncuran	Infrastruktur tempat tugas Anda berjalan. Untuk Runtime Monitoring dengan resource type <code>asECSCluster</code> , tipe peluncuran bisa berupa salah satu <code>EC2</code> atau <code>FARGATE</code> .
CPU	Jumlah unit CPU yang digunakan oleh tugas seperti yang dinyatakan dalam definisi tugas.

Acara pod Kubernetes

Tabel berikut mencakup nama bidang dan deskripsi dari peristiwa pod Kubernetes yang dikumpulkan oleh Runtime Monitoring untuk mendeteksi potensi ancaman.

Nama bidang	Deskripsi
ID Pod	ID dari pod Kubernetes.
Nama pod	Nama pod Kubernetes.
Ruang Nama Pod	Nama namespace Kubernetes tempat beban kerja Kubernetes berada.
Nama Cluster Kubernetes	Nama cluster Kubernetes.

Acara Sistem Nama Domain (DNS)

Peristiwa Sistem Nama Domain (DNS) mencakup rincian kueri DNS yang dibuat oleh jenis sumber daya Anda dan tanggapan yang sesuai. Tabel berikut mencakup nama bidang dan deskripsi peristiwa DNS yang dikumpulkan oleh Runtime Monitoring untuk mendeteksi potensi ancaman.

Nama bidang	Deskripsi
Jenis soket	Jenis soket untuk menunjukkan semantik komunikasi. Misalnya, SOCK_RAW.
Alamat Keluarga	Merupakan protokol komunikasi yang terkait dengan alamat. Misalnya, keluarga alamat AF_INET digunakan untuk protokol IP v4.
ID Arah	ID dari arah koneksi.
Nomor Protokol	Nomor protokol layer 4 seperti 17 untuk UDP dan 6 untuk TCP.
IP Titik Akhir Jarak Jauh DNS	IP jarak jauh dari koneksi.

Nama bidang	Deskripsi
Port Titik Akhir Jarak Jauh DNS	Nomor port koneksi.
IP Titik Akhir Lokal DNS	IP lokal dari koneksi.
Pelabuhan Titik Akhir Lokal DNS	Nomor port koneksi.
Muatan DNS	Payload paket DNS yang berisi kueri dan tanggapan DNS.

Buka acara

Acara terbuka dikaitkan dengan akses dan modifikasi file. Tabel berikut mencakup nama bidang dan deskripsi peristiwa terbuka yang dikumpulkan oleh Runtime Monitoring untuk mendeteksi potensi ancaman.

Nama bidang	Deskripsi
Filepath	Jalur file yang dibuka dalam acara ini.
Bendera	Menjelaskan mode akses file, seperti read-only, write-only, dan read-write.

Memuat acara modul

Tabel berikut mencakup nama bidang dan deskripsi peristiwa modul beban yang dikumpulkan oleh Runtime Monitoring untuk mendeteksi potensi ancaman.

Nama bidang	Deskripsi
Nama Modul	Nama modul dimuat ke dalam kernel.

Acara Mprotect

Acara Mprotect memberikan informasi tentang perubahan pada pengaturan perlindungan memori dari proses yang berjalan pada sistem yang dipantau. Tabel berikut mencakup nama bidang dan deskripsi peristiwa Mprotect yang dikumpulkan Runtime Monitoring untuk mendeteksi potensi ancaman.

Nama bidang	Deskripsi
Rentang Alamat	Rentang alamat tempat perlindungan aksesnya dimodifikasi.
Wilayah Memori	Menentukan Wilayah ruang alamat proses seperti tumpukan dan heap.
Bendera	Merupakan opsi yang mengontrol perilaku acara ini.

Acara gunung

Mount event memberikan informasi yang terkait dengan pemasangan dan pelepasan sistem file pada sumber daya yang dipantau. Tabel berikut mencakup nama bidang dan deskripsi peristiwa pemasangan yang dikumpulkan oleh Runtime Monitoring untuk mendeteksi potensi ancaman.

Nama bidang	Deskripsi
Target Gunung	Jalur tempat sumber mount dipasang.
Sumber Gunung	Jalur pada host yang dipasang di target mount.
Jenis Sistem File	Merupakan jenis FileSystem yang dipasang.
Bendera	Merupakan opsi yang mengontrol perilaku acara ini.

Tautkan acara

Peristiwa tautan memberikan visibilitas ke dalam aktivitas manajemen tautan sistem file di sumber daya yang dipantau. Tabel berikut mencakup nama bidang dan deskripsi peristiwa tautan yang dikumpulkan oleh Runtime Monitoring untuk mendeteksi potensi ancaman.

Nama bidang	Deskripsi
Jalur Tautan	Jalur tempat hard link dibuat.
Jalur Target	Jalur file di mana hard link menunjuk.

Acara Symlink

Acara Symlink memberikan visibilitas ke dalam aktivitas manajemen tautan simbolik sistem file di sumber daya yang dipantau. Tabel berikut mencakup nama bidang dan deskripsi peristiwa symlink yang dikumpulkan oleh Runtime Monitoring untuk mendeteksi potensi ancaman.

Nama bidang	Deskripsi
Jalur Tautan	Jalur tempat tautan simbolis dibuat.
Jalur Target	Jalur file di mana tautan simbolik menunjuk.

Acara Dup

Peristiwa Dup memberikan visibilitas ke dalam duplikasi deskriptor file dengan proses yang berjalan pada sumber daya yang dipantau. Tabel berikut mencakup nama bidang dan deskripsi peristiwa dup yang dikumpulkan oleh Runtime Monitoring untuk mendeteksi potensi ancaman.

Nama bidang	Deskripsi
Deskriptor File Lama	Deskriptor file yang mewakili objek file terbuka.
Deskriptor File Baru	Deskriptor file baru yang merupakan duplikat dari deskriptor file lama. Baik deskriptor file lama dan baru mewakili objek file terbuka yang sama.
IP Titik Akhir Jarak Jauh Dup	Alamat IP jarak jauh dari soket jaringan diwakili oleh deskriptor file lama. Hanya berlaku ketika deskriptor file lama mewakili soket jaringan.

Nama bidang	Deskripsi
Port Titik Akhir Jarak Jauh Dup	Port jarak jauh dari soket jaringan diwakili oleh deskriptor file lama. Hanya berlaku ketika deskriptor file lama mewakili soket jaringan.
IP Titik Akhir Lokal Dup	Alamat IP lokal dari soket jaringan diwakili oleh deskriptor file lama. Hanya berlaku ketika deskriptor file lama mewakili soket jaringan.
Pelabuhan Titik Akhir Lokal Dup	Port lokal soket jaringan diwakili oleh deskriptor file lama. Hanya berlaku ketika deskriptor file lama mewakili soket jaringan.

Acara peta memori

Tabel berikut mencakup nama bidang dan deskripsi peristiwa peta memori yang dikumpulkan oleh Runtime Monitoring untuk mendeteksi potensi ancaman.

Nama bidang	Deskripsi
Filepath	Jalur file tempat memori dipetakan.

Acara soket

Peristiwa soket memberikan informasi tentang koneksi soket jaringan yang digunakan dalam aktivitas sumber daya yang dipantau. Tabel berikut mencakup nama bidang dan deskripsi peristiwa soket yang dikumpulkan oleh Runtime Monitoring untuk mendeteksi potensi ancaman.

Nama bidang	Deskripsi
Keluarga alamat	Merupakan protokol komunikasi yang terkait dengan alamat. Misalnya, keluarga alamat AF_INET digunakan untuk protokol versi IP 4.
Jenis Soket	Jenis soket untuk menunjukkan semantik komunikasi. Misalnya, SOCK_RAW.

Nama bidang	Deskripsi
Nomor protokol	Menentukan protokol tertentu dalam keluarga alamat. Biasanya ada protokol tunggal dalam keluarga alamat. Misalnya, keluarga alamat AF_INET hanya memiliki protokol IP.

Connect event

Acara Connect memberikan visibilitas ke dalam koneksi jaringan yang dibuat oleh proses pada sumber daya yang dipantau. Tabel berikut mencakup nama bidang dan deskripsi peristiwa connect yang dikumpulkan oleh Runtime Monitoring untuk mendeteksi potensi ancaman.

Nama bidang	Deskripsi
Keluarga alamat	Merupakan protokol komunikasi yang terkait dengan alamat. Misalnya, keluarga alamat AF_INET digunakan untuk protokol IP v4.
Jenis Soket	Jenis soket untuk menunjukkan semantik komunikasi. Misalnya, SOCK_RAW.
Nomor Protokol	Menentukan protokol tertentu dalam keluarga alamat. Biasanya ada protokol tunggal dalam keluarga alamat. Misalnya, keluarga alamat AF_INET hanya memiliki protokol IP.
Filepath	Jalur file soket jika keluarga alamat adalah AF_UNIX.
IP Titik Akhir Jarak Jauh	IP jarak jauh dari koneksi.
Port Endpoint Jarak Jauh	Nomor port koneksi.
IP Titik Akhir Lokal	IP lokal dari koneksi.
Pelabuhan Endpoint Lokal	Nomor port koneksi.

Proses acara VM Readv

Proses peristiwa readv VM memberikan visibilitas ke dalam operasi baca yang dilakukan oleh proses di wilayah memori virtual mereka sendiri. Tabel berikut mencakup nama bidang dan deskripsi peristiwa readv VM proses yang dikumpulkan oleh Runtime Monitoring untuk mendeteksi potensi ancaman.

Nama bidang	Deskripsi
Bendera	Merupakan opsi yang mengontrol perilaku acara ini.
Target PID	ID proses dari proses dari mana memori sedang dibaca.
Proses Target UUID	ID unik dari proses target.
Target Jalur yang Dapat Dieksekusi	Jalur absolut dari file eksekusi proses target.

Proses acara VM Writev

Proses peristiwa VM writev memberikan visibilitas ke dalam operasi tulis yang dilakukan oleh proses di wilayah memori virtual mereka sendiri. Tabel berikut mencakup nama bidang dan deskripsi proses VM writev peristiwa yang dikumpulkan Runtime Monitoring untuk mendeteksi potensi ancaman.

Nama bidang	Deskripsi
Bendera	Merupakan opsi yang mengontrol perilaku acara ini.
Target PID	ID proses dari proses dimana memori sedang ditulis.
Proses Target UUID	ID unik dari proses target.
Target Jalur yang Dapat Dieksekusi	Jalur absolut dari file eksekusi proses target.

Peristiwa proses jejak (Ptrace)

Process trace (Ptrace) system call adalah mekanisme debugging dan tracing yang memungkinkan satu proses (tracer) untuk mengamati dan mengontrol eksekusi proses lain (tracee). Ini memberi pelacak kemampuan untuk memeriksa dan memodifikasi memori, register, dan alur eksekusi proses target.

Peristiwa Ptrace memberikan visibilitas ke dalam penggunaan panggilan sistem ptrace oleh proses yang berjalan pada sumber daya yang dipantau. Tabel berikut mencakup nama bidang dan deskripsi peristiwa ptrace yang dikumpulkan Runtime Monitoring untuk mendeteksi potensi ancaman.

Nama bidang	Deskripsi
Target PID	ID proses dari proses target.
Proses Target UUID	ID unik dari proses target.
Target Jalur yang Dapat Dieksekusi	Jalur absolut dari file eksekusi proses target.
Bendera	Merupakan opsi yang mengontrol perilaku acara ini.

Mengikat acara

Peristiwa Bind memberikan visibilitas ke dalam pengikatan soket jaringan dengan proses yang berjalan pada sumber daya yang dipantau. Tabel berikut mencakup nama bidang dan deskripsi peristiwa bind yang dikumpulkan oleh Runtime Monitoring untuk mendeteksi potensi ancaman.

Nama bidang	Deskripsi
Alamat Keluarga	Merupakan protokol komunikasi yang terkait dengan alamat. Misalnya, keluarga alamat AF_INET digunakan untuk protokol IP v4.
Jenis soket	Jenis soket untuk menunjukkan semantik komunikasi. Misalnya, SOCK_RAW.
Nomor protokol	Nomor protokol layer 4 seperti 17 untuk UDP dan 6 untuk TCP.

Nama bidang	Deskripsi
IP titik akhir lokal	IP lokal dari koneksi.
Port titik akhir lokal	Nomor port koneksi.

Dengarkan acara

Peristiwa mendengarkan memberikan visibilitas ke dalam keadaan mendengarkan soket jaringan, yang menunjukkan apakah soket jaringan siap menerima koneksi masuk atau tidak. Proses yang berjalan pada sumber daya yang dipantau akan menyetel soket jaringan ke status mendengarkan. Tabel berikut mencakup nama bidang dan deskripsi peristiwa mendengarkan yang dikumpulkan Runtime Monitoring untuk mendeteksi potensi ancaman.

Nama bidang	Deskripsi
Alamat Keluarga	Merupakan protokol komunikasi yang terkait dengan alamat. Misalnya, keluarga alamat AF_INET digunakan untuk protokol IP v4.
Jenis soket	Jenis soket untuk menunjukkan semantik komunikasi. Misalnya, SOCK_RAW.
Nomor protokol	Nomor protokol layer 4 seperti 17 untuk UDP dan 6 untuk TCP.
IP titik akhir lokal	IP lokal dari koneksi.
Port titik akhir lokal	Nomor port koneksi.

Ganti nama acara

Ganti nama acara memberikan informasi tentang penggantian nama file dan direktori dengan proses yang berjalan pada sumber daya yang dipantau. Tabel berikut mencakup nama bidang dan deskripsi peristiwa ganti nama yang dikumpulkan Runtime Monitoring untuk mendeteksi potensi ancaman.

Nama bidang	Deskripsi
Filepath	Path tempat file yang diganti namanya.
Target	Jalur baru file.

Mengatur peristiwa ID pengguna (UID)

Peristiwa set ID pengguna (UID) memberikan visibilitas ke dalam perubahan yang dibuat pada ID pengguna (UID) yang terkait dengan proses yang sedang berjalan pada sumber daya yang dipantau. Tabel berikut mencakup nama bidang dan deskripsi peristiwa UID set yang dikumpulkan oleh Runtime Monitoring untuk mendeteksi potensi ancaman.

Nama bidang	Deskripsi
EUID baru	ID pengguna baru yang efektif dari proses tersebut.
UID baru	ID pengguna baru dari proses tersebut.

Acara Chmod

Peristiwa Chmod memberikan visibilitas ke dalam perubahan izin (mode) file dan direktori pada sumber daya yang dipantau. Tabel berikut mencakup nama bidang dan deskripsi peristiwa chmod yang dikumpulkan oleh Runtime Monitoring untuk mendeteksi potensi ancaman.

Nama bidang	Deskripsi
Filepath	Path dari file yang memanggil acara ini.
Filemode	Izin akses yang diperbarui untuk file terkait.

Agen hosting repositori Amazon ECR GuardDuty

Bagian berikut mencantumkan repositori Amazon Elastic Container Registry (Amazon ECR) Registry (Amazon ECR) GuardDuty tempat menghosting agen keamanan yang akan digunakan di kluster Amazon EKS dan Amazon ECS Anda.

Prasyarat untuk [Prasyarat untuk akses gambar kontainer](#) mengharuskan Anda memberikan peran eksekusi tugas yang memiliki izin Amazon Elastic Container Registry (Amazon ECR) tertentu. Untuk lebih membatasi izin ini, Anda dapat menambahkan URI repositori Amazon ECR yang menghosting GuardDuty agen untuk sumber daya Fargate-Amazon ECS.

Repositori ECR untuk agen EKS versi 1.10.0 - 1.8.1 (eks.build.2)

Saat Anda mengaktifkan konfigurasi GuardDuty otomatis untuk Runtime Monitoring untuk EKS, GuardDuty akan menerapkan versi agen ini ke kluster Amazon EKS Anda. Untuk informasi tentang mengaktifkan agen otomatis, lihat [Mengelola agen keamanan secara otomatis untuk sumber daya Amazon EKS](#).

Tabel berikut menunjukkan repositori Amazon ECR URIs tempat versi agen GuardDuty keamanan 1.10.0.eks.build.21.9.0.eks.build.2, dan untuk 1.8.0.eks.build.2 Amazon EKS di-host.

Wilayah AWS	URI repositori Amazon ECR
AS Barat (Oregon)	602401143452.dkr.ecr.us-west-2.amazonaws.com
	039403964562.dkr.ecr.us-west-2.amazonaws.com
Eropa (Paris)	602401143452.dkr.ecr.eu-west-3.amazonaws.com
	113643092156.dkr.ecr.eu-west-3.amazonaws.com
Asia Pasifik (Mumbai)	602401143452.dkr.ecr.ap-south-1.amazonaws.com
	610108029387.dkr.ecr.ap-south-1.amazonaws.com
Asia Pasifik (Hyderabad)	900889452093.dkr.ecr.ap-south-2.amazonaws.com

Wilayah AWS	URI repositori Amazon ECR
	618745550137.dkr.ecr.ap-sou th-2.amazonaws.com
Kanada (Pusat)	602401143452.dkr.ecr.ca-cen tral-1.amazonaws.com
	001188825231.dkr.ecr.ca-cen tral-1.amazonaws.com
Kanada Barat (Calgary)	761377655185.dkr.ecr.ca-wes t-1.amazonaws.com
	—
Timur Tengah (UEA)	759879836304.dkr.ecr.me-cen tral-1.amazonaws.com
	601769779514.dkr.ecr.me-cen tral-1.amazonaws.com
Eropa (London)	602401143452.dkr.ecr.eu-wes t-2.amazonaws.com
	109118265657.dkr.ecr.eu-wes t-2.amazonaws.com
AS Barat (California Utara)	602401143452.dkr.ecr.us-wes t-1.amazonaws.com
	373421517865.dkr.ecr.us-wes t-1.amazonaws.com
Timur AS (N. Virginia)	602401143452.dkr.ecr.us-eas t-1.amazonaws.com
	031903291036.dkr.ecr.us-eas t-1.amazonaws.com

Wilayah AWS	URI repositori Amazon ECR
AS Timur (Ohio)	602401143452.dkr.ecr.us-east-2.amazonaws.com
	591382732059.dkr.ecr.us-east-2.amazonaws.com
Eropa (Irlandia)	602401143452.dkr.ecr.eu-west-1.amazonaws.com
	673884943994.dkr.ecr.eu-west-1.amazonaws.com
Amerika Selatan (Sao Paulo)	602401143452.dkr.ecr.sa-east-1.amazonaws.com
	941219317354.dkr.ecr.sa-east-1.amazonaws.com
Eropa (Stockholm)	602401143452.dkr.ecr.eu-north-1.amazonaws.com
	366771026645.dkr.ecr.eu-north-1.amazonaws.com
Eropa (Frankfurt)	602401143452.dkr.ecr.eu-central-1.amazonaws.com
	409493279830.dkr.ecr.eu-central-1.amazonaws.com
Eropa (Zürich)	900612956339.dkr.ecr.eu-central-2.amazonaws.com
	718440343717.dkr.ecr.eu-central-2.amazonaws.com
Asia Pasifik (Singapura)	602401143452.dkr.ecr.ap-southeast-1.amazonaws.com

Wilayah AWS	URI repositori Amazon ECR
	584580519942.dkr.ecr.ap-southeast-1.amazonaws.com
Asia Pasifik (Sydney)	602401143452.dkr.ecr.ap-southeast-2.amazonaws.com 011662287384.dkr.ecr.ap-southeast-2.amazonaws.com
Asia Pasifik (Jakarta)	296578399912.dkr.ecr.ap-southeast-3.amazonaws.com 617474730032.dkr.ecr.ap-southeast-3.amazonaws.com
Asia Pasifik (Tokyo)	602401143452.dkr.ecr.ap-northeast-1.amazonaws.com 781592569369.dkr.ecr.ap-northeast-1.amazonaws.com
Asia Pasifik (Seoul)	602401143452.dkr.ecr.ap-northeast-2.amazonaws.com 732248494576.dkr.ecr.ap-northeast-2.amazonaws.com
Asia Pasifik (Osaka)	602401143452.dkr.ecr.ap-northeast-3.amazonaws.com 810724417379.dkr.ecr.ap-northeast-3.amazonaws.com
Asia Pasifik (Hong Kong)	800184023465.dkr.ecr.ap-east-1.amazonaws.com 790429075973.dkr.ecr.ap-east-1.amazonaws.com

Wilayah AWS	URI repositori Amazon ECR
Middle East (Bahrain) (Middle East (Bahrain))	558608220178.dkr.ecr.me-sou th-1.amazonaws.com
	541829937850.dkr.ecr.me-sou th-1.amazonaws.com
Eropa (Milan)	590381155156.dkr.ecr.eu-sou th-1.amazonaws.com
	528450769569.dkr.ecr.eu-sou th-1.amazonaws.com
Eropa (Spanyol)	455263428931.dkr.ecr.eu-sou th-2.amazonaws.com
	531047660167.dkr.ecr.eu-sou th-2.amazonaws.com
Afrika (Cape Town)	877085696533.dkr.ecr.af-sou th-1.amazonaws.com
	379032919888.dkr.ecr.af-sou th-1.amazonaws.com
Asia Pasifik (Melbourne)	491585149902.dkr.ecr.ap-sou theast-4.amazonaws.com
	750462861327.dkr.ecr.ap-sou theast-4.amazonaws.com
Israel (Tel Aviv)	066635153087.dkr.ecr.il-cen tral-1.amazonaws.com
	292660727137.dkr.ecr.il-cen tral-1.amazonaws.com
Asia Pasifik (Malaysia)	151610086707.dkr.ecr.ap-sou theast-5.amazonaws.com

Wilayah AWS	URI repositori Amazon ECR
Asia Pasifik (Thailand)	121268973566.dkr.ecr.ap-southeast-7.amazonaws.com
Meksiko (Tengah)	730335286997.dkr.ecr.mx-central-1.amazonaws.com

Repositori ECR untuk agen EKS versi 1.8.1 () **eks.build.1**

Bagian ini menyediakan repositori Amazon ECR untuk agen Amazon EKS versi 1.8.1 (v1.8.1-eks-build.1). Jika Anda menggunakan v1.8.1-eks-build.1, GuardDuty merekomendasikan untuk beralih ke versi agen default yang biasanya merupakan versi agen terbaru. Untuk melakukannya, identifikasi agen terbaru dari [Versi agen yang dirilis untuk sumber daya Amazon EKS](#), dan kemudian lakukan langkah-langkahnya [Memperbarui agen keamanan secara manual untuk sumber daya Amazon EKS](#).

Tabel berikut menunjukkan repositori Amazon ECR URIs tempat versi agen GuardDuty keamanan untuk 1.8.1-eks-build.1 Amazon EKS di-host.

Wilayah AWS	URI repositori Amazon ECR
AS Barat (Oregon)	039403964562.dkr.ecr.us-west-2.amazonaws.com
Eropa (Paris)	113643092156.dkr.ecr.eu-west-3.amazonaws.com
Asia Pasifik (Mumbai)	610108029387.dkr.ecr.ap-south-1.amazonaws.com
Asia Pasifik (Hyderabad)	618745550137.dkr.ecr.ap-south-2.amazonaws.com
Kanada (Pusat)	001188825231.dkr.ecr.ca-central-1.amazonaws.com
Timur Tengah (UEA)	601769779514.dkr.ecr.me-central-1.amazonaws.com

Wilayah AWS	URI repositori Amazon ECR
Eropa (London)	109118265657.dkr.ecr.eu-west-2.amazonaws.com
AS Barat (California Utara)	373421517865.dkr.ecr.us-west-1.amazonaws.com
Timur AS (N. Virginia)	031903291036.dkr.ecr.us-east-1.amazonaws.com
AS Timur (Ohio)	591382732059.dkr.ecr.us-east-2.amazonaws.com
Eropa (Irlandia)	673884943994.dkr.ecr.eu-west-1.amazonaws.com
Amerika Selatan (Sao Paulo)	941219317354.dkr.ecr.sa-east-1.amazonaws.com
Eropa (Stockholm)	366771026645.dkr.ecr.eu-north-1.amazonaws.com
Eropa (Frankfurt)	409493279830.dkr.ecr.eu-central-1.amazonaws.com
Eropa (Zürich)	718440343717.dkr.ecr.eu-central-2.amazonaws.com
Asia Pasifik (Singapura)	584580519942.dkr.ecr.ap-southeast-1.amazonaws.com
Asia Pasifik (Sydney)	011662287384.dkr.ecr.ap-southeast-2.amazonaws.com
Asia Pasifik (Jakarta)	617474730032.dkr.ecr.ap-southeast-3.amazonaws.com
Asia Pasifik (Tokyo)	781592569369.dkr.ecr.ap-northeast-1.amazonaws.com

Wilayah AWS	URI repositori Amazon ECR
Asia Pasifik (Seoul)	732248494576.dkr.ecr.ap-northeast-2.amazonaws.com
Asia Pasifik (Osaka)	810724417379.dkr.ecr.ap-northeast-3.amazonaws.com
Asia Pasifik (Hong Kong)	790429075973.dkr.ecr.ap-east-1.amazonaws.com
Middle East (Bahrain) (Middle East (Bahrain))	541829937850.dkr.ecr.me-south-1.amazonaws.com
Eropa (Milan)	528450769569.dkr.ecr.eu-south-1.amazonaws.com
Eropa (Spanyol)	531047660167.dkr.ecr.eu-south-2.amazonaws.com
Afrika (Cape Town)	379032919888.dkr.ecr.af-south-1.amazonaws.com
Asia Pasifik (Melbourne)	750462861327.dkr.ecr.ap-southeast-4.amazonaws.com
Israel (Tel Aviv)	292660727137.dkr.ecr.il-central-1.amazonaws.com

Repositori ECR untuk GuardDuty agen di (hanya AWS Fargate Amazon ECS)

Sebagai prasyarat untuk menggunakan Runtime Monitoring untuk Amazon ECS-Fargate, Anda harus. [Prasyarat untuk akses gambar kontainer](#) Gambar wadah sespan GuardDuty agen disimpan di Amazon ECR, dengan lapisan gambarnya disimpan di Amazon S3. Untuk informasi selengkapnya, lihat [Bagaimana Runtime Monitoring bekerja dengan Fargate \(hanya Amazon ECS\)](#).

Tabel berikut menunjukkan repositori Amazon ECR yang menampung GuardDuty agen untuk (hanya AWS Fargate Amazon ECS) untuk masing-masing. Wilayah AWS

Wilayah AWS	URI repositori Amazon ECR
AS Barat (Oregon)	733349766148.dkr.ecr.us-west-2.amazonaws.com/aws-guard-duty-agent-fargate
Eropa (Paris)	665651866788.dkr.ecr.eu-west-3.amazonaws.com/aws-guard-duty-agent-fargate
Asia Pasifik (Mumbai)	251508486986.dkr.ecr.ap-south-1.amazonaws.com/aws-guard-duty-agent-fargate
Asia Pasifik (Hyderabad)	950823858135.dkr.ecr.ap-south-2.amazonaws.com/aws-guard-duty-agent-fargate
Kanada (Pusat)	354763396469.dkr.ecr.ca-central-1.amazonaws.com/aws-guard-duty-agent-fargate
Timur Tengah (UEA)	000014521398.dkr.ecr.me-central-1.amazonaws.com/aws-guard-duty-agent-fargate
Eropa (London)	892757235363.dkr.ecr.eu-west-2.amazonaws.com/aws-guard-duty-agent-fargate
AS Barat (California Utara)	684579721401.dkr.ecr.us-west-1.amazonaws.com/aws-guard-duty-agent-fargate
Timur AS (N. Virginia)	593207742271.dkr.ecr.us-east-1.amazonaws.com/aws-guard-duty-agent-fargate

Wilayah AWS	URI repositori Amazon ECR
AS Timur (Ohio)	<code>307168627858.dkr.ecr.us-east-2.amazonaws.com/aws-guard-duty-agent-fargate</code>
Eropa (Irlandia)	<code>694911143906.dkr.ecr.eu-west-1.amazonaws.com/aws-guard-duty-agent-fargate</code>
Amerika Selatan (Sao Paulo)	<code>758426053663.dkr.ecr.sa-east-1.amazonaws.com/aws-guard-duty-agent-fargate</code>
Eropa (Stockholm)	<code>591436053604.dkr.ecr.eu-north-1.amazonaws.com/aws-guard-duty-agent-fargate</code>
Eropa (Frankfurt)	<code>323658145986.dkr.ecr.eu-central-1.amazonaws.com/aws-guard-duty-agent-fargate</code>
Eropa (Zürich)	<code>529164026651.dkr.ecr.eu-central-2.amazonaws.com/aws-guard-duty-agent-fargate</code>
Asia Pasifik (Singapura)	<code>174946120834.dkr.ecr.ap-southeast-1.amazonaws.com/aws-guard-duty-agent-fargate</code>
Asia Pasifik (Sydney)	<code>005257825471.dkr.ecr.ap-southeast-2.amazonaws.com/aws-guard-duty-agent-fargate</code>
Asia Pasifik (Jakarta)	<code>510637619217.dkr.ecr.ap-southeast-3.amazonaws.com/aws-guard-duty-agent-fargate</code>

Wilayah AWS	URI repositori Amazon ECR
Asia Pasifik (Tokyo)	533107202818.dkr.ecr.ap-northeast-1.amazonaws.com/aws-guardduty-agent-fargate
Asia Pasifik (Seoul)	914738172881.dkr.ecr.ap-northeast-2.amazonaws.com/aws-guardduty-agent-fargate
Asia Pasifik (Osaka)	273192626886.dkr.ecr.ap-northeast-3.amazonaws.com/aws-guardduty-agent-fargate
Asia Pasifik (Hong Kong)	258348409381.dkr.ecr.ap-east-1.amazonaws.com/aws-guardduty-agent-fargate
Middle East (Bahrain) (Middle East (Bahrain))	536382113932.dkr.ecr.me-south-1.amazonaws.com/aws-guardduty-agent-fargate
Eropa (Milan)	266869475730.dkr.ecr.eu-south-1.amazonaws.com/aws-guardduty-agent-fargate
Eropa (Spanyol)	919611009337.dkr.ecr.eu-south-2.amazonaws.com/aws-guardduty-agent-fargate
Afrika (Cape Town)	197869348890.dkr.ecr.af-south-1.amazonaws.com/aws-guardduty-agent-fargate
Asia Pasifik (Melbourne)	251357961535.dkr.ecr.ap-southeast-4.amazonaws.com/aws-guardduty-agent-fargate

Wilayah AWS	URI repositori Amazon ECR
Israel (Tel Aviv)	870907303882.dkr.ecr.il-central-1.amazonaws.com/aws-guardduty-agent-fargate
Asia Pasifik (Malaysia)	156041399949.dkr.ecr.ap-southeast-5.amazonaws.com/aws-guardduty-agent-fargate
Asia Pasifik (Thailand)	054037130133.dkr.ecr.ap-southeast-7.amazonaws.com/aws-guardduty-agent-fargate
Kanada Barat (Calgary)	339712888787.dkr.ecr.ca-west-1.amazonaws.com/aws-guardduty-agent-fargate
Meksiko (Tengah)	311141559934.dkr.ecr.mx-central-1.amazonaws.com/aws-guardduty-agent-fargate

Dua agen keamanan pada host dasar yang sama

EC2 Instans Amazon dapat mendukung berbagai jenis beban kerja. Saat Anda mengonfigurasi agen keamanan otomatis di EC2 instans Amazon, instance yang sama EC2 mungkin memiliki agen keamanan lain melalui EKS.

Gambaran Umum

Pertimbangkan skenario di mana Anda telah mengaktifkan Runtime Monitoring. Sekarang, Anda mengaktifkan agen otomatis untuk Amazon EKS melalui GuardDuty. Anda juga telah mengaktifkan agen otomatis untuk Amazon EC2. Mungkin saja host dasar yang sama diinstal dengan dua agen keamanan - satu untuk Amazon EKS dan yang lainnya untuk Amazon EC2. Hal ini dapat mengakibatkan dua agen keamanan berjalan di dalam host yang sama, mengumpulkan peristiwa runtime dan mengirimkannya ke GuardDuty, dan berpotensi menghasilkan temuan duplikat.

Dampak

- Ketika ada lebih dari satu agen keamanan yang berjalan pada host yang sama, akun Anda mungkin mengalami dua kali lipat jumlah kebutuhan pemrosesan CPU dan memori. Untuk informasi tentang CPU dan batas memori untuk setiap jenis sumber daya, lihat [Prasyarat](#) sumber daya tersebut.
- GuardDuty telah merancang fitur Runtime Monitoring sedemikian rupa sehingga meskipun ada tumpang tindih dua agen keamanan yang mengumpulkan peristiwa runtime dari host dasar yang sama, akun Anda hanya akan dikenakan biaya untuk satu aliran peristiwa runtime.

Bagaimana GuardDuty menangani banyak agen

GuardDuty mendeteksi ketika dua agen keamanan berjalan pada host yang sama dan menunjuk hanya satu dari mereka untuk menjadi agen keamanan yang secara aktif mengumpulkan peristiwa runtime. Agen kedua akan mengkonsumsi sumber daya sistem minimum untuk mencegah dampak apa pun terhadap kinerja aplikasi Anda.

GuardDuty mempertimbangkan skenario berikut:

- Ketika sebuah EC2 instance berada di bawah lingkup agen keamanan Amazon EKS dan Amazon, agen EC2 keamanan EKS diprioritaskan. Ini hanya akan berlaku ketika Anda menggunakan agen keamanan v1.1.0 atau lebih tinggi untuk Amazon EC2. Versi agen yang lebih lama akan terus berjalan dan mengumpulkan peristiwa runtime karena versi agen yang lebih lama tidak terpengaruh oleh prioritas.
- Ketika Amazon EKS dan Amazon EC2 telah GuardDuty mengelola agen keamanan dan EC2 instans Amazon Anda juga dikelola SSM, kedua agen keamanan akan dipasang di tingkat host. Setelah agen diinstal, GuardDuty memutuskan agen keamanan mana yang akan terus berjalan. Ketika kedua agen keamanan berjalan, akhirnya hanya satu dari mereka yang akan mengumpulkan acara runtime.
- Ketika agen keamanan yang terkait dengan keduanya EC2 dan EKS berjalan pada saat yang sama, GuardDuty mungkin menghasilkan temuan duplikat selama periode tumpang tindih saja.

Ini bisa terjadi ketika:

- Agen keamanan untuk keduanya EC2 dan EKS dikonfigurasi melalui GuardDuty (secara otomatis), atau
- Sumber daya Amazon EKS Anda memiliki agen keamanan otomatis.

- Ketika agen keamanan EKS sudah berjalan, jika Anda menyebarkan agen EC2 keamanan secara manual pada host dasar yang sama dan memenuhi semua prasyarat, GuardDuty mungkin tidak menginstal agen keamanan kedua.

Pemantauan Runtime EKS di GuardDuty

EKS Runtime Monitoring menyediakan cakupan deteksi ancaman runtime untuk node dan container Amazon Elastic Kubernetes Service (Amazon EKS) di lingkungan Anda. AWS EKS Runtime Monitoring menggunakan agen GuardDuty keamanan yang menambahkan visibilitas runtime ke beban kerja EKS individual, misalnya, akses file, eksekusi proses, dan koneksi jaringan. Agen GuardDuty keamanan membantu GuardDuty mengidentifikasi kontainer tertentu dalam kluster EKS Anda yang berpotensi dikompromikan. Ini juga dapat mendeteksi upaya untuk meningkatkan hak istimewa dari wadah individu ke EC2 host yang mendasarinya, dan lingkungan yang lebih luas AWS .

Dengan ketersediaan Runtime Monitoring, GuardDuty telah mengkonsolidasikan pengalaman konsol untuk EKS Runtime Monitoring menjadi Runtime Monitoring. GuardDuty tidak akan memigrasikan pengaturan Pemantauan Runtime EKS Anda atas nama Anda secara otomatis. Ini membutuhkan tindakan di akhir Anda. Jika Anda ingin terus menggunakan hanya EKS Runtime Monitoring, Anda dapat menggunakan APIs atau AWS CLI untuk memeriksa dan memperbarui status konfigurasi yang ada untuk EKS Runtime Monitoring. Namun, GuardDuty merekomendasikan [Migrasi dari EKS Runtime Monitoring ke Runtime Monitoring](#) dan gunakan Runtime Monitoring untuk memantau kluster Amazon EKS Anda.

Topik

- [Mengkonfigurasi EKS Runtime Monitoring untuk lingkungan multi-akun \(API\)](#)
- [Mengkonfigurasi EKS Runtime Monitoring untuk akun mandiri \(API\)](#)
- [Migrasi dari EKS Runtime Monitoring ke Runtime Monitoring](#)

Mengkonfigurasi EKS Runtime Monitoring untuk lingkungan multi-akun (API)

Dalam lingkungan beberapa akun, hanya akun GuardDuty administrator yang didelegasikan yang dapat mengaktifkan atau menonaktifkan EKS Runtime Monitoring untuk akun anggota, dan mengelola manajemen GuardDuty agen untuk kluster EKS milik akun anggota di organisasi mereka. Akun GuardDuty anggota tidak dapat mengubah konfigurasi ini dari akun mereka. Akun akun GuardDuty administrator yang didelegasikan mengelola akun anggota mereka menggunakan

AWS Organizations. Untuk informasi selengkapnya tentang lingkungan multi-akun, lihat [Mengelola beberapa akun](#).

Mengkonfigurasi EKS Runtime Monitoring untuk akun administrator yang didelegasikan GuardDuty

Bagian ini menyediakan langkah-langkah untuk mengonfigurasi EKS Runtime Monitoring dan mengelola agen GuardDuty keamanan untuk kluster EKS yang termasuk dalam akun administrator yang didelegasikan GuardDuty .

Berdasarkan [Pendekatan untuk mengelola agen GuardDuty keamanan di kluster Amazon EKS](#), Anda dapat memilih pendekatan yang disukai dan mengikuti langkah-langkah seperti yang disebutkan dalam tabel berikut.

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-Langkah
Kelola agen keamanan melalui GuardDuty (Pantau semua kluster EKS)	Jalankan updateDetector API dengan menggunakan ID detektor regional Anda sendiri dan meneruskan nama <code>features</code> objek sebagai <code>EKS_RUNTIME_MONITORING</code> dan status sebagai <code>ENABLED</code>. Tetapkan status untuk <code>EKS_ADDON_MANAGEMENT</code> as <code>ENABLED</code>. GuardDuty akan mengelola penyebaran dan pembaruan ke agen keamanan untuk semua kluster Amazon EKS di akun Anda. Atau, Anda dapat menggunakan AWS CLI perintah dengan menggunakan ID detektor regional Anda sendiri. Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectors API. <code>detectorId</code> Contoh berikut memungkinkan keduanya <code>EKS_RUNTIME_MONITORING</code> dan <code>EKS_ADDON_MANAGEMENT</code> :

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-Langkah
	<pre>aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : "ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : "ENABLED"}] }]'</pre>

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-Langkah
Pantau semua cluster EKS tetapi kecualikan beberapa di antaranya (menggunakan tag pengecualian)	1. Tambahkan tag ke cluster EKS yang ingin Anda kecualikan agar tidak dipantau. Pasangkan kunci-nilai adalah GuardDutyManaged - false Untuk informasi selengkapnya tentang menambahkan tag, lihat Bekerja dengan tag menggunakan CLI, API, atau eksctl di Panduan Pengguna Amazon EKS. 2. Untuk mencegah modifikasi tag, kecuali oleh entitas tepercaya, gunakan kebijakan yang disediakan dalam Mencegah tag agar tidak dimodifikasi kecuali oleh prinsipal resmi dalam Panduan Pengguna AWS Organizations Dalam kebijakan ini, ganti detail berikut: • Ganti <i>ec2:CreateTags</i> dengan <i>eks:TagResource</i> . • Ganti <i>ec2:DeleteTags</i> dengan <i>eks:UntagResource</i> . • Ganti <i>access-project</i> dengan GuardDuty Managed • Ganti <i>123456789012</i> dengan Akun AWS ID entitas tepercaya. Jika Anda memiliki lebih dari satu entitas tepercaya , gunakan contoh berikut untuk menambahkan beberapaPrincipalArn : <pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre>

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-Langkah
	3.  Note Selalu tambahkan tag pengecualian ke kluster EKS Anda sebelum menyetel EKS_RUNTIME_MONITORING ke ENABLED; jika tidak, agen GuardDuty keamanan akan digunakan di semua kluster EKS di akun Anda. STATUS Jalankan updateDetector API dengan menggunakan ID detektor regional Anda sendiri dan meneruskan nama features objek sebagai EKS_RUNTIME_MONITORING dan status sebagai ENABLED. Tetapkan status untuk EKS_ADDON_MANAGEMENT as ENABLED. GuardDuty akan mengelola penyebaran dan pembaruan ke agen keamanan untuk semua kluster Amazon EKS yang belum dikecualikan dari pemantauan. Atau, Anda dapat menggunakan AWS CLI perintah dengan menggunakan ID detektor regional Anda sendiri. Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/ konsol, atau jalankan ListDetectors API. <code>detectorId</code> Contoh berikut memungkinkan keduanya EKS_RUNTIME_MONITORING dan EKS_ADDON_MANAGEMENT : <pre>aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --</pre>

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-Langkah
	<pre>features '[{"Name" : "EKS_RUNTIME_MONIT ORING", "Status" : " ENABLED", "Addition alConfiguration" : [{"Name" : "EKS_ADDO N_MANAGEMENT", "Status" : " ENABLED"}]]]'</pre>

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-Langkah
Pantau kluster EKS selektif (menggunakan tag inklusi)	1. Tambahkan tag ke cluster EKS yang ingin Anda kecualikan agar tidak dipantau. Pasangkan kunci-nilai adalah <code>GuardDutyManaged</code> - <code>true</code> Untuk informasi selengkapnya tentang menambahkan tag, lihat Bekerja dengan tag menggunakan CLI, API, atau eksctl di Panduan Pengguna Amazon EKS. 2. Untuk mencegah modifikasi tag, kecuali oleh entitas tepercaya, gunakan kebijakan yang disediakan dalam Mencegah tag agar tidak dimodifikasi kecuali oleh prinsipal resmi dalam Panduan Pengguna AWS Organizations. Dalam kebijakan ini, ganti detail berikut: • Ganti <code>ec2:CreateTags</code> dengan <code>eks:TagResource</code>. • Ganti <code>ec2:DeleteTags</code> dengan <code>eks:UntagResource</code>. • Ganti <code>access-project</code> dengan <code>GuardDutyManaged</code> • Ganti <code>123456789012</code> dengan Akun AWS ID entitas tepercaya. Jika Anda memiliki lebih dari satu entitas tepercaya, gunakan contoh berikut untuk menambahkan beberapa <code>PrincipalArn</code>: <pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre> 3. Jalankan updateDetector API dengan menggunakan ID detektor regional Anda sendiri dan meneruskan nama

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-Langkah
	features objek sebagai EKS_RUNTIME_MONITORING dan status sebagai ENABLED. Tetapkan status untuk EKS_ADDON_MANAGEMENT as DISABLED. GuardDuty akan mengelola penyebaran dan pembaruan ke agen keamanan untuk semua kluster Amazon EKS yang telah ditandai dengan - pair. GuardDutyManaged true Atau, Anda dapat menggunakan AWS CLI perintah dengan menggunakan ID detektor regional Anda sendiri. Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectorsAPI. detectorId Contoh berikut memungkinkan EKS_RUNTIME_MONITORING dan menonaktifkan EKS_ADDON_MANAGEMENT : <pre data-bbox="716 1276 1508 1549">aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : "ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : "DISABLED"}]]'</pre>

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-Langkah
Mengelola agen keamanan secara manual	Jalankan updateDetector API dengan menggunakan ID detektor regional Anda sendiri dan meneruskan nama features objek sebagai EKS_RUNTIME_MONITORING dan status sebagai ENABLED. Tetapkan status untuk EKS_ADDON_MANAGEMENT as DISABLED. Atau, Anda dapat menggunakan AWS CLI perintah dengan menggunakan ID detektor regional Anda sendiri. Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectors API. <code>detectorId</code> Contoh berikut memungkinkan EKS_RUNTIME_MONITORING dan menonaktifkan EKS_ADDON_MANAGEMENT : <pre>aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : "ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : "ENABLED"}] }]'</pre> Untuk mengelola agen keamanan, lihat Mengelola agen keamanan secara manual untuk kluster Amazon EKS.

Aktifkan otomatis EKS Runtime Monitoring untuk semua akun anggota

Bagian ini mencakup langkah-langkah untuk mengaktifkan EKS Runtime Monitoring dan mengelola agen keamanan untuk semua akun anggota. Ini termasuk akun GuardDuty administrator yang didelegasikan, akun anggota yang ada, dan akun baru yang bergabung dengan organisasi.

Berdasarkan [Pendekatan untuk mengelola agen GuardDuty keamanan di kluster Amazon EKS](#), Anda dapat memilih pendekatan yang disukai dan mengikuti langkah-langkah seperti yang disebutkan dalam tabel berikut.

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-Langkah
Kelola agen keamanan melalui GuardDuty (Pantau semua kluster EKS)	Untuk mengaktifkan EKS Runtime Monitoring secara selektif untuk akun anggota Anda, jalankan operasi updateMemberDetectors API menggunakan milik Anda sendiri. <i>detector ID</i> Tetapkan status untuk EKS_ADDON_MANAGEMENT asENABLED. GuardDuty akan mengelola penyebaran dan pembaruan ke agen keamanan untuk semua kluster Amazon EKS di akun Anda. Atau, Anda dapat menggunakan AWS CLI perintah dengan menggunakan ID detektor regional Anda sendiri. Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectors API. <i>detectorId</i> Contoh berikut memungkinkan keduanya EKS_RUNTIME_MONITORING dan EKS_ADDON_MANAGEMENT : <pre>aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : "ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : "ENABLED"}]]'</pre>  Note Anda juga dapat melewati daftar akun yang IDs dipisahkan oleh spasi.

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan

Langkah-Langkah

Ketika kode telah berhasil dijalankan, daftar `UnprocessedAccounts` akan kembali kosong. Jika ada masalah dalam mengubah pengaturan detektor untuk suatu akun, ID akun tersebut akan dicantumkan bersama dengan ringkasan masalahnya.

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-Langkah
Pantau semua cluster EKS tetapi kecualikan beberapa di antaranya (menggunakan tag pengecualian)	1. Tambahkan tag ke cluster EKS yang ingin Anda kecualikan agar tidak dipantau. Pasangan kunci-nilai adalah GuardDuty Managed -. false Untuk informasi selengkapnya tentang menambahkan tag, lihat Bekerja dengan tag menggunakan CLI, API, atau eksctl di Panduan Pengguna Amazon EKS. 2. Untuk mencegah modifikasi tag, kecuali oleh entitas tepercaya, gunakan kebijakan yang disediakan dalam Mencegah tag agar tidak dimodifikasi kecuali oleh prinsipal resmi dalam Panduan Pengguna AWS Organizations. Dalam kebijakan ini, ganti detail berikut: • Ganti <code>ec2:CreateTags</code> dengan <code>eks:TagResource</code> . • Ganti <code>ec2:DeleteTags</code> dengan <code>eks:UntagResource</code> . • Ganti <code>access-project</code> dengan <code>GuardDutyManaged</code> • Ganti <code>123456789012</code> dengan Akun AWS ID entitas tepercaya. Jika Anda memiliki lebih dari satu entitas tepercaya, gunakan contoh berikut untuk menambahkan beberapa <code>PrincipalArn</code> : <pre data-bbox="639 1333 1404 1482">"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre> 3.  Note Selalu tambahkan tag pengecualian ke kluster EKS Anda sebelum menyetel <code>EKS_RUNTIME_MONITORING</code> ke <code>ENABLED</code>; jika tidak, agen GuardDuty keamanan akan digunakan di semua kluster EKS di akun Anda. <code>STATUS</code>

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-Langkah
	Jalankan updateDetector API dengan menggunakan ID detektor regional Anda sendiri dan meneruskan nama features objek sebagai EKS_RUNTIME_MONITORING dan status sebagai ENABLED. Tetapkan status untuk EKS_ADDON_MANAGEMENT as ENABLED. GuardDuty akan mengelola penyebaran dan pembaruan ke agen keamanan untuk semua kluster Amazon EKS yang belum dikecualikan dari pemantauan. Atau, Anda dapat menggunakan AWS CLI perintah dengan menggunakan ID detektor regional Anda sendiri. Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectors API. detectorId Contoh berikut memungkinkan keduanya EKS_RUNTIME_MONITORING dan EKS_ADDON_MANAGEMENT : <pre>aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name": "EKS_RUNTIME_MONITORING", "Status": "ENABLED", "AdditionalConfiguration": [{"Name": "EKS_ADDON_MANAGEMENT", "Status": "ENABLED"}]]'</pre>  Note Anda juga dapat melewati daftar akun yang IDs dipisahkan oleh spasi.

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-Langkah
	Ketika kode telah berhasil dijalankan, daftar <code>UnprocessedAccounts</code> akan kembali kosong. Jika ada masalah dalam mengubah pengaturan detektor untuk suatu akun, ID akun tersebut akan dicantumkan bersama dengan ringkasan masalahnya.

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-Langkah
Pantau kluster EKS selektif (menggunakan tag inklusi)	1. Tambahkan tag ke cluster EKS yang ingin Anda kecualikan agar tidak dipantau. Pasangan kunci-nilai adalah GuardDuty Managed -. true Untuk informasi selengkapnya tentang menambahkan tag, lihat Bekerja dengan tag menggunakan CLI, API, atau eksctl di Panduan Pengguna Amazon EKS. 2. Untuk mencegah modifikasi tag, kecuali oleh entitas tepercaya, gunakan kebijakan yang disediakan dalam Mencegah tag agar tidak dimodifikasi kecuali oleh prinsipal resmi dalam Panduan Pengguna AWS Organizations. Dalam kebijakan ini, ganti detail berikut: • Ganti <code>ec2:CreateTags</code> dengan <code>eks:TagResource</code> . • Ganti <code>ec2:DeleteTags</code> dengan <code>eks:UntagResource</code> . • Ganti <code>access-project</code> dengan <code>GuardDutyManaged</code> • Ganti <code>123456789012</code> dengan Akun AWS ID entitas tepercaya. Jika Anda memiliki lebih dari satu entitas tepercaya, gunakan contoh berikut untuk menambahkan beberapa <code>PrincipalArn</code> : <pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre> 3. Jalankan updateDetector API dengan menggunakan ID detektor regional Anda sendiri dan meneruskan nama <code>features</code> objek sebagai <code>EKS_RUNTIME_MONITORING</code> dan status sebagai <code>ENABLED</code>. Tetapkan status untuk <code>EKS_ADDON_MANAGEMENT</code> as <code>DISABLED</code>.

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan

Langkah-Langkah

GuardDuty akan mengelola penyebaran dan pembaruan ke agen keamanan untuk semua kluster Amazon EKS yang telah ditandai dengan `- pair. GuardDutyManaged true`

Atau, Anda dapat menggunakan AWS CLI perintah dengan menggunakan ID detektor regional Anda sendiri. Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan `ListDetectors` API. `detectorId`

Contoh berikut memungkinkan `EKS_RUNTIME_MONITORING` dan menonaktifkan `EKS_ADDON_MANAGEMENT` :

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name": "EKS_RUNTIME_MONITORING", "Status": "ENABLED", "AdditionalConfiguration": [{"Name": "EKS_ADDON_MANAGEMENT", "Status": "DISABLED"}] ]'
```

Note

Anda juga dapat melewati daftar akun yang IDs dipisahkan oleh spasi.

Ketika kode telah berhasil dijalankan, daftar `UnprocessedAccounts` akan kembali kosong. Jika ada masalah dalam mengubah pengaturan detektor untuk suatu akun, ID akun tersebut akan dicantumkan bersama dengan ringkasan masalahnya.

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-Langkah
Mengelola agen keamanan secara manual	1. Jalankan updateDetector API dengan menggunakan ID detektor regional Anda sendiri dan meneruskan nama features objek sebagai EKS_RUNTIME_MONITORING dan status sebagai ENABLED. Tetapkan status untuk EKS_ADDON_MANAGEMENT as DISABLED. Atau, Anda dapat menggunakan AWS CLI perintah dengan menggunakan ID detektor regional Anda sendiri. Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectors API. <code>detectorId</code> Contoh berikut memungkinkan EKS_RUNTIME_MONITORING dan menonaktifkan EKS_ADDON_MANAGEMENT : <pre>aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 555555555555 --features '[{"Name": "EKS_RUNTIME_MONITORING", "Status": "ENABLED", "AdditionalConfiguration": [{"Name": "EKS_ADDON_MANAGEMENT", "Status": "ENABLED"}] }]'</pre> 2. Untuk mengelola agen keamanan, lihat Mengelola agen keamanan secara manual untuk kluster Amazon EKS.

Mengkonfigurasi EKS Runtime Monitoring untuk semua akun anggota aktif yang ada

Bagian ini mencakup langkah-langkah untuk mengaktifkan EKS Runtime Monitoring dan mengelola agen GuardDuty keamanan untuk akun anggota aktif yang ada di organisasi Anda.

Berdasarkan [Pendekatan untuk mengelola agen GuardDuty keamanan di kluster Amazon EKS](#), Anda dapat memilih pendekatan yang disukai dan mengikuti langkah-langkah seperti yang disebutkan dalam tabel berikut.

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-Langkah
Kelola agen keamanan melalui GuardDuty (Pantau semua kluster EKS)	Untuk mengaktifkan EKS Runtime Monitoring secara selektif untuk akun anggota Anda, jalankan operasi updateMemberDetectors API menggunakan milik Anda sendiri. <i>detector ID</i> Tetapkan status untuk EKS_ADDON_MANAGEMENT asENABLED. GuardDuty akan mengelola penyebaran dan pembaruan ke agen keamanan untuk semua kluster Amazon EKS di akun Anda. Atau, Anda dapat menggunakan AWS CLI perintah dengan menggunakan ID detektor regional Anda sendiri. Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectors API. <i>detectorId</i> Contoh berikut memungkinkan keduanya EKS_RUNTIME_MONITORING dan EKS_ADDON_MANAGEMENT : <pre>aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name": "EKS_RUNTIME_MONITORING", "Status": "ENABLED", "AdditionalConfiguration": [{"Name": "EKS_ADDON_MANAGEMENT", "Status": "ENABLED"}]]'</pre>  Note Anda juga dapat melewati daftar akun yang IDs dipisahkan oleh spasi. Ketika kode telah berhasil dijalankan, daftar UnprocessedAccounts akan kembali kosong. Jika ada masalah dalam

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan

Langkah-Langkah

mengubah pengaturan detektor untuk suatu akun, ID akun tersebut akan dicantumkan bersama dengan ringkasan masalahnya.

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-Langkah
Pantau semua cluster EKS tetapi kecualikan beberapa di antaranya (menggunakan tag pengecualian)	1. Tambahkan tag ke cluster EKS yang ingin Anda kecualikan agar tidak dipantau. Pasangan kunci-nilai adalah GuardDuty Managed -. false Untuk informasi selengkapnya tentang menambahkan tag, lihat Bekerja dengan tag menggunakan CLI, API, atau eksctl di Panduan Pengguna Amazon EKS. 2. Untuk mencegah modifikasi tag, kecuali oleh entitas tepercaya, gunakan kebijakan yang disediakan dalam Mencegah tag agar tidak dimodifikasi kecuali oleh prinsipal resmi dalam Panduan Pengguna AWS Organizations. Dalam kebijakan ini, ganti detail berikut: • Ganti <code>ec2:CreateTags</code> dengan <code>eks:TagResource</code> . • Ganti <code>ec2:DeleteTags</code> dengan <code>eks:UntagResource</code> . • Ganti <code>access-project</code> dengan <code>GuardDutyManaged</code> • Ganti <code>123456789012</code> dengan Akun AWS ID entitas tepercaya. Jika Anda memiliki lebih dari satu entitas tepercaya, gunakan contoh berikut untuk menambahkan beberapa <code>PrincipalArn</code> : <pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre> 3.  Note Selalu tambahkan tag pengecualian ke kluster EKS Anda sebelum menyetel <code>EKS_RUNTIME_MONITORING</code> ke <code>ENABLED</code>; jika tidak, agen GuardDuty keamanan akan digunakan di semua kluster EKS di akun Anda. <code>STATUS</code>

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-Langkah
	Untuk mengaktifkan EKS Runtime Monitoring secara selektif untuk akun anggota Anda, jalankan operasi updateMemberDetectors API menggunakan milik Anda sendiri. <i>detector ID</i> Tetapkan status untuk EKS_ADDON_MANAGEMENT asENABLED. GuardDuty akan mengelola penyebaran dan pembaruan ke agen keamanan untuk semua kluster Amazon EKS yang belum dikecualikan dari pemantauan. Atau, Anda dapat menggunakan AWS CLI perintah dengan menggunakan ID detektor regional Anda sendiri. Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectors API. <i>detectorId</i> Contoh berikut memungkinkan keduanya EKS_RUNTIME_MONITORING dan EKS_ADDON_MANAGEMENT : <pre>aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name": "EKS_RUNTIME_MONITORING", "Status": "ENABLED", "AdditionalConfiguration": [{"Name": "EKS_ADDON_MANAGEMENT", "Status": "ENABLED"}]]'</pre>  Note Anda juga dapat melewati daftar akun yang IDs dipisahkan oleh spasi.

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-Langkah
	Ketika kode telah berhasil dijalankan, daftar <code>UnprocessedAccounts</code> akan kembali kosong. Jika ada masalah dalam mengubah pengaturan detektor untuk suatu akun, ID akun tersebut akan dicantumkan bersama dengan ringkasan masalahnya.

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-Langkah
Pantau kluster EKS selektif (menggunakan tag inklusi)	1. Tambahkan tag ke cluster EKS yang ingin Anda kecualikan agar tidak dipantau. Pasangan kunci-nilai adalah GuardDuty Managed -. true Untuk informasi selengkapnya tentang menambahkan tag, lihat Bekerja dengan tag menggunakan CLI, API, atau eksctl di Panduan Pengguna Amazon EKS. 2. Untuk mencegah modifikasi tag, kecuali oleh entitas terpercaya, gunakan kebijakan yang disediakan dalam Mencegah tag agar tidak dimodifikasi kecuali oleh prinsipal resmi dalam Panduan Pengguna AWS Organizations. Dalam kebijakan ini, ganti detail berikut: • Ganti <i>ec2:CreateTags</i> dengan <code>eks:TagResource</code> . • Ganti <i>ec2>DeleteTags</i> dengan <code>eks:UntagResource</code> . • Ganti <i>access-project</i> dengan <code>GuardDutyManaged</code> • Ganti <i>123456789012</i> dengan Akun AWS ID entitas terpercaya. Jika Anda memiliki lebih dari satu entitas terpercaya, gunakan contoh berikut untuk menambahkan beberapa <code>PrincipalArn</code> : <pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre> 3. Untuk mengaktifkan EKS Runtime Monitoring secara selektif untuk akun anggota Anda, jalankan operasi updateMemberDetectors API menggunakan milik Anda sendiri. <i>detector ID</i> Tetapkan status untuk <code>EKS_ADDON_MANAGEMENT</code> as <code>DISABLED</code>.

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan

Langkah-Langkah

GuardDuty akan mengelola penyebaran dan pembaruan ke agen keamanan untuk semua kluster Amazon EKS yang telah ditandai dengan `- pair. GuardDutyManaged true`

Atau, Anda dapat menggunakan AWS CLI perintah dengan menggunakan ID detektor regional Anda sendiri. Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan `ListDetectors` API. `detectorId`

Contoh berikut memungkinkan `EKS_RUNTIME_MONITORING` dan menonaktifkan `EKS_ADDON_MANAGEMENT` :

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name": "EKS_RUNTIME_MONITORING", "Status": "ENABLED", "AdditionalConfiguration": [{"Name": "EKS_ADDON_MANAGEMENT", "Status": "DISABLED"}] ]'
```

Note

Anda juga dapat melewati daftar akun yang IDs dipisahkan oleh spasi.

Ketika kode telah berhasil dijalankan, daftar `UnprocessedAccounts` akan kembali kosong. Jika ada masalah dalam mengubah pengaturan detektor untuk suatu akun, ID akun tersebut akan dicantumkan bersama dengan ringkasan masalahnya.

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-Langkah
Mengelola agen keamanan secara manual	Untuk mengaktifkan EKS Runtime Monitoring secara selektif untuk akun anggota Anda, jalankan operasi updateMemberDetectors API menggunakan milik Anda sendiri. <i>detector ID</i> Tetapkan status untuk EKS_ADDON_MANAGEMENT asDISABLED. Atau, Anda dapat menggunakan AWS CLI perintah dengan menggunakan ID detektor regional Anda sendiri. Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectors API. <i>detectorId</i> Contoh berikut memungkinkan EKS_RUNTIME_MONITORING dan menonaktifkan EKS_ADDON_MANAGEMENT : <pre>aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 5555555555 --features '[{"Name": "EKS_RUNTIME_MONITORING", "Status": "ENABLED", "AdditionalConfiguration": [{"Name": "EKS_ADDON_MANAGEMENT", "Status": "ENABLED"}] }]'</pre> Untuk mengelola agen keamanan, lihat Mengelola agen keamanan secara manual untuk kluster Amazon EKS.

Aktifkan otomatis EKS Runtime Monitoring untuk anggota baru

Akun GuardDuty administrator yang didelegasikan dapat mengaktifkan EKS Runtime Monitoring secara otomatis dan memilih pendekatan untuk cara mengelola agen GuardDuty keamanan untuk akun baru yang bergabung dengan organisasi Anda.

Berdasarkan [Pendekatan untuk mengelola agen GuardDuty keamanan di kluster Amazon EKS](#), Anda dapat memilih pendekatan yang disukai dan mengikuti langkah-langkah seperti yang disebutkan dalam tabel berikut.

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-Langkah
Kelola agen keamanan melalui GuardDuty (Pantau semua kluster EKS)	Untuk mengaktifkan EKS Runtime Monitoring secara selektif untuk akun baru Anda, jalankan operasi UpdateOrganizationConfiguration API menggunakan akun Anda sendiri. <i>detector ID</i> Tetapkan status untuk EKS_ADDON_MANAGEMENT asENABLED. GuardDuty akan mengelola penyebaran dan pembaruan ke agen keamanan untuk semua kluster Amazon EKS di akun Anda. Atau, Anda dapat menggunakan AWS CLI perintah dengan menggunakan ID detektor regional Anda sendiri. Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectors API. <code>detectorId</code> Contoh berikut memungkinkan keduanya EKS_RUNTIME_MONITORING dan EKS_ADDON_MANAGEMENT untuk satu akun. Anda juga dapat melewati daftar akun yang IDs dipisahkan oleh spasi. Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectors API. <code>detectorId</code> <pre>aws guardduty update-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0</pre>

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-Langkah
	<pre data-bbox="656 300 1502 478">--autoEnable --features '[{"Name" : "EKS_RUNTIME_MONITORING", "AutoEnable": "NEW", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "AutoEnable": "NEW"}]]'</pre> Ketika kode telah berhasil dijalankan, daftar <code>UnprocessedAccounts</code> akan kembali kosong. Jika ada masalah dalam mengubah pengaturan detektor untuk suatu akun, ID akun tersebut akan dicantumkan bersama dengan ringkasan masalahnya.

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-Langkah
Pantau semua cluster EKS tetapi kecualikan beberapa di antaranya (menggunakan tag pengecualian)	1. Tambahkan tag ke cluster EKS yang ingin Anda kecualikan agar tidak dipantau. Pasangkan kunci-nilai adalah <code>GuardDutyManaged</code> - <code>false</code> Untuk informasi selengkapnya tentang menambahkan tag, lihat Bekerja dengan tag menggunakan CLI, API, atau eksctl di Panduan Pengguna Amazon EKS. 2. Untuk mencegah modifikasi tag, kecuali oleh entitas tepercaya, gunakan kebijakan yang disediakan dalam Mencegah tag agar tidak dimodifikasi kecuali oleh prinsipal resmi dalam Panduan Pengguna AWS Organizations. Dalam kebijakan ini, ganti detail berikut: • Ganti <code>ec2:CreateTags</code> dengan <code>eks:TagResource</code>. • Ganti <code>ec2:DeleteTags</code> dengan <code>eks:UntagResource</code>. • Ganti <code>access-project</code> dengan <code>GuardDutyManaged</code> • Ganti <code>123456789012</code> dengan Akun AWS ID entitas tepercaya. Jika Anda memiliki lebih dari satu entitas tepercaya, gunakan contoh berikut untuk menambahkan beberapaPrincipalArn : <pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre>

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-Langkah
	3.  Note Selalu tambahkan tag pengecualian ke kluster EKS Anda sebelum menyetel EKS_RUNTIME_MONITORING ke ENABLED; jika tidak, agen GuardDuty keamanan akan digunakan di semua kluster EKS di akun Anda. STATUS Untuk mengaktifkan EKS Runtime Monitoring secara selektif untuk akun baru Anda, jalankan operasi UpdateOrganizationConfiguration API menggunakan akun Anda sendiri. <i>detector ID</i> Tetapkan status untuk EKS_ADDON_MANAGEMENT as ENABLED. GuardDuty akan mengelola penyebaran dan pembaruan ke agen keamanan untuk semua kluster Amazon EKS yang belum dikecualikan dari pemantauan. Atau, Anda dapat menggunakan AWS CLI perintah dengan menggunakan ID detektor regional Anda sendiri. Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/ konsol, atau jalankan ListDetectors API. <code>detectorId</code> Contoh berikut memungkinkan keduanya EKS_RUNTIME_MONITORING dan EKS_ADDON_MANAGEMENT untuk satu akun. Anda juga dapat melewati daftar akun yang IDs dipisahkan oleh spasi.

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-Langkah
	Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/ konsol, atau jalankan ListDetectors API. <code>detectorId</code> <pre>aws guardduty update-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0 --autoEnable --features '[{"Name" : "EKS_RUNTIME_MONITORING", "AutoEnable": "NEW", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "AutoEnable": "NEW"}] }]'</pre> Ketika kode telah berhasil dijalankan, daftar <code>UnprocessedAccounts</code> akan kembali kosong. Jika ada masalah dalam mengubah pengaturan detektor untuk suatu akun, ID akun tersebut akan dicantumkan bersama dengan ringkasan masalahnya.

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-Langkah
Pantau kluster EKS selektif (menggunakan tag inklusi)	1. Tambahkan tag ke cluster EKS yang ingin Anda kecualikan agar tidak dipantau. Pasangkan kunci-nilai adalah <code>GuardDutyManaged</code> - <code>true</code> Untuk informasi selengkapnya tentang menambahkan tag, lihat Bekerja dengan tag menggunakan CLI, API, atau eksctl di Panduan Pengguna Amazon EKS. 2. Untuk mencegah modifikasi tag, kecuali oleh entitas tepercaya, gunakan kebijakan yang disediakan dalam Mencegah tag agar tidak dimodifikasi kecuali oleh prinsipal resmi dalam Panduan Pengguna AWS Organizations. Dalam kebijakan ini, ganti detail berikut: • Ganti <code>ec2:CreateTags</code> dengan <code>eks:TagResource</code>. • Ganti <code>ec2:DeleteTags</code> dengan <code>eks:UntagResource</code>. • Ganti <code>access-project</code> dengan <code>GuardDutyManaged</code> • Ganti <code>123456789012</code> dengan Akun AWS ID entitas tepercaya. Jika Anda memiliki lebih dari satu entitas tepercaya, gunakan contoh berikut untuk menambahkan beberapa <code>PrincipalArn</code>: <pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre> 3. Untuk mengaktifkan EKS Runtime Monitoring secara selektif untuk akun baru Anda, jalankan operasi

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan

Langkah-Langkah

[UpdateOrganizationConfiguration](#) API menggunakan akun Anda sendiri. *detector ID*

Tetapkan status untuk EKS_ADDON_MANAGEMENT asDISABLED.

GuardDuty akan mengelola penyebaran dan pembaruan ke agen keamanan untuk semua kluster Amazon EKS yang telah ditandai dengan - pair. GuardDutyManaged true

Atau, Anda dapat menggunakan AWS CLI perintah dengan menggunakan ID detektor regional Anda sendiri. Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan [ListDetectors](#) API. `detectorId`

Contoh berikut memungkinkan EKS_RUNTIME_MONITORING dan menonaktifkan EKS_ADDON_MANAGEMENT untuk satu akun. Anda juga dapat melewati daftar akun yang IDs dipisahkan oleh spasi.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan [ListDetectors](#) API. `detectorId`

```
aws guardduty update-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0 --autoEnable --features '[{"Name" : "EKS_RUNTIME_MONITORING", "AutoEnable": "NEW", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "AutoEnable": "NEW"}] }]'
```

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-Langkah
	Ketika kode telah berhasil dijalankan, daftar <code>UnprocessedAccounts</code> akan kembali kosong. Jika ada masalah dalam mengubah pengaturan detektor untuk suatu akun, ID akun tersebut akan dicantumkan bersama dengan ringkasan masalahnya.

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-Langkah
Mengelola agen keamanan secara manual	1. Untuk mengaktifkan EKS Runtime Monitoring secara selektif untuk akun baru Anda, jalankan operasi UpdateOrganizationConfiguration API menggunakan akun Anda sendiri. <i>detector ID</i> Tetapkan status untuk EKS_ADDON_MANAGEMENT asDISABLED. Atau, Anda dapat menggunakan AWS CLI perintah dengan menggunakan ID detektor regional Anda sendiri. Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectors API. <code>detectorId</code> Contoh berikut memungkinkan EKS_RUNTIME_MONITORING dan menonaktifkan EKS_ADDON_MANAGEMENT untuk satu akun. Anda juga dapat melewati daftar akun yang IDs dipisahkan oleh spasi. Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectors API. <code>detectorId</code> <pre>aws guardduty update-organization-configuration --detector-id <i>12abc34d567e8fa901bc2d34e56789f0</i> --autoEnable --features '[{"Name" : "EKS_RUNTIME_MONITORING", "AutoEnable": "NEW", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "AutoEnable": "NEW"}]]'</pre> Ketika kode telah berhasil dijalankan, daftar <code>UnprocessedAccounts</code> akan kembali kosong. Jika

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-Langkah
	ada masalah dalam mengubah pengaturan detektor untuk suatu akun, ID akun tersebut akan dicantumkan bersama dengan ringkasan masalahnya. 2. Untuk mengelola agen keamanan, lihat Mengelola agen keamanan secara manual untuk kluster Amazon EKS.

Aktifkan EKS Runtime Monitoring untuk akun anggota aktif individu

Bagian ini mencakup langkah-langkah untuk mengonfigurasi EKS Runtime Monitoring dan mengelola agen keamanan untuk akun anggota aktif individu.

Berdasarkan [Pendekatan untuk mengelola agen GuardDuty keamanan di kluster Amazon EKS](#), Anda dapat memilih pendekatan yang disukai dan mengikuti langkah-langkah seperti yang disebutkan dalam tabel berikut.

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-Langkah
Kelola agen keamanan melalui GuardDuty (Pantau semua kluster EKS)	Untuk mengaktifkan EKS Runtime Monitoring secara selektif untuk akun anggota Anda, jalankan operasi updateMemberDetectors API menggunakan milik Anda sendiri. <i>detector ID</i> Tetapkan status untuk EKS_ADDON_MANAGEMENT asENABLED. GuardDuty akan mengelola penyebaran dan pembaruan ke agen keamanan untuk semua kluster Amazon EKS di akun Anda. Atau, Anda dapat menggunakan AWS CLI perintah dengan menggunakan ID detektor regional Anda sendiri. Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan

Langkah-Langkah

Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan [ListDetectors](#) API. `detectorId`

Contoh berikut memungkinkan keduanya `EKS_RUNTIME_MONITORING` dan `EKS_ADDON_MANAGEMENT` :

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : "ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : "ENABLED"}] ]'
```

Note

Anda juga dapat melewati daftar akun yang IDs dipisahkan oleh spasi.

Ketika kode telah berhasil dijalankan, daftar `UnprocessedAccounts` akan kembali kosong. Jika ada masalah dalam mengubah pengaturan detektor untuk suatu akun, ID akun tersebut akan dicantumkan bersama dengan ringkasan masalahnya.

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-Langkah
Pantau semua cluster EKS tetapi kecualikan beberapa di antaranya (menggunakan tag pengecualian)	1. Tambahkan tag ke cluster EKS yang ingin Anda kecualikan agar tidak dipantau. Pasangkan kunci-nilai adalah GuardDutyManaged - false Untuk informasi selengkapnya tentang menambahkan tag, lihat Bekerja dengan tag menggunakan CLI, API, atau eksctl di Panduan Pengguna Amazon EKS. 2. Untuk mencegah modifikasi tag, kecuali oleh entitas tepercaya, gunakan kebijakan yang disediakan dalam Mencegah tag agar tidak dimodifikasi kecuali oleh prinsipal resmi dalam Panduan Pengguna AWS Organizations Dalam kebijakan ini, ganti detail berikut: • Ganti <i>ec2:CreateTags</i> dengan <i>eks:TagResource</i> . • Ganti <i>ec2:DeleteTags</i> dengan <i>eks:UntagResource</i> . • Ganti <i>access-project</i> dengan GuardDuty Managed • Ganti <i>123456789012</i> dengan Akun AWS ID entitas tepercaya. Jika Anda memiliki lebih dari satu entitas tepercaya , gunakan contoh berikut untuk menambahkan beberapaPrincipalArn : <pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre>

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-Langkah
	3.  Note Selalu tambahkan tag pengecualian ke kluster EKS Anda sebelum menyetel EKS_RUNTIME_MONITORING ke ENABLED; jika tidak, agen GuardDuty keamanan akan digunakan di semua kluster EKS di akun Anda. STATUS Untuk mengaktifkan EKS Runtime Monitoring secara selektif untuk akun anggota Anda, jalankan operasi updateMemberDetectors API menggunakan milik Anda sendiri. <i>detector ID</i> Tetapkan status untuk EKS_ADDON_MANAGEMENT as ENABLED. GuardDuty akan mengelola penyebaran dan pembaruan ke agen keamanan untuk semua kluster Amazon EKS yang belum dikecualikan dari pemantauan. Atau, Anda dapat menggunakan AWS CLI perintah dengan menggunakan ID detektor regional Anda sendiri. Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/ konsol, atau jalankan ListDetectors API. <code>detectorId</code> Contoh berikut memungkinkan keduanya EKS_RUNTIME_MONITORING dan EKS_ADDON_MANAGEMENT : <pre>aws guardduty update-member-detectors -- detector-id 12abc34d567e8fa901bc2d34e56 789f0 --account-ids 111122223333 --feature</pre>

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-Langkah
	<pre data-bbox="716 304 1507 478">s ' [{"Name" : "EKS_RUNTIME_MONITORING", "Status" : "ENABLED", "AdditionalConfigu ration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : "ENABLED"}] }] '</pre>  Note Anda juga dapat melewati daftar akun yang IDs dipisahkan oleh spasi. Ketika kode telah berhasil dijalankan, daftar UnprocessedAccounts akan kembali kosong. Jika ada masalah dalam mengubah pengaturan detektor untuk suatu akun, ID akun tersebut akan dicantumkan bersama dengan ringkasan masalahnya.

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-Langkah
Pantau kluster EKS selektif (menggunakan tag inklusi)	1. Tambahkan tag ke cluster EKS yang ingin Anda kecualikan agar tidak dipantau. Pasangkan kunci-nilai adalah <code>GuardDutyManaged</code> - <code>true</code>. Untuk informasi selengkapnya tentang menambahkan tag, lihat Bekerja dengan tag menggunakan CLI, API, atau eksctl di Panduan Pengguna Amazon EKS. 2. Untuk mencegah modifikasi tag, kecuali oleh entitas tepercaya, gunakan kebijakan yang disediakan dalam Mencegah tag agar tidak dimodifikasi kecuali oleh prinsipal resmi dalam Panduan Pengguna AWS Organizations. Dalam kebijakan ini, ganti detail berikut: • Ganti <code>ec2:CreateTags</code> dengan <code>eks:TagResource</code>. • Ganti <code>ec2:DeleteTags</code> dengan <code>eks:UntagResource</code>. • Ganti <code>access-project</code> dengan <code>GuardDutyManaged</code>. • Ganti <code>123456789012</code> dengan Akun AWS ID entitas tepercaya. Jika Anda memiliki lebih dari satu entitas tepercaya, gunakan contoh berikut untuk menambahkan beberapa <code>PrincipalArn</code>: <pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre> 3. Untuk mengaktifkan EKS Runtime Monitoring secara selektif untuk akun anggota Anda, jalankan operasi

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan

Langkah-Langkah

[updateMemberDetectors](#) API menggunakan milik Anda sendiri. *detector ID*

Tetapkan status untuk EKS_ADDON_MANAGEMENT asDISABLED.

GuardDuty akan mengelola penyebaran dan pembaruan ke agen keamanan untuk semua kluster Amazon EKS yang telah ditandai dengan - pair.
GuardDutyManaged true

Atau, Anda dapat menggunakan AWS CLI perintah dengan menggunakan ID detektor regional Anda sendiri. Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan [ListDetectors](#) API. `detectorId`

Contoh berikut memungkinkan EKS_RUNTIME_MONITORING dan menonaktifkan EKS_ADDON_MANAGEMENT :

```
aws guardduty update-member-detectors --
detector-id 12abc34d567e8fa901bc2d34e56
789f0 --account-ids 111122223333 --feature
s '[{"Name" : "EKS_RUNTIME_MONITORING",
"Status" : "ENABLED", "AdditionalConfigu
ration" : [{"Name" : "EKS_ADDON_MANAGEMENT",
"Status" : "DISABLED"}] }]'
```

Note

Anda juga dapat melewati daftar akun yang IDs dipisahkan oleh spasi.

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-Langkah
	Ketika kode telah berhasil dijalankan, daftar <code>UnprocessedAccounts</code> akan kembali kosong. Jika ada masalah dalam mengubah pengaturan detektor untuk suatu akun, ID akun tersebut akan dicantumkan bersama dengan ringkasan masalahnya.

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-Langkah
Mengelola agen keamanan secara manual	Untuk mengaktifkan EKS Runtime Monitoring secara selektif untuk akun anggota Anda, jalankan operasi updateMemberDetectors API menggunakan milik Anda sendiri. <i>detector ID</i> Tetapkan status untuk EKS_ADDON_MANAGEMENT asDISABLED. Atau, Anda dapat menggunakan AWS CLI perintah dengan menggunakan ID detektor regional Anda sendiri. Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectors API. <code>detectorId</code> Contoh berikut memungkinkan EKS_RUNTIME_MONITORING dan menonaktifkan EKS_ADDON_MANAGEMENT : <pre>aws guardduty update-member-detectors -- detector-id <i>12abc34d567e8fa901bc2d34e56789f0</i> --account-ids <i>5555555555</i> --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : "<i>ENABLED</i>", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : "<i>ENABLED</i>"}] }]'</pre> Untuk mengelola agen keamanan, lihat Mengelola agen keamanan secara manual untuk kluster Amazon EKS.

Mengkonfigurasi EKS Runtime Monitoring untuk akun mandiri (API)

Akun mandiri memiliki keputusan untuk mengaktifkan atau menonaktifkan rencana perlindungan di akun mereka Akun AWS secara spesifik. Wilayah AWS

Jika akun Anda dikaitkan dengan akun GuardDuty administrator melalui AWS Organizations, atau dengan metode undangan, bagian ini tidak berlaku untuk akun Anda. Untuk informasi selengkapnya, lihat [Mengkonfigurasi EKS Runtime Monitoring untuk lingkungan multi-akun \(API\)](#).

Setelah Anda mengaktifkan Runtime Monitoring, pastikan untuk menginstal agen GuardDuty keamanan melalui konfigurasi otomatis atau penerapan manual. Sebagai bagian dari menyelesaikan semua langkah yang tercantum dalam prosedur berikut, pastikan untuk menginstal agen keamanan.

Berdasarkan [Pendekatan untuk mengelola agen GuardDuty keamanan di kluster Amazon EKS](#), Anda dapat memilih pendekatan yang disukai dan mengikuti langkah-langkah seperti yang disebutkan dalam tabel berikut.

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-Langkah
Kelola agen keamanan melalui GuardDuty (Pantau semua kluster EKS)	Jalankan updateDetector API dengan menggunakan ID detektor regional Anda sendiri dan meneruskan nama <code>features</code> objek sebagai <code>EKS_RUNTIME_MONITORING</code> dan status sebagai <code>ENABLED</code>. Tetapkan status untuk <code>EKS_ADDON_MANAGEMENT</code> as <code>ENABLED</code>. GuardDuty akan mengelola penyebaran dan pembaruan ke agen keamanan untuk semua kluster Amazon EKS di akun Anda. Atau, Anda dapat menggunakan AWS CLI perintah dengan menggunakan ID detektor regional Anda sendiri. Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectors API. <code>detectorId</code> Contoh berikut memungkinkan keduanya <code>EKS_RUNTIME_MONITORING</code> dan <code>EKS_ADDON_MANAGEMENT</code> : <pre>aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --</pre>

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-Langkah
	<pre>features '[{"Name" : "EKS_RUNTIME_MONIT ORING", "Status" : " ENABLED", "Addition alConfiguration" : [{"Name" : "EKS_ADDO N_MANAGEMENT", "Status" : " ENABLED"}]]]'</pre>

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-Langkah
Pantau semua cluster EKS tetapi kecualikan beberapa di antaranya (menggunakan tag pengecualian)	1. Tambahkan tag ke cluster EKS yang ingin Anda kecualikan agar tidak dipantau. Pasangkan kunci-nilai adalah GuardDutyManaged - false Untuk informasi selengkapnya tentang menambahkan tag, lihat Bekerja dengan tag menggunakan CLI, API, atau eksctl di Panduan Pengguna Amazon EKS. 2. Untuk mencegah modifikasi tag, kecuali oleh entitas tepercaya, gunakan kebijakan yang disediakan dalam Mencegah tag agar tidak dimodifikasi kecuali oleh prinsipal resmi dalam Panduan Pengguna AWS Organizations Dalam kebijakan ini, ganti detail berikut: • Ganti <i>ec2:CreateTags</i> dengan <i>eks:TagResource</i> . • Ganti <i>ec2:DeleteTags</i> dengan <i>eks:UntagResource</i> . • Ganti <i>access-project</i> dengan GuardDuty Managed • Ganti <i>123456789012</i> dengan Akun AWS ID entitas tepercaya. Jika Anda memiliki lebih dari satu entitas tepercaya , gunakan contoh berikut untuk menambahkan beberapaPrincipalArn : <pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre>

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-Langkah
	3.  Note Selalu tambahkan tag pengecualian ke kluster EKS Anda sebelum menyetel EKS_RUNTIME_MONITORING ke ENABLED; jika tidak, agen GuardDuty keamanan akan digunakan di semua kluster EKS di akun Anda. STATUS Jalankan updateDetector API dengan menggunakan ID detektor regional Anda sendiri dan meneruskan nama features objek sebagai EKS_RUNTIME_MONITORING dan status sebagai ENABLED. Tetapkan status untuk EKS_ADDON_MANAGEMENT as ENABLED. GuardDuty akan mengelola penyebaran dan pembaruan ke agen keamanan untuk semua kluster Amazon EKS yang belum dikecualikan dari pemantauan. Atau, Anda dapat menggunakan AWS CLI perintah dengan menggunakan ID detektor regional Anda sendiri. Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/ konsol, atau jalankan ListDetectors API. <code>detectorId</code> Contoh berikut memungkinkan keduanya EKS_RUNTIME_MONITORING dan EKS_ADDON_MANAGEMENT : <pre>aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --</pre>

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-Langkah
	<pre>features '[{"Name" : "EKS_RUNTIME_MONIT ORING", "Status" : " ENABLED", "Addition alConfiguration" : [{"Name" : "EKS_ADDO N_MANAGEMENT", "Status" : " ENABLED"}]]'</pre>

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-Langkah
Pantau kluster EKS selektif (menggunakan tag inklusi)	1. Tambahkan tag ke cluster EKS yang ingin Anda kecualikan agar tidak dipantau. Pasangkan kunci-nilai adalah <code>GuardDutyManaged</code> - <code>true</code> Untuk informasi selengkapnya tentang menambahkan tag, lihat Bekerja dengan tag menggunakan CLI, API, atau eksctl di Panduan Pengguna Amazon EKS. 2. Untuk mencegah modifikasi tag, kecuali oleh entitas tepercaya, gunakan kebijakan yang disediakan dalam Mencegah tag agar tidak dimodifikasi kecuali oleh prinsipal resmi dalam Panduan Pengguna AWS Organizations. Dalam kebijakan ini, ganti detail berikut: • Ganti <code>ec2:CreateTags</code> dengan <code>eks:TagResource</code>. • Ganti <code>ec2:DeleteTags</code> dengan <code>eks:UntagResource</code>. • Ganti <code>access-project</code> dengan <code>GuardDutyManaged</code> • Ganti <code>123456789012</code> dengan Akun AWS ID entitas tepercaya. Jika Anda memiliki lebih dari satu entitas tepercaya, gunakan contoh berikut untuk menambahkan beberapa <code>PrincipalArn</code>: <pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre> 3. Jalankan updateDetector API dengan menggunakan ID detektor regional Anda sendiri dan meneruskan nama

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-Langkah
	features objek sebagai EKS_RUNTIME_MONITORING dan status sebagai ENABLED. Tetapkan status untuk EKS_ADDON_MANAGEMENT as DISABLED. GuardDuty akan mengelola penyebaran dan pembaruan ke agen keamanan untuk semua kluster Amazon EKS yang telah ditandai dengan - pair. GuardDutyManaged true Atau, Anda dapat menggunakan AWS CLI perintah dengan menggunakan ID detektor regional Anda sendiri. Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectorsAPI. detectorId Contoh berikut memungkinkan EKS_RUNTIME_MONITORING dan menonaktifkan EKS_ADDON_MANAGEMENT : <pre>aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name": "EKS_RUNTIME_MONITORING", "Status": "ENABLED", "AdditionalConfiguration": [{"Name": "EKS_ADDON_MANAGEMENT", "Status": "DISABLED"}]]'</pre>

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan	Langkah-Langkah
Mengelola agen keamanan secara manual	1. Jalankan updateDetector API dengan menggunakan ID detektor regional Anda sendiri dan meneruskan nama features objek sebagai EKS_RUNTIME_MONITORING dan status sebagai ENABLED. Tetapkan status untuk EKS_ADDON_MANAGEMENT as DISABLED. Atau, Anda dapat menggunakan AWS CLI perintah dengan menggunakan ID detektor regional Anda sendiri. Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di https://console.aws.amazon.com/guardduty/konsol, atau jalankan ListDetectors API. <code>detectorId</code> Contoh berikut memungkinkan EKS_RUNTIME_MONITORING dan menonaktifkan EKS_ADDON_MANAGEMENT : <pre>aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : "ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : "DISABLED"}]]'</pre> 2. Untuk mengelola agen keamanan, lihat Mengelola agen keamanan secara manual untuk klaster Amazon EKS.

Migrasi dari EKS Runtime Monitoring ke Runtime Monitoring

Dengan peluncuran GuardDuty Runtime Monitoring, cakupan deteksi ancaman telah diperluas ke wadah Amazon ECS dan instans Amazon EC2 . Pengalaman EKS Runtime Monitoring kini telah dikonsolidasikan ke dalam Runtime Monitoring. Anda dapat mengaktifkan Runtime Monitoring dan

mengelola agen GuardDuty keamanan individual untuk setiap jenis sumber daya (EC2 instans Amazon, klaster Amazon ECS, dan klaster Amazon EKS) yang ingin Anda pantau perilaku runtime.

GuardDuty telah mengkonsolidasikan pengalaman konsol untuk EKS Runtime Monitoring ke Runtime Monitoring. GuardDuty merekomendasikan [Memeriksa status konfigurasi EKS Runtime Monitoring](#) dan [Migrasi dari EKS Runtime Monitoring ke Runtime Monitoring](#).

Sebagai bagian dari migrasi ke Runtime Monitoring, pastikan untuk. [Nonaktifkan Pemantauan Runtime EKS](#) Ini penting karena jika nanti Anda memilih untuk menonaktifkan Runtime Monitoring dan Anda tidak menonaktifkan EKS Runtime Monitoring, Anda akan terus mengeluarkan biaya penggunaan untuk EKS Runtime Monitoring.

Untuk bermigrasi dari EKS Runtime Monitoring ke Runtime Monitoring

1. GuardDuty Konsol mendukung EKS Runtime Monitoring sebagai bagian dari Runtime Monitoring.

Anda dapat mulai menggunakan Runtime Monitoring oleh [Memeriksa status konfigurasi EKS Runtime Monitoring](#) organisasi dan akun Anda.

Pastikan untuk tidak menonaktifkan EKS Runtime Monitoring sebelum mengaktifkan Runtime Monitoring. Jika Anda menonaktifkan EKS Runtime Monitoring, manajemen add-on Amazon EKS juga akan dinonaktifkan. Lanjutkan dengan langkah-langkah berikut dalam urutan yang tercantum.

2. Pastikan Anda memenuhi semua [Prasyarat untuk mengaktifkan Runtime Monitoring](#).
3. Aktifkan Runtime Monitoring dengan mereplikasi pengaturan konfigurasi organisasi yang sama untuk Runtime Monitoring seperti yang Anda miliki untuk EKS Runtime Monitoring. Untuk informasi selengkapnya, lihat [Mengaktifkan Runtime Monitoring](#).

- Jika Anda memiliki akun mandiri, Anda harus mengaktifkan Runtime Monitoring.

Jika agen GuardDuty keamanan Anda sudah digunakan, pengaturan yang sesuai akan direplikasi secara otomatis dan Anda tidak perlu mengonfigurasi pengaturan lagi.

- Jika Anda memiliki organisasi dengan pengaturan auto-enablement, pastikan untuk mereplikasi pengaturan auto-enablement yang sama untuk Runtime Monitoring.
- Jika Anda memiliki organisasi dengan pengaturan yang dikonfigurasi untuk akun anggota aktif yang ada secara individual, pastikan untuk mengaktifkan Runtime Monitoring dan mengonfigurasi agen GuardDuty keamanan untuk anggota ini secara individual.

4. Setelah Anda memastikan bahwa pengaturan Runtime Monitoring dan agen GuardDuty keamanan sudah benar, [nonaktifkan EKS Runtime Monitoring](#) dengan menggunakan API atau perintah. AWS CLI

5. (Opsional) jika Anda ingin membersihkan sumber daya apa pun yang terkait dengan agen GuardDuty keamanan, lihat [Menonaktifkan, menghapus instalasi, dan membersihkan sumber daya di Runtime Monitoring](#).

Jika Anda ingin terus menggunakan EKS Runtime Monitoring tanpa mengaktifkan Runtime Monitoring, lihat. [Pemantauan Runtime EKS di GuardDuty](#) Berdasarkan kasus penggunaan Anda, pilih langkah-langkah untuk mengonfigurasi EKS Runtime Monitoring untuk akun mandiri atau untuk beberapa akun anggota.

Memeriksa status konfigurasi EKS Runtime Monitoring

Gunakan AWS CLI perintah berikut APIs atau untuk memeriksa status konfigurasi EKS Runtime Monitoring yang ada.

Untuk memeriksa status konfigurasi EKS Runtime Monitoring yang ada di akun Anda

- Jalankan [GetDetector](#) untuk memeriksa status konfigurasi akun Anda sendiri.
- Atau, Anda dapat menjalankan perintah berikut dengan menggunakan AWS CLI:

```
aws guardduty get-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --  
region us-east-1
```

Pastikan untuk mengganti ID detektor Wilayah Anda Akun AWS dan saat ini. Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/> konsol, atau jalankan [ListDetectors](#) API. `detectorId`

Untuk memeriksa status konfigurasi EKS Runtime Monitoring yang ada untuk organisasi Anda (hanya sebagai akun GuardDuty administrator yang didelegasikan)

- Jalankan [DescribeOrganizationConfiguration](#) untuk memeriksa status konfigurasi organisasi Anda.

Atau, Anda dapat menjalankan perintah berikut menggunakan AWS CLI:

```
aws guardduty describe-organization-configuration --detector-  
id 12abc34d567e8fa901bc2d34e56789f0 --region us-east-1
```

Pastikan untuk mengganti ID detektor dengan ID detektor akun GuardDuty administrator yang didelegasikan dan Wilayah dengan Wilayah Anda saat ini. Untuk menemukan akun Anda dan

Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan [ListDetectors](#) API. `detectorId`

Menonaktifkan EKS Runtime Monitoring setelah bermigrasi ke Runtime Monitoring

Setelah Anda memastikan bahwa pengaturan yang ada untuk akun atau organisasi Anda telah direplikasi ke Runtime Monitoring, Anda dapat menonaktifkan EKS Runtime Monitoring.

Untuk menonaktifkan EKS Runtime Monitoring

- Untuk menonaktifkan EKS Runtime Monitoring di akun Anda sendiri

Jalankan [UpdateDetector](#) API dengan regional Anda sendiri *detector-id*.

Atau, Anda dapat menggunakan AWS CLI perintah berikut. Ganti

12abc34d567e8fa901bc2d34e56789f0 dengan regional Anda sendiri *detector-id*.

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --  
features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : "DISABLED"}]'
```

- Untuk menonaktifkan EKS Runtime Monitoring untuk akun anggota di organisasi Anda

Jalankan [UpdateMemberDetectors](#) API dengan regional *detector-id* dari akun GuardDuty administrator yang didelegasikan dari organisasi.

Atau, Anda dapat menggunakan AWS CLI perintah berikut. Ganti

12abc34d567e8fa901bc2d34e56789f0 dengan regional *detector-id* akun GuardDuty administrator yang didelegasikan dari organisasi dan *111122223333* dengan Akun AWS ID akun anggota yang ingin Anda nonaktifkan fitur ini.

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0  
--account-ids 111122223333 --features '[{"Name" : "EKS_RUNTIME_MONITORING",  
"Status" : "DISABLED"}]'
```

- Untuk memperbarui EKS Runtime Monitoring, aktifkan pengaturan otomatis untuk organisasi Anda

Lakukan langkah berikut hanya jika Anda telah mengonfigurasi pengaturan pengaktifan otomatis EKS Runtime Monitoring ke akun anggota baru (NEW) atau semua (ALL) di organisasi. Jika Anda sudah mengonfigurasinya sebagai NONE, maka Anda dapat melewati langkah ini.

 Note

Menyetel konfigurasi pengaktifan otomatis EKS Runtime Monitoring NONE berarti bahwa EKS Runtime Monitoring tidak akan diaktifkan secara otomatis untuk akun anggota yang ada atau ketika akun anggota baru bergabung dengan organisasi Anda.

Jalankan [UpdateOrganizationConfiguration](#) API dengan regional *detector-id* dari akun GuardDuty administrator yang didelegasikan dari organisasi.

Atau, Anda dapat menggunakan AWS CLI perintah berikut. Ganti *12abc34d567e8fa901bc2d34e56789f0* dengan regional *detector-id* dari akun GuardDuty administrator yang didelegasikan dari organisasi. Ganti *EXISTING_VALUE* dengan konfigurasi Anda saat ini untuk mengaktifkan otomatis GuardDuty.

```
aws guardduty update-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0 --auto-enable-organization-members EXISTING_VALUE --features '[{"Name" : "EKS_RUNTIME_MONITORING", "AutoEnable": "NONE"}]'
```

GuardDuty versi rilis agen keamanan

GuardDuty merilis versi agen yang diperbarui dari waktu ke waktu. Ketika GuardDuty mengelola agen secara otomatis, GuardDuty dirancang untuk memperbarui agen atas nama Anda. Saat mengelola agen secara manual, Anda bertanggung jawab untuk memperbarui versi agen untuk jenis sumber daya Anda — EC2 instans Amazon, kluster Amazon ECS, dan kluster Amazon EKS.

Bagian berikut menyediakan versi rilis agen GuardDuty keamanan dan catatan rilis terkait untuk semua jenis sumber daya yang didukung.

Topik

- [GuardDuty versi agen keamanan untuk EC2 instans Amazon](#)
- [GuardDuty versi agen keamanan untuk AWS Fargate \(hanya Amazon ECS\)](#)
- [GuardDuty versi agen keamanan untuk sumber daya Amazon EKS](#)
- [Sumber daya tambahan - langkah selanjutnya](#)

GuardDuty versi agen keamanan untuk EC2 instans Amazon

Tabel berikut menunjukkan riwayat versi rilis untuk agen GuardDuty keamanan untuk Amazon EC2.

Versi agen	Catatan rilis	Tanggal ketersediaan
v1.7.1	Ditambahkan dukungan untuk Fedora 40 dan Fedora 41. Untuk daftar semua distribusi OS terverifikasi untuk EC2 sumber daya Amazon, lihat Validasi persyaratan arsitektur. Penyetelan dan peningkatan kinerja umum.	Juni 03, 2025
v1.7.0	Menambahkan dukungan untuk Oracle Linux versi 8.9 dan 9.3, dan Rocky Linux versi 9.5. Untuk daftar semua distribusi OS terverifikasi untuk EC2 sumber daya Amazon, lihat Validasi persyaratan arsitektur. Resolusi ID kontainer yang ditingkatkan. Penyetelan dan peningkatan kinerja umum.	April 03, 2025
v1.6.0	Penyetelan dan peningkatan kinerja umum.	Februari 6, 2025
v1.5.0	Menambahkan dukungan untuk CentOS Stream 9.0, RedHat 9.4, Fedora 34.0, dan Ubuntu 24.04.	November 20, 2024

Versi agen	Catatan rilis	Tanggal ketersediaan
	Support untuk instance ARM untuk .../Metad ataDNSRebind temuan. Penyetelan dan peningkatan kinerja umum.	
v1.3.1	Support untuk resolver DNS kustom.	September 12, 2024
v1.3.0	Penyetelan dan peningkatan kinerja umum. Termasuk dukungan untuk menangkap sinyal keamanan tambahan untuk masa depan GuardDuty Jenis penemuan Runtime Monitorin g.	Agustus 19, 2024
v1.2.0	Mendukung distribusi OS Ubuntu 20.04, Ubuntu 22.04, Debian 11, dan Debian 12. Mendukung kernel 6.5 dan 6.8. Penyetelan dan peningkatan kinerja umum.	Juni 13, 2024

Versi agen	Catatan rilis	Tanggal ketersediaan
v1.1.0	Mendukung konfigurasi agen GuardDuty otomatis dalam Runtime Monitoring untuk EC2 instans Amazon. Mendukung sinyal keamanan baru dan temuan yang dirilis dengan pengumuman ketersediaan umum Runtime Monitoring untuk EC2 instance. Penyetelan dan peningkatan kinerja umum.	26 Maret 2024
v1.0.2	Mendukung Amazon ECS AMIs terbaru.	Februari 2, 2024
v1.0.1	Versi agen yang dirilis sebelum v1.0.2 tidak kompatibel dengan Amazon ECS yang AMIs diluncurkan setelah 31 Januari 2024. Penyetelan dan peningkatan kinerja umum.	23 Januari 2024
v1.0.0	Pelepasan awal instalasi RPM. Versi agen yang dirilis sebelum v1.0.2 tidak kompatibel dengan Amazon ECS yang AMIs diluncurkan setelah 31 Januari 2024.	26 November 2023

GuardDuty versi agen keamanan untuk AWS Fargate (hanya Amazon ECS)

Tabel berikut menunjukkan riwayat versi rilis untuk agen GuardDuty keamanan untuk Fargate (hanya Amazon ECS).

Versi agen	Gambar kontainer	Catatan rilis	Tanggal ketersediaan
v1.7.0	x86_64 (): AMD64 sha256:bf 9197abdf8 53607e5fa 392b4f97c cdd6ca56d d179be3ce 8849e552d 96582ac8 Graviton () ARM64: sha256:56 c8683c948 bcd82c0db cebf75520 4365ac728 5994693c1 1717bd45f 86e279c2	Resolusi ID kontainer yang ditingkatkan. Penyetelan dan peningkatan kinerja umum.	April 04, 2025
v1.6.0	x86_64 (): AMD64 sha256:c8 dea71d372 bc47b2f23 6f7a091b9 a9b06bc81 93c1cfe4c 9346eb50f 89258897	Penyetelan dan peningkatan kinerja umum.	Februari 6, 2025

Versi agen	Gambar kontainer	Catatan rilis	Tanggal ketersediaan
	Graviton () ARM64: sha256:f4 032a566b9 0537646c2 a987bef42 eca1b4980 78ccc58a8 48603f877 971a8dbe		
v1.5.0	x86_64 (): AMD64 sha256:5e 6fdc41f9e b748219d0 498cd6c1d ba6a19d87 5daec5016 7a0ac80e5 028eac54 Graviton () ARM64: sha256:d5 6801ff686 4d6014740 103b70b1c 384318513 58d182613 bede20fe2 1090e734	Support untuk tugas ARM untuk .../ MetadataDNSReb ind temuan. Penyetelan dan peningkatan kinerja umum.	November 14, 2024

Versi agen	Gambar kontainer	Catatan rilis	Tanggal ketersediaan
v1.4.1	x86_64 (): AMD64 sha256:ef 36a11151e c2d3d7db2 2273bfb95 4750dee76 f0ac7bec3 7a7ba7e74 c3de1c78 Graviton () ARM64: sha256:a8 844544a59 d6b4cba98 f8e528b51 3ac2d9743 2f208e3ad 497cc16b3 31aa9faa	Pengerasan gambar kontainer. Penyetelan dan peningkatan kinerja umum.	Oktober 24, 2024

Versi agen	Gambar kontainer	Catatan rilis	Tanggal ketersediaan
v1.3.1	x86_64 (): AMD64 sha256:a6 e2307d796 e2875907b c4c1c6962 2c906f319 2ddc42ef2 7b99e0a8f 0979f3e0 Graviton () ARM64: sha256:ad 1b6539d80 6edb504f1 7e6bcfb8b 4026c5e82 2300afc31 c0d23c6a0 8f9b99e9	Support untuk resolver DNS kustom.	September 11, 2024

Versi agen	Gambar kontainer	Catatan rilis	Tanggal ketersediaan
v1.3.0	x86_64 (): AMD64 sha256:f1ad3fb2dc55a1110c60eecf4453b9f9c02f29acb261df39814e7d29296bf831 Graviton () ARM64: sha256:ff81a755d46681e409f55a95beeda e9ebbcf5336e1c0b1e6348af7c6518bdbb1	Penyetelan dan peningkatan kinerja umum. Termasuk dukungan untuk menangkap sinyal keamanan tambahan untuk masa depan GuardDuty GuardDuty Jenis penemuan Runtime Monitoring.	Agustus 9, 2024

Versi agen	Gambar kontainer	Catatan rilis	Tanggal ketersediaan
v1.2.0	x86_64 (): AMD64 sha256:1d bad20ac2d c66d52d00 bb28dde42 81fe0d3c5 f261b1649 b247c2369 d9e26b93 Graviton () ARM64: sha256:91 930f8446f 5f95b93b8 ccb187739 92affa401 eb3f42da8 9d68077a5 6bafa6cd	Penyetelan dan peningkatan kinerja umum.	31 Mei 2024

Versi agen	Gambar kontainer	Catatan rilis	Tanggal ketersediaan
v1.1.0	x86_64 (): AMD64 sha256:83 ce3cf2ef8 5a349ed17 97a8cf30a 008ac5d8c 9f673f283 5823957e9 dcf71657 Graviton () ARM64: sha256:0d 4b61648d7 bdeab8ab8 d94684f80 5498927c7 d437d3182 04dcccfe8 c9383dc7	Mendukung sinyal dan temuan keamanan baru. Penyetelan dan peningkatan kinerja umum.	01 Mei 2024

Versi agen	Gambar kontainer	Catatan rilis	Tanggal ketersediaan
v1.0.1	x86_64 (): AMD64 sha256:9f8cd438fb66f62d09bf c641286439f7ed5177988a314a6021ef4ff880642e68 Graviton () ARM64: sha256:82c66bb615bd0d1e96db77b1f1fb51dc03220caa593b1962249571bf7147d1b7	Penyetelan dan peningkatan kinerja umum.	Januari 26, 2024

Versi agen	Gambar kontainer	Catatan rilis	Tanggal ketersediaan
v1.0.0	x86_64 (): AMD64 sha256:35 9b8b014e5 076c625da a1056090e 522631587 a7afa3b2e 055edda6b d1141017 Graviton () ARM64: sha256:b9 438690fa8 a86067180 a11658bec 0f4f838ae 3fbd225d0 4b9306250 648b3984	Rilis awal agen GuardDuty keamanan untuk AWS Fargate (hanya Amazon ECS).	26 November 2023

GuardDuty versi agen keamanan untuk sumber daya Amazon EKS

GuardDuty merilis versi agen yang diperbarui dari waktu ke waktu. Ketika GuardDuty mengelola agen secara otomatis, itu dirancang untuk mengelola pembaruan agen atas nama Anda. Saat Anda mengelola agen secara manual, Anda bertanggung jawab untuk memperbarui versi agen untuk kluster Amazon EKS Anda.

Sebelum memperbarui agen ke versi tertentu, tambahkan registri gambar GuardDuty ke `allowed-container-registries` dalam pengontrol penerimaan Anda. Untuk informasi selengkapnya, lihat [Agen hosting repositori Amazon ECR GuardDuty](#).

Tabel berikut menunjukkan riwayat versi rilis [GuardDuty agen add-on Amazon EKS](#).

Versi agen	Gambar kontainer	Catatan rilis	Tanggal ketersediaan	Akhir dari dukungan standar ¹
v1.10.0	x86_64 (): AMD64 sha256:6d cbe5b055e 1ef0af903 071ede0b0 8f755ad5b 7e9774a67 df5399efd aa1f3d7d Graviton () ARM64: sha256:f0 536882268 9610a4bab 543abf93d 3e070b1b5 59e62a2e6 7d82dfa98 37600f72	Resolusi ID kontainer yang ditingkatkan. Penyetelan dan peningkatan kinerja umum.	April 04, 2025	–
v1.9.0	x86_64 (): AMD64 sha256:51 c5789ef65 70f9bec87 9ac48a8f4 769718cbc 31e454300 32569917e 219af63f	Penyetelan dan peningkatan kinerja umum.	02 Maret 2025	–

Versi agen	Gambar kontainer	Catatan rilis	Tanggal ketersediaan	Akhir dari dukungan standar ¹
	Graviton () ARM64: sha256:9c 2f74e7ea0 827b7e422 ae4c91fff c6c2bc41a 1cdb96c71 91d05259d 337154e1			
v1.8.1	x86_64 (): AMD64 sha256:f2 ce8cf89db e17e3388c ecb350535 44dadf21a f7770545f 8d4b50384 076aff47 Graviton () ARM64: sha256:30 f586e4b69 4e704bcaf adfa9081a b0aeff3cf bcde39743 a0f1e24f7 7d79627f	Menambahkan dukungan untuk CentOS Stream 9.0, RedHat 9.4, Fedora 34.0, dan Ubuntu 24.04. Support untuk instance ARM untuk .../Metad ataDNSReb ind menemukan. Penyetelan dan peningkatan kinerja umum.	November 23, 2024	–

Versi agen	Gambar kontainer	Catatan rilis	Tanggal ketersediaan	Akhir dari dukungan standar ¹
v1.7.1	x86_64 (): AMD64 sha256:b8b86b5d0872c8b67fecf64ec3d172666360545435a1752447d510951a7fd749 Graviton () ARM64: sha256:40ac4cfc354fd430ba7897ca1632e9a500ed13eeb0c315c5bcad38680e76b6e9	Penyetelan dan peningkatan kinerja umum. Termasuk dukungan untuk menangkap sinyal keamanan tambahan untuk masa depan GuardDuty Jenis penemuan Runtime Monitoring . Support untuk resolver DNS kustom.	September 13, 2024	–

Versi agen	Gambar kontainer	Catatan rilis	Tanggal ketersediaan	Akhir dari dukungan standar ¹
v1.7.0	x86_64 (): AMD64 sha256:f3a2a8806e6c2a7fd63a91cccf6f7dffc7e68554a423d610cea8c7e8f2185ec Graviton () ARM64: sha256:b1a6db35a072c0de3c695e5e909a03e6c4e1fdbe47ecfaeb2784435cf67ebe0a	Penyetelan dan peningkatan kinerja umum. Termasuk dukungan untuk menangkap sinyal keamanan tambahan untuk masa depan GuardDuty Jenis penemuan Runtime Monitoring .	Agustus 17, 2024	–

Versi agen	Gambar kontainer	Catatan rilis	Tanggal ketersediaan	Akhir dari dukungan standar ¹
v1.6.1	x86_64 (): AMD64 sha256:30650708a6601f6d6b9046f54b30f5fd65af296b1e40b8c24426b9bd07c3ab1 Graviton () ARM64: sha256:5f637c42ffb306b20f776d9d83e1e0b4be40ce245be44afcf43a8902b4d71019	Penyetelan dan peningkatan kinerja umum.	14 Mei 2024	–

Versi agen	Gambar kontainer	Catatan rilis	Tanggal ketersediaan	Akhir dari dukungan standar ¹
v1.6.0	x86_64 (): AMD64 sha256:7d abcb3e30d 8b0536767 52fbc19e8 9f77272d9 a6a53cc93 731f58721 80ef9010 Graviton () ARM64: sha256:97 10f53afcc df4f22b26 5a1a6fc27 f1469403a f1f7d5d08 c4869a726 9cdd2650	- Mendukung konfigurasi agen GuardDuty otomatis untuk EC2 EKS/ sumber daya. - Mendukung sinyal dan temuan keamanan baru. Untuk informasi selengkapnya, lihat Mengumpulkan jenis peristiwa runtime yang menggunakan GuardDuty dan GuardDuty Jenis penemuan Runtime Monitoring. - Penyetelan dan peningkatan kinerja umum.	April 29, 2024	–

Versi agen	Gambar kontainer	Catatan rilis	Tanggal ketersediaan	Akhir dari dukungan standar ¹
v1.5.0	x86_64 (): AMD64 sha256:e09a4e70af4058a212f172cc8eb3fc23ad9bed547ed609faa2bb82cf7cc5532d Graviton () ARM64: sha256:afc9a3f8f17ae12499d76069efcf1b46271a5a4b2b3f6ba5de54637b8f55d5c6	• Penyetelan dan peningkatan kinerja umum. • Peningkatan keamanan termasuk jenis acara baru di bawah. Jenis acara runtime yang dikumpulkan • Peningkatan kinerja seputar penggunaan CPU.	07 Maret 2024	–

Versi agen	Gambar kontainer	Catatan rilis	Tanggal ketersediaan	Akhir dari dukungan standar ¹
v1.4.1	x86_64 (): AMD64 sha256:66d491927763742660faa87cc2c39bb97b7873039157ae8b90bc999cb73d0b9c Graviton () ARM64: sha256:537a330b2dd82357024fb6daeb8761034b7defd43b10dff e0792c9e6d0778b40	Penyetelan dan peningkatan kinerja umum.	Januari 16, 2024	–

Versi agen	Gambar kontainer	Catatan rilis	Tanggal ketersediaan	Akhir dari dukungan standar ¹
v1.4.0	x86_64 (): AMD64 sha256:848ce13d9430bad554ac23d4699551505326ada2a88e1a721fe9f86b56b52c0f Graviton () ARM64: sha256:0c650aeafee b5f2bcb8b989ac849bedc1fae1a4de1cf6306ffdd9c6aebe67f8e	Manifest mount point mendukung pengumpulan data yang lebih baik AppArmor konfigurasi dalam manifes Kumpulkan argumen baris perintah Penyetelan dan peningkatan kinerja umum	21 Desember 2023	–

Versi agen	Gambar kontainer	Catatan rilis	Tanggal ketersediaan	Akhir dari dukungan standar ¹
v1.3.1	x86_64 (): AMD64 sha256:55 578fcb7b7 3097ade5c 8404390ef 16cf76a7b 568490aba ae01ac759 92b3ea29 Graviton () ARM64: sha256:e3 ce8d66ac2 121f8d476 eb58f8bc5 0ab513366 47615eb7c f514c2142 1cb818fd	Patch dan pembaruan keamanan penting.	23 Oktober 2023	–

Versi agen	Gambar kontainer	Catatan rilis	Tanggal ketersediaan	Akhir dari dukungan standar ¹
v1.3.0	x86_64 (): AMD64 sha256:6d ace2337df bb7609811 be89fb4b2 3ae0b865f 1027ad78f be69530bf bd46c694 Graviton () ARM64: sha256:49 28a7c6ef4 0e77c8ec9 5841323bb 9a110db31 f12c0ee7a b965e08b4 3efd01bb	Mendukung platform Ubuntu Mendukung Kubernetes versi 1.28 Peningkatan kinerja umum dan peningkatan stabilitas.	Oktober 05, 2023	–

Versi agen	Gambar kontainer	Catatan rilis	Tanggal ketersediaan	Akhir dari dukungan standar ¹
v1.2.0	x86_64 (): AMD64 sha256:d610413d662ec042057f05d6942496d7f2c08e9f5a077ea307ffdb5d3f11bcc3 Graviton () ARM64: sha256:174d7ab28b2f95e5309da80d95b88ad26f602dfe72c2b351a0ef9297a1412bfa	Selain instance AMD64 berbasis, v1.2.0 sekarang juga mendukung instance ARM64 berbasis. Menambahkan dan memverifikasi dukungan untuk Bottlerocket Mendukung Kubernetes versi 1.27 Peningkatan kinerja umum dan peningkatan stabilitas.	Juni 16, 2023	–

Versi agen	Gambar kontainer	Catatan rilis	Tanggal ketersediaan	Akhir dari dukungan standar ¹
v1.1.0	sha256:b19ba3a3c1a508d153263ae2fda891a7928b5ca9b3a5692db6c101829303281c	Selain itu Versi Kubernetes didukung oleh agen keamanan GuardDuty , rilis agen ini juga mendukung Kubernetes versi 1.26. Peningkatan kinerja umum dan peningkatan stabilitas.	2 Mei 2023	14 Mei 2024
v1.0.0	sha256:e38bdd2b1323e89113f1a31bd4bc8e5a8098525dd98e6981a28b9906b1e4411e	Rilis awal agen add-on Amazon EKS.	30 Maret 2023	14 Mei 2024

¹ Untuk informasi tentang memperbarui versi agen Anda saat ini yang mendekati akhir dukungan standar, lihat [Memperbarui agen keamanan secara manual untuk sumber daya Amazon EKS](#).

Sumber daya tambahan - langkah selanjutnya

Untuk informasi selengkapnya tentang langkah selanjutnya, lihat topik berikut:

- [Prasyarat untuk mengaktifkan Runtime Monitoring](#)- Dengan versi agen baru, mungkin ada pembaruan ke bagian prasyarat. Verifikasi dan validasi bahwa sumber daya Anda memenuhi prasyarat terbaru.
- [Mengelola agen GuardDuty keamanan](#)- Ketika Anda mengelola agen secara manual, maka Anda bertanggung jawab untuk mengelola pembaruan ke versi agen yang berjalan pada sumber daya Anda. Berdasarkan jenis sumber daya Anda (Amazon EKS atau Amazon EC2 -Amazon ECS), lakukan langkah-langkah untuk memperbarui agen keamanan. Pastikan juga untuk memvalidasi konfigurasi titik akhir [VPC](#) Anda.
- [Meninjau statistik cakupan runtime dan masalah pemecahan masalah](#)- Setelah Anda memperbarui agen keamanan, Anda dapat menilai cakupan runtime sumber daya Anda. Jika ada masalah cakupan, gunakan langkah pemecahan masalah terkait.

Menonaktifkan, menghapus instalasi, dan membersihkan sumber daya di Runtime Monitoring

Bagian ini berlaku untuk Anda Akun AWS jika Anda memilih untuk menonaktifkan Runtime Monitoring, atau hanya konfigurasi agen GuardDuty otomatis untuk jenis sumber daya.

Menonaktifkan konfigurasi agen GuardDuty otomatis

GuardDuty tidak menghapus agen keamanan yang digunakan pada sumber daya Anda. Namun, GuardDuty akan berhenti mengelola pembaruan ke agen keamanan.

GuardDuty terus menerima peristiwa runtime dari jenis sumber daya Anda. Untuk mencegah dampak pada statistik penggunaan Anda, pastikan untuk menghapus agen GuardDuty keamanan dari sumber daya Anda.

Apakah Akun AWS menggunakan titik akhir VPC bersama atau tidak, GuardDuty tidak menghapus titik akhir VPC. Jika diperlukan, Anda harus menghapus titik akhir VPC secara manual.

Menonaktifkan Runtime Monitoring dan EKS Runtime Monitoring

Bagian ini berlaku untuk Anda dalam skenario berikut:

- Anda tidak pernah mengaktifkan EKS Runtime Monitoring secara terpisah dan sekarang Anda menonaktifkan Runtime Monitoring.

- Anda menonaktifkan Runtime Monitoring dan EKS Runtime Monitoring. Jika Anda tidak yakin tentang status konfigurasi EKS Runtime Monitoring, lihat. [Memeriksa status konfigurasi EKS Runtime Monitoring](#)



Menonaktifkan Runtime Monitoring tanpa menonaktifkan EKS Runtime Monitoring

Dalam skenario ini, di beberapa titik waktu, Anda mengaktifkan EKS Runtime Monitoring, dan kemudian, juga mengaktifkan Runtime Monitoring tanpa menonaktifkan EKS Runtime Monitoring.

Sekarang, ketika Anda menonaktifkan Runtime Monitoring, Anda juga perlu menonaktifkan EKS Runtime Monitoring; jika tidak, Anda akan terus mengeluarkan biaya penggunaan untuk EKS Runtime Monitoring.

Jika skenario yang tercantum sebelumnya berlaku untuk Anda, maka GuardDuty akan mengambil tindakan berikut di akun Anda:

- GuardDuty menghapus titik akhir VPC yang memiliki GuardDutyManaged tag: `true` Ini adalah VPC yang GuardDuty telah dibuat untuk mengelola agen keamanan otomatis.
- GuardDuty menghapus grup keamanan yang ditandai sebagai GuardDutyManaged: `true`
- Untuk VPC bersama yang telah digunakan oleh setidaknya satu akun peserta, GuardDuty tidak menghapus titik akhir VPC maupun grup keamanan yang terkait dengan sumber daya VPC bersama.
- Untuk sumber daya Amazon GuardDuty EKS, hapus agen keamanan. Ini independen dari apakah dikelola secara manual atau melalui GuardDuty.

Untuk sumber daya Amazon ECS, karena tugas ECS tidak dapat diubah, tidak GuardDuty dapat menghapus instalasi agen keamanan dari sumber daya tersebut. Ini tidak tergantung pada bagaimana Anda mengelola agen keamanan — secara manual atau otomatis melalui GuardDuty. Setelah Anda menonaktifkan Runtime Monitoring, tidak GuardDuty akan melampirkan wadah sespan saat tugas ECS baru mulai berjalan. Untuk informasi tentang bekerja dengan tugas Fargate-ECS, lihat. [Bagaimana Runtime Monitoring bekerja dengan Fargate \(hanya Amazon ECS\)](#)

Untuk EC2 sumber daya Amazon, GuardDuty hapus instalasi agen keamanan dari semua EC2 instans Amazon yang dikelola Systems Manager (SSM) hanya jika memenuhi ketentuan berikut:

- Sumber daya Anda tidak ditandai dengan GuardDutyManaged: tag `false` pengecualian.

- GuardDuty harus memiliki izin untuk mengakses tag dalam metadata instance. Untuk EC2 sumber daya ini, Access to tag dalam metadata instance disetel ke Allow.

Ketika Anda berhenti mengelola agen keamanan secara manual

Terlepas dari pendekatan mana yang Anda gunakan untuk menyebarkan dan mengelola agen GuardDuty keamanan, untuk berhenti memantau peristiwa runtime di sumber daya Anda, Anda harus menghapus agen GuardDuty keamanan. Jika Anda ingin berhenti memantau peristiwa runtime dari jenis sumber daya di akun, Anda juga dapat menghapus titik akhir Amazon VPC.

Menghapus instalasi agen keamanan secara manual untuk sumber daya Amazon EC2

Bagian ini menyediakan metode untuk menghapus instalasi agen GuardDuty keamanan dari EC2 sumber daya Amazon Anda. Ketika Anda mengelola agen keamanan secara manual, Anda bertanggung jawab untuk menghapus agen dari sumber daya. GuardDuty tidak akan mengambil tindakan apa pun pada sumber daya yang Anda kelola.

Jika Anda membuat titik akhir VPC Amazon secara manual, maka setelah Anda menghapus instalasi agen keamanan pada semua jenis sumber daya yang dipantau di akun Anda, Anda dapat memilih untuk menghapus titik akhir VPC. Ini adalah langkah terpisah. Untuk informasi selengkapnya, lihat [To delete a VPC endpoint](#).

Berdasarkan cara Anda menginstal agen keamanan di sumber daya Anda, pilih salah satu metode berikut untuk menghapusnya.

Topik

- [Metode 1 - Dengan menggunakan perintah Run](#)
- [Metode 2 - Dengan menggunakan Linux Package Managers](#)

Metode 1 - Dengan menggunakan perintah Run

Saat Anda menginstal agen keamanan [Metode 1 - Menggunakan AWS Systems Manager](#), lakukan langkah-langkah berikut untuk menghapus instalasi agen:

Untuk menghapus instalasi agen GuardDuty keamanan

1. Anda dapat menghapus instalasi agen GuardDuty keamanan dengan mengikuti langkah-langkah seperti yang ditentukan dalam [AWS Systems Manager Jalankan Perintah](#) di Panduan AWS

Systems Manager Pengguna. Gunakan tindakan Uninstall dalam parameter untuk menghapus instalasi agen GuardDuty keamanan.

Di bagian Target, pastikan dampaknya hanya pada EC2 instans Amazon yang ingin Anda hapus instalasi agen keamanan.

Gunakan GuardDuty dokumen dan distributor berikut:

- Nama dokumen: AmazonGuardDuty-ConfigureRuntimeMonitoringSsmPlugin
 - Distributor: AmazonGuardDuty-RuntimeMonitoringSsmPlugin
2. Setelah memberikan semua detail, saat Anda memilih Jalankan, agen keamanan yang disebarkan pada EC2 instans Amazon yang ditargetkan akan dihapus.

Untuk menghapus konfigurasi endpoint Amazon VPC, Anda harus menonaktifkan Runtime Monitoring dan Amazon EKS Runtime Monitoring.

3. Jika Anda juga ingin menghapus titik akhir VPC yang terkait dengan agen keamanan ini, lihat. [To delete a VPC endpoint](#)

Metode 2 - Dengan menggunakan Linux Package Managers

Saat Anda menginstal agen keamanan [Metode 2 - Menggunakan Linux Package Manager](#), lakukan langkah-langkah berikut untuk menghapus instalasi agen:

Untuk menghapus instalasi agen GuardDuty keamanan

1. Connect ke instans Anda. Untuk langkah-langkah tentang cara melakukannya, lihat [Connect ke instans Linux Anda menggunakan klien SSH](#) di Panduan EC2 Pengguna Amazon.
2. Perintah untuk menghapus instalasi

Perintah berikut akan menghapus instalasi agen GuardDuty keamanan dari EC2 instans Amazon yang Anda sambungkan:

- Untuk RPM:

```
sudo rpm -e amazon-guardduty-agent
```

- Untuk Debian:

```
sudo dpkg --purge amazon-guardduty-agent
```

Setelah Anda menjalankan perintah, Anda juga dapat memeriksa log yang terkait dengan perintah.

3. Jika Anda juga ingin menghapus titik akhir VPC yang terkait dengan agen keamanan ini, lihat. [To delete a VPC endpoint](#)

Membersihkan sumber daya agen keamanan

Bagian ini menjelaskan bagaimana Anda dapat membersihkan AWS sumber daya yang terkait dengan agen keamanan. Seperti yang tercantum dalam [Menonaktifkan, menghapus instalasi, dan pembersihan sumber daya](#), tidak GuardDuty akan menghapus atau menghapus semua sumber daya agen keamanan. Bagian berikut memberikan petunjuk tentang bagaimana Anda dapat menghapus sumber daya agen keamanan.

Untuk menghapus titik akhir Amazon VPC

Saat Anda mengelola agen keamanan secara manual, Anda mungkin telah membuat titik akhir VPC Amazon secara manual. Setelah menghapus instalasi agen keamanan untuk semua sumber daya yang dipantau di akun Anda, Anda dapat memilih untuk menghapus titik akhir VPC ini.

Daftar berikut menyediakan skenario saat menggunakan VPC bersama dibandingkan dengan tidak menggunakan VPC bersama.

- Tanpa VPC bersama — Saat Anda tidak lagi ingin memantau sumber daya di akun, pertimbangkan untuk menghapus titik akhir VPC Amazon.
- Dengan VPC bersama — Saat akun pemilik VPC bersama menghapus sumber daya VPC bersama yang masih digunakan, status cakupan Runtime Monitoring (dan bila berlaku, EKS Runtime Monitoring) untuk sumber daya di akun pemilik VPC bersama Anda dan akun yang berpartisipasi mungkin menjadi tidak sehat. Untuk informasi tentang status cakupan, lihat [Meninjau statistik cakupan runtime dan masalah pemecahan masalah](#).

Untuk menghapus titik akhir VPC, [lihat Menghapus titik akhir antarmuka](#) di Panduan.AWS PrivateLink

Untuk menghapus grup keamanan

- Tanpa VPC bersama - Jika Anda tidak lagi ingin memantau jenis sumber daya di akun, pertimbangkan untuk menghapus grup keamanan yang terkait dengan VPC Amazon.
- Dengan VPC bersama — Saat akun pemilik VPC bersama menghapus grup keamanan, akun peserta apa pun yang saat ini menggunakan grup keamanan yang terkait dengan VPC bersama, status cakupan Pemantauan Waktu Proses untuk sumber daya di akun pemilik VPC bersama Anda dan akun yang berpartisipasi mungkin menjadi tidak sehat. Untuk informasi selengkapnya, lihat [Meninjau statistik cakupan runtime dan masalah pemecahan masalah](#).

Untuk selengkapnya tentang langkah-langkah, lihat [Menghapus grup EC2 keamanan Amazon](#) di Panduan EC2 Pengguna Amazon.

Untuk menghapus agen GuardDuty keamanan dari kluster EKS

Untuk menghapus agen keamanan dari kluster EKS yang tidak ingin Anda pantau lagi, lihat [Menghapus add-on Amazon EKS dari klaster](#) di Panduan Pengguna Amazon EKS.

Menghapus agen add-on EKS tidak menghapus amazon-guardduty namespace dari cluster EKS. Untuk menghapus amazon-guardduty namespace, lihat [Menghapus namespace](#).

Untuk menghapus **amazon-guardduty** namespace (kluster EKS)

Menonaktifkan konfigurasi agen otomatis tidak secara otomatis menghapus amazon-guardduty namespace dari kluster EKS Anda. Untuk menghapus amazon-guardduty namespace, lihat [Menghapus namespace](#).

GuardDuty Perlindungan Malware untuk EC2

Perlindungan Malware for EC2 membantu Anda mendeteksi potensi keberadaan malware dengan memindai volume [Amazon Elastic Block Store \(Amazon EBS\) yang dilampirkan ke instans Amazon Elastic Compute Cloud \(Amazon\)](#) dan beban kerja kontainer yang berjalan di EC2 Amazon. EC2 Perlindungan Malware untuk EC2 menyediakan opsi pemindaian di mana Anda dapat memutuskan apakah Anda ingin menyertakan atau mengecualikan EC2 instans Amazon tertentu pada saat pemindaian. Ini juga menyediakan opsi untuk menyimpan snapshot volume Amazon EBS yang dilampirkan ke EC2 instans Amazon atau beban kerja kontainer, di akun Anda. GuardDuty Cuplikan disimpan hanya ketika malware ditemukan dan Perlindungan Malware untuk EC2 temuan dihasilkan.

Perlindungan Malware untuk EC2 dirancang sedemikian rupa sehingga tidak akan mempengaruhi kinerja sumber daya Anda. Untuk informasi tentang cara EC2 kerja Perlindungan Malware di dalamnya GuardDuty, lihat [Cara GuardDuty memindai volume EBS untuk deteksi malware](#). Untuk informasi tentang ketersediaan Perlindungan Malware untuk EC2 di berbagai jenis Wilayah AWS, lihat [Wilayah dan titik akhir](#).

Catatan

Perlindungan Malware untuk EC2 mendukung pemindaian malware pada instans terkelola untuk Mode Otomatis Amazon EKS.

Perlindungan Malware untuk EC2 tidak mendukung pemindaian malware untuk AWS Fargate beban kerja yang berjalan dengan Amazon EKS atau Amazon ECS.

Untuk informasi tentang fitur Amazon EKS ini, lihat [Apa itu Amazon EKS?](#) di Panduan Pengguna Amazon EKS.

Topik

- [Membandingkan GuardDuty pemindaian malware yang dimulai dan pemindaian malware sesuai permintaan](#)
- [Cara GuardDuty memindai volume EBS untuk deteksi malware](#)
- [Volume Amazon EBS yang didukung untuk pemindaian malware](#)
- [Mengatur retensi snapshot dan cakupan EC2 pemindaian](#)
- [GuardDuty-pemindaian malware yang dimulai](#)
- [Pemindaian malware sesuai permintaan di GuardDuty](#)

- [Memantau status pemindaian dan hasil dalam Perlindungan Malware untuk EC2](#)
- [GuardDuty akun layanan oleh Wilayah AWS](#)
- [Kuota dalam Perlindungan Malware untuk EC2](#)

Membandingkan GuardDuty pemindaian malware yang dimulai dan pemindaian malware sesuai permintaan

Perlindungan Malware for EC2 menawarkan dua jenis pemindaian untuk mendeteksi aktivitas yang berpotensi berbahaya di EC2 instans Amazon dan beban kerja kontainer Anda — pemindaian malware yang GuardDuty dimulai dan pemindaian malware sesuai permintaan. Tabel berikut menunjukkan perbandingan antara kedua jenis pemindaian.

Faktor	GuardDuty-pemindaian malware yang dimulai	Pemindaian malware sesuai permintaan
Bagaimana pemindaian dipanggil	Setelah Anda mengaktifkan GuardDuty pemindaian malware yang dimulai, setiap kali GuardDuty menghasilkan temuan yang menunjukkan potensi keberadaan malware di EC2 instans Amazon atau beban kerja kontainer, GuardDuty secara otomatis memulai pemindaian malware tanpa agen pada volume Amazon EBS yang dilampirkan ke sumber daya yang berpotensi terkena dampak. Untuk informasi selengkapnya, lihat GuardDuty-pemindaian malware yang dimulai .	Anda dapat memulai pemindaian malware sesuai permintaan dengan memberikan Nama Sumber Daya Amazon (ARN) instans Amazon Anda. EC2 Anda dapat memulai pemindaian malware On-Demand bahkan ketika tidak ada GuardDuty temuan yang dihasilkan untuk sumber daya Anda. Untuk informasi selengkapnya, lihat Pemindaian malware sesuai permintaan di GuardDuty .
Konfigurasi diperlukan	Untuk menggunakan GuardDuty pemindaian malware yang dimulai, Anda	Akun Anda harus GuardDuty diaktifkan. Untuk menggunakan pemindaian malware On-

Faktor	GuardDuty-pemindaian malware yang dimulai	Pemindaian malware sesuai permintaan
	harus mengaktifkannya untuk akun Anda. Untuk mengelola beberapa akun dengan menggunakan AWS Organizations atau metode berbasis undangan, lihat Mengaktifkan GuardDuty pemindaian malware yang dimulai di lingkungan beberapa akun. Untuk mengaktifkan GuardDuty pemindaian malware yang dimulai di akun Anda sendiri, lihat. Mengaktifkan GuardDuty pemindaian malware yang dimulai untuk akun mandiri	Demand, tidak ada konfigurasi yang diperlukan di tingkat fitur.
Tunggu waktu untuk memulai pemindaian baru	Setiap kali GuardDuty menghasilkan salah satu Temuan yang memanggil pemindaian GuardDuty malware yang dimulai, pemindaian malware dimulai secara otomatis hanya sekali setiap 24 jam.	Anda dapat memulai pemindaian malware On-Demand pada sumber daya yang sama kapan saja setelah 1 jam dari waktu mulai pemindaian sebelumnya.

Faktor	GuardDuty-pemindaian malware yang dimulai	Pemindaian malware sesuai permintaan
Ketersediaan periode uji coba gratis 30 hari ¹	Saat Anda mengaktifkan GuardDuty pemindaian malware yang dimulai untuk pertama kalinya di akun Anda, Anda dapat menggunakan periode uji coba gratis 30 hari. Untuk informasi selengkapnya, lihat Uji coba gratis 30 hari dalam pemindaian GuardDuty malware yang dimulai.	Tidak ada periode uji coba gratis dengan pemindaian malware On-Demand untuk GuardDuty akun baru atau yang sudah ada.
Opsi pemindaian ²	Setelah Anda mengonfigurasi GuardDuty pemindaian malware yang dimulai, Perlindungan Malware untuk EC2 menyediakan opsi untuk memindai atau melewati EC2 sumber daya Amazon tertentu dengan menggunakan tag. Perlindungan Malware for tidak EC2 akan memulai pemindaian otomatis pada sumber daya yang Anda pilih untuk dikecualikan dari pemindaian. Untuk informasi selengkapnya, lihat Opsi pindai dengan tag yang ditentukan pengguna.	Karena Anda menyediakan sumber daya ARN untuk memulai pemindaian malware sesuai permintaan secara manual, penggunaan Opsi pindai dengan tag yang ditentukan pengguna tidak berlaku.

¹ Anda akan dikenakan biaya penggunaan untuk membuat snapshot volume EBS dan mempertahankan snapshot. Untuk informasi selengkapnya tentang mengonfigurasi akun Anda untuk menyimpan snapshot, lihat. [Retensi snapshot](#)

² Baik GuardDuty pemindaian malware yang dimulai dan pemindaian malware sesuai permintaan mendukung menggunakan tag global untuk mengecualikan EC2 sumber daya Amazon dari pemindaian malware. Untuk informasi selengkapnya, lihat [GuardDutyExcludedTag global](#).

Cara GuardDuty memindai volume EBS untuk deteksi malware

Bagian ini menjelaskan cara Perlindungan Malware untuk EC2, termasuk pemindaian malware yang GuardDuty dimulai dan pemindaian malware sesuai permintaan, memindai volume Amazon EBS yang terkait dengan instans Amazon dan beban kerja kontainer EC2 Anda. Sebelum melanjutkan, pertimbangkan penyesuaian berikut:

- Opsi pemindaian — Perlindungan Malware for EC2 menawarkan kemampuan untuk menentukan tag untuk menyertakan atau mengecualikan EC2 instans Amazon dan volume Amazon EBS dari proses pemindaian. Hanya GuardDuty pemindaian malware yang dimulai yang mendukung opsi pemindaian dengan tag yang ditentukan pengguna. Baik GuardDuty pemindaian malware yang dimulai dan pemindaian malware sesuai permintaan mendukung tag global. GuardDutyExcluded Untuk informasi selengkapnya, lihat [Opsi pindai dengan tag yang ditentukan pengguna](#).
- Retensi snapshot — Perlindungan Malware untuk EC2 menyediakan opsi untuk menyimpan snapshot volume Amazon EBS Anda di akun Anda. AWS Secara default, pengaturan ini dimatikan. Anda dapat memilih penyimpanan snapshot untuk pemindaian malware GuardDuty yang dimulai dan sesuai permintaan. Untuk informasi selengkapnya, lihat [Retensi snapshot](#).

Ketika GuardDuty menghasilkan satu atau lebih [Temuan yang memanggil pemindaian GuardDuty malware yang dimulai](#), maka aktivitas ini akan menjadi alasan GuardDuty untuk memulai pemindaian malware. Jika opsi pemindaian Anda tidak mengecualikan instance ini, maka GuardDuty akan memulai pemindaian.

Untuk memulai pemindaian malware On-Demand pada volume Amazon EBS yang terkait dengan EC2 instans Amazon, berikan Nama Sumber Daya Amazon (ARN) dari instans Amazon. EC2

Sebagai tanggapan untuk memulai pemindaian malware sesuai permintaan atau pemindaian malware yang GuardDuty dimulai secara otomatis, GuardDuty buat snapshot dari volume EBS yang relevan yang melekat pada sumber daya yang berpotensi terkena dampak, dan membagikannya dengan. [GuardDuty akun layanan](#) Saat GuardDuty membuat snapshot volume EBS Anda, ia menambahkan tag default yang disebut. GuardDutyScanId Tag ini GuardDuty membantu mengakses snapshot. Pastikan Anda tidak menghapus tag ini. Dari snapshot ini, GuardDuty buat volume replika EBS terenkripsi di akun layanan.

Setelah pemindaian selesai, GuardDuty hapus volume EBS replika terenkripsi dan snapshot volume EBS Anda. Secara default, pengaturan retensi snapshot dimatikan. Namun, snapshot dipertahankan jika [penguncian snapshot Amazon EBS](#) diaktifkan untuk mereka, terlepas dari hasil dan pengaturan pemindaian. GuardDuty tidak dapat mengubah pengaturan kunci snapshot Amazon EBS.

Daftar berikut menjelaskan perilaku retensi snapshot, terlepas dari penguncian snapshot EBS:

Retensi snapshot diaktifkan:

- Ketika malware ditemukan, GuardDuty simpan snapshot di Anda. Akun AWS
- Ketika tidak ada malware yang ditemukan, GuardDuty tidak menyimpan snapshot kecuali terkunci.

Retensi snapshot dimatikan (pengaturan default):

- Apakah malware ditemukan atau tidak, snapshot tidak dipertahankan.
- GuardDuty tidak dapat menghapus snapshot Amazon EBS yang terkunci.

GuardDuty akan mempertahankan setiap replika volume EBS di akun layanan hingga 55 jam. Jika ada pemadaman layanan, atau kegagalan dengan volume EBS replika dan pemindaian malware, GuardDuty akan mempertahankan volume EBS tersebut selama tidak lebih dari tujuh hari. Periode retensi volume yang diperpanjang adalah untuk melakukan triase dan mengatasi pemadaman atau kegagalan. GuardDuty Perlindungan Malware for EC2 akan menghapus replika volume EBS dari akun layanan setelah pemadaman atau kegagalan ditangani, atau setelah periode retensi yang diperpanjang berakhir.

Untuk informasi tentang metodologi deteksi GuardDuty malware dan mesin pemindaian yang digunakannya, lihat [GuardDuty mesin pemindai deteksi malware](#).

Volume Amazon EBS yang didukung untuk pemindaian malware

Di semua Wilayah AWS tempat GuardDuty mendukung fitur Perlindungan Malware untuk EC2 fitur, Anda dapat memindai volume Amazon EBS yang tidak terenkripsi atau dienkripsi. Anda dapat memiliki volume Amazon EBS yang dienkripsi dengan salah satu [Kunci yang dikelola AWS](#) atau kunci yang dikelola [pelanggan](#). Saat ini, beberapa Wilayah tempat Perlindungan Malware EC2 tersedia, dapat mendukung kedua cara untuk mengenkripsi volume Amazon EBS Anda, sementara yang lain hanya mendukung kunci yang dikelola pelanggan. Untuk informasi tentang Wilayah yang didukung, lihat dan [GuardDuty akun layanan oleh Wilayah AWS](#). Untuk informasi tentang Wilayah yang GuardDuty tersedia tetapi Perlindungan Malware untuk tidak EC2 tersedia, lihat [Ketersediaan fitur khusus wilayah](#).

Daftar berikut menjelaskan kunci yang GuardDuty menggunakan apakah volume Amazon EBS Anda dienkripsi atau tidak:

- Volume Amazon EBS yang tidak dienkripsi atau dienkripsi Kunci yang dikelola AWS- GuardDuty menggunakan kuncinya sendiri untuk mengenkripsi replika volume Amazon EBS.

Jika Wilayah Anda tidak mendukung pemindaian volume Amazon EBS yang dienkripsi dengan enkripsi [Amazon EBS secara default](#), maka Anda perlu mengubah kunci default untuk menjadi kunci yang dikelola pelanggan. Ini akan membantu GuardDuty mengakses volume EBS ini. Dengan memodifikasi kunci, bahkan volume EBS future akan dibuat dengan kunci yang diperbarui sehingga GuardDuty dapat mendukung pemindaian malware. Untuk langkah-langkah untuk mengubah kunci default, lihat [Ubah ID AWS KMS kunci default dari volume Amazon EBS](#) di bagian berikutnya.

- Volume Amazon EBS yang dienkripsi dengan kunci yang dikelola pelanggan — GuardDuty menggunakan kunci yang sama untuk mengenkripsi volume replika EBS. Untuk informasi tentang kebijakan terkait AWS KMS enkripsi yang didukung, lihat [Izin peran terkait layanan untuk Perlindungan Malware untuk EC2](#).

Ubah ID AWS KMS kunci default dari volume Amazon EBS

[Saat Anda menggunakan buat volume Amazon EBS dengan menggunakan enkripsi Amazon EBS, dan tidak menentukan ID AWS KMS kunci, volume Amazon EBS Anda akan dienkripsi dengan kunci default untuk enkripsi.](#) Saat Anda mengaktifkan enkripsi secara default, Amazon EBS akan secara otomatis mengenkripsi volume dan snapshot baru dengan menggunakan kunci KMS default Anda untuk enkripsi Amazon EBS.

Anda dapat memodifikasi kunci enkripsi default dan menggunakan kunci yang dikelola pelanggan untuk enkripsi Amazon EBS. Ini akan membantu GuardDuty mengakses volume Amazon EBS ini. Untuk mengubah ID kunci default EBS, tambahkan izin yang diperlukan berikut ke kebijakan IAM Anda — `ec2:modifyEbsDefaultKmsKeyId` Setiap volume Amazon EBS yang baru dibuat yang Anda pilih untuk dienkripsi tetapi tidak menentukan ID kunci KMS terkait, akan menggunakan ID kunci default. Gunakan salah satu metode berikut untuk memperbarui ID kunci default EBS:

Untuk mengubah ID kunci KMS default dari volume Amazon EBS

Lakukan salah satu tindakan berikut:

- Menggunakan API — Anda dapat menggunakan [ModifyEbsDefaultKmsKeyId](#) API. Untuk informasi tentang cara melihat status enkripsi volume, lihat [Membuat volume Amazon EBS](#).
- Menggunakan AWS CLI perintah - Contoh berikut memodifikasi ID kunci KMS default yang akan mengenkripsi volume Amazon EBS jika Anda tidak memberikan ID kunci KMS. Pastikan untuk mengganti Region dengan ID kunci KM Anda. Wilayah AWS

```
aws ec2 modify-ebs-default-kms-key-id --region us-west-2 --kms-key-id AKIAIOSFODNN7EXAMPLE
```

Perintah di atas akan menghasilkan output yang mirip dengan output berikut:

```
{  
  "KmsKeyId": "arn:aws:kms:us-west-2:444455556666:key/AKIAIOSFODNN7EXAMPLE"  
}
```

Untuk informasi selengkapnya, lihat [modify-ebs-default-kms-key-id](#).

Mengatur retensi snapshot dan cakupan EC2 pemindaian

Bagian ini menjelaskan cara menyesuaikan opsi pemindaian malware untuk EC2 instans Amazon Anda. Kustomisasi ini berlaku untuk pemindaian malware On-Demand dan yang diprakarsai oleh GuardDuty Anda dapat melakukan tindakan berikut:

- Aktifkan retensi snapshot — Saat diaktifkan sebelum pemindaian, snapshot Amazon EBS GuardDuty akan tetap GuardDuty terdeteksi berbahaya.
- Pilih EC2 instans Amazon mana yang akan dipindai — Gunakan tag untuk menyertakan atau mengecualikan EC2 instans Amazon tertentu dari pemindaian malware.

Retensi snapshot

GuardDuty memberi Anda opsi untuk menyimpan snapshot volume EBS Anda di akun Anda AWS . Secara default, pengaturan retensi snapshot dimatikan. Snapshot hanya akan dipertahankan jika pengaturan ini diaktifkan sebelum pemindaian dimulai.

Saat pemindaian dimulai, GuardDuty hasilkan replika volume EBS berdasarkan snapshot volume EBS Anda. Setelah pemindaian selesai dan pengaturan retensi snapshot di akun Anda sudah diaktifkan, snapshot volume EBS Anda akan dipertahankan hanya ketika malware ditemukan dan

dihasilkan. [Perlindungan Malware untuk EC2 menemukan jenis](#) Ketika tidak ada malware yang ditemukan, terlepas dari pengaturan snapshot Anda, GuardDuty secara otomatis menghapus snapshot volume EBS Anda kecuali [penguncian snapshot Amazon EBS telah diaktifkan pada snapshot](#) yang dibuat.

Biaya penggunaan snapshot

Selama pemindaian malware, seperti GuardDuty membuat snapshot volume Amazon EBS Anda, ada biaya penggunaan yang terkait dengan langkah ini. Jika Anda mengaktifkan pengaturan retensi snapshot untuk akun Anda, ketika malware ditemukan dan snapshot dipertahankan, Anda akan dikenakan biaya penggunaan untuk hal yang sama. Untuk informasi tentang biaya snapshot dan retensinya, lihat [harga Amazon EBS](#).

Sebagai akun GuardDuty administrator yang didelegasikan, hanya Anda yang dapat melakukan pembaruan ini atas nama akun anggota organisasi. Namun, jika akun anggota [dikelola dengan metode undangan](#), mereka dapat membuat perubahan ini sendiri. Untuk informasi selengkapnya, lihat [Akun administrator dan hubungan akun anggota](#).

Pilih metode akses pilihan Anda untuk mengaktifkan pengaturan retensi snapshot.

Console

1. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.
2. Di panel navigasi, di bawah Paket perlindungan, pilih Perlindungan Malware untuk EC2.
3. Pilih Pengaturan umum di bagian bawah konsol. Untuk mempertahankan snapshot, aktifkan retensi Snapshots.

API/CLI

Jalankan [UpdateMalwareScanSettings](#) untuk memperbarui konfigurasi saat ini untuk pengaturan retensi snapshot.

Atau, Anda dapat menjalankan AWS CLI perintah berikut untuk menyimpan snapshot secara otomatis saat Perlindungan GuardDuty Malware untuk EC2 menghasilkan temuan.

Pastikan untuk mengganti *detector-id* dengan valid Anda sendiri `detectorId`.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/> konsol, atau jalankan [ListDetectors](#) API. `detectorId`

```
aws guardduty update-malware-scan-settings --detector-id 60b8777933648562554d637e0e4bb3b2 --ebs-snapshot-preservation "RETENTION_WITH_FINDING"
```

Jika Anda ingin mematikan retensi snapshot, ganti `RETENTION_WITH_FINDING` dengan `NO_RETENTION`.

Opsi pindai dengan tag yang ditentukan pengguna

Dengan menggunakan GuardDuty pemindaian malware yang dimulai, Anda juga dapat menentukan tag untuk menyertakan atau mengecualikan EC2 instans Amazon dan volume Amazon EBS dari proses pemindaian dan deteksi ancaman. Anda dapat menyesuaikan setiap GuardDuty pemindaian malware yang dimulai dengan mengedit tag di daftar tag penyertaan atau pengecualian. Setiap daftar dapat mencakup hingga 50 tag.

Jika Anda belum memiliki tag yang ditentukan pengguna yang terkait dengan EC2 sumber daya Anda, lihat [Menandai EC2 sumber daya Amazon](#) Anda di EC2 Panduan Pengguna Amazon.

Note

Pemindaian malware sesuai permintaan tidak mendukung opsi pemindaian dengan tag yang ditentukan pengguna. Ini mendukung [GuardDutyExcludedTag global](#).

Untuk mengecualikan EC2 instance dari pemindaian malware

Jika Anda ingin mengecualikan EC2 instans Amazon atau volume Amazon EBS selama proses pemindaian, Anda dapat mengatur `GuardDutyExcluded` tag `true` untuk EC2 instans Amazon atau volume Amazon EBS apa pun, dan tidak GuardDuty akan memindainya. Untuk informasi selengkapnya tentang `GuardDutyExcluded` tag, lihat [izin peran terkait layanan untuk Perlindungan Malware untuk EC2](#). Anda juga dapat menambahkan tag EC2 instans Amazon ke daftar pengecualian. Jika Anda menambahkan beberapa tag ke daftar tag pengecualian, EC2 instans Amazon apa pun yang berisi setidaknya satu tag ini akan dikecualikan dari proses pemindaian malware.

Sebagai akun GuardDuty administrator yang didelegasikan, hanya Anda yang dapat melakukan pembaruan ini atas nama akun anggota organisasi. Namun, jika akun anggota [dikelola dengan](#)

[metode undangan](#), mereka dapat membuat perubahan ini sendiri. Untuk informasi selengkapnya, lihat [Akun administrator dan hubungan akun anggota](#).

Pilih metode akses pilihan Anda untuk menambahkan tag yang terkait dengan EC2 instans Amazon, ke daftar pengecualian.

Console

1. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.
2. Di panel navigasi, di bawah Paket perlindungan, pilih Perlindungan Malware untuk EC2.
3. Perluas bagian tag Inklusi/Pengecualian. Pilih Tambahkan tag.
4. Pilih tag Pengecualian dan kemudian pilih untuk Konfirmasi.
5. Tentukan tag **Key** dan **Value** pasangan yang ingin Anda kecualikan. Ini opsional untuk menyediakan **Value**. Setelah Anda menambahkan semua tag, pilih Simpan.



Important

Kunci dan nilai tag peka huruf besar dan kecil. Untuk informasi selengkapnya, lihat [Pembatasan tag](#) di Panduan EC2 Pengguna Amazon.

Jika nilai untuk kunci tidak disediakan dan EC2 instance ditandai dengan kunci yang ditentukan, EC2 instance ini akan dikecualikan dari proses pemindaian malware GuardDuty yang dimulai, terlepas dari nilai yang ditetapkan tag.

API/CLI

Jalankan [UpdateMalwareScanSettings](#) dengan mengecualikan EC2 instance atau beban kerja kontainer dari proses pemindaian.

Perintah AWS CLI contoh berikut menambahkan tag baru ke daftar tag pengecualian. Ganti contoh *detector-id* dengan valid Anda sendiri `detectorId`.

MapEquals adalah daftar Key Value /pasangan.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/> konsol, atau jalankan [ListDetectors](#) API. `detectorId`

```
aws guardduty update-malware-scan-settings --detector-id 60b8777933648562554d637e0e4bb3b2 --scan-resource-criteria '{"Exclude":{"EC2_INSTANCE_TAG" : {"MapEquals": [{ "Key": "TestKeyWithValue", "Value": "TestValue" }, {"Key":"TestKeyWithoutValue"} ]}}}' --ebs-snapshot-preservation "RETENTION_WITH_FINDING"
```

Important

Kunci dan nilai tag peka huruf besar dan kecil. Untuk informasi selengkapnya, lihat [Pembatasan tag](#) di Panduan EC2 Pengguna Amazon.

Untuk memasukkan EC2 instance dalam pemindaian malware

Jika Anda ingin memindai EC2 instance, tambahkan tagnya ke daftar inklusi. Saat Anda menambahkan tag ke daftar tag inklusi, EC2 instance yang tidak berisi tag yang ditambahkan akan dilewati dari pemindaian malware. Jika Anda menambahkan beberapa tag ke daftar tag inklusi, EC2 instance yang berisi setidaknya satu dari tag tersebut disertakan dalam pemindaian malware. Terkadang, sebuah EC2 instance dapat dilewati selama proses pemindaian karena alasan lain. Untuk informasi selengkapnya, lihat [Alasan melewatkan sumber daya selama pemindaian malware](#).

Sebagai akun GuardDuty administrator yang didelegasikan, hanya Anda yang dapat melakukan pembaruan ini atas nama akun anggota organisasi. Namun, jika akun anggota [dikelola dengan metode undangan](#), mereka dapat membuat perubahan ini sendiri. Untuk informasi selengkapnya, lihat [Akun administrator dan hubungan akun anggota](#).

Pilih metode akses pilihan Anda untuk menambahkan tag yang terkait dengan EC2 instance, ke daftar inklusi.

Console

1. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.
2. Di panel navigasi, di bawah Paket perlindungan, pilih Perlindungan Malware untuk EC2.
3. Perluas bagian tag Inklusi/Pengecualian. Pilih Tambahkan tag.
4. Pilih tag Inklusi dan kemudian pilih Konfirmasi.
5. Pilih Tambahkan tag inklusi baru dan tentukan tag **Key** dan **Value** pasangan yang ingin Anda sertakan. Ini opsional untuk menyediakan **Value**.

Setelah Anda menambahkan semua tag inklusi, pilih Simpan.

Jika nilai untuk kunci tidak diberikan, EC2 instance ditandai dengan kunci yang ditentukan, EC2 instance akan disertakan dalam proses Perlindungan Malware untuk EC2 pemindaian, terlepas dari nilai yang ditetapkan tag.

API/CLI

- Jalankan [UpdateMalwareScanSettings](#) untuk menyertakan EC2 instance atau beban kerja kontainer dalam proses pemindaian.

AWS CLI Contoh perintah berikut menambahkan tag baru ke daftar tag inklusi. Pastikan Anda mengganti contoh *detector-id* dengan valid Anda sendiri `detectorId`. Ganti contoh *TestKey* dan *TestValue* dengan Key dan Value pasangan tag yang terkait dengan EC2 sumber daya Anda.

MapEquals adalah daftar Key Value /pasangan.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan [ListDetectors](#) API. `detectorId`

```
aws guardduty update-malware-scan-settings --detector-id 60b8777933648562554d637e0e4bb3b2 --scan-resource-criteria '{"Include": {"EC2_INSTANCE_TAG" : {"MapEquals": [{"Key": "TestKeyWithValue", "Value": "TestValue" }, {"Key": "TestKeyWithoutValue"} ]}}}' --ebs-snapshot-preservation "RETENTION_WITH_FINDING"
```

Important

Kunci dan nilai tag peka huruf besar dan kecil. Untuk informasi selengkapnya, lihat [Pembatasan tag](#) di Panduan EC2 Pengguna Amazon.

Note

Mungkin diperlukan waktu hingga 5 menit GuardDuty untuk mendeteksi tag baru.

Kapan saja, Anda dapat memilih tag Inklusi atau tag Pengecualian tetapi tidak keduanya. Jika Anda ingin beralih di antara tag, pilih tag itu dari menu tarik-turun saat Anda menambahkan tag baru, dan Konfirmasikan pilihan Anda. Tindakan ini menghapus semua tag Anda saat ini.

GuardDutyExcludedTag global

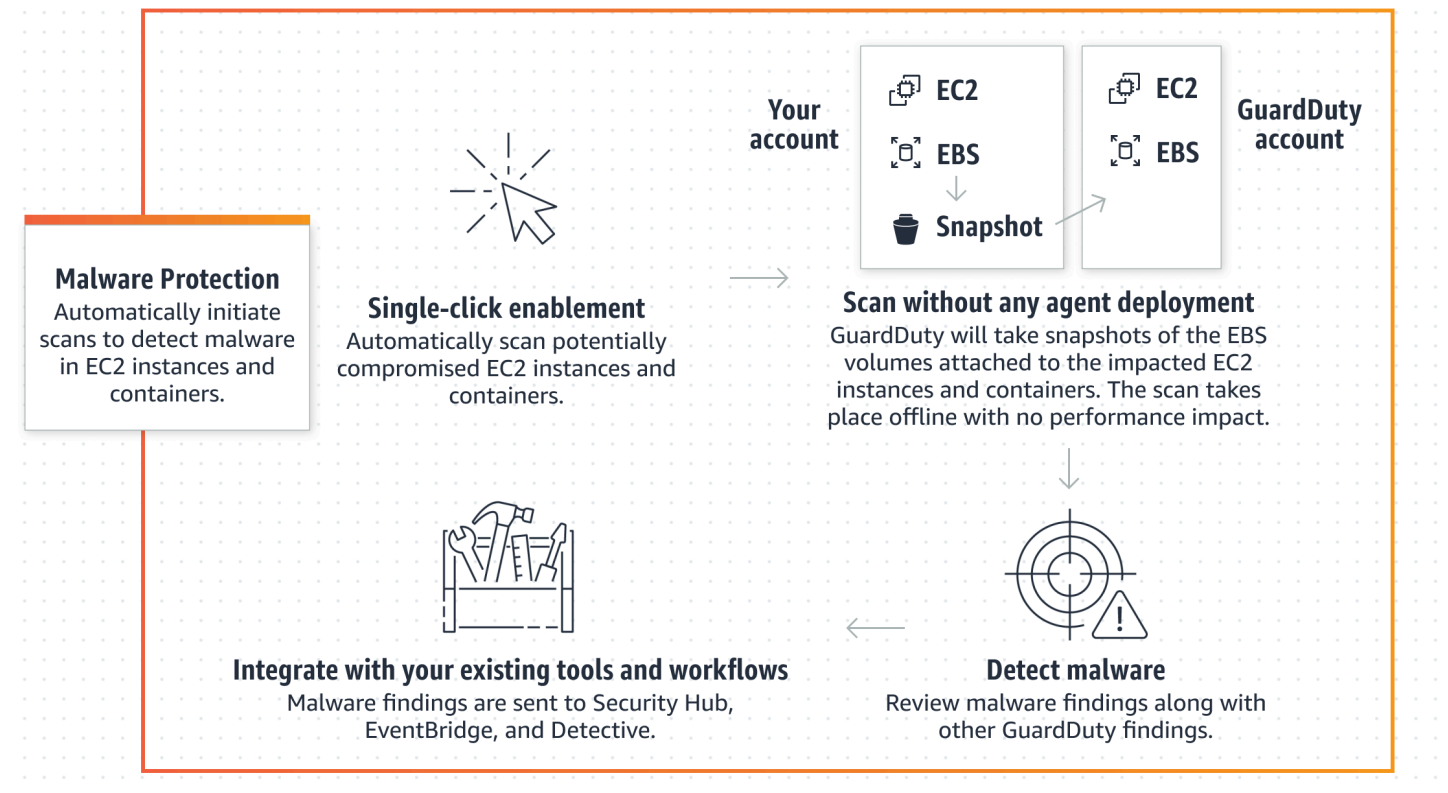
GuardDuty menggunakan kunci tag global, `GuardDutyExcluded`, yang dapat Anda tambahkan ke EC2 sumber daya Amazon Anda dan atur nilai `tag: true`. EC2 Sumber daya Amazon ini yang memiliki kunci tag dan pasangan nilai ini akan dikecualikan dari pemindaian malware. Kedua jenis pemindaian (pemindaian malware GuardDuty yang dimulai dan pemindaian malware On-Demand) mendukung tag global. Jika Anda memulai pemindaian malware sesuai permintaan di Amazon EC2, ID pemindaian akan dihasilkan. Namun, pemindaian akan dilewati dengan suatu `EXCLUDED_BY_SCAN_SETTINGS` alasan. Untuk informasi selengkapnya, lihat [Alasan melewati sumber daya selama pemindaian malware](#).

GuardDuty-pemindaian malware yang dimulai

Dengan GuardDuty pemindaian malware yang dimulai diaktifkan, kapan pun GuardDuty menghasilkan [Temuan yang memanggil pemindaian GuardDuty malware yang dimulai](#), pemindaian malware tanpa agen di volume Amazon Elastic Block Store (Amazon EBS) Elastic Block Store (Amazon EBS) yang dilampirkan ke sumber daya Amazon yang berpotensi terkena dampak akan dimulai. EC2 Sebelum pemindaian dimulai, Anda harus menyiapkan akun Anda untuk penyesuaian apa pun. Dengan opsi pemindaian, Anda dapat menambahkan tag inklusi yang terkait dengan sumber daya yang ingin Anda pindai, atau menambahkan tag pengecualian yang terkait dengan sumber daya yang ingin Anda lewati dari proses pemindaian. Inisiasi pemindaian otomatis akan selalu mempertimbangkan opsi pemindaian Anda. GuardDuty juga mendukung pasangan global `GuardDutyExcluded: true tag key:value`. Saat Anda menambahkan tag global ini ke EC2 sumber daya Amazon, GuardDuty akan memulai pemindaian dan kemudian melewatinya. Anda juga dapat memilih untuk mengaktifkan pengaturan retensi snapshot untuk mempertahankan snapshot volume EBS Anda di mana malware berpotensi terdeteksi. Untuk informasi selengkapnya tentang opsi pemindaian, tag pengecualian global, dan setelan snapshot, lihat [Mengatur retensi snapshot dan cakupan EC2 pemindaian](#).

Ketika GuardDuty menghasilkan beberapa temuan untuk EC2 sumber daya Amazon yang sama, GuardDuty akan dapat memulai pemindaian hanya setelah 24 jam telah berlalu sejak pemindaian malware terakhir GuardDuty yang dimulai. Untuk informasi tentang bagaimana volume Amazon EBS yang dilampirkan ke EC2 instans Amazon atau beban kerja penampung dipindai, lihat [Cara GuardDuty memindai volume EBS untuk deteksi malware](#).

Gambar berikut menjelaskan cara kerja pemindaian malware GuardDuty yang dimulai.



Untuk informasi tentang metodologi deteksi GuardDuty malware dan mesin pemindaian yang digunakannya, lihat [GuardDuty mesin pemindai deteksi malware](#).

Ketika malware ditemukan, GuardDuty hasilkan [Perlindungan Malware untuk EC2 menemukan jenis](#). Jika GuardDuty tidak menghasilkan temuan yang menunjukkan malware pada sumber daya yang sama, tidak ada GuardDuty pemindaian malware yang dimulai yang akan dipanggil. Anda juga dapat memulai pemindaian malware On-Demand pada sumber daya yang sama. Untuk informasi selengkapnya, lihat [Pemindaian malware sesuai permintaan di GuardDuty](#).

Uji coba gratis 30 hari dalam pemindaian GuardDuty malware yang dimulai

Anda dapat memilih untuk mengaktifkan atau menonaktifkan GuardDuty pemindaian malware yang dimulai untuk perangkat Akun AWS yang didukung Wilayah AWS kapan saja. Jika Anda memiliki organisasi, setiap akun anggota memiliki uji coba gratis 30 hari sendiri.

Untuk memahami cara kerja uji coba gratis 30 hari, pertimbangkan skenario berikut:

- Saat Anda mengaktifkan GuardDuty untuk pertama kalinya (GuardDuty akun baru), GuardDuty pemindaian malware yang dimulai juga akan diaktifkan dan disertakan dalam uji coba gratis 30 hari yang terkait dengan layanan. GuardDuty
- GuardDuty Akun yang ada dapat mengaktifkan GuardDuty pemindaian malware yang dimulai untuk pertama kalinya dengan uji coba gratis 30 hari. Saat Anda mengaktifkan fitur ini di Wilayah yang berbeda untuk pertama kalinya, Anda akan mendapatkan uji coba gratis 30 hari di Wilayah tersebut.
- Jika Anda telah menggunakan Perlindungan Malware Wilayah AWS sebelum rencana perlindungan ini dibagi menjadi dua jenis pemindaian — pemindaian malware yang GuardDuty dimulai dan pemindaian malware sesuai permintaan, Anda dapat terus menggunakan GuardDuty pemindaian malware yang dimulai dengan model harga yang sama. EC2 Wilayah AWS Jika Anda mengaktifkan GuardDuty pemindaian malware yang dimulai untuk pertama kalinya di Wilayah baru, akun Anda akan mendapatkan uji coba gratis 30 hari.

Note

Bahkan jika Anda berada dalam masa uji coba gratis 30 hari, biaya penggunaan standar untuk membuat snapshot volume Amazon EBS dan retensinya berlaku. Untuk informasi selengkapnya, lihat [harga Amazon EBS](#).

Mengaktifkan GuardDuty pemindaian malware yang dimulai di lingkungan beberapa akun

Dalam lingkungan beberapa akun, hanya akun GuardDuty administrator yang dapat mengaktifkan pemindaian malware GuardDuty yang dimulai atas nama akun anggota mereka. Selain itu, akun administrator yang mengelola akun anggota dengan AWS Organizations dukungan dapat memilih untuk mengaktifkan pemindaian malware GuardDuty yang dimulai secara otomatis pada semua akun yang ada dan yang baru di organisasi. Untuk informasi selengkapnya, lihat [Mengelola GuardDuty akun dengan AWS Organizations](#).

Membangun akses tepercaya untuk mengaktifkan GuardDuty pemindaian malware yang dimulai

Jika akun administrator GuardDuty yang didelegasikan tidak sama dengan akun manajemen di organisasi Anda, akun manajemen harus mengaktifkan pemindaian malware GuardDuty yang dimulai

untuk organisasi mereka. Dengan cara ini, akun administrator yang didelegasikan dapat membuat akun anggota [Izin peran terkait layanan untuk Perlindungan Malware untuk EC2](#) di yang dikelola. AWS Organizations

 Note

Sebelum Anda menetapkan akun GuardDuty administrator yang didelegasikan, lihat [Pertimbangan dan rekomendasi](#)

Pilih metode akses pilihan Anda untuk mengizinkan akun GuardDuty administrator yang didelegasikan mengaktifkan GuardDuty pemindaian malware yang dimulai untuk akun anggota di organisasi.

Console

1. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.

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

2. a. Jika Anda belum menetapkan akun GuardDuty administrator yang didelegasikan, maka:

Pada halaman Pengaturan, di bawah akun GuardDuty administrator yang didelegasikan, masukkan 12 digit **account ID** yang ingin Anda tetapkan untuk mengelola GuardDuty kebijakan di organisasi Anda. Pilih Delegasikan.
- b. i. Jika Anda telah menetapkan akun GuardDuty administrator yang didelegasikan yang berbeda dari akun manajemen, maka:

Pada halaman Pengaturan, di bawah Administrator Delegasi, aktifkan pengaturan Izin. Tindakan ini akan memungkinkan akun GuardDuty administrator yang didelegasikan untuk melampirkan izin yang relevan ke akun anggota dan mengaktifkan GuardDuty pemindaian malware yang dimulai di akun anggota ini.
- ii. Jika Anda telah menetapkan akun GuardDuty administrator yang didelegasikan yang sama dengan akun manajemen, maka Anda dapat langsung mengaktifkan GuardDuty pemindaian malware yang dimulai untuk akun anggota. Untuk informasi selengkapnya, lihat [Aktifkan GuardDuty pemindaian malware yang dimulai secara otomatis untuk semua akun anggota](#).

 Tip

Jika akun GuardDuty administrator yang didelegasikan berbeda dari akun manajemen Anda, Anda harus memberikan izin ke akun GuardDuty administrator yang didelegasikan untuk memungkinkan mengaktifkan GuardDuty pemindaian malware yang dimulai untuk akun anggota.

3. Jika Anda ingin mengizinkan akun GuardDuty administrator yang didelegasikan untuk mengaktifkan GuardDuty pemindaian malware yang dimulai untuk akun anggota di Wilayah lain, ubah Wilayah AWS, dan ulangi langkah-langkah di atas.

API/CLI

1. Dengan menggunakan kredensi akun manajemen Anda, jalankan perintah berikut:

```
aws organizations enable-aws-service-access --service-principal malware-protection.guardduty.amazonaws.com
```

2. (Opsional) untuk mengaktifkan GuardDuty pemindaian malware yang dimulai untuk akun manajemen yang bukan akun administrator yang didelegasikan, akun manajemen pertama-tama akan membuat secara [Izin peran terkait layanan untuk Perlindungan Malware untuk EC2](#) eksplisit di akun mereka, dan kemudian mengaktifkan GuardDuty pemindaian malware yang dimulai dari akun administrator yang didelegasikan, mirip dengan akun anggota lainnya.

```
aws iam create-service-linked-role --aws-service-name malware-protection.guardduty.amazonaws.com
```

3. Anda telah menetapkan akun GuardDuty administrator yang didelegasikan dalam yang dipilih Wilayah AWS saat ini. Jika Anda telah menetapkan akun sebagai akun GuardDuty administrator yang didelegasikan di satu wilayah, akun tersebut harus merupakan akun GuardDuty administrator yang didelegasikan di semua wilayah lain. Ulangi langkah di atas untuk semua Wilayah lainnya.

Mengkonfigurasi GuardDuty pemindaian malware yang dimulai untuk akun administrator yang didelegasikan GuardDuty

Pilih metode akses pilihan Anda untuk mengaktifkan atau menonaktifkan GuardDuty pemindaian malware yang dimulai untuk akun administrator yang didelegasikan GuardDuty .

Console

1. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.
2. Di panel navigasi, pilih Perlindungan Malware untuk EC2.
3. Pada EC2 halaman Perlindungan Malware untuk, pilih Edit di samping GuardDutypemindaian malware yang dimulai.
4. Lakukan salah satu tindakan berikut:

Menggunakan Aktifkan untuk semua akun

- Pilih Aktifkan untuk semua akun. Ini akan memungkinkan rencana perlindungan untuk semua GuardDuty akun aktif di AWS organisasi Anda, termasuk akun baru yang bergabung dengan organisasi.
- Pilih Simpan.

Menggunakan Konfigurasi akun secara manual

- Untuk mengaktifkan paket perlindungan hanya untuk akun akun GuardDuty administrator yang didelegasikan, pilih Konfigurasi akun secara manual.
- Pilih Aktifkan di bawah bagian akun GuardDuty administrator yang didelegasikan (akun ini).
- Pilih Simpan.

API/CLI

Jalankan operasi [updateDetector](#) API menggunakan ID detektor regional Anda sendiri dan meneruskan features objek name sebagai EBS_MALWARE_PROTECTION dan status sebagai ENABLED.

Anda dapat mengaktifkan GuardDuty pemindaian malware yang dimulai dengan menjalankan perintah berikut AWS CLI . Pastikan untuk menggunakan akun GuardDuty administrator yang didelegasikan valid *detector ID*.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan [ListDetectors](#) API. `detectorId`

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 /  
    --account-ids 55555555555 /  
    --features '[{"Name": "EBS_MALWARE_PROTECTION", "Status": "ENABLED"}]'
```

Aktifkan GuardDuty pemindaian malware yang dimulai secara otomatis untuk semua akun anggota

Pilih metode akses pilihan Anda untuk mengaktifkan fitur pemindaian malware GuardDuty yang dimulai untuk semua akun anggota. Ini termasuk akun anggota yang ada dan akun baru yang bergabung dengan organisasi.

Console

1. Masuk ke AWS Management Console dan buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.

Pastikan untuk menggunakan kredensial akun GuardDuty administrator yang didelegasikan.

2. Lakukan salah satu tindakan berikut:

Menggunakan Perlindungan Malware untuk EC2 halaman

1. Di panel navigasi, pilih Perlindungan Malware untuk EC2.
2. Pada EC2 halaman Perlindungan Malware untuk, pilih Edit di bagian GuardDutypemindaian malware yang dimulai.
3. Pilih Aktifkan untuk semua akun. Tindakan ini secara otomatis memungkinkan GuardDuty pemindaian malware yang dimulai untuk akun yang ada dan baru di organisasi.
4. Pilih Simpan.

Note

Mungkin diperlukan waktu hingga 24 jam untuk memperbarui konfigurasi akun anggota.

Menggunakan halaman Akun

1. Di panel navigasi, pilih Akun.
2. Pada halaman Akun, pilih Preferensi Aktifkan otomatis sebelum Tambahkan akun berdasarkan undangan.
3. Di jendela Kelola preferensi aktifkan otomatis, pilih Aktifkan untuk semua akun di bawah GuardDuty pemindaian malware yang dimulai.
4. Pada EC2 halaman Perlindungan Malware untuk, pilih Edit di bagian GuardDuty pemindaian malware yang dimulai.
5. Pilih Aktifkan untuk semua akun. Tindakan ini secara otomatis memungkinkan GuardDuty pemindaian malware yang dimulai untuk akun yang ada dan baru di organisasi.
6. Pilih Simpan.

Note

Mungkin diperlukan waktu hingga 24 jam untuk memperbarui konfigurasi akun anggota.

Menggunakan halaman Akun

1. Di panel navigasi, pilih Akun.
2. Pada halaman Akun, pilih Preferensi Aktifkan otomatis sebelum Tambahkan akun berdasarkan undangan.
3. Di jendela Kelola preferensi aktifkan otomatis, pilih Aktifkan untuk semua akun di bawah GuardDuty pemindaian malware yang dimulai.
4. Pilih Simpan.

Jika Anda tidak dapat menggunakan opsi Aktifkan untuk semua akun, lihat [Aktifkan pemindaian malware GuardDuty yang dimulai secara selektif untuk akun anggota](#).

API/CLI

- Untuk mengaktifkan GuardDuty pemindaian malware yang dimulai secara selektif untuk akun anggota Anda, jalankan operasi [updateMemberDetectors](#) API menggunakan milik Anda sendiri. *detector ID*
- Contoh berikut menunjukkan bagaimana Anda dapat mengaktifkan GuardDuty pemindaian malware yang dimulai untuk satu akun anggota. Untuk menonaktifkan akun anggota, ganti `ENABLED` dengan `DISABLED`.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan [ListDetectors](#) API. `detectorId`

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name": "EBS_MALWARE_PROTECTION", "Status": "ENABLED"}]'
```

Anda juga dapat melewati daftar akun yang IDs dipisahkan oleh spasi.

- Ketika kode telah berhasil dijalankan, daftar `UnprocessedAccounts` akan kembali kosong. Jika ada masalah dalam mengubah pengaturan detektor untuk suatu akun, ID akun tersebut akan dicantumkan bersama dengan ringkasan masalahnya.

Aktifkan GuardDuty pemindaian malware yang dimulai untuk semua akun anggota aktif yang ada

Pilih metode akses pilihan Anda untuk mengaktifkan GuardDuty pemindaian malware yang dimulai untuk semua akun anggota aktif yang ada di organisasi.

Untuk mengonfigurasi GuardDuty pemindaian malware yang dimulai untuk semua akun anggota aktif yang ada

1. Masuk ke AWS Management Console dan buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.

Masuk menggunakan kredensi akun GuardDuty administrator yang didelegasikan.

2. Di panel navigasi, pilih Perlindungan Malware untuk EC2.
3. Pada Perlindungan Malware for EC2, Anda dapat melihat status saat ini dari konfigurasi pemindaian malware GuardDuty yang dimulai. Di bawah bagian Akun anggota aktif, pilih Tindakan.
4. Dari menu tarik-turun Tindakan, pilih Aktifkan untuk semua akun anggota aktif yang ada.

5. Pilih Simpan.

Aktifkan otomatis GuardDuty pemindaian malware yang dimulai untuk akun anggota baru

Akun anggota yang baru ditambahkan harus Aktifkan GuardDuty sebelum memilih mengkonfigurasi GuardDuty pemindaian malware yang dimulai. Akun anggota yang dikelola oleh undangan dapat mengonfigurasi GuardDuty pemindaian malware yang dimulai secara manual untuk akun mereka. Untuk informasi selengkapnya, lihat [Step 3 - Accept an invitation](#).

Pilih metode akses pilihan Anda untuk mengaktifkan GuardDuty pemindaian malware yang dimulai untuk akun baru yang bergabung dengan organisasi Anda.

Console

Akun GuardDuty administrator yang didelegasikan dapat mengaktifkan GuardDuty pemindaian malware yang dimulai untuk akun anggota baru di organisasi, baik menggunakan halaman Perlindungan Malware untuk EC2 atau Akun.

Untuk mengaktifkan pemindaian malware GuardDuty yang dimulai secara otomatis untuk akun anggota baru

1. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.

Pastikan untuk menggunakan kredensial akun GuardDuty administrator yang didelegasikan.

2. Lakukan salah satu tindakan berikut:

- Menggunakan Perlindungan Malware untuk EC2 halaman:
 1. Di panel navigasi, pilih Perlindungan Malware untuk EC2.
 2. Pada EC2 halaman Perlindungan Malware untuk, pilih Edit dalam GuardDuty pemindaian malware yang dimulai.
 3. Pilih Konfigurasi akun secara manual.
 4. Pilih Aktifkan secara otomatis untuk akun anggota baru. Langkah ini memastikan bahwa setiap kali akun baru bergabung dengan organisasi Anda, GuardDuty pemindaian malware yang dimulai akan diaktifkan secara otomatis untuk akun mereka. Hanya akun GuardDuty administrator yang didelegasikan organisasi yang dapat mengubah konfigurasi ini.
 5. Pilih Simpan.
- Menggunakan halaman Akun:

1. Di panel navigasi, pilih Akun.
2. Pada halaman Akun, pilih Preferensi Aktifkan otomatis.
3. Di jendela Kelola preferensi aktifkan otomatis, pilih Aktifkan untuk akun baru di bawah GuardDuty pemindaian malware yang dimulai.
4. Pilih Simpan.

API/CLI

- Untuk mengaktifkan atau menonaktifkan GuardDuty pemindaian malware yang dimulai untuk akun anggota baru, jalankan operasi [UpdateOrganizationConfiguration](#) API menggunakan milik Anda sendiri. *detector ID*
- Contoh berikut menunjukkan bagaimana Anda dapat mengaktifkan GuardDuty pemindaian malware yang dimulai untuk satu akun anggota. Untuk menonaktifkannya, lihat [Aktifkan pemindaian malware GuardDuty yang dimulai secara selektif untuk akun anggota](#). Jika Anda tidak ingin mengaktifkannya untuk semua akun baru yang bergabung dengan organisasi, setel `AutoEnable` ke `NONE`.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan [ListDetectors](#) API. `detectorId`

```
aws guardduty update-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0 --AutoEnable --features '[{"Name": "EBS_MALWARE_PROTECTION", "AutoEnable": NEW}]'
```

Anda juga dapat melewati daftar akun yang IDs dipisahkan oleh spasi.

- Ketika kode telah berhasil dijalankan, daftar `UnprocessedAccounts` akan kembali kosong. Jika ada masalah dalam mengubah pengaturan detektor untuk suatu akun, ID akun tersebut akan dicantumkan bersama dengan ringkasan masalahnya.

Aktifkan pemindaian malware GuardDuty yang dimulai secara selektif untuk akun anggota

Pilih metode akses pilihan Anda untuk mengonfigurasi GuardDuty pemindaian malware yang dimulai untuk akun anggota secara selektif.

Console

1. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.
2. Di panel navigasi, pilih Akun.
3. Pada halaman Akun, tinjau kolom pemindaian malware yang GuardDuty dimulai untuk mengetahui status akun anggota Anda.
4. Pilih akun yang ingin Anda konfigurasi GuardDuty -initiated malware scan. Anda dapat memilih beberapa akun sekaligus.
5. Dari menu Edit paket perlindungan, pilih opsi yang sesuai untuk GuardDuty pemindaian malware yang dimulai.

API/CLI

Untuk mengaktifkan atau menonaktifkan GuardDuty pemindaian malware yang dimulai secara selektif untuk akun anggota Anda, jalankan operasi [updateMemberDetectors](#) API menggunakan milik Anda sendiri. *detector ID*

Contoh berikut menunjukkan bagaimana Anda dapat mengaktifkan GuardDuty pemindaian malware yang dimulai untuk satu akun anggota.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan [ListDetectors](#) API. `detectorId`

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
--account-ids 111122223333 --features '[{"Name": "EBS_MALWARE_PROTECTION",
"Status": "ENABLED"}]'
```

Anda juga dapat melewati daftar akun yang IDs dipisahkan oleh spasi.

Ketika kode telah berhasil dijalankan, daftar `UnprocessedAccounts` akan kembali kosong. Jika ada masalah dalam mengubah pengaturan detektor untuk suatu akun, ID akun tersebut akan dicantumkan bersama dengan ringkasan masalahnya.

Untuk mengaktifkan GuardDuty pemindaian malware yang dimulai secara selektif untuk akun anggota Anda, jalankan operasi [updateMemberDetectors](#) API menggunakan milik Anda sendiri. *detector ID* Contoh berikut menunjukkan bagaimana Anda dapat mengaktifkan GuardDuty pemindaian malware yang dimulai untuk satu akun anggota.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan [ListDetectors](#) API. `detectorId`

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
--account-ids 111122223333 --data-sources '{"MalwareProtection":
{"ScanEc2InstanceWithFindings":{"EbsVolumes":true}}}'
```

Anda juga dapat melewati daftar akun yang IDs dipisahkan oleh spasi.

Ketika kode telah berhasil dijalankan, daftar `UnprocessedAccounts` akan kembali kosong. Jika ada masalah dalam mengubah pengaturan detektor untuk suatu akun, ID akun tersebut akan dicantumkan bersama dengan ringkasan masalahnya.

Aktifkan GuardDuty pemindaian malware yang dimulai untuk akun yang ada di Organisasi yang dikelola melalui undangan

Perlindungan GuardDuty Malware untuk peran EC2 terkait layanan (SLR) harus dibuat di akun anggota. Akun administrator tidak dapat mengaktifkan fitur pemindaian malware GuardDuty yang dimulai di akun anggota yang tidak dikelola oleh AWS Organizations

Saat ini, Anda dapat melakukan langkah-langkah berikut melalui GuardDuty konsol di <https://console.aws.amazon.com/guardduty/> untuk mengaktifkan GuardDuty pemindaian malware yang dimulai untuk akun anggota yang ada.

Console

1. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.

Masuk menggunakan kredensi akun administrator Anda.

2. Di panel navigasi, pilih Akun.
3. Pilih akun anggota yang ingin Anda aktifkan pemindaian malware GuardDuty yang dimulai. Anda dapat memilih beberapa akun sekaligus.
4. Pilih Tindakan.
5. Pilih anggota Disassociate.
6. Di akun anggota Anda, pilih Perlindungan Malware di bawah Paket Perlindungan di panel navigasi.

7. Pilih Aktifkan GuardDuty pemindaian malware yang dimulai. GuardDuty akan membuat SLR untuk akun anggota. Untuk informasi lebih lanjut tentang SLR, lihat [izin peran terkait layanan untuk Perlindungan Malware untuk EC2](#).
8. Di akun administrator Anda, pilih Akun di panel navigasi.
9. Pilih akun anggota yang perlu ditambahkan kembali ke organisasi.
10. Pilih Tindakan dan kemudian, pilih Tambah anggota.

API/CLI

1. Gunakan akun administrator untuk menjalankan [DisassociateMembers](#) API pada akun anggota yang ingin mengaktifkan GuardDuty pemindaian malware yang dimulai.
2. Gunakan akun anggota Anda untuk memanggil [UpdateDetector](#) untuk mengaktifkan pemindaian GuardDuty malware yang dimulai.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan [ListDetectors](#) API. `detectorId`

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0
--data-sources '{"MalwareProtection":{"ScanEc2InstanceWithFindings":
{"EbsVolumes":true}}}'
```

3. Gunakan akun administrator untuk menjalankan [CreateMembers](#) API guna menambahkan anggota kembali ke organisasi.

Mengaktifkan GuardDuty pemindaian malware yang dimulai untuk akun mandiri

Akun mandiri memiliki keputusan untuk mengaktifkan atau menonaktifkan rencana perlindungan di akun mereka Akun AWS secara spesifik. Wilayah AWS

Jika akun Anda dikaitkan dengan akun GuardDuty administrator melalui AWS Organizations, atau dengan metode undangan, bagian ini tidak berlaku untuk akun Anda. Untuk informasi selengkapnya, lihat [Mengaktifkan GuardDuty pemindaian malware yang dimulai di lingkungan beberapa akun](#).

Setelah Anda mengaktifkan GuardDuty pemindaian malware yang dimulai, GuardDuty akan memulai pemindaian malware dari volume Amazon EBS yang dilampirkan ke EC2 instans Amazon yang

terlibat dalam file. GuardDuty Untuk daftar temuan yang memulai pemindaian malware, lihat [Temuan yang memanggil pemindaian GuardDuty malware yang dimulai](#).

Pilih metode akses pilihan Anda untuk mengonfigurasi GuardDuty pemindaian malware yang dimulai untuk akun mandiri.

Console

1. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.
2. Di panel navigasi, di bawah Paket perlindungan, pilih Perlindungan Malware untuk EC2.
3. EC2 Panel Perlindungan Malware untuk mencantumkan status pemindaian malware GuardDuty yang dimulai saat ini untuk akun Anda. Pilih Aktifkan untuk mengaktifkan GuardDuty pemindaian malware yang dimulai di akun ini.
4. Pilih Simpan untuk mengonfirmasi pilihan Anda.

API/CLI

Jalankan operasi [updateDetector](#) API menggunakan ID detektor regional Anda sendiri dan teruskan dataSources objek dengan EbsVolumes disetel ke true.

Anda juga dapat mengaktifkan pemindaian malware GuardDuty -initiated menggunakan AWS CLI dengan menjalankan perintah berikut AWS CLI . Pastikan untuk menggunakan valid Anda sendiri *detector ID*.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/> konsol, atau jalankan [ListDetectors](#) API. detectorId

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features [{"Name" : "EBS_MALWARE_PROTECTION", "Status" : "ENABLED"}]
```

Temuan yang memanggil pemindaian GuardDuty malware yang dimulai

Ketika GuardDuty mendeteksi perilaku mencurigakan yang menunjukkan malware pada EC2 instans Amazon atau beban kerja kontainer yang berjalan pada EC2 instans Amazon, GuardDuty akan menghasilkan temuan. Jika temuan yang dihasilkan ini termasuk dalam daftar GuardDuty temuan berikut, maka secara otomatis GuardDuty akan memulai pemindaian malware pada volume Amazon EBS yang melekat pada EC2 instans Amazon yang terlibat dalam temuan tersebut. Setelah scan,

jika GuardDuty mendeteksi malware, maka itu juga akan menghasilkan satu atau lebih [Perlindungan Malware untuk EC2 menemukan jenis](#).

Jika salah satu GuardDuty temuan berikut dihasilkan di akun Anda, secara otomatis GuardDuty akan memulai pemindaian malware dalam volume Amazon EBS dari instans Amazon EC2 yang berpotensi dikompromikan.

- [Backdoor:EC2/C&CActivity.B](#)
- [Backdoor:EC2/C&CActivity.B!DNS](#)
- [Backdoor:EC2/DenialOfService.Dns](#)
- [Backdoor:EC2/DenialOfService.Tcp](#)
- [Backdoor:EC2/DenialOfService.Udp](#)
- [Backdoor:EC2/DenialOfService.UdpOnTcpPorts](#)
- [Backdoor:EC2/DenialOfService.UnusualProtocol](#)
- [Backdoor:EC2/Spambot](#)
- [CryptoCurrency:EC2/BitcoinTool.B](#)
- [CryptoCurrency:EC2/BitcoinTool.B!DNS](#)
- [DefenseEvasion:Runtime/PtraceAntiDebugging](#)
- [DefenseEvasion:Runtime/SuspiciousCommand](#)
- [Execution:Runtime/MaliciousFileExecuted](#)
- [Execution:Runtime/SuspiciousCommand](#)
- [Execution:Runtime/SuspiciousShellCreated](#)
- [Execution:Runtime/SuspiciousTool](#)
- [Impact:EC2/AbusedDomainRequest.Reputation](#)
- [Impact:EC2/BitcoinDomainRequest.Reputation](#)
- [Impact:EC2/MaliciousDomainRequest.Reputation](#)
- [Impact:EC2/PortSweep](#)
- [Impact:EC2/SuspiciousDomainRequest.Reputation](#)
- [Impact:EC2/WinRMBruteForce](#)(Hanya keluar)
- [PrivilegeEscalation:Runtime/ElevationToRoot](#)
- [Recon:EC2/Portscan](#)

- [Trojan:EC2/BlackholeTraffic](#)
- [Trojan:EC2/BlackholeTraffic!DNS](#)
- [Trojan:EC2/DGADomainRequest.B](#)
- [Trojan:EC2/DGADomainRequest.C!DNS](#)
- [Trojan:EC2/DNSDataExfiltration](#)
- [Trojan:EC2/DriveBySourceTraffic!DNS](#)
- [Trojan:EC2/DropPoint](#)
- [Trojan:EC2/DropPoint!DNS](#)
- [Trojan:EC2/PhishingDomainRequest!DNS](#)
- [UnauthorizedAccess:EC2/RDPBruteForce](#)(Hanya keluar)
- [UnauthorizedAccess:EC2/SSHBruteForce](#)(Hanya keluar)
- [UnauthorizedAccess:EC2/TorClient](#)
- [UnauthorizedAccess:EC2/TorRelay](#)
- [Backdoor:Runtime/C&CAActivity.B](#)
- [Backdoor:Runtime/C&CAActivity.B!DNS](#)
- [CryptoCurrency:Runtime/BitcoinTool.B](#)
- [CryptoCurrency:Runtime/BitcoinTool.B!DNS](#)
- [Execution:Runtime/NewBinaryExecuted](#)
- [Execution:Runtime/NewLibraryLoaded](#)
- [Execution:Runtime/ReverseShell](#)
- [Impact:Runtime/AbusedDomainRequest.Reputation](#)
- [Impact:Runtime/BitcoinDomainRequest.Reputation](#)
- [Impact:Runtime/CryptoMinerExecuted](#)
- [Impact:Runtime/MaliciousDomainRequest.Reputation](#)
- [Impact:Runtime/SuspiciousDomainRequest.Reputation](#)
- [PrivilegeEscalation:Runtime/CGroupsReleaseAgentModified](#)
- [PrivilegeEscalation:Runtime/ContainerMountsHostDirectory](#)
- [PrivilegeEscalation:Runtime/DockerSocketAccessed](#)

- [PrivilegeEscalation:Runtime/RuncContainerEscape](#)
- [PrivilegeEscalation:Runtime/UserfaultfdUsage](#)
- [Trojan:Runtime/BlackholeTraffic](#)
- [Trojan:Runtime/BlackholeTraffic!DNS](#)
- [Trojan:Runtime/DropPoint](#)
- [Trojan:Runtime/DropPoint!DNS](#)
- [Trojan:Runtime/DGADomainRequest.C!DNS](#)
- [Trojan:Runtime/DriveBySourceTraffic!DNS](#)
- [Trojan:Runtime/PhishingDomainRequest!DNS](#)
- [UnauthorizedAccess:Runtime/MetadataDNSRebind](#)

Pemindaian malware sesuai permintaan di GuardDuty

Pemindaian malware sesuai permintaan membantu Anda mendeteksi keberadaan malware di volume Amazon Elastic Block Store (Amazon EBS) yang dilampirkan ke instans Amazon Anda. EC2 Tanpa konfigurasi yang diperlukan, Anda dapat memulai pemindaian malware sesuai permintaan dengan memberikan Nama Sumber Daya Amazon (ARN) dari instans EC2 Amazon yang ingin Anda pindai. Anda dapat memulai pemindaian malware sesuai permintaan baik melalui GuardDuty konsol atau API. Sebelum memulai pemindaian malware sesuai permintaan, Anda dapat mengatur pengaturan pilihan [Retensi snapshot](#) Anda. Skenario berikut dapat membantu Anda mengidentifikasi kapan harus menggunakan jenis pemindaian malware On-Demand dengan GuardDuty:

- Anda ingin mendeteksi keberadaan malware di EC2 instans Amazon Anda tanpa mengaktifkan pemindaian malware GuardDuty yang dimulai.
- Anda telah mengaktifkan GuardDuty pemindaian malware yang dimulai dan pemindaian dipanggil secara otomatis. Setelah mengikuti perbaikan yang disarankan untuk Perlindungan Malware yang dihasilkan untuk jenis EC2 pencarian, jika Anda ingin memulai pemindaian pada sumber daya yang sama, Anda dapat memulai pemindaian malware sesuai permintaan setelah 1 jam berlalu dari waktu mulai pemindaian sebelumnya.

Pemindaian malware sesuai permintaan tidak mengharuskan 24 jam berlalu sejak pemindaian malware sebelumnya dimulai. Seharusnya satu jam berlalu sebelum memulai pemindaian malware On-Demand pada sumber daya yang sama. Untuk menghindari duplikasi pemindaian malware pada EC2 contoh yang sama, lihat [Memindai ulang instans Amazon yang dipindai sebelumnya EC2](#).

 Note

Pemindaian malware sesuai permintaan tidak termasuk dalam periode uji coba gratis 30 hari dengan. GuardDuty Biaya penggunaan berlaku untuk total volume Amazon EBS yang dipindai untuk setiap pemindaian malware. Untuk informasi selengkapnya, lihat [GuardDuty harga Amazon](#). Untuk informasi tentang biaya pembuatan snapshot volume Amazon EBS dan retensinya, lihat harga [Amazon EBS](#).

Cara kerja pemindaian malware sesuai permintaan

Dengan pemindaian malware sesuai permintaan, Anda dapat memulai permintaan pemindaian malware untuk EC2 instans Amazon Anda bahkan saat sedang digunakan. Setelah Anda memulai pemindaian malware sesuai permintaan, GuardDuty buat snapshot volume Amazon EBS yang dilampirkan ke instans Amazon EC2 yang Nama Sumber Daya Amazon (ARN) disediakan untuk pemindaian. Selanjutnya, GuardDuty bagikan foto-foto ini dengan. [GuardDuty akun layanan](#) GuardDuty membuat volume EBS replika terenkripsi dari snapshot tersebut di akun layanan. GuardDuty Untuk informasi selengkapnya tentang bagaimana volume Amazon EBS dipindai, lihat. [Cara GuardDuty memindai volume EBS untuk deteksi malware](#)

 Note

GuardDuty membuat snapshot dari data yang telah ditulis ke volume Amazon EBS pada point-in-time saat Anda memulai pemindaian malware On-Demand.

Jika malware ditemukan dan Anda telah mengaktifkan pengaturan retensi snapshot, snapshot volume EBS Anda secara otomatis disimpan di Anda. Akun AWS Pemindaian malware sesuai permintaan menghasilkan. [Perlindungan Malware untuk EC2 menemukan jenis](#) Jika malware tidak ditemukan, maka terlepas dari pengaturan retensi snapshot, snapshot volume EBS Anda akan dihapus.

GuardDuty menggunakan kunci tag global,GuardDutyExcluded, yang dapat Anda tambahkan ke EC2 sumber daya Amazon Anda dan atur nilai tagtrue. EC2 Sumber daya Amazon ini yang memiliki kunci tag dan pasangan nilai ini akan dikecualikan dari pemindaian malware. Kedua jenis pemindaian (pemindaian malware GuardDuty yang dimulai dan pemindaian malware On-Demand) mendukung tag global. Jika Anda memulai pemindaian malware sesuai permintaan di Amazon EC2, ID pemindaian akan dihasilkan. Namun, pemindaian akan dilewati dengan suatu

EXCLUDED_BY_SCAN_SETTINGS alasan. Untuk informasi selengkapnya, lihat [Alasan melewati sumber daya selama pemindaian malware](#).

Memulai pemindaian malware sesuai permintaan GuardDuty

Bagian ini menyediakan daftar prasyarat sebelum memulai pemindaian malware sesuai permintaan dan langkah-langkah untuk memulai pemindaian pada sumber daya untuk pertama kalinya.

Sebagai akun GuardDuty administrator, Anda dapat memulai pemindaian malware sesuai permintaan atas nama akun anggota aktif Anda yang memiliki prasyarat berikut di akun mereka. Akun mandiri dan akun anggota aktif juga GuardDuty dapat memulai pemindaian malware sesuai permintaan untuk instance Amazon EC2 mereka sendiri.

Prasyarat

Sebelum Anda memulai pemindaian malware sesuai permintaan, akun Anda harus memenuhi prasyarat berikut:

- GuardDuty harus diaktifkan di Wilayah AWS tempat Anda ingin memulai pemindaian malware sesuai permintaan.
- Pastikan bahwa [AWS kebijakan terkelola: AmazonGuardDutyFullAccess_v2 \(disarankan\)](#) terpasang ke pengguna IAM atau peran IAM. Anda akan memerlukan kunci akses dan kunci rahasia yang terkait dengan pengguna IAM atau peran IAM.
- Sebagai akun GuardDuty administrator yang didelegasikan, Anda memiliki opsi untuk memulai pemindaian malware sesuai permintaan atas nama akun anggota yang aktif.
- Sebelum Anda memulai pemindaian malware sesuai permintaan, pastikan tidak ada pemindaian yang dimulai pada sumber daya yang sama dalam 1 jam terakhir; jika tidak, itu akan dihapus. Untuk informasi selengkapnya, lihat [Memindai ulang instans Amazon yang dipindai sebelumnya EC2](#).
- Jika Anda adalah akun anggota yang tidak memilikinya [izin peran terkait layanan untuk Perlindungan Malware untuk EC2](#), maka memulai pemindaian malware sesuai permintaan untuk EC2 instance Amazon milik akun Anda, akan secara otomatis membuat SLR untuk Perlindungan Malware. EC2

Important

Pastikan tidak ada yang menghapus [izin SLR untuk Perlindungan Malware EC2](#) saat pemindaian malware masih berlangsung. Pemindaian malware ini dapat dimulai oleh

GuardDuty atau dimulai sesuai permintaan. Menghapus SLR akan mencegah pemindaian selesai dengan sukses, dan memberikan hasil pemindaian yang pasti.

Mulai pemindaian malware sesuai permintaan

Anda dapat memulai pemindaian malware sesuai permintaan di akun Anda melalui GuardDuty konsol atau dengan menggunakan AWS CLI. Anda harus memberikan Nama Sumber Daya EC2 Amazon (ARN) yang ingin Anda mulai pemindaian. Langkah-langkah terperinci disediakan di konsol dan AWS CLI API/instruksi di bagian berikut.

Pilih metode akses pilihan Anda untuk memulai pemindaian malware sesuai permintaan.

Console

1. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.
2. Mulai pemindaian menggunakan salah satu opsi berikut:
 - a. Menggunakan Perlindungan Malware untuk EC2 halaman:
 - i. Di panel navigasi, di bawah Paket perlindungan, pilih Perlindungan Malware untuk EC2.
 - ii. Pada EC2 halaman Perlindungan Malware untuk, berikan EC2 contoh Amazon ARN ¹ yang ingin Anda mulai pemindaian.
 - b. Menggunakan halaman Pemindaian Malware:
 - i. Di panel navigasi, pilih Pemindaian Malware.
 - ii. Pilih Mulai pemindaian sesuai permintaan dan berikan ^{ARN} 1 EC2 instans Amazon yang ingin Anda mulai pemindaian.
 - iii. Jika ini adalah pemindaian ulang, pilih ID EC2 instans Amazon di halaman Pemindaian Malware.

Perluas dropdown Mulai pemindaian sesuai permintaan dan pilih Pindai ulang instance yang dipilih.

3. Setelah Anda berhasil memulai pemindaian menggunakan salah satu metode, ID pemindaian akan dihasilkan. Anda dapat menggunakan ID pemindaian ini untuk melacak kemajuan pemindaian. Untuk informasi selengkapnya, lihat [Memantau status dan hasil pemindaian malware](#).

API/CLI

Invoke [StartMalwareScan](#) yang menerima EC2 instans Amazon ¹ yang Anda inginkan untuk memulai pemindaian malware sesuai permintaan. resourceArn

```
aws guardduty start-malware-scan --resource-arn "arn:aws:ec2:us-east-1:555555555555:instance/i-b188560f"
```

Setelah Anda berhasil memulai pemindaian, StartMalwareScan mengembalikan filescanId. [DescribeMalwareScans](#) Memanggil memantau kemajuan pemindaian yang dimulai.

¹ Untuk informasi tentang format ARN EC2 instans Amazon Anda, lihat [Nama Sumber Daya Amazon \(ARN\)](#). Untuk EC2 instans Amazon, Anda dapat menggunakan contoh format ARN berikut dengan mengganti nilai untuk partisi, Wilayah Akun AWS, ID, dan ID instans EC2 Amazon. Untuk informasi tentang panjang ID instans Anda, lihat [Sumber daya IDs](#).

```
arn:aws:ec2:us-east-1:555555555555:instance/i-b188560f
```

AWS Organizations kebijakan kontrol layanan - Akses ditolak

Menggunakan [kebijakan kontrol Layanan \(SCPs\)](#) di AWS Organizations, akun GuardDuty administrator yang didelegasikan dapat membatasi izin dan menolak tindakan seperti memulai pemindaian malware sesuai permintaan untuk EC2 instans Amazon yang dimiliki oleh akun Anda.

Sebagai akun GuardDuty anggota, saat Anda memulai pemindaian malware sesuai permintaan untuk EC2 instans Amazon Anda, Anda mungkin menerima kesalahan. Anda dapat terhubung dengan akun manajemen untuk memahami mengapa SCP disiapkan untuk akun anggota Anda. Untuk informasi selengkapnya, lihat [efek SCP pada izin](#).

Memindai ulang instans Amazon yang dipindai sebelumnya EC2

Baik pemindaian dimulai atau GuardDuty dimulai sesuai permintaan, Anda dapat memulai pemindaian malware sesuai permintaan baru pada EC2 instans Amazon yang sama setelah 1 jam dari waktu mulai pemindaian malware sebelumnya. Jika pemindaian malware baru dimulai dalam waktu 1 jam sejak inisiasi pemindaian malware sebelumnya, permintaan Anda akan menghasilkan kesalahan berikut, dan tidak ada ID pemindaian yang akan dihasilkan untuk permintaan ini.

A scan was started on this resource recently. You can request a scan on the same resource one hour after the previous scan start time.

Langkah-langkah untuk memindai ulang instance tetap sama dengan memulai pemindaian malware sesuai permintaan untuk pertama kalinya. Untuk informasi tentang langkah-langkahnya, lihat [Mulai pemindaian malware sesuai permintaan](#).

Untuk melacak status pemindaian malware, lihat [Memantau status pemindaian dan hasil dalam Perlindungan Malware untuk EC2](#).

Memantau status pemindaian dan hasil dalam Perlindungan Malware untuk EC2

Setelah pemindaian malware dimulai pada EC2 instans Amazon, GuardDuty berikan bidang status dan hasil secara otomatis. Anda dapat memantau status melalui transisi, dan melihat apakah malware terdeteksi. Tabel berikut memberikan nilai yang mungkin terkait dengan pemindaian malware.

Nilai potensial

Running,Completed ,Skipped, atau Failed

Clean atau Infected

GuardDuty initiated atau On demand

* Hasil pemindaian hanya diisi ketika status pemindaian menjadi. Completed Hasil pemindaian Infected berarti GuardDuty mendeteksi keberadaan malware.

Hasil pemindaian untuk setiap pemindaian malware memiliki periode retensi 90 hari. Pilih metode akses pilihan Anda untuk melacak status pemindaian malware Anda.

Console

1. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.
2. Di panel navigasi, pilih pemindaian EC2 malware.
3. Anda dapat memfilter pemindaian malware dengan Properti berikut yang tersedia di bilah pencarian filter.
 - Scan ID — Pengidentifikasi unik yang terkait dengan pemindaian EC2 malware.
 - ID Akun — Akun AWS ID tempat pemindaian malware dimulai.
 - EC2 instance ARN — Amazon Resource Name (ARN) yang terkait dengan EC2 instans Amazon yang terkait dengan pemindaian.
 - Status pemindaian — Status pemindaian volume EBS, seperti Running, Skipped, dan Completed
 - Jenis pemindaian - Menunjukkan apakah ini pemindaian malware sesuai permintaan atau pemindaian malware yang GuardDuty dimulai.

API/CLI

- Setelah pemindaian malware memiliki hasil pemindaian, gunakan [DescribeMalwareScans](#) untuk memfilter pemindaian malware berdasarkan `EC2_INSTANCE_ARN`, `SCAN_ID`, `ACCOUNT_ID`, `SCAN_TYPE` `GUARDDUTY_FINDING_ID`, `SCAN_STATUS`, dan `SCAN_START_TIME`.

Kriteria `GUARDDUTY_FINDING_ID` filter `SCAN_TYPE` tersedia saat GuardDuty dimulai.

- Anda dapat mengubah contoh pada perintah *filter-criteria* di bawah ini. Saat ini, Anda dapat memfilter berdasarkan satu CriterionKey per satu. Pilihan untuk CriterionKey adalah `EC2_INSTANCE_ARN`, `SCAN_ID`, `ACCOUNT_ID`, `SCAN_TYPE`, `GUARDDUTY_FINDING_ID`, `SCAN_STATUS`, dan `SCAN_START_TIME`.

Anda dapat mengubah *max-results* (hingga 50) dan *sort-criteria*. AttributeName `scanStartTime` wajib dan harus `scanStartTime`.

Dalam contoh berikut, nilai-nilai di *red* adalah placeholder. Ganti dengan nilai yang sesuai untuk akun Anda. Misalnya, ganti contoh `detector-id` *60b8777933648562554d637e0e4bb3b2* dengan valid Anda sendiri `detector-id`. Jika Anda menggunakan yang sama CriterionKey seperti di bawah ini, pastikan untuk mengganti contoh `EqualsValue` dengan valid Anda sendiri AWS *scan-id*.

```
aws guardduty describe-malware-scans --detector-id 60b8777933648562554d637e0e4bb3b2 --max-results 1 --sort-criteria '{"AttributeName": "scanStartTime", "OrderBy": "DESC"}' --filter-criteria '{"FilterCriterion":[{"CriterionKey":"SCAN_ID", "FilterCondition":{"EqualsValue":"123456789012"}}] }'
```

- Respons dari perintah ini menampilkan maksimal satu hasil dengan rincian tentang sumber daya yang terpengaruh dan temuan malware (jikaInfected).

GuardDuty akun layanan oleh Wilayah AWS

Saat snapshot dibuat dan dibagikan dengan akun GuardDuty layanan, acara baru akan dibuat di CloudTrail log Anda. Acara ini menentukan yang sesuai snapshotId dan userId (akun GuardDuty layanan untuk itu Wilayah AWS). Untuk informasi selengkapnya, lihat [Cara GuardDuty memindai volume EBS untuk deteksi malware](#).

Contoh berikut adalah cuplikan dari CloudTrail peristiwa yang menunjukkan badan permintaan untuk permintaan: ModifySnapshotAttribute

```
{
  "requestParameters": {
    "snapshotId": "snap-1234567890abcdef0",
    "createVolumePermission": {
      "add": {
        "items": [
          {
            "userId": "111122223333"
          }
        ]
      }
    },
    "attributeType": "CREATE_VOLUME_PERMISSION"
  }
}
```

Tabel berikut menunjukkan akun GuardDuty layanan untuk setiap Wilayah. userIdIni adalah akun GuardDuty layanan dan tergantung pada Wilayah yang dipilih.

Wilayah AWS	Kode Wilayah	GuardDuty ID akun layanan (userId)
AS Timur (Virginia Utara)	us-east-1	652050842985

Wilayah AWS	Kode Wilayah	GuardDuty ID akun layanan (userId)
AS Timur (Ohio)	us-east-2	178123968615
AS Barat (California Utara)	us-west-1	669213148797
AS Barat (Oregon)	us-west-2	447226417196
Asia Pasifik (Mumbai)	ap-south-1	913179291432
Asia Pasifik (Osaka)	ap-northeast-3	089661699081
Asia Pasifik (Seoul)	ap-northeast-2	039163547507
Asia Pasifik (Tokyo)	ap-northeast-1	874749492622
Asia Pasifik (Singapura)	ap-southeast-1	247460962669
Asia Pasifik (Sydney)	ap-southeast-2	124839743349
Kanada (Pusat)	ca-central-1	175877067165
Kanada Barat (Calgary)	ca-west-1	894794104037
Eropa (Frankfurt)	eu-central-1	002294850712
Eropa (Irlandia)	eu-west-1	283769539786
Eropa (London)	eu-west-2	310125036783
Eropa (Paris)	eu-west-3	866607715269
Eropa (Stockholm)	eu-north-1	693780578038
Tiongkok (Beijing)	cn-north-1	448721096076
Tiongkok (Ningxia)	cn-northwest-1	480864352451
Amerika Selatan (Sao Paulo)	sa-east-1	546914126324

Wilayah AWS	Kode Wilayah	GuardDuty ID akun layanan (userId)
Asia Pasifik (Hyderabad) (Keikutsertaan)	ap-south-2	682251015962
Asia Pasifik (Melbourne) (Keikutsertaan)	ap-southeast-4	353488359550
Asia Pasifik (Malaysia) (Keikutsertaan)	ap-southeast-5	009160069308
Asia Pasifik (Thailand) (Keikutsertaan)	ap-southeast-7	941377115582
Eropa (Spanyol) (Opt-in)	eu-south-2	936182149045
Eropa (Zurich) (Opt-in)	eu-central-2	867642063380
Israel (Tel Aviv) (Keikutsertaan)	il-central-1	619233833001
Eropa (Milan) (Opt-in)	eu-south-1	977238331021
Asia Pasifik (Hong Kong) (Keikutsertaan)	ap-east-1	249472122084
Timur Tengah (Bahrain) (Opt-in)	me-south-1	404001805210
Afrika (Cape Town) (Opt-in)	af-south-1	957664736811
Asia Pasifik (Jakarta) (Keikutsertaan)	ap-southeast-3	452118225523
Timur Tengah (UEA) (Opt-in)	me-central-1	828603743433
Meksiko (Tengah) (Opt-in)	mx-central-1	557690616787

Wilayah AWS	Kode Wilayah	GuardDuty ID akun layanan (userId)
AWS GovCloud (AS-Timur)	us-gov-east-1	226283551151
AWS GovCloud (AS-Barat)	us-gov-west-1	226300430612

Kuota dalam Perlindungan Malware untuk EC2

Bagian ini mencakup kuota yang terkait dengan penggunaan Perlindungan Malware untuk EC2. Untuk kuota yang terkait dengan GuardDuty, lihat [GuardDuty kuota](#).

Tabel berikut menyediakan ketersediaan default berbagai sumber daya saat Anda menggunakan Perlindungan Malware untuk EC2.

Cakupan	Bawaan	Komentar
Ekstraksi dan analisis data dalam file terkompresi atau diarsipkan	5	Jumlah maksimum level bersarang yang diizinkan dalam file yang diarsipkan.
Jumlah file dalam file yang diarsipkan	1000	Jumlah maksimum file yang dapat dipindai dalam arsip. Hitungan ini adalah jumlah dari jumlah file yang diekstrak dari arsip dan jumlah file yang diekstrak dari semua arsip bersarang.
Jumlah Ancaman	32	Jumlah maksimum ancaman yang dapat Anda lihat di panel temuan. GuardDuty Perlindungan Malware untuk EC2 mungkin telah mendeteksi lebih banyak nama ancaman. Jika jumlah nama ancaman

Cakupan	Bawaan	Komentar
		yang terdeteksi lebih tinggi dari nilai default, Anda dapat melihat detail JSON dengan memilih ID Menemukan di bawah nama temuan di panel detail GuardDuty konsol.
Jumlah file per ancaman yang terdeteksi	5	Jumlah maksimum file yang diidentifikasi per ancaman yang terdeteksi. Misalnya, jika GuardDuty mendeteksi 10 file yang terkait dengan ancaman tunggal, ancaman akan menampilkan maksimal 5 file.
Volume EBS per pemindaian per instance	11	Jumlah maksimum volume EBS yang GuardDuty dapat memindai per EC2 instance. Jika ada lebih dari 11 volume EBS yang perlu dipindai, Perlindungan GuardDuty Malware untuk EC2 mengurutkan <code>deviceName</code> berdasarkan abjad, dan memilih 11 volume EBS pertama.

Cakupan	Bawaan	Komentar
Ukuran volume EBS	2048 GB	Terkait dengan EC2 instans Amazon dan beban kerja kontainer, Perlindungan GuardDuty Malware for EC2 dapat memindai setiap volume Amazon EBS yang berukuran hingga 2048 GB. Kuota ini berlaku untuk masing-masing Wilayah AWS tempat dukungan untuk Perlindungan Malware EC2 tersedia.
Jenis sistem file yang didukung	GuardDuty Perlindungan Malware untuk EC2 dapat memindai jenis sistem file berikut: • Sistem File Teknologi Baru (NTFS) • Sistem File X (XFS) • Sistem File kedua diperpanjang (ext2) • Sistem File diperpanjang keempat (ext4) • Sistem File Tabel Alokasi File (FAT) • Sistem File Tabel Alokasi File Virtual (VFAT)	N/A.

Cakupan	Bawaan	Komentar
Tag opsi pindai	50	Jumlah maksimum tag sumber daya yang dapat Anda tambahkan untuk menyesuaikan pengaturan opsi pemindaian malware Anda. Untuk informasi selengkapnya, lihat Opsii pindai dengan tag yang ditentukan pengguna .
Menemukan periode retensi	90	Jumlah hari maksimum yang GuardDuty mempertahankan temuan. Untuk informasi terbaru, lihat GuardDuty Kuota Amazon .
Periode retensi pemindaian malware	90	Jumlah hari maksimum Perlindungan GuardDuty Malware untuk EC2 mempertahankan riwayat pemindaian. Untuk informasi selengkapnya tentang melihat pemindaian malware terbaru, lihat Memantau status pemindaian dan hasil dalam Perlindungan Malware untuk EC2 .
Transaksi per detik (TPS) untuk pemindaian malware On-Demand	1	Jumlah permintaan pemindaian malware On-Demand yang dapat dimulai per detik di setiap Wilayah.

Cakupan	Bawaan	Komentar
Batas burst untuk pemindaian malware On-Demand	1	Jumlah permintaan pemindaian malware On-Demand bersamaan yang dapat dimulai per detik di setiap Wilayah.

GuardDuty Perlindungan Malware untuk S3

Perlindungan Malware untuk S3 membantu Anda mendeteksi potensi keberadaan malware dengan memindai objek yang baru diunggah ke bucket Amazon Simple Storage Service (Amazon S3) pilihan Anda. Ketika objek S3 atau versi baru dari objek S3 yang ada diunggah ke bucket yang Anda pilih, GuardDuty secara otomatis memulai pemindaian malware.

[Perlindungan Malware untuk S3 - Ikhtisar dan Demo](#)

Dua pendekatan untuk mengaktifkan Perlindungan Malware untuk S3

Anda dapat mengaktifkan Perlindungan Malware untuk S3 ketika Anda Akun AWS mengaktifkan GuardDuty layanan dan Anda menggunakan Perlindungan Malware untuk S3 sebagai bagian dari keseluruhan GuardDuty pengalaman, atau ketika Anda ingin menggunakan fitur Perlindungan Malware untuk S3 dengan sendirinya tanpa mengaktifkan layanan. GuardDuty Saat Anda mengaktifkan Perlindungan Malware untuk S3 dengan sendirinya, GuardDuty dokumentasi merujuknya sebagai menggunakan Perlindungan Malware untuk S3 sebagai fitur independen.

Pertimbangan untuk menggunakan Perlindungan Malware untuk S3 secara independen

- GuardDuty temuan keamanan — Detector ID adalah pengenalan unik yang dikaitkan dengan akun Anda di Wilayah. Ketika Anda mengaktifkan GuardDuty di satu atau beberapa Wilayah dalam akun, ID detektor akan dibuat secara otomatis untuk akun ini di setiap Wilayah tempat Anda mengaktifkan GuardDuty. Untuk informasi selengkapnya, lihat Detektor dalam [Konsep dan istilah kunci di Amazon GuardDuty](#) dokumen.

Saat Anda mengaktifkan Perlindungan Malware untuk S3 secara independen di akun, akun tersebut tidak akan memiliki ID detektor terkait. Ini memengaruhi GuardDuty fitur apa yang mungkin tersedia untuk Anda. Misalnya, ketika pemindaian malware S3 mendeteksi keberadaan malware, tidak ada GuardDuty temuan yang akan dihasilkan di Akun AWS karena semua GuardDuty temuan terkait dengan ID detektor.

- Memeriksa apakah objek yang dipindai berbahaya — Secara default, GuardDuty mempublikasikan hasil pemindaian malware ke bus EventBridge acara Amazon default Anda dan namespace Amazon CloudWatch . Saat Anda mengaktifkan penandaan pada saat mengaktifkan Perlindungan Malware untuk S3 untuk bucket, objek S3 yang dipindai mendapatkan tag yang menyebutkan hasil pemindaian. Untuk informasi lebih lanjut tentang penandaan, lihat [Penandaan opsional objek berdasarkan hasil pemindaian](#).

Pertimbangan umum untuk mengaktifkan Perlindungan Malware untuk S3

Pertimbangan umum berikut berlaku apakah Anda menggunakan Perlindungan Malware untuk S3 secara independen atau sebagai bagian dari GuardDuty pengalaman:

- Anda dapat mengaktifkan Perlindungan Malware untuk S3 untuk bucket Amazon S3 milik akun Anda sendiri. Sebagai akun GuardDuty administrator yang didelegasikan, Anda tidak dapat mengaktifkan fitur ini di bucket Amazon S3 milik akun anggota.
- Anda dapat mengaktifkan fitur ini di bucket S3 milik Wilayah yang sama yang saat ini dipilih di GuardDuty konsol. GuardDuty tidak mendukung pengaktifan fitur ini di bucket S3 lintas wilayah.
- Sebagai akun GuardDuty administrator yang didelegasikan, Anda akan menerima EventBridge notifikasi Amazon setiap kali ada perubahan pada bucket S3 yang dikonfigurasi oleh salah satu akun anggota organisasi Anda untuk fitur ini. [Melihat dan memahami status bucket yang dilindungi](#)

Konten

- [Harga dan biaya penggunaan untuk Perlindungan Malware untuk S3](#)
- [Bagaimana cara kerja Perlindungan Malware untuk S3?](#)
- [Kemampuan Perlindungan Malware untuk S3](#)
- [\(Opsional\) Memulai Perlindungan GuardDuty Malware untuk S3 secara independen \(hanya konsol\)](#)
- [Mengonfigurasi Perlindungan Malware untuk S3 untuk bucket Anda](#)
- [Langkah-langkah setelah mengaktifkan Perlindungan Malware untuk S3](#)
- [Menggunakan kontrol akses berbasis tag based tag \(TBAC\) dengan Perlindungan Malware untuk S3](#)
- [Melihat dan memahami status bucket yang dilindungi](#)
- [Memecahkan masalah status paket Perlindungan Malware](#)
- [Memantau pemindaian objek S3 di Perlindungan Malware untuk S3](#)
- [Mengedit paket Perlindungan Malware untuk bucket yang dilindungi](#)
- [Menonaktifkan Perlindungan Malware untuk S3 untuk bucket yang dilindungi](#)
- [Dukungan fitur Amazon S3](#)
- [Kuota dalam Perlindungan Malware untuk S3](#)

Harga dan biaya penggunaan untuk Perlindungan Malware untuk S3

Harga dalam Perlindungan Malware untuk S3 bekerja secara berbeda dari paket perlindungan lainnya di GuardDuty. Sementara sebagian besar paket GuardDuty perlindungan mengikuti uji coba gratis jangka pendek 30 hari, Perlindungan Malware untuk S3 mengikuti paket Tingkat Gratis 12 bulan. AWS Untuk informasi tentang GuardDuty harga, lihat [Harga di GuardDuty](#).

Daftar berikut memberikan biaya harga yang terkait dengan penggunaan Perlindungan Malware untuk S3.

Paket Tingkat Gratis (biaya pemindaian)

Masing-masing Akun AWS mendapat Tingkat Gratis 12 bulan yang mencakup penggunaan hingga batas tertentu per bulan untuk setiap Wilayah. Jika penggunaan Anda melampaui batas yang ditentukan, Anda akan mulai mengeluarkan biaya penggunaan untuk batas yang terlampaui. Untuk informasi tentang batas yang ditentukan dan contoh harga, lihat [harga paket GuardDuty perlindungan](#).

- Semua yang Akun AWS ada memenuhi syarat untuk menggunakan Tingkat Gratis 12 bulan untuk fitur ini yang dimulai dari 11 Juni 2024 dan berakhir pada 11 Juni 2025. Tingkat Gratis 12 bulan yang diperpanjang ini untuk akun Anda berlaku untuk menggunakan Perlindungan Malware untuk S3, dan tidak ada fitur lain Layanan AWS GuardDuty atau lainnya.

Jika yang sudah ada Akun AWS mulai menggunakan Perlindungan Malware untuk S3 setelah 11 Juni 2025 atau setelah Tingkat Gratis 12 bulan akun berakhir, maka Anda akan mulai mengeluarkan biaya penggunaan terkait.

- Jika Anda memiliki Tingkat Gratis baru Akun AWS dan 12 bulan Anda dimulai setelah ketersediaan umum (11 Juni 2024) Perlindungan Malware untuk S3, maka periode Tingkat Gratis 12 bulan Anda untuk fitur ini akan sama dengan periode Tingkat Gratis 12 bulan untuk akun Anda.

Untuk informasi tentang biaya penggunaan setelah mengaktifkan Perlindungan Malware untuk S3, lihat. [Meninjau biaya penggunaan untuk Perlindungan Malware untuk S3](#)

Biaya penggunaan Penandaan Objek S3

Saat Anda mengaktifkan Perlindungan Malware untuk S3, itu opsional untuk mengaktifkan penandaan untuk objek S3 yang dipindai. Ketika Anda memilih untuk mengaktifkan S3 Object

Tagging, ada biaya penggunaan terkait. Untuk informasi selengkapnya tentang biaya, lihat [tab Manajemen & wawasan](#) di halaman harga Amazon S3.

Biaya penggunaan Penandaan Objek S3 tidak termasuk dalam paket Tingkat Gratis.

Amazon S3 APIs - GET and PUT biaya penggunaan

Anda akan dikenakan biaya penggunaan saat GuardDuty menjalankan Amazon APIs S3 berdasarkan peran IAM. Misalnya, setelah mengasumsikan peran IAM, GuardDuty jalankan PutObject API untuk menambahkan objek pengujian ke bucket yang Anda pilih. Ini membantu GuardDuty menilai status fitur yang diaktifkan.

Untuk informasi tentang harga panggilan API S3 di Anda Wilayah AWS, lihat [Permintaan & pengambilan data di bawah tab Penyimpanan & permintaan](#) di halaman harga Amazon S3.

Meninjau biaya penggunaan untuk Perlindungan Malware untuk S3

Akun Anda mulai mengeluarkan biaya penggunaan saat Anda menggunakan Perlindungan Malware untuk S3 di luar batas spesifik di bawah paket Tingkat Gratis, atau ketika paket Tingkat Gratis 12 bulan akun Anda berakhir. Untuk informasi tentang paket Tingkat Gratis, lihat [Harga dan biaya penggunaan untuk Perlindungan Malware untuk S3](#).

GuardDuty Konsol tidak mendukung peninjauan Perlindungan Malware untuk biaya penggunaan S3. Untuk melihat biaya penggunaan, navigasikan ke Cost Explorer di <https://console.aws.amazon.com/costmanagement/konsol>. Untuk informasi tentang Akun AWS penagihan, lihat [Panduan AWS Billing Pengguna](#).

Untuk informasi tentang perkiraan biaya penggunaan di GuardDuty, lihat [Memperkirakan biaya penggunaan](#).

Bagaimana cara kerja Perlindungan Malware untuk S3?

Bagian ini menjelaskan komponen Perlindungan Malware untuk S3, cara kerjanya setelah Anda mengaktifkannya untuk bucket S3, dan bagaimana Anda dapat meninjau status dan hasil pemindaian malware.

Gambaran Umum

Anda dapat mengaktifkan Perlindungan Malware untuk S3 untuk bucket Amazon S3 milik Anda sendiri. Akun AWS GuardDuty memberi Anda fleksibilitas untuk mengaktifkan fitur ini untuk seluruh

bucket Anda, atau membatasi cakupan pemindaian malware ke [awalan objek](#) tertentu tempat GuardDuty memindai setiap objek yang diunggah yang dimulai dengan salah satu awalan yang dipilih. Anda dapat menambahkan hingga 5 awalan. Saat Anda mengaktifkan fitur untuk bucket S3, bucket tersebut disebut bucket yang dilindungi.

Izin peran IAM

Perlindungan Malware untuk S3 menggunakan peran IAM yang memungkinkan GuardDuty untuk melakukan tindakan pemindaian malware atas nama Anda. Tindakan ini termasuk diberi tahu tentang objek yang baru diunggah di bucket yang dipilih, memindai objek tersebut, dan secara opsional menambahkan tag ke objek yang dipindai. Ini adalah prasyarat untuk mengonfigurasi bucket S3 Anda dengan fitur ini.

Anda memiliki opsi untuk memperbarui peran IAM yang ada, atau membuat peran baru untuk tujuan ini. Saat mengaktifkan Perlindungan Malware untuk S3 untuk lebih dari satu bucket, Anda dapat memperbarui peran IAM yang ada untuk menyertakan nama bucket lainnya, sesuai kebutuhan. Untuk informasi selengkapnya, lihat [Membuat atau memperbarui kebijakan peran IAM](#).

Penandaan opsional objek berdasarkan hasil pemindaian

Pada saat mengaktifkan Perlindungan Malware untuk S3 untuk bucket Anda, ada langkah opsional untuk mengaktifkan penandaan objek S3 yang dipindai. Peran IAM sudah menyertakan izin untuk menambahkan tag ke objek Anda setelah pemindaian. Namun, GuardDuty akan menambahkan tag hanya ketika Anda mengaktifkan opsi ini pada saat setup.

Anda harus mengaktifkan opsi ini sebelum objek diunggah. Setelah pemindaian berakhir, GuardDuty tambahkan tag yang telah ditentukan ke objek S3 yang dipindai dengan pasangan key:value berikut:

GuardDutyMalwareScanStatus:*Potential scan result*

Nilai tag hasil pemindaian potensial

meliputi NO_THREATS_FOUND, THREATS_FOUND, UNSUPPORTED, ACCESS_DENIED, dan FAILED.

Untuk informasi lebih lanjut tentang nilai-nilai ini, lihat [the section called “Status pemindaian potensial objek S3 dan status hasil”](#).

Mengaktifkan penandaan adalah salah satu cara untuk mengetahui tentang hasil pemindaian objek S3. Anda dapat menggunakan tag ini lebih lanjut untuk menambahkan kebijakan sumber daya S3 kontrol akses berbasis tag (TBAC) sehingga Anda dapat mengambil tindakan pada objek yang berpotensi berbahaya. Untuk informasi selengkapnya, lihat [Menambahkan TBAC pada sumber daya bucket S3](#).

Kami menyarankan Anda untuk mengaktifkan penandaan pada saat mengonfigurasi Perlindungan Malware untuk S3 untuk bucket Anda. Jika Anda mengaktifkan penandaan setelah objek diunggah dan berpotensi pemindaian dimulai, tidak GuardDuty akan dapat menambahkan tag ke objek yang dipindai. Untuk informasi tentang biaya Penandaan Objek S3 terkait, lihat. [Harga dan biaya penggunaan untuk Perlindungan Malware untuk S3](#)

Proses setelah Anda mengaktifkan Perlindungan Malware untuk S3 untuk ember

Setelah Anda mengaktifkan Perlindungan Malware untuk S3, sumber daya paket Perlindungan Malware akan dibuat secara eksklusif untuk bucket S3 yang dipilih. Sumber daya ini dikaitkan dengan ID paket Perlindungan Malware, pengenal unik untuk sumber daya Anda yang dilindungi. Dengan menggunakan salah satu izin IAM, GuardDuty kemudian membuat dan mengelola aturan EventBridge terkelola dengan nama. `DO-NOT-DELETE-AmazonGuardDutyMalwareProtectionS3*`

Bagaimana GuardDuty menangani data Anda - pagar pembatas untuk perlindungan data

Perlindungan Malware untuk S3 mendengarkan notifikasi Amazon EventBridge . Saat objek diunggah ke bucket yang dipilih atau salah satu awalan, GuardDuty unduh objek tersebut dari bucket S3 dengan menggunakan lalu membaca, mendekripsi, [AWS PrivateLink](#) dan memindainya di lingkungan terisolasi di Wilayah yang sama. Lingkungan pemindaian berjalan di cloud pribadi virtual (VPC) yang terkunci tanpa akses internet. VPC dilampirkan ke grup aturan DNS Firewall yang memungkinkan komunikasi hanya ke domain allowlisted yang dimiliki. AWS Selama pemindaian, simpan GuardDuty sementara objek S3 yang diunduh dalam lingkungan pemindaian yang dienkripsi dengan kunci [AWS Key Management Service \(AWS KMS\)](#).

Note

Secara default, semua Amazon S3 yang APIs tercantum di bawah [jenis Peristiwa yang Dibuat Objek](#) di Panduan Pengguna Amazon S3, akan memulai Perlindungan Malware untuk pemindaian S3.

Jenis Event ini termasuk [PutObject](#), [POST Object CopyObject](#), dan [CompleteMultipartUpload](#).

Untuk informasi tentang metodologi deteksi GuardDuty malware dan mesin pemindaian yang digunakannya, lihat [GuardDuty mesin pemindai deteksi malware](#).

Setelah pemindaian malware selesai, GuardDuty proses metadata pemindaian dengan status pemindaian dan kemudian menghapus salinan objek yang diunduh.

GuardDuty membersihkan lingkungan pemindaian setiap kali sebelum pemindaian baru dimulai. GuardDuty menggunakan otorisasi kontingen untuk akses operator ke lingkungan pemindaian, dan setiap permintaan akses ditinjau, disetujui, dan diaudit.

Meninjau status dan hasil pemindaian objek S3

GuardDuty menerbitkan peristiwa hasil pemindaian objek S3 ke bus acara EventBridge default Amazon. GuardDuty juga mengirimkan metrik pemindaian seperti jumlah objek yang dipindai dan byte yang dipindai ke Amazon. CloudWatch Jika Anda mengaktifkan penandaan, maka GuardDuty akan menambahkan tag yang telah ditentukan GuardDutyMalwareScanStatus dan hasil pemindaian potensial sebagai nilai tag.

Important

GuardDuty menggunakan at-least-once pengiriman, yang berarti Anda mungkin menerima beberapa hasil pemindaian untuk objek yang sama. Kami merekomendasikan merancang aplikasi Anda untuk menangani hasil duplikat. Anda hanya ditagih sekali untuk setiap objek yang dipindai.

Untuk informasi selengkapnya, lihat [Memantau pemindaian objek S3 di Perlindungan Malware untuk S3](#).

Meninjau temuan yang dihasilkan

Meninjau temuan tergantung pada apakah Anda menggunakan Perlindungan Malware untuk S3 dengan atau tidak. GuardDuty Pertimbangkan skenario berikut:

Menggunakan Perlindungan Malware untuk S3 ketika Anda mengaktifkan GuardDuty layanan (ID detektor)

Jika pemindaian malware mendeteksi file yang berpotensi berbahaya di objek S3, GuardDuty akan menghasilkan temuan terkait. Anda dapat melihat detail temuan dan menggunakan langkah-langkah yang disarankan untuk berpotensi memulihkan temuan tersebut. Berdasarkan [frekuensi temuan Ekspor](#) Anda, temuan yang dihasilkan akan diekspor ke bucket S3 dan bus EventBridge acara.

Untuk informasi tentang jenis temuan yang akan dihasilkan, lihat [Perlindungan Malware untuk tipe pencarian S3](#).

Menggunakan Perlindungan Malware untuk S3 sebagai fitur independen (tidak ada ID detektor)

GuardDuty tidak akan dapat menghasilkan temuan karena tidak ada ID detektor terkait. Untuk mengetahui status pemindaian malware objek S3, Anda dapat melihat hasil pemindaian yang GuardDuty secara otomatis dipublikasikan ke bus acara default Anda. Anda juga dapat melihat CloudWatch metrik untuk menilai jumlah objek dan byte yang GuardDuty mencoba memindai. Anda dapat mengatur CloudWatch alarm untuk mendapatkan pemberitahuan tentang hasil pemindaian. Jika Anda telah mengaktifkan S3 Object Tagging, Anda juga dapat melihat status pemindaian malware dengan memeriksa objek S3 untuk kunci GuardDutyMalwareScanStatus tag dan nilai tag hasil pemindaian.

Untuk informasi tentang status dan hasil pemindaian objek S3, lihat [Memantau pemindaian objek S3 di Perlindungan Malware untuk S3](#).

Kemampuan Perlindungan Malware untuk S3

Daftar berikut memberikan ikhtisar tentang apa yang dapat Anda harapkan atau lakukan setelah mengaktifkan Perlindungan Malware untuk S3 untuk bucket Anda:

- Pilih apa yang akan dipindai — Pindai file saat diunggah ke semua atau awalan tertentu (hingga 5) yang terkait dengan bucket S3 pilihan Anda.
- Pemindaian otomatis pada objek yang diunggah — Setelah Anda mengaktifkan Perlindungan Malware untuk S3 untuk ember, secara otomatis GuardDuty akan memulai pemindaian untuk mendeteksi potensi malware di objek yang baru diunggah.
- Aktifkan melalui konsol, dengan menggunakan API/AWS CLI, atau AWS CloudFormation — Pilih metode yang disukai untuk mengaktifkan Perlindungan Malware untuk S3.

Anda dapat mengaktifkan Perlindungan Malware untuk S3 dengan menggunakan platform Infrastructure as code (IAC) seperti Terraform. Untuk informasi lebih lanjut, lihat [Sumber Daya: aws_guardduty_malware_protection_plan](#).

- Format file yang didukung, Perlindungan Malware untuk kuota S3, dan fitur Amazon S3 - Perlindungan Malware untuk S3 mendukung semua format file yang dapat Anda unggah ke bucket S3. Jika file yang diunggah dilindungi kata sandi, maka GuardDuty akan melewati pemindaian file. Untuk informasi tentang kuota yang terkait dengan ukuran objek, tingkat kedalaman arsip maksimum, dan detail lainnya, lihat [Kuota dalam Perlindungan Malware untuk S3](#).

Untuk informasi tentang apakah fitur Amazon S3 didukung atau tidak, lihat [Dukungan fitur Amazon S3](#)

- Mendukung penandaan objek S3 yang dipindai - Ketika Anda mengaktifkan [Penandaan opsional objek berdasarkan hasil pemindaian](#), maka setelah setiap pemindaian malware, GuardDuty akan menambahkan tag yang menunjukkan status pemindaian. Anda dapat menggunakan tag ini untuk mengatur kontrol akses berbasis tag (TBAC) untuk objek S3. Misalnya, Anda dapat membatasi akses ke objek S3 yang diindikasikan sebagai berbahaya dan memiliki nilai tag sebagai. THREATS_FOUND
- EventBridge Pemberitahuan Amazon — GuardDuty mengirimkan peristiwa ke Amazon EventBridge saat status sumber daya paket Perlindungan Malware berubah, atau pemindaian malware objek S3 selesai. Peristiwa ini dikirim ke bus acara default. Anda dapat menggunakan EventBridge dan peristiwa ini untuk menulis aturan yang mengambil tindakan, seperti memantau kapan peristiwa ini terjadi. Untuk informasi selengkapnya, lihat [Memantau pemindaian objek S3 dengan Amazon EventBridge](#).
- CloudWatch metrik — Lihat CloudWatch metrik untuk mengaktifkan alarm pada status pemindaian malware tertentu. Lihat informasi yang lebih lengkap di [Metrik status pemindaian objek S3 di CloudWatch](#).

(Opsional) Memulai Perlindungan GuardDuty Malware untuk S3 secara independen (hanya konsol)

Gunakan langkah opsional ini ketika Anda ingin memulai dengan Perlindungan Malware untuk opsi deteksi ancaman S3 terlepas dari GuardDuty status di Akun AWS.

Jika Anda juga ingin menggunakan paket perlindungan khusus lainnya di GuardDuty, Anda harus memulai dengan GuardDuty layanan Amazon. Untuk informasi tentang rencana GuardDuty perlindungan, lihat [Fitur dari GuardDuty](#). Ketika Anda telah mengaktifkan GuardDuty di akun Anda, maka Anda dapat melewati langkah ini dan melanjutkan dengan [Mengonfigurasi Perlindungan Malware untuk S3 untuk bucket Anda](#).

Langkah-langkah untuk memulai dengan Perlindungan Malware untuk deteksi ancaman S3 saja

1. Masuk ke AWS Management Console dan buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.

2. Pilih Perlindungan GuardDuty Malware hanya untuk S3. Ini membantu Anda mendeteksi apakah file yang baru diunggah di bucket Amazon Simple Storage Service (Amazon S3) berpotensi mengandung malware.

Try threat detection with GuardDuty

☐ Amazon GuardDuty - all features

Experience threat detection capabilities in your AWS environment.

☒ GuardDuty Malware Protection for S3 only

Detect malicious file upload to your Amazon S3 buckets. You don't need to enable Amazon GuardDuty.

Get started

3. Pilih Mulai. Anda sekarang dapat melanjutkan dengan langkah-langkah di bawah [Mengonfigurasi Perlindungan Malware untuk S3 untuk bucket Anda](#).

Mengonfigurasi Perlindungan Malware untuk S3 untuk bucket Anda

Agar Perlindungan Malware untuk S3 dapat memindai dan (opsional) menambahkan tag ke objek S3 Anda, Anda dapat menggunakan peran layanan yang memiliki izin yang diperlukan untuk melakukan tindakan pemindaian malware atas nama Anda. Untuk informasi selengkapnya tentang penggunaan

peran layanan guna mengaktifkan perlindungan malware untuk S3, lihat [Akses Layanan](#). Peran ini berbeda dengan peran [terkait layanan Perlindungan GuardDuty Malware](#).

Jika Anda lebih suka menggunakan peran IAM, Anda dapat melampirkan peran IAM yang menyertakan izin yang diperlukan untuk memindai dan (opsional) menambahkan tag ke objek S3 Anda. GuardDuty kemudian mengasumsikan peran IAM ini untuk melakukan tindakan ini atas nama Anda. Anda akan memerlukan nama peran IAM ini pada saat mengaktifkan paket perlindungan ini untuk bucket Amazon S3 Anda.

Jika Anda menggunakan peran IAM, untuk setiap kali Anda ingin melindungi bucket Amazon S3, Anda harus melakukan kedua langkah yang tercantum di bagian ini.

Untuk mengaktifkan Perlindungan Malware untuk S3, Anda memerlukan detail seperti nama bucket S3, awalan objek jika Anda ingin memfokuskan perlindungan untuk awalan tertentu, dan nama peran IAM dengan izin yang diperlukan.

Langkah-langkahnya tetap sama apakah Anda memulai dengan Perlindungan Malware untuk S3 secara independen atau mengaktifkannya sebagai bagian dari GuardDuty layanan.

Topik

1. [Membuat atau memperbarui kebijakan peran IAM](#)
2. [Mengaktifkan Perlindungan Malware untuk S3 untuk bucket Anda](#)
3. [Memecahkan masalah kesalahan izin peran IAM](#)

Mengaktifkan Perlindungan Malware untuk S3 untuk bucket Anda

Bagian ini memberikan langkah-langkah terperinci tentang cara mengaktifkan Perlindungan Malware untuk S3 untuk ember di akun Anda sendiri. Sebelum Anda melanjutkan, tinjau pertimbangan berikut:

- Bila Anda mengaktifkan paket perlindungan ini menggunakan GuardDuty konsol, itu termasuk langkah untuk membuat peran baru atau menggunakan peran yang ada di bawah bagian Akses layanan.
- Ketika Anda mengaktifkan paket perlindungan ini menggunakan GuardDuty API atau CLI, maka Anda harus [Membuat atau memperbarui kebijakan peran IAM](#) sebelum melanjutkan lebih jauh.
- Terlepas dari bagaimana Anda mengaktifkan rencana perlindungan ini, Anda harus memiliki yang diperlukan [izin untuk membuat sumber daya paket Perlindungan Malware](#).

Mempertimbangkan pelambatan bucket Amazon S3

S3 Throttling mungkin membatasi kecepatan transfer data ke atau dari bucket Amazon S3 Anda. Ini berpotensi menunda pemindaian malware dari objek yang baru Anda unggah.

Jika Anda mengharapkan volume GET dan PUT permintaan yang tinggi ke bucket S3 Anda, pertimbangkan untuk menerapkan langkah-langkah untuk mencegah pelambatan. Untuk informasi tentang cara melakukannya, lihat [Mencegah pelambatan Amazon S3](#) di Panduan Pengguna Amazon Athena.

Izin untuk membuat sumber daya paket Perlindungan Malware

Saat Anda mengaktifkan Perlindungan Malware untuk S3 untuk bucket Amazon S3 GuardDuty , buat sumber daya paket Perlindungan Malware yang berfungsi sebagai pengenal untuk paket perlindungan bucket. Jika Anda belum menggunakan [AWS kebijakan terkelola: AmazonGuardDutyFullAccess_v2 \(disarankan\)](#), maka Anda harus menambahkan izin berikut untuk membuat sumber daya ini:

- guardDuty:CreateMalwareProtectionPlan
- iam:PassRole

Anda dapat menggunakan contoh kebijakan kustom berikut dan menggantinya *placeholder values* dengan nilai yang sesuai untuk akun Anda:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iam:PassRole"
      ],
      "Resource": "arn:aws:iam::111122223333:role/role-name",
      "Condition": {
        "StringEquals": {
          "iam:PassedToService": "malware-protection-
plan.guarddduty.amazonaws.com"
        }
      }
    }
  ],
}
```

```
{
  "Effect": "Allow",
  "Action": [
    "guardduty:CreateMalwareProtectionPlan"
  ],
  "Resource": "*"
}
```

Mengaktifkan Perlindungan Malware untuk S3 dengan menggunakan konsol GuardDuty

Bagian berikut memberikan step-by-step panduan seperti yang akan Anda alami di konsol GuardDuty

Untuk mengaktifkan Perlindungan Malware untuk S3 dengan menggunakan konsol GuardDuty

Masukkan detail bucket S3

Gunakan langkah-langkah berikut untuk memberikan detail bucket Amazon S3:

1. Masuk ke AWS Management Console dan buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.
2. Dengan menggunakan Wilayah AWS pemilih di sudut kanan atas halaman, pilih Wilayah tempat Anda ingin mengaktifkan Perlindungan Malware untuk S3.
3. Di panel navigasi, pilih Perlindungan Malware untuk S3.
4. Di bagian Protected Bucket, pilih Aktifkan untuk mengaktifkan Perlindungan Malware untuk S3 untuk bucket S3 milik Anda. Akun AWS
5. Di bawah Masukkan detail bucket S3, masukkan nama bucket Amazon S3. Atau, pilih Browse S3 untuk memilih bucket S3.

Bucket S3 dan Akun AWS tempat Anda mengaktifkan Perlindungan Malware untuk S3 harus sama. Wilayah AWS Misalnya, jika akun Anda milik us-east-1 Wilayah, maka Wilayah bucket Amazon S3 Anda juga harus us-east-1

6. Di bawah Awalan, Anda dapat memilih All the objects in the S3 bucket atau Objects yang dimulai dengan awalan tertentu.
 - Pilih Semua objek di bucket S3 bila Anda mau GuardDuty dapat memindai semua objek yang baru diunggah di bucket yang dipilih.

- Pilih Objek yang dimulai dengan awalan tertentu saat Anda ingin memindai objek yang baru diunggah milik awalan tertentu. Opsi ini membantu Anda memfokuskan ruang lingkup pemindaian malware pada awalan objek yang dipilih saja. Untuk informasi selengkapnya tentang penggunaan awalan, lihat [Mengatur objek di konsol Amazon S3 menggunakan folder](#) di Panduan Pengguna Amazon S3.

Pilih Tambahkan awalan dan masukkan awalan. Anda dapat menambahkan hingga lima awalan.

Aktifkan penandaan untuk objek yang dipindai

Ini adalah langkah opsional. Saat Anda mengaktifkan opsi penandaan sebelum objek diunggah ke bucket Anda, maka setelah menyelesaikan pemindaian, GuardDuty akan menambahkan tag yang telah ditentukan dengan kunci sebagai `GuardDutyMalwareScanStatus` dan nilai sebagai hasil pemindaian. Untuk menggunakan Perlindungan Malware untuk S3 secara optimal, kami sarankan untuk mengaktifkan opsi untuk menambahkan tag ke objek S3 setelah pemindaian berakhir. Biaya Penandaan Objek S3 standar berlaku. Untuk informasi selengkapnya, lihat [Harga dan biaya penggunaan untuk Perlindungan Malware untuk S3](#).

Mengapa Anda harus mengaktifkan penandaan?

- Mengaktifkan penandaan adalah salah satu cara untuk mengetahui tentang hasil pemindaian malware. Untuk informasi tentang hasil pemindaian malware S3, lihat [Memantau pemindaian objek S3 di Perlindungan Malware untuk S3](#).
- Siapkan kebijakan kontrol akses berbasis tag (TBAC) di bucket S3 Anda yang berisi objek yang berpotensi berbahaya. Untuk informasi tentang pertimbangan dan cara menerapkan kontrol akses berbasis tag (TBAC), lihat [Menggunakan kontrol akses berbasis tag based tag \(TBAC\) dengan Perlindungan Malware untuk S3](#)

Pertimbangan GuardDuty untuk menambahkan tag ke objek S3 Anda:

- Secara default, Anda dapat mengaitkan hingga 10 tag dengan objek. Untuk informasi selengkapnya, lihat [Mengategorikan penyimpanan menggunakan tag](#) di Panduan Pengguna Amazon S3.

Jika semua 10 tag sudah digunakan, tidak GuardDuty dapat menambahkan tag yang telah ditentukan ke objek yang dipindai. GuardDuty juga menerbitkan hasil pemindaian ke bus

EventBridge acara default Anda. Untuk informasi selengkapnya, lihat [Memantau pemindaian objek S3 dengan Amazon EventBridge](#).

- Jika peran IAM yang dipilih tidak menyertakan izin GuardDuty untuk menandai objek S3, bahkan dengan penandaan diaktifkan untuk bucket Anda yang dilindungi, tidak GuardDuty akan dapat menambahkan tag ke objek S3 yang dipindai ini. Untuk informasi selengkapnya tentang izin peran IAM yang diperlukan untuk penandaan, lihat [Membuat atau memperbarui kebijakan peran IAM](#)

GuardDuty juga menerbitkan hasil pemindaian ke bus EventBridge acara default Anda. Untuk informasi selengkapnya, lihat [Memantau pemindaian objek S3 dengan Amazon EventBridge](#).

Untuk memilih opsi di bawah Tag objek yang dipindai

- Saat Anda ingin GuardDuty menambahkan tag ke objek S3 yang dipindai, pilih objek Tag.
- Bila Anda tidak ingin menambahkan tag GuardDuty ke objek S3 yang dipindai, pilih Jangan beri tag objek.

Akses layanan

Gunakan langkah-langkah berikut untuk memilih peran layanan yang ada atau membuat peran layanan baru yang memiliki izin yang diperlukan untuk melakukan tindakan pemindaian malware atas nama Anda. Tindakan ini mungkin termasuk memindai objek S3 yang baru diunggah dan (opsional) menambahkan tag ke objek tersebut. Untuk informasi tentang izin yang akan dimiliki peran ini, lihat [Membuat atau memperbarui kebijakan peran IAM](#).

Di bagian Akses Layanan, Anda dapat melakukan salah satu hal berikut:

1. Buat dan gunakan peran layanan baru — Anda dapat menggunakan buat peran layanan baru yang memiliki izin yang diperlukan untuk melakukan pemindaian malware.

Di bawah nama Peran, Anda dapat memilih untuk menggunakan nama yang telah diisi sebelumnya GuardDuty atau memasukkan nama yang berarti dari pilihan Anda untuk mengidentifikasi peran tersebut. Sebagai contoh, GuardDutyS3MalwareScanRole. Nama peran harus 1-64 karakter. Karakter yang valid adalah karakter a-z, A-Z, 0-9, dan '+', '@', '-', '_'.

2. Menggunakan peran layanan yang ada — Anda dapat memilih peran layanan yang ada dari daftar nama peran Layanan.
 - a. Di bawah Templat kebijakan, Anda dapat melihat kebijakan untuk bucket S3 Anda. Pastikan Anda memasukkan atau memilih bucket S3 di bagian Enter S3 bucket details.

- b. Di bawah Nama peran Layanan pilih peran layanan dari daftar peran layanan.

Anda dapat membuat perubahan pada kebijakan berdasarkan persyaratan Anda Untuk detail selengkapnya tentang cara membuat atau memperbarui peran IAM, lihat [Membuat atau memperbarui kebijakan peran IAM](#).

Untuk masalah dengan izin peran IAM, lihat. [Memecahkan masalah kesalahan izin peran IAM](#)

(Opsional) Tandai ID paket Perlindungan Malware

Ini adalah langkah opsional yang membantu Anda menambahkan tag ke sumber daya paket Perlindungan Malware yang akan dibuat untuk sumber daya bucket S3 Anda.

Setiap tag memiliki dua bagian: Kunci tag dan nilai tag opsional. Untuk informasi selengkapnya tentang penandaan dan manfaatnya, lihat [Menandai sumber daya AWS](#).

Untuk menambahkan tag ke sumber daya paket Perlindungan Malware

1. Masukkan Kunci dan Nilai opsional untuk tag. Baik kunci tag dan nilai tag peka huruf besar/kecil. Untuk informasi tentang nama kunci tag dan nilai tag, lihat [Batas dan persyaratan penamaan tag](#).
2. Untuk menambahkan lebih banyak tag ke sumber daya paket Perlindungan Malware Anda, pilih Tambahkan tag baru dan ulangi langkah sebelumnya. Anda dapat menambahkan hingga 50 tanda ke setiap sumber daya .
3. Pilih Aktifkan.

Mengaktifkan Perlindungan Malware untuk S3 dengan menggunakan API/CLI

Bagian ini mencakup langkah-langkah kapan Anda ingin mengaktifkan Perlindungan Malware untuk S3 secara terprogram di lingkungan Anda. AWS Ini memerlukan peran IAM Amazon Resource Name (ARN) yang Anda buat pada langkah ini -. [Membuat atau memperbarui kebijakan peran IAM](#)

Untuk mengaktifkan Perlindungan Malware untuk S3 secara terprogram dengan menggunakan API/CLI

- Dengan menggunakan API

Jalankan [CreateMalwareProtectionPlan](#) untuk mengaktifkan Perlindungan Malware untuk S3 untuk bucket milik akun Anda sendiri.

- Dengan menggunakan AWS CLI

Bergantung pada bagaimana Anda ingin mengaktifkan Perlindungan Malware untuk S3, daftar berikut memberikan AWS CLI contoh perintah untuk kasus penggunaan tertentu. Saat Anda menjalankan perintah ini, ganti *placeholder examples shown in red*, dengan nilai yang sesuai untuk akun Anda.

AWS CLI contoh perintah

- Gunakan AWS CLI perintah berikut untuk mengaktifkan Perlindungan Malware untuk S3 untuk bucket tanpa penandaan untuk objek S3 yang dipindai:

```
aws guardduty create-malware-protection-plan --role
"arn:aws:iam::<111122223333:role/role-name" --protected-resource
"S3Bucket"={"BucketName"="amzn-s3-demo-bucket1"}
```

- Gunakan AWS CLI perintah berikut untuk mengaktifkan Perlindungan Malware untuk S3 untuk bucket dengan awalan objek tertentu dan tanpa penandaan untuk objek S3 yang dipindai:

```
aws guardduty create-malware-protection-plan --role
"arn:aws:iam::<111122223333:role/role-name" --protected-resource '{"S3Bucket":
{"BucketName":"amzn-s3-demo-bucket1", "ObjectPrefixes": ["Object1","Object1"]}]'
```

- Gunakan AWS CLI perintah berikut untuk mengaktifkan Perlindungan Malware untuk S3 untuk bucket dengan penandaan objek S3 yang dipindai diaktifkan:

```
aws guardduty create-malware-protection-plan --role
"arn:aws:iam::<111122223333:role/role-name" --protected-resource
"S3Bucket"={"BucketName"="amzn-s3-demo-bucket1"} --actions
"Tagging"={"Status"="ENABLED"}
```

Setelah Anda menjalankan perintah ini dengan sukses, ID paket Perlindungan Malware yang unik akan dihasilkan. Untuk melakukan tindakan seperti memperbarui atau menonaktifkan paket perlindungan untuk bucket Anda, Anda memerlukan ID paket Perlindungan Malware ini.

Untuk masalah dengan izin peran IAM, lihat. [Memecahkan masalah kesalahan izin peran IAM](#)

Membuat atau memperbarui kebijakan peran IAM

Agar Perlindungan Malware untuk S3 dapat memindai dan (opsional) menambahkan tag ke objek S3 Anda, Anda dapat menggunakan peran layanan yang memiliki izin yang diperlukan untuk melakukan

tindakan pemindaian malware atas nama Anda. Untuk informasi selengkapnya tentang penggunaan peran layanan guna mengaktifkan perlindungan malware untuk S3, lihat [Akses Layanan](#). Peran ini berbeda dengan peran [terkait layanan Perlindungan GuardDuty Malware](#).

Jika Anda lebih suka menggunakan peran IAM, Anda dapat melampirkan peran IAM yang menyertakan izin yang diperlukan untuk memindai dan (opsional) menambahkan tag ke objek S3 Anda. Anda harus membuat peran IAM atau memperbarui peran yang ada untuk menyertakan izin ini. Karena izin ini diperlukan untuk setiap bucket Amazon S3 yang Anda aktifkan Perlindungan Malware untuk S3, Anda perlu melakukan langkah ini untuk setiap bucket Amazon S3 yang harus Anda lindungi.

Daftar berikut menjelaskan bagaimana izin tertentu membantu GuardDuty melakukan pemindaian malware atas nama Anda:

- Izinkan EventBridge tindakan Amazon membuat dan mengelola aturan EventBridge terkelola sehingga Perlindungan Malware untuk S3 dapat mendengarkan pemberitahuan objek S3 Anda.

Untuk informasi selengkapnya, lihat [Aturan EventBridge terkelola Amazon](#) di Panduan EventBridge Pengguna Amazon.

- Izinkan Amazon S3 dan EventBridge tindakan mengirim pemberitahuan ke semua peristiwa di bucket EventBridge ini

Untuk informasi selengkapnya, lihat [Mengaktifkan Amazon EventBridge](#) di Panduan Pengguna Amazon S3.

- Izinkan tindakan Amazon S3 mengakses objek S3 yang diunggah dan menambahkan tag yang telah ditentukan GuardDutyMalwareScanStatus, ke objek S3 yang dipindai. Saat menggunakan awalan objek, tambahkan `s3:prefix` kondisi pada awalan yang ditargetkan saja. Ini GuardDuty mencegah mengakses semua objek S3 di bucket Anda.
- Izinkan tindakan kunci KMS untuk mengakses objek sebelum memindai dan meletakkan objek uji pada ember dengan enkripsi DSSE-KMS dan SSE-KMS yang didukung.

Note

Langkah ini diperlukan setiap kali Anda mengaktifkan Perlindungan Malware untuk S3 untuk ember di akun Anda. Jika Anda sudah memiliki peran IAM yang sudah ada, Anda dapat memperbarui kebijakannya untuk menyertakan detail sumber daya bucket Amazon

S3 lainnya. [Menambahkan izin kebijakan IAM](#) Topik ini memberikan contoh tentang cara melakukan ini.

Gunakan kebijakan berikut untuk membuat atau memperbarui peran IAM.

Kebijakan

- [Menambahkan izin kebijakan IAM](#)
- [Menambahkan kebijakan hubungan Trust](#)

Menambahkan izin kebijakan IAM

Anda dapat memilih untuk memperbarui kebijakan inline peran IAM yang ada, atau membuat peran IAM baru. Untuk selengkapnya tentang langkah-langkahnya, lihat [Membuat peran IAM](#) atau [Memodifikasi kebijakan izin peran di Panduan](#) Pengguna IAM.

Tambahkan templat izin berikut ke peran IAM pilihan Anda. Ganti nilai placeholder berikut dengan nilai yang sesuai yang terkait dengan akun Anda:

- Untuk *amzn-s3-demo-bucket*, ganti dengan nama bucket Amazon S3 Anda.

Untuk menggunakan peran IAM yang sama untuk lebih dari satu sumber daya bucket S3, perbarui kebijakan yang ada seperti yang ditampilkan dalam contoh berikut:

```
...
...
"Resource": [
    "arn:aws:s3:::amzn-s3-demo-bucket/*",
    "arn:aws:s3:::amzn-s3-demo-bucket2/*"
],
...
...
```

Pastikan untuk menambahkan koma (,) sebelum menambahkan ARN baru yang terkait dengan bucket S3. Lakukan ini di mana pun Anda merujuk ke bucket S3 Resource di template kebijakan.

- Untuk *111122223333*, ganti dengan Akun AWS ID Anda.
- Untuk *us-east-1*, ganti dengan Anda Wilayah AWS.

- Untuk **APKAEIBAERJR2EXAMPLE**, ganti dengan ID kunci terkelola pelanggan Anda. Jika bucket S3 Anda dienkripsi menggunakan AWS KMS kunci, kami menambahkan izin yang relevan jika Anda memilih opsi [Buat peran baru](#) saat mengonfigurasi perlindungan malware untuk bucket Anda.

```
"Resource": "arn:aws:kms:us-east-1:111122223333:key/*"
```

Templat kebijakan peran IAM

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "AllowManagedRuleToSendS3EventsToGuardDuty",
    "Effect": "Allow",
    "Action": [
      "events:PutRule",
      "events>DeleteRule",
      "events:PutTargets",
      "events:RemoveTargets"
    ],
    "Resource": [
      "arn:aws:events:us-east-1:111122223333:rule/DO-NOT-DELETE-AmazonGuardDutyMalwareProtectionS3*"
    ],
    "Condition": {
      "StringLike": {
        "events:ManagedBy": "malware-protection-plan.guardduty.amazonaws.com"
      }
    }
  },
  {
    "Sid": "AllowGuardDutyToMonitorEventBridgeManagedRule",
    "Effect": "Allow",
    "Action": [
      "events:DescribeRule",
      "events:ListTargetsByRule"
    ],
    "Resource": [
      "arn:aws:events:us-east-1:111122223333:rule/DO-NOT-DELETE-AmazonGuardDutyMalwareProtectionS3*"
    ]
  },
}
```

```

{
  "Sid": "AllowPostScanTag",
  "Effect": "Allow",
  "Action": [
    "s3:PutObjectTagging",
    "s3:GetObjectTagging",
    "s3:PutObjectVersionTagging",
    "s3:GetObjectVersionTagging"
  ],
  "Resource": [
    "arn:aws:s3:::amzn-s3-demo-bucket/*"
  ]
},
{
  "Sid": "AllowEnableS3EventBridgeEvents",
  "Effect": "Allow",
  "Action": [
    "s3:PutBucketNotification",
    "s3:GetBucketNotification"
  ],
  "Resource": [
    "arn:aws:s3:::amzn-s3-demo-bucket"
  ]
},
{
  "Sid": "AllowPutValidationObject",
  "Effect": "Allow",
  "Action": [
    "s3:PutObject"
  ],
  "Resource": [
    "arn:aws:s3:::amzn-s3-demo-bucket/malware-protection-resource-validation-object"
  ]
},
{
  "Sid": "AllowCheckBucketOwnership",
  "Effect": "Allow",
  "Action": [
    "s3:ListBucket"
  ],
  "Resource": [
    "arn:aws:s3:::amzn-s3-demo-bucket"
  ]
}

```

```

    },
    {
      "Sid": "AllowMalwareScan",
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket/*"
      ]
    },
    {
      "Sid": "AllowDecryptForMalwareScan",
      "Effect": "Allow",
      "Action": [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource": "arn:aws:kms:us-east-1:111122223333:key/APKAEIBAERJR2EXAMPLE",
      "Condition": {
        "StringLike": {
          "kms:ViaService": "s3.us-east-1.amazonaws.com"
        }
      }
    }
  ]
}

```

Menambahkan kebijakan hubungan Trust

Lampirkan kebijakan kepercayaan berikut ke peran IAM Anda. Untuk selengkapnya tentang langkah-langkah, lihat [Memodifikasi kebijakan kepercayaan peran](#).

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "malware-protection-plan.guardduty.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}

```

```
}  
]  
}
```

Memecahkan masalah kesalahan izin peran IAM

Saat mengaktifkan Perlindungan Malware untuk S3, GuardDuty memeriksa apakah peran layanan IAM Anda memiliki izin yang diperlukan untuk memvalidasi kepemilikan bucket Amazon S3. Jika izin ini hilang atau salah dikonfigurasi, Anda mungkin mendapatkan pesan berikut:

```
"message": "The request was rejected because provided IAM role does not have the  
required permissions to validate S3 bucket ownership."  
"type": "InvalidInputException"
```

Skenario berikut dapat membantu Anda memecahkan masalah kesalahan ini:

Izin peran IAM tidak ada

- Peran IAM harus memiliki izin yang diperlukan untuk memungkinkan Perlindungan Malware untuk S3 untuk mengambil peran.
- GuardDuty memvalidasi kepemilikan bucket dengan "s3:ListBucket" izin. Ini harus ada dalam peran IAM yang Anda gunakan.

Untuk informasi tentang izin, lihat [Membuat atau memperbarui kebijakan peran IAM](#).

Ketersediaan peran IAM

- Saat Anda membuat peran IAM baru, biarkan beberapa menit agar perubahan mencapai konsistensi akhirnya sebelum mengaktifkan Perlindungan Malware untuk S3. Jika Anda mencoba mengaktifkan rencana perlindungan segera setelah membuat peran, validasi mungkin gagal.
- Untuk penyebaran Infrastructure as Code (IaC), GuardDuty merekomendasikan untuk mendeklarasikan ketergantungan sumber daya untuk memastikan peran IAM mencapai konsistensi akhirnya.

Untuk contoh templat tentang cara melakukannya, lihat [GuardDuty GitHubrepositori](#).

Pemberdayaan lintas wilayah

Pastikan bucket Amazon S3 Anda berada di Wilayah yang sama tempat Anda mengaktifkan Perlindungan Malware untuk S3. GuardDuty

Langkah-langkah setelah mengaktifkan Perlindungan Malware untuk S3

Bagian ini mencantumkan langkah-langkah yang mungkin Anda ambil setelah mengaktifkan Perlindungan Malware untuk S3 untuk ember. Langkah-langkah berikut tercantum dalam urutan yang akan membantu Anda menavigasi langkah-langkah selanjutnya:

Untuk mengikuti setelah Anda mengaktifkan Perlindungan Malware untuk S3 untuk bucket Anda

1. Tambahkan kebijakan sumber daya kontrol akses berbasis tag (TBAC) — Saat Anda mengaktifkan penandaan, sebelum objek diunggah ke bucket yang dipilih, pastikan untuk menambahkan kebijakan TBAC ke sumber daya bucket S3 Anda. Untuk informasi selengkapnya, lihat [Menambahkan TBAC pada sumber daya bucket S3](#).
2. Pantau status paket Perlindungan Malware — Pantau kolom Status untuk setiap bucket yang dilindungi. Untuk informasi tentang status potensial dan apa artinya, lihat [Melihat dan memahami status bucket yang dilindungi](#).
3. Unggah objek:
 1. Buka konsol Amazon S3 di <https://console.aws.amazon.com/s3/>
 2. Unggah file ke bucket S3 atau awalan objek yang Anda aktifkan fitur ini. Untuk langkah-langkah mengunggah file, lihat [Mengunggah objek ke bucket Anda](#) di Panduan Pengguna Amazon S3.
4. Pantau status pemindaian objek S3 dan hasil pemindaian — Langkah ini mencakup informasi tentang cara memeriksa status pemindaian malware objek S3.

Diaktifkan keduanya GuardDuty dan Perlindungan Malware untuk S3	Perlindungan Malware yang Diaktifkan hanya untuk S3
• Ketika GuardDuty diaktifkan, itu dapat menghasilkan Perlindungan Malware untuk tipe pencarian S3 untuk menunjukkan keberadaan malware di objek S3 yang dipindai. • Anda berpotensi dapat memeriksa hasil pemindaian objek S3 dengan menggunakan satu atau beberapa opsi	Anda berpotensi dapat memeriksa hasil pemindaian objek S3 dengan menggunakan satu atau beberapa opsi di bawah Memantau pemindaian objek S3 di Perlindungan Malware untuk S3. Ini termasuk menggunakan Amazon EventBridge, CloudWatch metrik untuk paket Perlindungan Malware, dan menandai objek yang dipindai.

Diaktifkan keduanya GuardDuty dan Perlindungan Malware untuk S3

Perlindungan Malware yang Diaktifkan hanya untuk S3

di bawah [Memantau pemindaian objek S3 di Perlindungan Malware untuk S3](#).

Ini termasuk menggunakan Amazon EventBridge, CloudWatch metrik untuk paket Perlindungan Malware, dan menandai objek yang dipindai.

Menggunakan kontrol akses berbasis tag based tag (TBAC) dengan Perlindungan Malware untuk S3

Saat mengaktifkan Perlindungan Malware untuk S3 untuk bucket Anda, Anda dapat memilih untuk mengaktifkan penandaan secara opsional. Setelah mencoba memindai objek S3 yang baru diunggah di bucket yang dipilih, GuardDuty tambahkan tag ke objek yang dipindai untuk memberikan status pemindaian malware. Ada biaya penggunaan langsung yang terkait saat Anda mengaktifkan penandaan. Untuk informasi selengkapnya, lihat [Harga dan biaya penggunaan untuk Perlindungan Malware untuk S3](#).

GuardDuty menggunakan tag yang telah ditentukan dengan kunci sebagai GuardDutyMalwareScanStatus dan nilai sebagai salah satu status pemindaian malware. Untuk informasi tentang nilai-nilai tersebut, lihat [the section called “Status pemindaian potensial objek S3 dan status hasil”](#).

Pertimbangan GuardDuty untuk menambahkan tag ke objek S3 Anda:

- Secara default, Anda dapat mengaitkan hingga 10 tag dengan objek. Untuk informasi selengkapnya, lihat [Mengategorikan penyimpanan menggunakan tag](#) di Panduan Pengguna Amazon S3.

Jika semua 10 tag sudah digunakan, tidak GuardDuty dapat menambahkan tag yang telah ditentukan ke objek yang dipindai. GuardDuty juga menerbitkan hasil pemindaian ke bus EventBridge acara default Anda. Untuk informasi selengkapnya, lihat [Memantau pemindaian objek S3 dengan Amazon EventBridge](#).

- Jika peran IAM yang dipilih tidak menyertakan izin GuardDuty untuk menandai objek S3, bahkan dengan penandaan diaktifkan untuk bucket Anda yang dilindungi, tidak GuardDuty akan dapat

menambahkan tag ke objek S3 yang dipindai ini. Untuk informasi lebih lanjut tentang izin peran IAM yang diperlukan untuk menandai, lihat [Membuat atau memperbarui kebijakan peran IAM](#)

GuardDuty juga menerbitkan hasil pemindaian ke bus EventBridge acara default Anda. Untuk informasi selengkapnya, lihat [Memantau pemindaian objek S3 dengan Amazon EventBridge](#).

Menambahkan TBAC pada sumber daya bucket S3

Anda dapat menggunakan kebijakan sumber daya bucket S3 untuk mengelola tag based access control (TBAC) untuk objek S3 Anda. Anda dapat memberikan akses ke pengguna tertentu untuk mengakses dan membaca objek S3. Jika Anda memiliki organisasi yang dibuat dengan menggunakan AWS Organizations, Anda harus menegaskan bahwa tidak ada yang dapat memodifikasi tag yang ditambahkan oleh GuardDuty. Untuk informasi selengkapnya, lihat [Mencegah tag diubah kecuali oleh prinsipal resmi di Panduan Pengguna AWS Organizations](#). Contoh yang digunakan dalam topik terkait menyebutkan `ec2`. Saat Anda menggunakan contoh ini, ganti `ec2` dengan `s3`.

Daftar berikut menjelaskan apa yang dapat Anda lakukan dengan menggunakan TBAC:

- Cegah semua pengguna kecuali Perlindungan Malware untuk prinsipal layanan S3 membaca objek S3 yang belum ditandai dengan pasangan nilai kunci tag berikut:

GuardDutyMalwareScanStatus:*Potential key value*

- Izinkan hanya GuardDuty untuk menambahkan kunci tag GuardDutyMalwareScanStatus dengan nilai sebagai hasil pemindaian, ke objek S3 yang dipindai. Templat kebijakan berikut dapat mengizinkan pengguna tertentu yang memiliki akses, untuk berpotensi mengganti pasangan nilai kunci tag.

Contoh kebijakan sumber daya bucket S3:

Ganti nilai-nilai placeholder berikut dalam contoh kebijakan:

- *IAM-role-name*- Berikan peran IAM yang Anda gunakan untuk mengonfigurasi Perlindungan Malware untuk S3 di bucket Anda.
- *555555555555*- Berikan yang Akun AWS terkait dengan ember yang dilindungi.
- *amzn-s3-demo-bucket*- Berikan nama bucket yang dilindungi.

```

{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "NoReadUnlessClean",
    "Effect": "Deny",
    "NotPrincipal": {
      "AWS": [
        "arn:aws:sts::555555555555:assumed-role/IAM-role-name/
GuardDutyMalwareProtection",
        "arn:aws:iam::555555555555:role/IAM-role-name"
      ]
    },
    "Action": [
      "s3:GetObject",
      "s3:GetObjectVersion"
    ],
    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
    "Condition": {
      "StringNotEquals": {
        "s3:ExistingObjectTag/GuardDutyMalwareScanStatus":
"NO_THREATS_FOUND"
      }
    }
  },
  {
    "Sid": "OnlyGuardDutyCanTagScanStatus",
    "Effect": "Deny",
    "NotPrincipal": {
      "AWS": [
        "arn:aws:sts::555555555555:assumed-role/IAM-role-name/
GuardDutyMalwareProtection",
        "arn:aws:iam::555555555555:role/IAM-role-name"
      ]
    },
    "Action": "s3:PutObjectTagging",
    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
    "Condition": {
      "ForAnyValue:StringEquals": {
        "s3:RequestObjectTagKeys": "GuardDutyMalwareScanStatus"
      }
    }
  }
]

```

```
}
```

Untuk informasi selengkapnya tentang menandai sumber daya S3 Anda, kebijakan [Penandaan dan kontrol akses](#).

Melihat dan memahami status bucket yang dilindungi

Setelah mengaktifkan Perlindungan Malware untuk S3 untuk bucket, status menunjukkan apakah fitur tersebut dikonfigurasi dan berfungsi seperti yang diharapkan. Status ini dikaitkan dengan pengenalan paket Perlindungan Malware (ID) yang unik. GuardDuty membuat ID ini pada saat mengaktifkan fitur.

Gunakan prosedur berikut untuk melihat status bucket yang dilindungi:

1. Masuk ke AWS Management Console dan buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.
2. Di panel navigasi, pilih Perlindungan Malware untuk S3.
3. Di tabel bucket Protected, lihat kolom Status yang sesuai untuk bucket S3 Anda.

Tabel berikut mencantumkan dan menjelaskan nilai status yang terkait dengan sumber daya paket Perlindungan Malware Anda. Dengan memahami apa arti status ini bagi bucket yang dilindungi, Anda dapat memastikan bahwa GuardDuty memulai pemindaian malware otomatis saat objek diunggah.

Status	Deskripsi
Aktif	Bucket S3 Anda telah berhasil dikonfigurasi dengan Perlindungan Malware untuk S3. Saat status Aktif, perubahan pada peran IAM (penghapusan atau modifikasi izin) tidak akan memperbarui status ke Peringatan atau Kesalahan. Kami merekomendasikan untuk memantau status pemindaian secara terus menerus dengan menggunakan salah satu metode yang dijelaskan dalam Memantau pemindaian objek S3.
Peringatan [*] -	Perlindungan Malware untuk S3 dirancang agar tidak terpengaruh saat peringatan muncul. Ketika GuardDuty melihat objek S3 baru, itu akan memulai pemindaian malware. Setelah berhasil memulai pemindaian, nilai kolom Status mungkin memerlukan

Status	Deskripsi
	n beberapa menit untuk berubah menjadi Aktif. Anda akan menerima EventBridge pemberitahuan setelah pembaruan nilai kolom Status.
Kesalahan [*]	Ember Anda tidak terlindungi. Tak satu pun dari pemindaian malware yang terkait dengan bucket S3 ini akan selesai. Mungkin ada satu atau lebih akar penyebab potensial.

^{*} Untuk informasi tentang potensi masalah dan langkah-langkah terkait untuk menyelesaikannya, lihat [Memecahkan masalah status paket Perlindungan Malware](#).

Memecahkan masalah status paket Perlindungan Malware

Untuk bucket yang dilindungi, GuardDuty menampilkan Status berdasarkan peringkat. Misalnya, jika bucket yang dilindungi memiliki masalah di kategori Kesalahan dan Peringatan, pertama-tama GuardDuty akan menampilkan masalah yang terkait dengan status Kesalahan.

Daftar berikut mencakup kesalahan dan peringatan untuk status paket Perlindungan Malware.

Kesalahan

- [EventBridge pemberitahuan dinonaktifkan untuk bucket S3 ini](#)
- [EventBridge aturan terkelola untuk menerima peristiwa bucket S3 tidak ada](#)
- [Bucket S3 tidak ada lagi](#)

Peringatan

[Tidak dapat menempatkan objek uji](#)

EventBridge pemberitahuan dinonaktifkan untuk bucket S3 ini

Kode alasan status terkait adalah `EVENTBRIDGE_MANAGED_EVENTS_DELIVERY_DISABLED`.

Detail status

GuardDuty menggunakan EventBridge untuk menerima pemberitahuan saat objek baru diunggah ke bucket S3 ini. Izin ini tidak ada dalam peran IAM Anda.

Langkah-langkah untuk memecahkan masalah

Opsi 1: Tambahkan pernyataan izin berikut ke peran IAM Anda:

```
{
  "Sid": "AllowEnableS3EventBridgeEvents",
  "Effect": "Allow",
  "Action": [
    "s3:PutBucketNotification",
    "s3:GetBucketNotification"
  ],
  "Resource": [
    "arn:aws:s3:::amzn-s3-demo-bucket"
  ]
}
```

Ganti *amzn-s3-demo-bucket* dengan nama bucket Amazon S3 Anda.

Opsi 2: Aktifkan EventBridge notifikasi dengan menggunakan konsol Amazon S3

1. Buka konsol Amazon S3 di <https://console.aws.amazon.com/s3/>
2. Pada halaman Bucket, di bawah tab Bucket tujuan umum, pilih nama bucket yang terkait dengan kesalahan ini.
3. Pada halaman bucket ini, pilih tab Properties.
4. Di bawah EventBridge bagian Amazon, pilih Edit.
5. Di EventBridge halaman Edit Amazon, untuk Kirim pemberitahuan ke Amazon EventBridge untuk semua acara di bucket ini, pilih Aktif.
6. Pilih Simpan perubahan.

Mungkin perlu beberapa menit agar nilai kolom Status berubah menjadi Aktif.

EventBridge aturan terkelola untuk menerima peristiwa bucket S3 tidak ada

Kode alasan status terkait adalah `EVENTBRIDGE_MANAGED_RULE_DISABLED`.

Detail status

EventBridge Izin aturan terkelola untuk mengelola pengaturan EventBridge aturan tidak ada.

Langkah-langkah untuk memecahkan masalah

Tambahkan pernyataan izin berikut ke peran IAM Anda:

```
{
  "Sid": "AllowManagedRuleToSendS3EventsToGuardDuty",
  "Effect": "Allow",
  "Action": [
    "events:PutRule",
    "events>DeleteRule",
    "events:PutTargets",
    "events:RemoveTargets"
  ],
  "Resource": [
    "arn:aws:events::*:rule/DO-NOT-DELETE-AmazonGuardDutyMalwareProtectionS3*"
  ],
  "Condition": {
    "StringEquals": {
      "events:ManagedBy": "malware-protection-plan.guardduty.amazonaws.com"
    }
  }
}
```

Mungkin perlu beberapa menit agar nilai kolom Status berubah menjadi Aktif.

Bucket S3 tidak ada lagi

Kode alasan status terkait adalah `PROTECTED_RESOURCE_DELETED`.

Detail status

Bucket S3 ini telah dihapus dari akun Anda dan tidak ada lagi.

Langkah untuk memecahkan masalah

Jika menghapus bucket S3 tidak disengaja, maka Anda dapat membuat bucket baru dengan menggunakan konsol Amazon S3.

Setelah berhasil membuat bucket, aktifkan Perlindungan Malware untuk S3 dengan mengikuti langkah-langkah di bawah [Mengonfigurasi Perlindungan Malware untuk S3 untuk bucket Anda](#) halaman.

Tidak dapat menempatkan objek uji

Kode alasan status terkait adalah `INSUFFICIENT_TEST_OBJECT_PERMISSIONS`.

Note

Izin untuk menambahkan objek uji adalah opsional. Kehilangan izin ini dalam peran IAM Anda tidak mencegah Perlindungan Malware untuk S3 untuk memulai pemindaian malware pada objek yang baru diunggah. Setelah pemindaian berhasil dimulai, mungkin diperlukan beberapa menit agar Status paket Perlindungan Malware berubah dari Peringatan menjadi Aktif.

Jika peran IAM sudah menyertakan izin ini, maka peringatan ini menunjukkan kebijakan bucket Amazon S3 terbatas yang tidak mengizinkan akses IAM untuk menempatkan objek pengujian di bucket S3 ini.

Detail status

Untuk memvalidasi penyiapan bucket yang dipilih, GuardDuty letakkan objek uji di bucket Anda.

Langkah-langkah untuk memecahkan masalah

Anda dapat memilih untuk memperbarui peran IAM untuk menyertakan izin yang hilang. Untuk peran IAM yang dipilih, tambahkan izin berikut sehingga GuardDuty dapat menempatkan objek uji ke sumber daya yang dipilih:

```
{
  "Sid": "AllowPutValidationObject",
  "Effect": "Allow",
  "Action": [
    "s3:PutObject"
  ],
  "Resource": [
    "arn:aws:s3:::amzn-s3-demo-bucket/malware-protection-resource-validation-object"
  ]
}
```

Ganti *amzn-s3-demo-bucket* dengan nama bucket Amazon S3 Anda. Untuk informasi tentang izin peran IAM, lihat [Membuat atau memperbarui kebijakan peran IAM](#)

Mungkin perlu beberapa menit agar nilai kolom Status berubah menjadi Aktif.

Memantau pemindaian objek S3 di Perlindungan Malware untuk S3

Saat menggunakan Perlindungan Malware untuk S3 dengan ID GuardDuty detektor, jika objek Amazon S3 Anda berpotensi berbahaya GuardDuty, akan dihasilkan. [Perlindungan Malware untuk tipe pencarian S3](#) Menggunakan GuardDuty konsol dan APIs, Anda dapat melihat temuan yang dihasilkan. Untuk informasi tentang memahami jenis temuan ini, lihat [Detail temuan](#).

Saat menggunakan Perlindungan Malware untuk S3 tanpa mengaktifkan GuardDuty (tanpa ID detektor), bahkan ketika objek Amazon S3 yang dipindai berpotensi berbahaya, tidak GuardDuty dapat menghasilkan temuan apa pun.

Daftar Isi

- [Status pemindaian potensial objek S3 dan status hasil](#)
- [Memantau pemindaian objek S3 dengan Amazon EventBridge](#)
- [Memantau pemindaian objek S3 dengan GuardDuty tag terkelola](#)
- [Metrik status pemindaian objek S3 di CloudWatch](#)

Status pemindaian potensial objek S3 dan status hasil

Bagian ini menjelaskan potensi nilai status pemindaian objek S3 dan nilai hasil pemindaian.

Status pemindaian objek S3 menunjukkan status pemindaian malware, seperti selesai, dilewati, atau gagal.

Status hasil pemindaian malware objek S3 menunjukkan hasil pemindaian berdasarkan nilai status pemindaian. Setiap nilai status hasil pemindaian malware memetakan ke status pemindaian.

Daftar berikut memberikan nilai hasil pemindaian objek S3 potensial. Jika Anda telah mengaktifkan penandaan, Anda dapat memantau hasil pemindaian dengan [Menggunakan Tag Objek S3](#). Setelah pemindaian, nilai tag akan memiliki salah satu nilai hasil pemindaian berikut.

Nilai status hasil pemindaian malware potensial objek S3

- NO_THREATS_FOUND— GuardDuty mendeteksi tidak ada ancaman potensial yang terkait dengan objek yang dipindai.

- **THREATS_FOUND**— GuardDuty mendeteksi potensi ancaman yang terkait dengan objek yang dipindai.
- **UNSUPPORTED**— Ada beberapa alasan mengapa Perlindungan Malware untuk S3 akan melewati pemindaian. Alasan potensial termasuk file yang dilindungi kata sandi, arsip dengan rasio kompresi yang sangat tinggi [Perlindungan Malware untuk kuota S3](#), dan dukungan untuk fitur Amazon S3 tertentu mungkin tidak tersedia. Untuk informasi selengkapnya, lihat [Kemampuan Perlindungan Malware untuk S3](#).
- **ACCESS_DENIED**— tidak GuardDuty dapat mengakses objek ini untuk pemindaian. Periksa izin peran IAM yang terkait dengan bucket ini. Untuk informasi selengkapnya, lihat [Membuat atau memperbarui kebijakan peran IAM](#).

Jika Anda telah mengaktifkan penandaan objek S3 pasca-pemindaian, lihat. [Memecahkan masalah kegagalan tag pasca-pemindaian objek S3](#)

- **FAILED**— tidak GuardDuty dapat melakukan pemindaian malware pada objek ini karena kesalahan internal.

Daftar berikut memberikan nilai status pemindaian objek S3 potensial dan pemetaannya ke hasil pemindaian objek S3.

Nilai status pemindaian potensial objek S3

- **Selesai** — Pemindaian berhasil diselesaikan dan menunjukkan apakah objek S3 memiliki malware. Dalam hal ini, potensi nilai hasil pemindaian objek S3 dapat berupa **THREATS_FOUND** atau **NO_THREATS_FOUND**.
- **Dilewati** — GuardDuty melewati pemindaian malware saat memindai objek S3 ini tidak didukung oleh Perlindungan Malware untuk S3, atau GuardDuty tidak memiliki akses ke objek S3 yang diunggah di bucket yang dipilih.

Dalam hal ini, potensi nilai hasil pemindaian objek S3 dapat berupa **UNSUPPORTED** atau **ACCESS_DENIED**.

GuardDuty juga akan melewati pemindaian jika peran IAM yang diperlukan dihapus.

- **Gagal** — Mirip dengan nilai hasil pemindaian objek S3 **FAILED**, status pemindaian GuardDuty ini berarti tidak dapat melakukan pemindaian malware pada objek S3 karena kesalahan internal.

Memantau pemindaian objek S3 dengan Amazon EventBridge

Amazon EventBridge adalah layanan bus acara tanpa server yang memudahkan untuk menghubungkan aplikasi Anda dengan data dari berbagai sumber. EventBridge mengirimkan aliran data real-time dari aplikasi Anda sendiri, aplikasi Software-as-a-Service (SaaS), AWS dan layanan dan rute data tersebut ke target seperti Lambda. Hal ini memungkinkan Anda memantau kejadian yang terjadi dalam layanan, dan membangun arsitektur yang didorong kejadian. Untuk informasi selengkapnya, lihat [Panduan EventBridge Pengguna Amazon](#).

Sebagai akun pemilik bucket S3 yang dilindungi dengan Perlindungan Malware untuk S3, GuardDuty menerbitkan EventBridge notifikasi ke bus acara default dalam skenario berikut:

- Perubahan status sumber daya paket Perlindungan Malware untuk setiap bucket Anda yang dilindungi. Untuk informasi tentang berbagai status, lihat [Melihat dan memahami status bucket yang dilindungi](#).

Untuk menyiapkan aturan Amazon EventBridge (EventBridge) untuk status sumber daya, lihat [Status sumber daya paket Perlindungan Malware](#).

- Hasil pemindaian objek S3 akan dipublikasikan ke bus EventBridge acara default Anda.

`s3ThrottledBidang` menunjukkan apakah ada penundaan dalam mengunggah atau mengambil penyimpanan dari Amazon S3 atau tidak. Nilai `true` menunjukkan bahwa ada penundaan, dan `false` menunjukkan bahwa tidak ada penundaan.

Jika `s3Throttled true` untuk hasil pemindaian Anda, Amazon S3 merekomendasikan pengaturan awalan dengan cara yang membantu Anda mengurangi transaksi per detik (TPS) untuk setiap awalan. Untuk informasi selengkapnya, lihat [Pola desain praktik terbaik: mengoptimalkan kinerja Amazon S3](#) di Panduan Pengguna Amazon S3.

Untuk menyiapkan aturan Amazon EventBridge (EventBridge) untuk hasil pemindaian objek S3, lihat [Hasil pemindaian objek S3](#).

- Ada peristiwa kegagalan tag pasca-pemindaian karena alasan berikut:
 - Peran IAM Anda tidak memiliki izin untuk menandai objek.

[Menambahkan izin kebijakan IAM](#) Template termasuk izin GuardDuty untuk menandai objek.

- Sumber daya bucket atau objek yang ditentukan dalam peran IAM tidak ada lagi.

- Objek S3 terkait telah mencapai batas tag maksimum. Untuk informasi selengkapnya tentang batas tag, lihat [Mengategorikan penyimpanan menggunakan tag](#) di Panduan Pengguna Amazon S3.

Untuk menyiapkan aturan Amazon EventBridge (EventBridge) untuk peristiwa kegagalan tag pasca-pemindaian, lihat [Peristiwa kegagalan tag pasca-pemindaian](#).

Menyiapkan EventBridge aturan

Anda dapat mengatur EventBridge aturan di akun Anda untuk mengirim status sumber daya, peristiwa kegagalan tag pasca-pemindaian, atau hasil pemindaian objek S3 ke yang lain. Layanan AWS Sebagai akun GuardDuty administrator yang didelegasikan, Anda akan menerima pemberitahuan status sumber daya paket Perlindungan Malware ketika ada perubahan status.

EventBridge Harga standar akan berlaku. Untuk informasi selengkapnya, lihat [EventBridge harga Amazon](#).

Semua nilai yang muncul di *red* adalah placeholder untuk contoh. Nilai-nilai ini akan berubah berdasarkan nilai di akun Anda, dan apakah malware terdeteksi atau tidak.

Topik

- [Status sumber daya paket Perlindungan Malware](#)
- [Hasil pemindaian objek S3](#)
- [Peristiwa kegagalan tag pasca-pemindaian](#)

Status sumber daya paket Perlindungan Malware

Anda dapat membuat pola EventBridge acara berdasarkan skenario berikut:

detail-type Nilai potensial

- "GuardDuty Malware Protection Resource Status Active"
- "GuardDuty Malware Protection Resource Status Warning"
- "GuardDuty Malware Protection Resource Status Error"

Pola acara

```
{
  "detail-type": ["potential detail-type"],
  "source": ["aws.guarddduty"]
}
```

Contoh skema pemberitahuan untuk **GuardDuty Malware Protection Resource Status Active**:

```
{
  "version": "0",
  "id": "6a7e8feb-b491-4cf7-a9f1-bf3703467718",
  "detail-type": "GuardDuty Malware Protection Resource Status Active",
  "source": "aws.guarddduty",
  "account": "111122223333",
  "time": "2017-12-22T18:43:48Z",
  "region": "us-east-1",
  "resources": ["arn:aws:guardduty:us-east-1:111122223333:malware-protection-plan/b4c7f464ab3a4EXAMPLE"],
  "detail": {
    "schemaVersion": "1.0",
    "eventTime": "2024-02-28T01:01:01Z",
    "s3BucketDetails": {
      "bucketName": "amzn-s3-demo-bucket"
    },
    "resourceStatus": "ACTIVE"
  }
}
```

Contoh skema pemberitahuan untuk **GuardDuty Malware Protection Resource Status Warning**:

```
{
  "version": "0",
  "id": "6a7e8feb-b491-4cf7-a9f1-bf3703467718",
  "detail-type": "GuardDuty Malware Protection Resource Status warning",
  "source": "aws.guarddduty",
  "account": "111122223333",
  "time": "2017-12-22T18:43:48Z",
  "region": "us-east-1",
  "resources": ["arn:aws:guardduty:us-east-1:111122223333:malware-protection-plan/b4c7f464ab3a4EXAMPLE"],
  "detail": {
```

```

    "schemaVersion": "1.0",
    "eventTime": "2024-02-28T01:01:01Z",
    "s3BucketDetails": {
      "bucketName": "amzn-s3-demo-bucket"
    },
    "resourceStatus": "WARNING",
    "statusReasons": [
      {
        "code": "INSUFFICIENT_TEST_OBJECT_PERMISSIONS"
      }
    ]
  }
}

```

Contoh skema pemberitahuan untuk **GuardDuty Malware Protection Resource Status Error**:

```

{
  "version": "0",
  "id": "fc7a35b7-83bd-3c1f-ecfa-1b8de9e7f7d2",
  "detail-type": "GuardDuty Malware Protection Resource Status Error",
  "source": "aws.guardduty",
  "account": "111122223333",
  "time": "2017-12-22T18:43:48Z",
  "region": "us-east-1",
  "resources": ["arn:aws:guardduty:us-east-1:111122223333:malware-protection-plan/b4c7f464ab3a4EXAMPLE"],
  "detail": {
    "schemaVersion": "1.0",
    "eventTime": "2024-02-28T01:01:01Z",
    "s3BucketDetails": {
      "bucketName": "amzn-s3-demo-bucket"
    },
    "resourceStatus": "ERROR",
    "statusReasons": [
      {
        "code": "EVENTBRIDGE_MANAGED_EVENTS_DELIVERY_DISABLED"
      }
    ]
  }
}

```

Berdasarkan alasan di balik resourceStatusERROR, statusReasons nilainya akan terisi.

Untuk informasi tentang langkah-langkah pemecahan masalah untuk peringatan dan kesalahan berikut, lihat. [Memecahkan masalah status paket Perlindungan Malware](#)

Hasil pemindaian objek S3

```
{
  "detail-type": ["GuardDuty Malware Protection Object Scan Result"],
  "source": ["aws.guarddduty"]
}
```

Contoh skema pemberitahuan untuk **NO_THREATS_FOUND**:

```
{
  "version": "0",
  "id": "72c7d362-737a-6dce-fc78-9e27a0171419",
  "detail-type": "GuardDuty Malware Protection Object Scan Result",
  "source": "aws.guarddduty",
  "account": "111122223333",
  "time": "2024-02-28T01:01:01Z",
  "region": "us-east-1",
  "resources": ["arn:aws:guarddduty:us-east-1:111122223333:malware-protection-plan/b4c7f464ab3a4EXAMPLE"],
  "detail": {
    "schemaVersion": "1.0",
    "scanStatus": "COMPLETED",
    "resourceType": "S3_OBJECT",
    "s3ObjectDetails": {
      "bucketName": "amzn-s3-demo-bucket",
      "objectKey": "APKAEIBAERJR2EXAMPLE",
      "eTag": "ASIAI44QH8DHBEXAMPLE",
      "versionId": "d41d8cd98f00b204e9800998eEXAMPLE",
      "s3Throttled": false
    },
    "scanResultDetails": {
      "scanResultStatus": "NO_THREATS_FOUND",
      "threats": null
    }
  }
}
```

Contoh skema pemberitahuan untuk **THREATS_FOUND**:

```
{
```



```

"version": "0",
"id": "72c7d362-737a-6dce-fc78-9e27a0171419",
"detail-type": "GuardDuty Malware Protection Object Scan Result",
"source": "aws.guardduty",
"account": "111122223333",
"time": "2024-02-28T01:01:01Z",
"region": "us-east-1",
"resources": ["arn:aws:guardduty:us-east-1:111122223333:malware-protection-plan/
b4c7f464ab3a4EXAMPLE"],
"detail": {
  "schemaVersion": "1.0",
  "scanStatus": "COMPLETED",
  "resourceType": "S3_OBJECT",
  "s3ObjectDetails": {
    "bucketName": "amzn-s3-demo-bucket",
    "objectKey": "APKAEIBAERJR2EXAMPLE",
    "eTag": "ASIAI44QH8DHBEXAMPLE",
    "versionId": "d41d8cd98f00b204e9800998eEXAMPLE",
    "s3Throttled": false
  },
  "scanResultDetails": {
    "scanResultStatus": "THREATS_FOUND",
    "threats": [
      {
        "name": "EICAR-Test-File (not a virus)"
      }
    ]
  }
}
}

```

Note

scanResultDetails.ThreatsBidang ini hanya berisi satu ancaman. Secara default, Perlindungan Malware untuk pemindaian S3 melaporkan ancaman pertama yang terdeteksi. Setelah ini, scanStatus diatur keCOMPLETED.

Skema pemberitahuan sampel untuk status hasil pemindaian **UNSUPPORTED** (Dilewati):

```

{
  "version": "0",

```

```

    "id": "72c7d362-737a-6dce-fc78-9e27a0EXAMPLE",
    "detail-type": "GuardDuty Malware Protection Object Scan Result",
    "source": "aws.guardduty",
    "account": "111122223333",
    "time": "2024-02-28T01:01:01Z",
    "region": "us-east-1",
    "resources": ["arn:aws:guardduty:us-east-1:111122223333:malware-protection-plan/
b4c7f464ab3a4EXAMPLE"],
    "detail": {
      "schemaVersion": "1.0",
      "scanStatus": "SKIPPED",
      "resourceType": "S3_OBJECT",
      "s3ObjectDetails": {
        "bucketName": "amzn-s3-demo-bucket",
        "objectKey": "APKAEIBAERJR2EXAMPLE",
        "eTag": "ASIAI44QH8DHBEXAMPLE",
        "versionId": "d41d8cd98f00b204e9800998eEXAMPLE",
        "s3Throttled": false
      },
      "scanResultDetails": {
        "scanResultStatus": "UNSUPPORTED",
        "threats": null
      }
    }
  }
}

```

Skema pemberitahuan sampel untuk status hasil pemindaian **ACCESS_DENIED** (Dilewati):

```

{
  "version": "0",
  "id": "72c7d362-737a-6dce-fc78-9e27a0EXAMPLE",
  "detail-type": "GuardDuty Malware Protection Object Scan Result",
  "source": "aws.guardduty",
  "account": "111122223333",
  "time": "2024-02-28T01:01:01Z",
  "region": "us-east-1",
  "resources": ["arn:aws:guardduty:us-east-1:111122223333:malware-protection-plan/
b4c7f464ab3a4EXAMPLE"],
  "detail": {
    "schemaVersion": "1.0",
    "scanStatus": "SKIPPED",
    "resourceType": "S3_OBJECT",
    "s3ObjectDetails": {

```

```

        "bucketName": "amzn-s3-demo-bucket",
        "objectKey": "APKAEIBAERJR2EXAMPLE",
        "eTag": "ASIAI44QH8DHBEXAMPLE",
        "versionId" : "d41d8cd98f00b204e9800998eEXAMPLE",
        "s3Throttled": false
    },
    "scanResultDetails": {
        "scanResultStatus": "ACCESS_DENIED",
        "threats": null
    }
}

```

Skema pemberitahuan sampel untuk status **FAILED** hasil pemindaian:

```

{
  "version": "0",
  "id": "72c7d362-737a-6dce-fc78-9e27a0EXAMPLE",
  "detail-type": "GuardDuty Malware Protection Object Scan Result",
  "source": "aws.guardduty",
  "account": "111122223333",
  "time": "2024-02-28T01:01:01Z",
  "region": "us-east-1",
  "resources": ["arn:aws:guardduty:us-east-1:111122223333:malware-protection-plan/b4c7f464ab3a4EXAMPLE"],
  "detail": {
    "schemaVersion": "1.0",
    "scanStatus": "FAILED",
    "resourceType": "S3_OBJECT",
    "s3ObjectDetails": {
      "bucketName": "amzn-s3-demo-bucket",
      "objectKey": "APKAEIBAERJR2EXAMPLE",
      "eTag": "ASIAI44QH8DHBEXAMPLE",
      "versionId" : "d41d8cd98f00b204e9800998eEXAMPLE",
      "s3Throttled": false
    },
    "scanResultDetails": {
      "scanResultStatus": "FAILED",
      "threats": null
    }
  }
}

```

Peristiwa kegagalan tag pasca-pemindaian

Pola acara:

```
{
  "detail-type": "GuardDuty Malware Protection Post Scan Action Failed",
  "source": "aws.guarddduty"
}
```

Contoh skema pemberitahuan untuk **ACCESS_DENIED**:

```
{
  "version": "0",
  "id": "746acd83-d75c-5b84-91d2-dad5f13ba0d7",
  "detail-type": "GuardDuty Malware Protection Post Scan Action Failed",
  "source": "aws.guarddduty",
  "account": "111122223333",
  "time": "2024-06-10T16:16:08Z",
  "region": "us-east-1",
  "resources": ["arn:aws:guarddduty:us-east-1:111122223333:malware-protection-plan/b4c7f464ab3a4EXAMPLE"],
  "detail": {
    "schemaVersion": "1.0",
    "eventTime": "2024-06-10T16:16:08Z",
    "s3ObjectDetails": {
      "bucketName": "amzn-s3-demo-bucket",
      "objectKey": "2024-03-10-16-16-00-7D723DE8DBE9Y2E0",
      "eTag": "0e9eeec810ad8b61d69112c15c2a5hb6",
      "versionId": "d41d8cd98f00b204e9800998eEXAMPLE",
      "s3Throttled": false
    },
    "postScanActions": [{
      "actionType": "TAGGING",
      "failureReason": "ACCESS_DENIED"
    }]
  }
}
```

Contoh skema pemberitahuan untuk **MAX_TAG_LIMIT_EXCEEDED**:

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

```
{
  "id": "746acd83-d75c-5b84-91d2-dad5f13ba0d7",
  "detail-type": "GuardDuty Malware Protection Post Scan Action Failed",
  "source": "aws.guardduty",
  "account": "111122223333",
  "time": "2024-06-10T16:16:08Z",
  "region": "us-east-1",
  "resources": ["arn:aws:guardduty:us-east-1:111122223333:malware-protection-plan/b4c7f464ab3a4EXAMPLE"],
  "detail": {
    "schemaVersion": "1.0",
    "eventTime": "2024-06-10T16:16:08Z",
    "s3objectDetails": {
      "bucketName": "amzn-s3-demo-bucket",
      "objectKey": "2024-03-10-16-16-00-7D723DE8DBE9Y2E0",
      "eTag": "0e9eeec810ad8b61d69112c15c2a5hb6",
      "versionId": "d41d8cd98f00b204e9800998eEXAMPLE",
      "s3Throttled": false
    },
    "postScanActions": [{
      "actionType": "TAGGING",
      "failureReason": "MAX_TAG_LIMIT_EXCEEDED"
    }]
  }
}
```

Untuk memecahkan masalah alasan kegagalan ini, lihat [Memecahkan masalah kegagalan tag pasca-pemindaian objek S3](#)

Memantau pemindaian objek S3 dengan GuardDuty tag terkelola

Gunakan opsi aktifkan penandaan sehingga GuardDuty dapat menambahkan tag ke objek Amazon S3 Anda setelah menyelesaikan pemindaian malware.

Pertimbangan untuk mengaktifkan penandaan

- Ada biaya penggunaan terkait saat GuardDuty menandai objek S3 Anda. Untuk informasi selengkapnya, lihat [Harga dan biaya penggunaan untuk Perlindungan Malware untuk S3](#).
- Anda harus menyimpan izin penandaan yang diperlukan untuk peran IAM pilihan yang terkait dengan bucket ini; jika tidak, tidak GuardDuty dapat menambahkan tag ke objek yang dipindai. Peran IAM sudah menyertakan izin untuk menambahkan tag ke objek S3 yang dipindai. Untuk informasi selengkapnya, lihat [Membuat atau memperbarui kebijakan peran IAM](#).

- Secara default, Anda dapat mengaitkan hingga 10 tag dengan objek S3. Untuk informasi selengkapnya, lihat [Menggunakan kontrol akses berbasis tag \(TBAC\)](#).

Setelah Anda mengaktifkan penandaan untuk bucket S3 atau awalan tertentu, objek apa pun yang baru diunggah yang dipindai, akan memiliki tag terkait dalam format pasangan nilai kunci berikut:

GuardDutyMalwareScanStatus:*Scan-Result-Status*

Untuk informasi tentang nilai tag potensial, lihat [Status pemindaian potensial objek S3 dan status hasil](#).

Memecahkan masalah kegagalan tag pasca-pemindaian objek S3 di Perlindungan Malware untuk S3

Bagian ini hanya berlaku untuk Anda jika Anda [Aktifkan penandaan untuk objek yang dipindai](#) berada dalam ember yang dilindungi.

Saat GuardDuty mencoba menambahkan tag ke objek S3 yang dipindai, tindakan penandaan dapat mengakibatkan kegagalan. Alasan potensial mengapa hal ini dapat terjadi pada ember Anda adalah ACCESS_DENIED dan MAX_TAG_LIMIT_EXCEEDED. Gunakan topik berikut untuk memahami alasan potensial untuk alasan kegagalan tag pasca-pemindaian ini dan selesaikan masalahnya.

ACCESS_DITOLAK

Daftar berikut memberikan alasan potensial yang dapat menyebabkan masalah ini:

- Peran IAM yang digunakan untuk bucket S3 yang dilindungi ini tidak memiliki izin. AllowPostScanTag Verifikasi bahwa peran IAM terkait menggunakan kebijakan bucket ini. Untuk informasi selengkapnya, lihat [Membuat atau memperbarui kebijakan peran IAM](#).
- Kebijakan bucket S3 yang dilindungi tidak memungkinkan GuardDuty untuk menambahkan tag ke objek ini.
- Objek S3 yang dipindai tidak ada lagi.

MAX_TAG_LIMIT_EXCEEDED

Secara default, Anda dapat mengaitkan hingga 10 tag dengan objek S3. Untuk informasi selengkapnya, lihat Pertimbangan GuardDuty untuk menambahkan tag ke objek S3 Anda di bawah. [Aktifkan penandaan untuk objek yang dipindai](#)

Metrik status pemindaian objek S3 di CloudWatch

Anda dapat memantau GuardDuty penggunaan CloudWatch, yang mengumpulkan data mentah dan memprosesnya menjadi metrik yang dapat dibaca, mendekati waktu nyata. Statistik ini disimpan selama 15 bulan, sehingga Anda dapat mengakses informasi historis dan mendapatkan perspektif yang lebih baik tentang bagaimana kinerja Perlindungan Malware untuk S3. Anda juga dapat mengatur alarm yang memperhatikan ambang batas tertentu dan mengirim notifikasi atau mengambil tindakan saat ambang batas tersebut terpenuhi. Untuk informasi selengkapnya, lihat [Panduan CloudWatch Pengguna Amazon](#).

CloudWatch Metrik untuk Perlindungan Malware untuk S3 tersedia di tingkat sumber daya. Anda dapat menanyakan metrik ini untuk setiap sumber daya yang dilindungi secara terpisah. Metrik dilaporkan di `AWS/GuardDuty/MalwareProtection` namespace. Anda dapat mengatur alarm pada sumber daya tertentu untuk memantau postur keamanan.

Metrik status pemindaian malware

Metrik	Deskripsi
CompletedScanCount	Jumlah pemindaian malware objek S3 yang diselesaikan dalam jangka waktu tertentu. Dimensi yang Valid: Malware Protection Plan Id Resource Name Unit: Hitungan
FailedScanCount	Jumlah pemindaian malware objek S3 yang gagal dalam jangka waktu tertentu. Dimensi yang Valid: Malware Protection Plan Id Resource Name

Unit: Hitungan

SkippedScanCount

Jumlah pemindaian malware objek S3 yang dilewati dalam jangka waktu tertentu.

Dimensi yang Valid:

- Malware Protection Plan Id

Resource Name

Skipped Reason

Nilai potensial

- Unsupported
- MissingPermissions

Unit: Hitungan

Metrik hasil pemindaian malware

InfectedScanCount

Jumlah pemindaian malware objek S3 yang mendeteksi objek yang berpotensi berbahaya dalam jangka waktu tertentu.

Dimensi yang Valid:

- Malware Protection Plan Id

Resource Name

Unit: Hitungan

CompletedScanBytes

Jumlah byte objek S3 yang dipindai dalam kerangka waktu tertentu.

Dimensi yang Valid:

- Malware Protection Plan Id

Resource Name

Unit: Hitungan

 Note

Secara default, statistik dalam CloudWatch metrik adalah AVG.

Dimensi berikut didukung untuk metrik Perlindungan Malware untuk S3.

Dimensi	Deskripsi
Malware Protection Plan Id	Pengidentifikasi unik yang terkait dengan sumber daya paket Perlindungan Malware yang GuardDuty dibuat untuk sumber daya Anda yang dilindungi.
Resource Name	Nama sumber daya yang dilindungi.
Skipped Reason	Alasan mengapa pemindaian malware objek S3 dilewati.
	Nilai potensial • Unsupported • MissingPermissions

Untuk informasi tentang mengakses dan menanyakan metrik ini, lihat Menggunakan metrik [Amazon CloudWatch di Panduan Pengguna](#) Amazon. CloudWatch

Untuk informasi tentang mengatur alarm, lihat [Menggunakan CloudWatch alarm Amazon](#) di CloudWatch Panduan Pengguna Amazon.

Mengedit paket Perlindungan Malware untuk bucket yang dilindungi

Anda mungkin perlu mengedit kebijakan izin IAM yang disukai, mengaktifkan atau menonaktifkan penandaan objek S3 yang dipindai, atau menambah atau menghapus awalan objek S3. Misalnya, saat mengaktifkan Perlindungan Malware untuk S3 untuk bucket, Anda memutuskan untuk tidak mengaktifkan penandaan objek S3 yang dipindai dengan hasil pemindaian. Namun, sekarang Anda GuardDuty ingin menambahkan tag yang telah ditentukan dan hasil pemindaian sebagai nilai tag.

Pilih metode akses pilihan untuk memperbarui paket Perlindungan Malware untuk bucket S3 Anda yang dilindungi.

Console

Untuk mengedit paket Perlindungan Malware

1. Masuk ke AWS Management Console dan buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.
2. Di panel navigasi, pilih Perlindungan Malware untuk S3.
3. Di dalam bucket Protected, pilih bucket yang ingin Anda edit konfigurasi yang ada.
4. Pilih Edit.
5. Perbarui konfigurasi dan pengaturan yang ada untuk bucket Anda dan konfirmasi perubahannya. Untuk informasi tentang deskripsi dan langkah-langkah untuk setiap bagian, lihat [Mengaktifkan Perlindungan Malware untuk S3 untuk bucket Anda](#).

Pantau kolom Status untuk bucket yang dilindungi ini. Jika muncul sebagai Peringatan atau Kesalahan, lihat [Memecahkan masalah status paket Perlindungan Malware](#).

API/CLI

Untuk mengedit paket Perlindungan Malware dengan menggunakan API atau AWS CLI

- Dengan menggunakan API

Jalankan [UpdateMalwareProtectionPlan](#) API dengan menggunakan ID paket Perlindungan Malware yang terkait dengan sumber daya paket ini.

Untuk mengambil ID paket Perlindungan Malware di Wilayah tertentu, Anda dapat menjalankan [ListMalwareProtectionPlans](#) API di Wilayah tersebut.

- Dengan menggunakan AWS CLI

Daftar berikut memberikan AWS CLI contoh perintah untuk memperbarui sumber daya paket Perlindungan Malware. Anda akan memerlukan ID paket Perlindungan Malware yang terkait dengan bucket S3 Anda.

AWS CLI contoh perintah

- Gunakan AWS CLI perintah berikut untuk mengaktifkan atau menonaktifkan penandaan untuk sumber daya paket Perlindungan Malware yang terkait dengan bucket S3 Anda:

```
aws guardduty update-malware-protection-plan --malware-protection-plan-id 4cc8bf26c4d75EXAMPLE --actions "Tagging"={"Status"="ENABLED|DISABLED"}
```

- Gunakan AWS CLI perintah berikut untuk menambahkan awalan objek ke sumber daya paket Perlindungan Malware yang terkait dengan bucket S3 Anda:

```
aws guardduty update-malware-protection-plan --malware-protection-plan-id 4cc8bf26c4d75EXAMPLE --protected-resource "S3Bucket"={"ObjectPrefixes"=["amzn-s3-demo-1", "amzn-s3-demo-2"]}
```

Pastikan untuk menyertakan awalan objek yang ada dalam perintah ini; jika tidak, GuardDuty akan menghapus awalan tersebut saat mengedit sumber daya paket Perlindungan Malware.

- Gunakan AWS CLI perintah berikut untuk menghapus awalan objek dari sumber daya paket Perlindungan Malware yang terkait dengan bucket S3 Anda:

```
aws guardduty update-malware-protection-plan --malware-protection-plan-id 4cc8bf26c4d75EXAMPLE --protected-resource "S3Bucket"={"ObjectPrefixes"=[""]}
```

Jika Anda belum memiliki ID paket Perlindungan Malware untuk sumber daya ini, Anda dapat menjalankan AWS CLI perintah berikut dan menggantinya *us-east-1* dengan Wilayah yang ingin Anda daftarkan paket Perlindungan Malware IDs.

```
aws guardduty list-malware-protection-plans --region us-east-1
```

Menonaktifkan Perlindungan Malware untuk S3 untuk bucket yang dilindungi

Saat Anda menonaktifkan Perlindungan Malware untuk S3 untuk bucket yang dilindungi, GuardDuty menghapus ID paket Perlindungan Malware yang terkait dengan bucket tersebut. GuardDuty tidak akan lagi memulai pemindaian malware ketika objek baru diunggah ke bucket ini atau salah satu awalan objek yang dipilih.

Jika Anda telah mengaktifkan GuardDuty dan sekarang ingin menangguhkan atau menonaktifkan GuardDuty, lihat [Menangguhkan atau menonaktifkan GuardDuty](#). Karena tidak ada konsep ID detektor dalam Perlindungan Malware untuk S3, menonaktifkan atau menangguhkan GuardDuty tidak memengaruhi status bucket yang dilindungi di akun Anda. Anda dapat terus menggunakan fitur Perlindungan Malware untuk S3 secara independen dengan harga standar terkait. Untuk informasi selengkapnya, lihat [Meninjau biaya penggunaan untuk Perlindungan Malware untuk S3](#). Untuk berhenti menggunakan Perlindungan Malware untuk S3, Anda harus menonaktifkannya untuk semua ember yang dilindungi di akun Anda. Jika Anda ingin terus menggunakan GuardDuty dan menonaktifkan hanya Perlindungan Malware untuk S3 untuk bucket, langkah-langkah berikut tidak akan memengaruhi konfigurasi GuardDuty layanan dan paket perlindungan lain yang mungkin telah Anda aktifkan.

Pilih metode akses pilihan untuk menonaktifkan Perlindungan Malware untuk S3 di bucket S3 Anda yang dilindungi.

Console

Untuk menonaktifkan Perlindungan Malware untuk S3 dengan menggunakan konsol GuardDuty

1. Masuk ke AWS Management Console dan buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.
2. Di panel navigasi, pilih Perlindungan Malware untuk S3.
3. Di dalam bucket Protected, pilih bucket yang ingin Anda nonaktifkan Perlindungan Malware untuk S3.

Anda hanya dapat memilih satu ember yang dilindungi sekaligus. Untuk menonaktifkan Perlindungan Malware untuk S3 selama lebih dari satu bucket, ikuti langkah-langkah ini lagi untuk bucket S3 lainnya.

4. Pilih Nonaktifkan untuk mengonfirmasi pilihan.

API/CLI

Untuk menonaktifkan Perlindungan Malware untuk S3 dengan menggunakan API atau AWS CLI

- Dengan menggunakan API

Jalankan [DeleteMalwareProtectionPlan](#) API dengan menggunakan ID paket Perlindungan Malware yang terkait dengan sumber daya paket ini.

Untuk mengambil ID paket Perlindungan Malware, Anda dapat menjalankan [ListMalwareProtectionPlans](#) API.

- Dengan menggunakan AWS CLI

Atau, Anda dapat menjalankan AWS CLI perintah berikut untuk menonaktifkan Perlindungan Malware untuk S3 `4cc8bf26c4d75EXAMPLE` dengan menggantinya dengan ID paket Perlindungan Malware yang terkait dengan bucket S3 ini:

```
aws guardduty delete-malware-protection-plan --malware-protection-plan-id 4cc8bf26c4d75EXAMPLE
```

Jika Anda belum memiliki ID paket Perlindungan Malware untuk bucket S3 ini, Anda dapat menjalankan AWS CLI perintah berikut dan menggantinya `us-east-1` dengan Wilayah yang ingin Anda daftarkan paket IDs Perlindungan Malware.

```
aws guardduty list-malware-protection-plans --region us-east-1
```

Dukungan fitur Amazon S3

Tabel berikut menentukan apakah Perlindungan Malware untuk S3 mendukung fitur Amazon S3 yang terdaftar atau tidak.

Apakah dukungan tersedia?	Deskripsi
Ya	Objek S3 dapat diambil tanpa memulihkan secara asinkron.

Apakah dukungan tersedia?	Deskripsi

Apakah dukungan tersedia?	Deskripsi
Bersyarat	• Dukungan Intelligent Tiering tersedia untuk objek S3 di tingkatan Akses Instans Sering, Jarang, dan Arsip. • Tingkat opt-in Archive dan Deep Archive tidak didukung. • Intelligent Tiering selalu membuat objek baru di tingkat Frequent Access. Oleh karena itu, pemindaian objek saat membuat didukung. • Fitur tiering Cerdas Masa Depan mungkin memulai objek di Arsip. Karena itu, ini tidak didukung.
Tidak	GuardDuty hanya mendukung bucket tujuan umum untuk Perlindungan Malware untuk S3.

Apakah dukungan tersedia?	Deskripsi
Tidak	Objek S3 harus dipulihkan sebelum dapat diakses.
Tidak	Perlindungan Malware untuk S3 tidak didukung di Outposts.
Ya	Semua objek S3 yang diunggah dipindai untuk malware. Jika Anda mengunggah objek dengan file versi v1 dan segera mengunggah versi lain yang diganti dengan v2, maka GuardDuty akan memindai file objek versi v1 dan v2. Namun, waktu mulai pemindaian mungkin tidak dalam urutan yang sama.

Apakah dukungan tersedia?	Deskripsi
Ya	Jika bucket tujuan adalah sumber daya yang dilindungi, maka GuardDuty akan memindai semua objek S3 direplikasi ke awalan yang dilindungi dan dipantau.
Tidak	Anda tidak dapat menentukan aturan replikasi berdasarkan tag hasil pemindaian. Amazon S3 tidak mendukung replikasi untuk tag, kecuali saat membuat.

Apakah dukungan tersedia?	Deskripsi
Ya	GuardDuty mendukung pemindaian malware untuk objek S3 yang dienkripsi dengan kunci yang dikelola dan dikelola pelanggan. Pastikan bahwa peran IAM mencakup izin untuk menggunakan kunci. Untuk informasi selengkapnya, lihat Menambahkan izin kebijakan IAM.
Tidak	Perlindungan Malware untuk S3 tidak mendukung pemindaian objek S3 yang dienkripsi dengan kunci yang tidak dapat diakses.

Apakah dukungan tersedia?	Deskripsi
Tidak	Saat objek Amazon S3 Anda dienkripsi dengan menggunakan Klien Enkripsi Amazon S3, objek Anda tidak akan terpapar ke pihak ketiga mana pun, termasuk AWS. Untuk informasi tentang alasan ini tidak didukung, lihat Melindungi data dengan menggunakan enkripsi sisi klien.  Note Objek terenkripsi CSE-KMS diterima sebagai gumpalan terenkripsi di mana enkripsi tidak dapat ditentukan. Oleh karena itu, GuardDuty memprosesnya saat diterima, dan memindai gumpalan terenkripsi sebagai file biasa. GuardDuty tidak mengembalikan status UNSUPPORTED pemindaian untuk objek tersebut, kecuali salah satu yang Kuota dalam Perlindungan Malware untuk S3 melebihi.
Ya	Objek S3 yang terkunci dikunci berdasarkan WORM - Tulis Setelah Membaca Banyak. Perlindungan Malware untuk S3 dapat mengakses dan memindai objek.
Ya	Perlindungan Malware untuk S3 dapat memindai bucket yang diatur dengan Requester Pays. Pemohon akan membayar untuk panggilan S3. Untuk informasi selengkapnya, lihat Menggunakan bucket Requester Pays untuk transfer penyimpanan dan penggunaan di Panduan Pengguna Amazon S3.

Apakah dukungan tersedia?	Deskripsi
Ya	Anda dapat menentukan kebijakan siklus hidup berdasarkan tag hasil pemindaian. Misalnya, hapus objek berbahaya secara otomatis. Untuk informasi selengkapnya tentang konfigurasi lifecycle, lihat Mengelola siklus hidup penyimpanan Anda di Panduan Pengguna Amazon S3 .
Ya	Anda dapat menentukan kebijakan sumber daya bucket berdasarkan tag hasil pemindaian objek S3. Misalnya, mencegah akses ke objek S3 yang belum dipindai, atau ancaman yang GuardDuty terdeteksi. Lihat informasi yang lebih lengkap di Menggunakan kontrol akses berbasis tag based tag (TBAC) dengan Perlindungan Malware untuk S3 .

Kuota dalam Perlindungan Malware untuk S3

Bagian ini menyediakan kuota default, sering disebut sebagai batas. Kecuali ditentukan, setiap kuota adalah Region-specific. Untuk melihat kuota default khusus untuk menggunakan GuardDuty layanan dasar, lihat. [GuardDuty Kuota Amazon](#)

Tabel berikut menjelaskan beberapa kuota yang akan berlaku untuk Anda Akun AWS.

AWS nilai kuota default	Apakah itu dapat disesuaikan?	Deskripsi
5 GB	Tidak	Ukuran objek S3 maksimum yang GuardDuty akan mencoba memindai malware.
5 GB	Tidak	Jumlah maksimum data (dalam GB) yang GuardDuty dapat mengekstr

AWS nilai kuota default	Apakah itu dapat disesuaikan?	Deskripsi
		ak dan menganalisis dari file arsip. GuardDuty akan melewati file arsip yang mengekstrak ke lebih dari 5 GB.
1.000	Tidak	Jumlah maksimum file yang GuardDuty dapat mengekstrak dan menganalisis dalam file arsip. Jika arsip berisi lebih dari 1.000 file, maka GuardDuty harus melewati file yang diarsipkan.  Note Jenis file majemuk berpotensi tunduk pada batasan ini. Jenis file termasuk, tetapi tidak terbatas pada, pesan email yang disandikan Multipurpose Internet Mail Extensions (MIME), file Compiled Python (PYC), file Compiled HTML Help (CHM), semua installer, dan dokumen Format (ODF). OpenDocument
5	Tidak	Tingkat maksimum arsip bersarang yang GuardDuty dapat mengekstrak. Jika arsip menyertakan file yang bersarang di luar nilai ini, maka GuardDuty akan melewati file bersarang tersebut.

AWS nilai kuota default	Apakah itu dapat disesuaikan?	Deskripsi
25	Tidak	Jumlah maksimum bucket S3 yang dapat Anda aktifkan Perlindungan Malware untuk S3. Batas kuota ini adalah per akun di setiap Wilayah.

GuardDuty Perlindungan RDS

[Perlindungan RDS di Amazon GuardDuty menganalisis dan memprofilkan aktivitas login RDS untuk potensi ancaman akses ke database Amazon Aurora Anda \(Amazon Aurora MySQL Compatible Edition dan Aurora PostgreSQL Compatible Edition\) dan Amazon RDS for PostgreSQL.](#)

Perlindungan RDS membantu Anda mengidentifikasi perilaku login yang berpotensi mencurigakan pada basis data yang didukung ini. GuardDuty terus memantau dan profil [Aktivitas login RDS](#) untuk aktivitas anomali. Misalnya, aktor eksternal yang sebelumnya tidak terlihat memiliki akses tidak sah ke database Anda, atau musuh mencoba akses brute-force dengan menebak kata sandi database.

Dengan peluncuran [Amazon Aurora PostgreSQL Limitless Database](#), GuardDuty memperluas [Perlindungan RDS untuk sekarang juga mendukung pemantauan aktivitas login dari Limitless Databases](#). Untuk Akun AWS itu sudah mengaktifkan RDS Protection, secara otomatis GuardDuty akan mulai memantau data login dari Limitless Databases mereka. Untuk akun yang belum mengaktifkan Perlindungan RDS, Anda dapat mempelajari lebih lanjut tentang [30-day free trial](#) dan memilih untuk mengaktifkan fitur ini. Untuk mengaktifkan fitur ini, lihat [Mengaktifkan Perlindungan RDS di lingkungan multi-akun](#) atau [Mengaktifkan Perlindungan RDS untuk akun mandiri](#).

Catatan

RDS untuk instance replika baca PostgreSQL memerlukan instance database utama berada pada versi database yang didukung, dan berhasil direplikasi dari database primer. Untuk informasi tentang replika baca, lihat [Bekerja dengan replika baca instans DB di Panduan Pengguna Amazon RDS](#).

Perlindungan RDS tidak memerlukan infrastruktur tambahan; itu dirancang agar tidak mempengaruhi kinerja instance database Anda. Ketika RDS Protection mendeteksi upaya login yang berpotensi mencurigakan atau tidak normal, GuardDuty hasilkan satu atau lebih detail tentang database yang berpotensi [Jenis temuan Perlindungan RDS](#) dikompromikan.

Uji coba gratis 30 hari

- Saat Anda mengaktifkan GuardDuty di Wilayah baru untuk pertama kalinya, Anda mendapatkan uji coba gratis 30 hari. Akun AWS Dalam hal ini, juga GuardDuty akan mengaktifkan Perlindungan RDS, yang termasuk dalam uji coba gratis. Perlindungan RDS akan mulai memantau perilaku login database Anda.

- Ketika Anda sudah menggunakan GuardDuty dan memutuskan untuk mengaktifkan Perlindungan RDS di Wilayah baru untuk pertama kalinya, akun Anda di Wilayah ini akan mendapatkan uji coba gratis 30 hari untuk Perlindungan RDS.
- Jika Anda telah mengaktifkan Perlindungan RDS, maka dengan peluncuran [Amazon Aurora PostgreSQL Limitless Database](#), secara otomatis akan mulai memantau aktivitas login untuk GuardDuty Database Limitless. Jika uji coba gratis 30 hari Perlindungan RDS Anda telah kedaluwarsa, maka Anda akan mulai mengeluarkan biaya penggunaan yang terkait dengan pemantauan Limitless Databases.
- Anda dapat memilih untuk menonaktifkan Perlindungan RDS di Wilayah mana pun kapan saja.
- Selama uji coba gratis 30 hari, Anda bisa mendapatkan perkiraan biaya penggunaan Anda di akun dan Wilayah tersebut. Setelah uji coba gratis 30 hari berakhir, Perlindungan RDS tidak dinonaktifkan secara otomatis. Akun Anda di Wilayah ini akan mulai menimbulkan biaya penggunaan. Untuk informasi selengkapnya, lihat [Memperkirakan biaya GuardDuty penggunaan](#).

Ketika fitur Perlindungan RDS tidak diaktifkan, GuardDuty tidak mendeteksi perilaku login anomali atau mencurigakan. Jika Anda menonaktifkan Perlindungan RDS, GuardDuty segera berhenti memantau aktivitas login RDS, dan tidak akan mendeteksi potensi ancaman apa pun terhadap instance database yang didukung atau menghasilkan jenis temuan terkait.

[Untuk Wilayah AWS tempat Aurora PostgreSQL Limitless Database didukung, lihat Persyaratan untuk Aurora PostgreSQL Limitless Database.](#)

Basis data Amazon Aurora, Amazon RDS, dan Aurora Limitless yang didukung

Tabel berikut menunjukkan versi database Aurora dan Amazon RDS yang didukung untuk Perlindungan RDS.

Mesin Amazon Aurora dan Amazon RDS DB	Versi mesin yang didukung
Aurora MySQL	• 2.10.2 atau yang lebih baru • 3.02.1 atau yang lebih baru
Aurora PostgreSQL	• 10.23 atau yang lebih baru

Mesin Amazon Aurora dan Amazon RDS DB	Versi mesin yang didukung
	• 11.12 atau yang lebih baru • 12.7 atau yang lebih baru • 13.3 atau yang lebih baru • 14.3 atau yang lebih baru • 15.2 atau lebih baru • 16.1 atau lebih baru
RDS for PostgreSQL	• 14.5 atau lebih baru • 13.8 atau lebih baru • 12.12 atau yang lebih baru • 11.17 atau yang lebih baru • RDS untuk PostgreSQL versi 15 • RDS untuk PostgreSQL versi 16
Basis Data Tanpa Batas Amazon Aurora PostgreSQL	16.4-limitless

Aktivitas login RDS

Saat Anda mengaktifkan fitur Perlindungan RDS, GuardDuty secara otomatis mulai memantau aktivitas login RDS untuk database Anda, langsung dari layanan Aurora dan Amazon RDS. Aktivitas login RDS menangkap upaya login yang berhasil dan gagal yang dilakukan ke lingkungan [Basis data Amazon Aurora, Amazon RDS, dan Aurora Limitless yang didukung](#) Anda AWS. Jika ada indikasi perilaku login anomali, GuardDuty buat temuan dengan detail tentang database yang berpotensi dikompromikan. Saat Anda mengaktifkan Perlindungan RDS untuk pertama kalinya atau Anda memiliki instance database yang baru dibuat, ada periode pembelajaran untuk mendasar perilaku normal. Untuk alasan ini, instance database yang baru diaktifkan atau yang baru dibuat mungkin tidak memiliki temuan login anomali terkait hingga dua minggu.

Ketika Perlindungan RDS mendeteksi potensi ancaman, seperti pola yang tidak biasa dalam serangkaian upaya login yang berhasil, gagal, atau tidak lengkap, GuardDuty menghasilkan satu atau lebih. [Jenis temuan Perlindungan RDS](#) Berdasarkan jenis temuan, mungkin termasuk rincian tentang perilaku anomali, seperti. [Anomali berbasis aktivitas login RDS](#)

GuardDuty tidak mengelola aktivitas login Anda [Database yang didukung](#) atau RDS, atau membuat aktivitas login RDS tersedia untuk Anda.

Mengaktifkan Perlindungan RDS di lingkungan multi-akun

Dalam lingkungan beberapa akun, hanya akun GuardDuty administrator yang didelegasikan yang memiliki opsi untuk mengaktifkan atau menonaktifkan fitur Perlindungan RDS untuk akun anggota di organisasi mereka. Akun GuardDuty anggota tidak dapat mengubah konfigurasi ini dari akun mereka. Akun GuardDuty administrator yang didelegasikan mengelola akun anggota mereka menggunakan AWS Organizations. Akun GuardDuty administrator yang didelegasikan ini dapat memilih untuk mengaktifkan pemantauan aktivitas login RDS secara otomatis untuk semua akun baru saat mereka bergabung dengan organisasi. Untuk informasi selengkapnya tentang lingkungan multi-akun, lihat.

[Beberapa akun di GuardDuty](#)

Mengaktifkan Perlindungan RDS untuk akun administrator yang didelegasikan GuardDuty

Pilih metode akses pilihan Anda untuk mengonfigurasi Pemantauan Aktivitas Login RDS untuk akun GuardDuty administrator yang didelegasikan.

Console

1. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.
2. Di panel navigasi, pilih Perlindungan RDS.
3. Pada halaman Perlindungan RDS, pilih Edit.
4. Lakukan salah satu tindakan berikut:

Menggunakan Aktifkan untuk semua akun

- Pilih Aktifkan untuk semua akun. Ini akan memungkinkan rencana perlindungan untuk semua GuardDuty akun aktif di AWS organisasi Anda, termasuk akun baru yang bergabung dengan organisasi.
- Pilih Simpan.

Menggunakan Konfigurasi akun secara manual

- Untuk mengaktifkan paket perlindungan hanya untuk akun GuardDuty administrator yang didelegasikan, pilih Konfigurasi akun secara manual.

- Pilih Aktifkan di bawah bagian akun GuardDuty administrator yang didelegasikan (akun ini).
- Pilih Simpan.

API/CLI

Jalankan operasi [updateDetector](#) API menggunakan ID detektor regional Anda sendiri dan meneruskan `features` objek name sebagai `RDS_LOGIN_EVENTS` dan status sebagai `ENABLED`.

Atau, Anda dapat menggunakan AWS CLI untuk mengaktifkan Perlindungan RDS. Jalankan perintah berikut, dan ganti `12abc34d567e8fa901bc2d34e56789f0` dengan ID detektor akun Anda dan `us-east-1` dengan Wilayah tempat Anda ingin mengaktifkan Perlindungan RDS.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan [ListDetectors](#) API. `detectorId`

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --  
region us-east-1 --features '[{"Name": "RDS_LOGIN_EVENTS", "Status": "ENABLED"}]'
```

Aktifkan Perlindungan RDS secara otomatis untuk semua akun anggota

Pilih metode akses pilihan Anda untuk mengaktifkan fitur Perlindungan RDS untuk semua akun anggota. Ini termasuk akun anggota yang ada dan akun baru yang bergabung dengan organisasi.

Console

1. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.

Pastikan untuk menggunakan kredensial akun GuardDuty administrator yang didelegasikan.

2. Lakukan salah satu tindakan berikut:

Menggunakan halaman Perlindungan RDS

1. Di panel navigasi, pilih Perlindungan RDS.
2. Pilih Aktifkan untuk semua akun. Tindakan ini secara otomatis memungkinkan Perlindungan RDS untuk akun yang ada dan baru di organisasi.
3. Pilih Simpan.

 Note

Mungkin diperlukan waktu hingga 24 jam untuk memperbarui konfigurasi akun anggota.

Menggunakan halaman Akun

1. Di panel navigasi, pilih Akun.
2. Pada halaman Akun, pilih Preferensi Aktifkan otomatis sebelum Tambahkan akun berdasarkan undangan.
3. Di jendela Kelola preferensi aktifkan otomatis, pilih Aktifkan untuk semua akun di bawah Pemantauan Aktivitas Login RDS.
4. Pilih Simpan.

Jika Anda tidak dapat menggunakan opsi Aktifkan untuk semua akun, lihat [Aktifkan Perlindungan RDS secara selektif untuk akun anggota](#).

API/CLI

Untuk mengaktifkan atau menonaktifkan Perlindungan RDS secara selektif untuk akun anggota Anda, jalankan operasi [updateMemberDetectors](#) API menggunakan milik Anda sendiri. *detector ID*

Atau, Anda dapat menggunakan AWS CLI untuk mengaktifkan Perlindungan RDS. Jalankan perintah berikut, dan ganti *12abc34d567e8fa901bc2d34e56789f0* dengan ID detektor akun Anda dan *us-east-1* dengan Wilayah tempat Anda ingin mengaktifkan Perlindungan RDS.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan [ListDetectors](#) API. `detectorId`

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
--region us-east-1 --account-ids 111122223333 --features '[{"name":
"RDS_LOGIN_EVENTS", "status": "ENABLED"}]'
```

Anda juga dapat melewati daftar akun yang IDs dipisahkan oleh spasi.

Ketika kode telah berhasil dijalankan, daftar `UnprocessedAccounts` akan kembali kosong. Jika ada masalah dalam mengubah pengaturan detektor untuk suatu akun, ID akun tersebut akan dicantumkan bersama dengan ringkasan masalahnya.

Aktifkan Perlindungan RDS untuk semua akun anggota aktif yang ada

Pilih metode akses pilihan Anda untuk mengaktifkan Perlindungan RDS untuk semua akun anggota aktif yang ada di organisasi Anda. Akun anggota yang sudah GuardDuty diaktifkan, disebut sebagai anggota aktif yang ada.

Console

1. Masuk ke AWS Management Console dan buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.

Masuk menggunakan kredensi akun GuardDuty administrator yang didelegasikan.

2. Di panel navigasi, pilih Perlindungan RDS.
3. Pada halaman Perlindungan RDS, Anda dapat melihat status konfigurasi saat ini. Di bawah bagian Akun anggota aktif, pilih Tindakan.
4. Dari menu tarik-turun Tindakan, pilih Aktifkan untuk semua akun anggota aktif yang ada.
5. Pilih Konfirmasi.

API/CLI

Jalankan operasi [updateMemberDetectors](#) API menggunakan milik Anda sendiri *detector ID*.

Atau, Anda dapat menggunakan AWS CLI untuk mengaktifkan Perlindungan RDS. Jalankan perintah berikut, dan ganti *12abc34d567e8fa901bc2d34e56789f0* dengan ID detektor akun Anda dan *us-east-1* dengan Wilayah tempat Anda ingin mengaktifkan Perlindungan RDS.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/> konsol, atau jalankan [ListDetectors](#) API. `detectorId`

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
--region us-east-1 --account-ids 111122223333 --features '[{"name":
"RDS_LOGIN_EVENTS", "status": "ENABLED"}]'
```

Anda juga dapat melewati daftar akun yang IDs dipisahkan oleh spasi.

Ketika kode telah berhasil dijalankan, daftar `UnprocessedAccounts` akan kembali kosong. Jika ada masalah dalam mengubah pengaturan detektor untuk suatu akun, ID akun tersebut akan dicantumkan bersama dengan ringkasan masalahnya.

Aktifkan Perlindungan RDS secara otomatis untuk akun anggota baru

Pilih metode akses pilihan Anda untuk mengaktifkan aktivitas login RDS untuk akun baru yang bergabung dengan organisasi Anda.

Console

Akun GuardDuty administrator yang didelegasikan dapat mengaktifkan akun anggota baru di organisasi melalui konsol, menggunakan halaman Perlindungan RDS atau Akun.

Untuk mengaktifkan Perlindungan RDS secara otomatis untuk akun anggota baru

1. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.

Pastikan untuk menggunakan kredensial akun GuardDuty administrator yang didelegasikan.

2. Lakukan salah satu tindakan berikut:

- Menggunakan halaman Perlindungan RDS:

1. Di panel navigasi, pilih Perlindungan RDS.
2. Pada halaman Perlindungan RDS, pilih Edit.
3. Pilih Konfigurasi akun secara manual.
4. Pilih Aktifkan secara otomatis untuk akun anggota baru. Langkah ini memastikan bahwa setiap kali akun baru bergabung dengan organisasi Anda, Perlindungan RDS akan diaktifkan secara otomatis untuk akun mereka. Hanya akun GuardDuty administrator yang didelegasikan organisasi yang dapat mengubah konfigurasi ini.
5. Pilih Simpan.

- Menggunakan halaman Akun:

1. Di panel navigasi, pilih Akun.
2. Pada halaman Akun, pilih Preferensi Aktifkan otomatis.
3. Di jendela Kelola preferensi aktifkan otomatis, pilih Aktifkan untuk akun baru di bawah Pemantauan Aktivitas Login RDS.
4. Pilih Simpan.

API/CLI

Untuk mengaktifkan atau menonaktifkan Perlindungan RDS secara selektif untuk akun anggota Anda, jalankan operasi [UpdateOrganizationConfiguration](#) API menggunakan milik Anda sendiri. *detector ID*

Atau, Anda dapat menggunakan AWS CLI untuk mengaktifkan Perlindungan RDS. Jalankan perintah berikut, dan ganti *12abc34d567e8fa901bc2d34e56789f0* dengan ID detektor akun Anda dan *us-east-1* dengan Wilayah tempat Anda ingin mengaktifkan Perlindungan RDS. Jika Anda tidak ingin mengaktifkannya untuk semua akun baru yang bergabung dengan organisasi, setel `autoEnable` ke `NONE`.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/> konsol, atau jalankan [ListDetectors](#) API. `detectorId`

```
aws guardduty update-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0 --region us-east-1 --auto-enable --features '[{"Name": "RDS_LOGIN_EVENTS", "AutoEnable": "NEW"}]'
```

Ketika kode telah berhasil dijalankan, daftar `UnprocessedAccounts` akan kembali kosong. Jika ada masalah dalam mengubah pengaturan detektor untuk suatu akun, ID akun tersebut akan dicantumkan bersama dengan ringkasan masalahnya.

Aktifkan Perlindungan RDS secara selektif untuk akun anggota

Pilih metode akses pilihan Anda untuk secara selektif mengaktifkan pemantauan aktivitas login RDS untuk akun anggota.

Console

1. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.

Pastikan untuk menggunakan kredensial akun GuardDuty administrator yang didelegasikan.

2. Di panel navigasi, pilih Akun.

Pada halaman Akun, tinjau kolom aktivitas login RDS untuk status akun anggota Anda.

3. Untuk mengaktifkan atau menonaktifkan aktivitas login RDS secara selektif

Pilih akun yang ingin Anda konfigurasi Perlindungan RDS. Anda dapat memilih beberapa akun sekaligus. Di menu tarik-turun Edit Rencana Perlindungan, pilih Aktivitas Login RDS, lalu pilih opsi yang sesuai.

API/CLI

Untuk mengaktifkan atau menonaktifkan Perlindungan RDS secara selektif untuk akun anggota Anda, jalankan operasi [updateMemberDetectors](#) API menggunakan milik Anda sendiri. *detector ID*

Atau, Anda dapat menggunakan AWS CLI untuk mengaktifkan Perlindungan RDS. Jalankan perintah berikut, dan ganti *12abc34d567e8fa901bc2d34e56789f0* dengan ID detektor akun Anda dan *us-east-1* dengan Wilayah tempat Anda ingin mengaktifkan Perlindungan RDS.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan [ListDetectors](#) API. `detectorId`

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
--region us-east-1 --account-ids 111122223333 --features '[{"Name":
"RDS_LOGIN_EVENTS", "Status": "ENABLED"}]'
```

Note

Anda juga dapat melewati daftar akun yang IDs dipisahkan oleh spasi.

Ketika kode telah berhasil dijalankan, daftar `UnprocessedAccounts` akan kembali kosong. Jika ada masalah dalam mengubah pengaturan detektor untuk suatu akun, ID akun tersebut akan dicantumkan bersama dengan ringkasan masalahnya.

Mengaktifkan Perlindungan RDS untuk akun mandiri

Akun mandiri memiliki keputusan untuk mengaktifkan atau menonaktifkan rencana perlindungan di akun mereka Akun AWS secara spesifik. Wilayah AWS

Jika akun Anda dikaitkan dengan akun GuardDuty administrator melalui AWS Organizations, atau dengan metode undangan, bagian ini tidak berlaku untuk akun Anda. Untuk informasi selengkapnya, lihat [Mengaktifkan Perlindungan RDS di lingkungan multi-akun](#).

Setelah Anda mengaktifkan Perlindungan RDS, GuardDuty akan mulai memantau [Aktivitas login RDS](#) basis data yang didukung di akun Anda.

Pilih metode akses pilihan Anda untuk mengonfigurasi Perlindungan RDS untuk akun mandiri.

Console

1. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.
2. Di panel navigasi, pilih Perlindungan RDS.
3. Halaman Perlindungan RDS menunjukkan status saat ini untuk akun Anda. Pilih Aktifkan untuk mengaktifkan Perlindungan RDS.
4. Pilih Konfirmasi untuk menyimpan pilihan Anda.

API/CLI

Jalankan operasi [updateDetector](#) API menggunakan ID detektor regional Anda sendiri dan meneruskan features objek name sebagai RDS_LOGIN_EVENTS dan status sebagai ENABLED.

Atau, Anda dapat menggunakan AWS CLI untuk mengaktifkan Perlindungan RDS. Jalankan perintah berikut, dan ganti `12abc34d567e8fa901bc2d34e56789f0` dengan ID detektor akun Anda dan `us-east-1` dengan Wilayah tempat Anda ingin mengaktifkan Perlindungan RDS.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/> konsol, atau jalankan [ListDetectors](#) API. `detectorId`

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --  
region us-east-1 --features '[{"Name" : "RDS_LOGIN_EVENTS", "Status" : "ENABLED"}]'
```

GuardDuty Perlindungan Lambda

Perlindungan Lambda membantu Anda mengidentifikasi potensi ancaman keamanan saat suatu [AWS Lambda](#) fungsi dipanggil di lingkungan Anda. AWS Saat Anda mengaktifkan Perlindungan Lambda, GuardDuty mulai memantau log aktivitas jaringan Lambda. Ini termasuk [Log Alur VPC](#) dari semua fungsi Lambda untuk akun Anda (termasuk log yang tidak menggunakan jaringan VPC) dan log yang dihasilkan saat fungsi Lambda dipanggil. Ketika GuardDuty mengidentifikasi lalu lintas jaringan yang mencurigakan yang menunjukkan adanya potongan kode yang berpotensi berbahaya dalam fungsi Lambda Anda, GuardDuty menghasilkan satu atau lebih. [Jenis temuan Perlindungan Lambda](#)

Uji coba gratis 30 hari

Daftar berikut menjelaskan cara kerja uji coba gratis 30 hari untuk akun Anda:

- Saat Anda mengaktifkan GuardDuty di Wilayah baru untuk pertama kalinya, Anda mendapatkan uji coba gratis 30 hari. Akun AWS Dalam hal ini, juga GuardDuty akan mengaktifkan Perlindungan Lambda, yang termasuk dalam uji coba gratis.
- Ketika Anda sudah menggunakan GuardDuty dan memutuskan untuk mengaktifkan Perlindungan Lambda untuk pertama kalinya, akun Anda di Wilayah ini akan mendapatkan uji coba gratis 30 hari untuk Perlindungan Lambda.
- Anda dapat memilih untuk menonaktifkan Perlindungan Lambda di Wilayah mana pun kapan saja.
- Selama uji coba gratis 30 hari, Anda bisa mendapatkan perkiraan biaya penggunaan Anda di akun dan Wilayah tersebut. Setelah uji coba gratis 30 hari berakhir, Perlindungan Lambda tidak dinonaktifkan secara otomatis. Akun Anda di Wilayah ini akan mulai menimbulkan biaya penggunaan. Untuk informasi selengkapnya, lihat [Memperkirakan biaya GuardDuty penggunaan](#).

Log aktivitas jaringan Lambda dapat berubah, termasuk ekspansi ke aktivitas jaringan lain seperti data kueri DNS yang dihasilkan dengan menjalankan fungsi Lambda. Ekspansi ke bentuk lain dari pemantauan aktivitas jaringan akan meningkatkan volume data yang GuardDuty akan diproses untuk Perlindungan Lambda. Ini akan berdampak langsung pada biaya penggunaan Perlindungan Lambda. Setiap kali GuardDuty mulai memantau log aktivitas jaringan tambahan, itu akan memberikan pemberitahuan ke akun yang telah mengaktifkan Perlindungan Lambda, setidaknya 30 hari sebelum rilis.

 Note

Pemantauan Aktivitas Jaringan Lambda tidak menyertakan log untuk fungsi [Lambda @Edge](#).

Pemantauan Aktivitas Jaringan Lambda

Saat Anda mengaktifkan Perlindungan Lambda, memantau log aktivitas jaringan GuardDuty Lambda yang dihasilkan saat fungsi Lambda, yang terkait dengan akun Anda, dipanggil. Ini membantu Anda mendeteksi potensi ancaman keamanan terhadap fungsi Lambda. Untuk fungsi Lambda yang dikonfigurasi untuk menggunakan jaringan VPC, Anda tidak perlu mengaktifkan log aliran VPC untuk antarmuka jaringan elastis (ENI) yang dibuat oleh Lambda untuk. GuardDuty GuardDuty hanya mengenakan biaya untuk jumlah data log aktivitas jaringan Lambda yang diproses (dalam GB) untuk menghasilkan temuan. GuardDuty mengoptimalkan biaya dengan menerapkan filter pintar dan menganalisis subset log aktivitas jaringan Lambda yang relevan dengan deteksi ancaman.

GuardDuty tidak mengelola log aktivitas jaringan Lambda Anda (termasuk log aliran VPC dan non-VPC), atau membuatnya dapat diakses di akun Anda.

Mengaktifkan Perlindungan Lambda di lingkungan multi-akun

Dalam lingkungan multi-akun, hanya akun GuardDuty administrator yang didelegasikan yang memiliki opsi untuk mengaktifkan atau menonaktifkan Perlindungan Lambda untuk akun anggota di organisasi mereka. Akun GuardDuty anggota tidak dapat mengubah konfigurasi ini dari akun mereka. Akun GuardDuty administrator yang didelegasikan mengelola akun anggota menggunakan AWS Organizations. Akun GuardDuty administrator yang didelegasikan dapat memilih untuk mengaktifkan secara otomatis Pemantauan Aktivitas Jaringan Lambda untuk semua akun baru saat mereka bergabung dengan organisasi. Untuk informasi selengkapnya tentang lingkungan beberapa akun, lihat [Mengelola beberapa akun di Amazon](#). GuardDuty

Mengaktifkan Perlindungan Lambda untuk akun administrator yang didelegasikan GuardDuty

Pilih metode akses pilihan Anda untuk mengaktifkan atau menonaktifkan Pemantauan Aktivitas Jaringan Lambda untuk akun administrator yang didelegasikan GuardDuty .

Console

1. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.
2. Di panel navigasi, di bawah Pengaturan, pilih Perlindungan Lambda.
3. Pada halaman Perlindungan Lambda, pilih Edit.
4. Lakukan salah satu hal berikut ini:

Menggunakan Aktifkan untuk semua akun

- Pilih Aktifkan untuk semua akun. Ini akan memungkinkan rencana perlindungan untuk semua GuardDuty akun aktif di AWS organisasi Anda, termasuk akun baru yang bergabung dengan organisasi.
- Pilih Simpan.

Menggunakan Konfigurasi akun secara manual

- Untuk mengaktifkan paket perlindungan hanya untuk akun GuardDuty administrator yang didelegasikan, pilih Konfigurasi akun secara manual.
- Pilih Aktifkan di bawah bagian akun GuardDuty administrator yang didelegasikan (akun ini).
- Pilih Simpan.

API/CLI

Jalankan [updateDetector](#) Operasi API menggunakan ID detektor regional Anda sendiri dan meneruskan features objek name sebagai LAMBDA_NETWORK_LOGS dan status sebagai ENABLED.

Atau, Anda dapat menggunakan AWS CLI untuk mengaktifkan Perlindungan Lambda. Jalankan perintah berikut, dan ganti `12abc34d567e8fa901bc2d34e56789f0` dengan ID detektor akun Anda dan `us-east-1` dengan Wilayah tempat Anda ingin mengaktifkan Perlindungan Lambda.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/> konsol, atau jalankan `detectorId` [ListDetectors](#) API.

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --  
region us-east-1 --features '[{"Name": "LAMBDA_NETWORK_LOGS", "Status": "ENABLED"}]'
```

Aktifkan Pemantauan Aktivitas Jaringan Lambda secara otomatis untuk semua akun anggota

Pilih metode akses pilihan Anda untuk mengaktifkan fitur Pemantauan Aktivitas Jaringan Lambda untuk semua akun anggota. Ini termasuk akun anggota yang ada dan akun baru yang bergabung dengan organisasi.

Console

1. Masuk ke AWS Management Console dan buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.

Pastikan untuk menggunakan kredensi akun GuardDuty administrator yang didelegasikan.

2. Lakukan salah satu hal berikut ini:

Menggunakan halaman Perlindungan Lambda

1. Di panel navigasi, pilih Perlindungan Lambda.
2. Pilih Aktifkan untuk semua akun. Tindakan ini secara otomatis memungkinkan Pemantauan Aktivitas Jaringan Lambda untuk akun yang ada dan baru di organisasi.
3. Pilih Simpan.

Note

Mungkin diperlukan waktu hingga 24 jam untuk memperbarui konfigurasi akun anggota.

Menggunakan halaman Akun

1. Di panel navigasi, pilih Akun.
2. Pada halaman Akun, pilih Preferensi Aktifkan otomatis sebelum Tambahkan akun berdasarkan undangan.
3. Di jendela Kelola preferensi aktifkan otomatis, pilih Aktifkan untuk semua akun di bawah Pemantauan Aktivitas Jaringan Lambda.

 Note

Secara default, tindakan ini secara otomatis mengaktifkan opsi Aktifkan otomatis GuardDuty untuk akun anggota baru.

4. Pilih Simpan.

Jika Anda tidak dapat menggunakan opsi Aktifkan untuk semua akun, lihat [Aktifkan atau nonaktifkan Pemantauan Aktivitas Jaringan Lambda secara selektif untuk akun anggota](#).

API/CLI

Untuk mengaktifkan atau menonaktifkan Pemantauan Aktivitas Jaringan Lambda secara selektif untuk akun anggota Anda, panggil [updateMemberDetectors](#) Operasi API menggunakan milik Anda sendiri *detector ID*.

Atau, Anda dapat menggunakan AWS CLI untuk mengaktifkan Perlindungan Lambda. Jalankan perintah berikut, dan ganti *12abc34d567e8fa901bc2d34e56789f0* dengan ID detektor akun Anda dan *us-east-1* dengan Wilayah tempat Anda ingin mengaktifkan Perlindungan Lambda.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan `detectorId` [ListDetectors](#) API.

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
--account-ids 111122223333 --region us-east-1 --features '[{"Name":
"LAMBDA_NETWORK_LOGS", "Status": "ENABLED"}]'
```

Anda juga dapat melewati daftar akun yang IDs dipisahkan oleh spasi.

Ketika kode telah berhasil dijalankan, daftar `UnprocessedAccounts` akan kembali kosong. Jika ada masalah dalam mengubah pengaturan detektor untuk suatu akun, ID akun tersebut akan dicantumkan bersama dengan ringkasan masalahnya.

Aktifkan Pemantauan Aktivitas Jaringan Lambda untuk semua akun anggota aktif yang ada

Pilih metode akses pilihan Anda untuk mengaktifkan Pemantauan Aktivitas Jaringan Lambda untuk semua akun anggota aktif yang ada di organisasi.

Console

Untuk mengonfigurasi Pemantauan Aktivitas Jaringan Lambda untuk semua akun anggota aktif yang ada

1. Masuk ke AWS Management Console dan buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.

Masuk menggunakan kredensi akun GuardDuty administrator yang didelegasikan.

2. Di panel navigasi, pilih Perlindungan Lambda.
3. Pada halaman Perlindungan Lambda, Anda dapat melihat status konfigurasi saat ini. Di bawah bagian Akun anggota aktif, pilih Tindakan.
4. Dari menu tarik-turun Tindakan, pilih Aktifkan untuk semua akun anggota aktif yang ada.
5. Pilih Konfirmasi.

API/CLI

Untuk mengaktifkan atau menonaktifkan Pemantauan Aktivitas Jaringan Lambda secara selektif untuk akun anggota Anda, panggil [updateMemberDetectors](#) Operasi API menggunakan milik Anda sendiri *detector ID*.

Atau, Anda dapat menggunakan AWS CLI untuk mengaktifkan Perlindungan Lambda. Jalankan perintah berikut, dan ganti *12abc34d567e8fa901bc2d34e56789f0* dengan ID detektor akun Anda dan *us-east-1* dengan Wilayah tempat Anda ingin mengaktifkan Perlindungan Lambda.

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
--region us-east-1 --account-ids 111122223333 --features '[{"Name":
"LAMBDA_NETWORK_LOGS", "Status": "ENABLED"}]'
```

Anda juga dapat melewati daftar akun yang IDs dipisahkan oleh spasi.

Ketika kode telah berhasil dijalankan, daftar `UnprocessedAccounts` akan kembali kosong. Jika ada masalah dalam mengubah pengaturan detektor untuk suatu akun, ID akun tersebut akan dicantumkan bersama dengan ringkasan masalahnya.

Aktifkan Pemantauan Aktivitas Jaringan Lambda secara otomatis untuk akun anggota baru

Pilih metode akses pilihan Anda untuk mengaktifkan Pemantauan Aktivitas Jaringan Lambda untuk akun baru yang bergabung dengan organisasi Anda.

Console

Akun GuardDuty administrator yang didelegasikan dapat mengaktifkan Pemantauan Aktivitas Jaringan Lambda untuk akun anggota baru di organisasi, menggunakan halaman Perlindungan Lambda atau Akun.

Untuk mengaktifkan secara otomatis Pemantauan Aktivitas Jaringan Lambda untuk akun anggota baru

1. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.

Pastikan untuk menggunakan kredensi akun GuardDuty administrator yang didelegasikan.

2. Lakukan salah satu hal berikut ini:

- Menggunakan halaman Perlindungan Lambda:

1. Di panel navigasi, pilih Perlindungan Lambda.
2. Pada halaman Perlindungan Lambda, pilih Edit.
3. Pilih Konfigurasi akun secara manual.
4. Pilih Aktifkan secara otomatis untuk akun anggota baru. Langkah ini memastikan bahwa setiap kali akun baru bergabung dengan organisasi Anda, Perlindungan Lambda akan diaktifkan secara otomatis untuk akun mereka. Hanya akun GuardDuty administrator yang didelegasikan organisasi yang dapat mengubah konfigurasi ini.
5. Pilih Simpan.

- Menggunakan halaman Akun:

1. Di panel navigasi, pilih Akun.
2. Pada halaman Akun, pilih Preferensi Aktifkan otomatis.

3. Di jendela Kelola preferensi aktifkan otomatis, pilih Aktifkan untuk akun baru di bawah Pemantauan Aktivitas Jaringan Lambda.
4. Pilih Simpan.

API/CLI

Untuk mengaktifkan Pemantauan Aktivitas Jaringan Lambda untuk akun anggota baru, panggil [UpdateOrganizationConfiguration](#) Operasi API menggunakan milik Anda sendiri *detector ID*.

Atau, Anda dapat menggunakan AWS CLI untuk mengaktifkan Perlindungan Lambda. Contoh berikut menunjukkan bagaimana Anda dapat mengaktifkan Pemantauan Aktivitas Jaringan Lambda untuk satu akun anggota. Ganti *12abc34d567e8fa901bc2d34e56789f0* dengan ID detektor akun Anda dan *us-east-1* dengan Wilayah tempat Anda ingin mengaktifkan Perlindungan Lambda. Jika Anda tidak ingin mengaktifkannya untuk semua akun baru yang bergabung dengan organisasi, setel `AutoEnable` ke `NONE`.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/> konsol, atau jalankan `detectorId` [ListDetectors](#) API.

```
aws guardduty update-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0 --region us-east-1 --auto-enable --features '[{"Name": "LAMBDA_NETWORK_LOGS", "AutoEnable": "NEW"}]'
```

Ketika kode telah berhasil dijalankan, daftar `UnprocessedAccounts` akan kembali kosong. Jika ada masalah dalam mengubah pengaturan detektor untuk suatu akun, ID akun tersebut akan dicantumkan bersama dengan ringkasan masalahnya.

Aktifkan atau nonaktifkan Pemantauan Aktivitas Jaringan Lambda secara selektif untuk akun anggota

Pilih metode akses pilihan Anda untuk mengaktifkan atau menonaktifkan Pemantauan Aktivitas Jaringan Lambda secara selektif untuk akun anggota.

Console

1. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.

Pastikan untuk menggunakan kredensi akun GuardDuty administrator yang didelegasikan.

2. Di panel navigasi, di bagian Pengaturan, pilih Akun.

Pada halaman Akun, tinjau kolom Pemantauan Aktivitas Jaringan Lambda. Ini menunjukkan apakah Pemantauan Aktivitas Jaringan Lambda diaktifkan atau tidak.

3. Pilih akun yang ingin Anda konfigurasi Perlindungan Lambda. Anda dapat memilih beberapa akun sekaligus.
4. Dari menu tarik-turun Edit Rencana Perlindungan, pilih Pemantauan Aktivitas Jaringan Lambda, lalu pilih tindakan yang sesuai.

API/CLI

Memohon [updateMemberDetectors](#) API menggunakan milik Anda sendiri *detector ID*.

Atau, Anda dapat menggunakan AWS CLI untuk mengaktifkan Perlindungan Lambda. Ganti *12abc34d567e8fa901bc2d34e56789f0* dengan ID detektor akun Anda dan *us-east-1* dengan Wilayah tempat Anda ingin mengaktifkan Perlindungan Lambda.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan `detectorId` [ListDetectors](#) API.

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
--region us-east-1 --account-ids 111122223333 --features '[{"Name":
"LAMBDA_NETWORK_LOGS", "Status": "ENABLED"}]'
```

Anda juga dapat melewati daftar akun yang IDs dipisahkan oleh spasi.

Ketika kode telah berhasil dijalankan, daftar `UnprocessedAccounts` akan kembali kosong. Jika ada masalah dalam mengubah pengaturan detektor untuk suatu akun, ID akun tersebut akan dicantumkan bersama dengan ringkasan masalahnya.

Mengaktifkan Perlindungan Lambda untuk akun mandiri

Akun mandiri memiliki keputusan untuk mengaktifkan atau menonaktifkan rencana perlindungan di akun mereka Akun AWS secara spesifik. Wilayah AWS

Jika akun Anda dikaitkan dengan akun GuardDuty administrator melalui AWS Organizations, atau dengan metode undangan, bagian ini tidak berlaku untuk akun Anda. Untuk informasi selengkapnya, lihat [Mengaktifkan Perlindungan Lambda di lingkungan multi-akun](#).

Setelah Anda mengaktifkan Perlindungan Lambda, GuardDuty akan mulai memantau [Pemantauan Aktivitas Jaringan Lambda](#) di akun Anda.

Pilih metode akses pilihan Anda untuk mengonfigurasi Perlindungan Lambda untuk akun mandiri.

Console

1. Buka GuardDuty konsol di <https://console.aws.amazon.com/guarddduty/>.
2. Di panel navigasi, di bawah Pengaturan, pilih Perlindungan Lambda.
3. Halaman Perlindungan Lambda menunjukkan status saat ini untuk akun Anda. Pilih Aktifkan untuk mengaktifkan Perlindungan Lambda di akun Anda.
4. Pilih Konfirmasi untuk menyimpan pilihan Anda.

API/CLI

Jalankan [updateDetector](#) Operasi API menggunakan ID detektor regional Anda sendiri dan meneruskan features objek name sebagai LAMBDA_NETWORK_LOGS dan status sebagai ENABLED.

Atau, Anda dapat menggunakan AWS CLI untuk mengaktifkan Perlindungan Lambda. Jalankan perintah berikut, dan ganti *12abc34d567e8fa901bc2d34e56789f0* dengan ID detektor akun Anda dan *us-east-1* dengan Wilayah tempat Anda ingin mengaktifkan Perlindungan Lambda.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guarddduty/> konsol, atau jalankan detectorId [ListDetectors](#) API.

```
aws guarddduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0
--region us-east-1 --features [{"Name" : "LAMBDA_NETWORK_LOGS", "Status" :
"ENABLED"}]'
```

Melindungi beban kerja AI dengan GuardDuty

[Deteksi ancaman GuardDuty dasar](#) Amazon dan Perlindungan [Lambda](#) membantu Anda mengamankan dan mendeteksi ancaman terhadap beban kerja AI yang dibangun dengan lebih baik. AWS

[Deteksi GuardDuty ancaman dasar memantau peristiwa AWS CloudTrail manajemen untuk mendeteksi aktivitas mencurigakan dan berbahaya dalam beban kerja AI generatif yang dibuat dengan menggunakan layanan AWS , termasuk Amazon Bedrock dan Amazon AI. SageMaker](#)

Misalnya, GuardDuty dapat mengidentifikasi kegiatan seperti:

- Penghapusan pagar keamanan Amazon Bedrock yang tidak biasa
- Perubahan sumber data pelatihan model yang berpotensi menyebabkan serangan keracunan data
- Doa model Amazon Bedrock yang mencurigakan
- Contoh notebook yang tidak biasa atau pelatihan penciptaan lapangan kerja di SageMaker AI
- Kredensi Amazon Elastic Compute Cloud yang diekstraksi yang mungkin telah digunakan untuk menelepon APIs Amazon Bedrock, Amazon SageMaker AI, atau beban kerja AI yang dikelola sendiri pada EC2 instans, kluster EKS, atau tugas ECS.

GuardDuty Lambda Protection dapat membantu mendeteksi potensi ancaman terkait agen Amazon Bedrock. Ini mungkin termasuk aktivitas jaringan yang mencurigakan seperti cryptomining, dan berkomunikasi dengan server perintah dan kontrol berbahaya yang dapat disebabkan oleh serangan rantai pasokan atau dorongan kompleks.

Video berikut menunjukkan bagaimana temuan terkait akan terlihat.

Video berikut menunjukkan bagaimana temuan terkait akan terlihat. [Menggunakan Amazon GuardDuty untuk memantau dan mengamankan beban kerja AI Anda AWS](#)

Beberapa akun di Amazon GuardDuty

Ketika AWS lingkungan Anda memiliki beberapa akun, Anda dapat mengelolanya dengan menunjuk satu Akun AWS sebagai akun administrator. Anda kemudian dapat mengaitkan beberapa Akun AWS dengan akun administrator ini sebagai akun anggotanya. Dengan konfigurasi ini, akun GuardDuty administrator yang ditunjuk dapat menilai dan memantau keamanan keseluruhan organisasi Anda. Akun administrator juga dapat melakukan tugas manajemen akun, seperti meninjau semua temuan yang dihasilkan dan mengonfigurasi rencana perlindungan di dalamnya. GuardDuty

Dalam GuardDuty, organisasi terdiri dari akun GuardDuty administrator yang didelegasikan dan satu atau lebih akun anggota terkait. Anda dapat mengaitkan akun dengan dua cara — dengan mengintegrasikan dengan AWS Organizations, atau dengan menggunakan metode lama untuk mengirim dan menerima undangan keanggotaan di konsol. GuardDuty GuardDuty merekomendasikan agar Anda berintegrasi dengan AWS Organizations.

AWS Organizations adalah layanan manajemen akun global yang memungkinkan AWS administrator untuk mengkonsolidasikan dan mengelola beberapa secara terpusat. Akun AWS Ini menyediakan manajemen akun dan fitur penagihan terkonsolidasi yang dirancang untuk mendukung kebutuhan anggaran, keamanan, dan kepatuhan. Ini ditawarkan tanpa biaya tambahan dan terintegrasi dengan beberapa Layanan AWS, termasuk Macie, AWS Security Hub, dan Amazon. GuardDuty Untuk informasi selengkapnya, silakan lihat [Panduan Pengguna AWS Organizations](#).

Daftar Isi

- [Memahami hubungan antara akun GuardDuty administrator dan akun anggota](#)
- [Mengelola GuardDuty akun dengan AWS Organizations](#)
- [Mengelola GuardDuty akun dengan undangan](#)
- [GuardDuty pertimbangan untuk mengeksport detail akun anggota dalam format CSV](#)

Memahami hubungan antara akun GuardDuty administrator dan akun anggota

Saat Anda menggunakan GuardDuty di lingkungan beberapa akun, akun administrator dapat mengelola aspek-aspek tertentu GuardDuty atas nama akun anggota. Akun administrator dapat melakukan fungsi utama berikut:

- Menambah dan menghapus akun anggota terkait — Proses di mana akun administrator dapat melakukan ini berbeda berdasarkan cara Anda mengelola akun — melalui AWS Organizations atau dengan metode GuardDuty undangan.

GuardDuty merekomendasikan mengelola akun anggota Anda melalui AWS Organizations.

- Akun GuardDuty administrator yang didelegasikan mengaktifkan GuardDuty akun manajemen — Jika akun AWS Organizations manajemen pernah dinonaktifkan GuardDuty, akun GuardDuty administrator yang didelegasikan dapat diaktifkan GuardDuty di akun manajemen. Namun, diperlukan bahwa akun manajemen harus belum secara eksplisit menghapus. [Izin peran terkait layanan untuk GuardDuty](#)
- Konfigurasi status akun anggota — Akun administrator dapat mengaktifkan atau menonaktifkan status rencana GuardDuty perlindungan, dan mengaktifkan, menangguhkan, atau menonaktifkan status GuardDuty atas nama akun anggota terkait.

Akun GuardDuty administrator yang didelegasikan yang dikelola dengan AWS Organizations dapat secara otomatis mengaktifkan GuardDuty ketika Akun AWS ditambahkan sebagai anggota.

- Sesuaikan kapan harus menghasilkan temuan — Akun administrator dapat menyesuaikan temuan dalam GuardDuty jaringan dengan membuat dan mengelola aturan penindasan, daftar IP tepercaya, dan daftar ancaman. Dalam lingkungan multi-akun, dukungan untuk mengonfigurasi fitur ini hanya tersedia untuk akun administrator yang GuardDuty didelegasikan. Akun anggota tidak dapat memperbarui konfigurasi ini.

Tabel berikut merinci hubungan antara akun GuardDuty administrator dan akun anggota.

Kunci untuk tabel

- Self — Akun dapat melakukan tindakan yang terdaftar hanya untuk akun mereka sendiri.
- Apa saja — Akun dapat melakukan tindakan yang tercantum untuk akun terkait apa pun.
- Semua — Akun dapat melakukan tindakan yang tercantum dan berlaku untuk semua akun terkait. Biasanya, akun yang mengambil tindakan ini adalah akun GuardDuty administrator yang ditunjuk
- Sel dengan tanda hubung (—) — Sel tabel dengan tanda hubung (—) menunjukkan bahwa akun tidak dapat melakukan tindakan yang tercantum.

Tindakan

Melalui AWS Organizations

Dengan undangan

	Akun GuardDuty administrator yang didelegasikan	Akun anggota terkait	GuardDuty akun administrator	Akun anggota terkait
Aktifkan GuardDuty	Setiap	–	Mandiri	Mandiri
Aktifkan GuardDuty secara otomatis untuk seluruh organisasi (ALL,NEW,NONE)	Semua	–	–	–
Lihat semua akun anggota Organizations terlepas dari GuardDuty statusnya	Setiap	–	–	–
Membuat temuan sampel	Mandiri	Mandiri	Mandiri	Mandiri
Lihat semua GuardDuty temuan	Setiap	Mandiri	Setiap	Mandiri
GuardDuty Temuan arsip	Setiap	–	Setiap	–
Menerapkan aturan penekanan	Semua	–	Semua	–

Buat daftar IP tepercaya atau daftar ancaman	Semua	—	Semua	—
Perbarui daftar IP tepercaya atau daftar ancaman	Semua	—	Semua	—
Hapus daftar IP tepercaya atau daftar ancaman	Semua	—	Semua	—
Atur frekuensi EventBridge notifikasi	Semua	—	Semua	—
Mengatur lokasi Amazon S3 untuk mengekspor temuan	Semua	Diri Sendiri	Semua	Diri Sendiri
Aktifkan satu atau lebih rencana perlindungan opsional untuk seluruh organisasi (ALL,NEW,NONE)	Semua	—	—	—
Ini tidak termasuk Perlindungan Malware untuk S3.				

Aktifkan paket GuardDuty perlindungan apa pun untuk akun individu	Setiap	—	Setiap	—
Ini tidak termasuk Perlindungan Malware untuk EC2 dan Perlindungan Malware untuk S3.				
Perlindungan Malware untuk EC2	Setiap	—	Mandiri	—
Perlindungan Malware untuk EC2 — Pemindaian malware sesuai permintaan	Setiap	Mandiri	Mandiri	Mandiri
Perlindungan Malware untuk S3	—	Mandiri	—	Mandiri
Putus hubungan akun anggota	Setiap ⁺	—	Setiap	—
Putus hubungan dari akun administrator	—	—	—	Mandiri

Menghapus akun anggota yang tidak terkait	Setiap	–	Setiap	–
Menangguhkan GuardDuty	Apa saja*	–	Apa saja*	–
Nonaktifkan GuardDuty	Apa saja*	–	Apa saja*	–

⁺ Menunjukkan bahwa akun GuardDuty administrator yang didelegasikan dapat mengambil tindakan ini hanya jika mereka belum menyiapkan preferensi aktifkan otomatis ke ALL anggota organisasi.

^{*} Menunjukkan bahwa akun GuardDuty administrator yang didelegasikan tidak dapat menonaktifkan GuardDuty di akun anggota secara langsung. Akun GuardDuty administrator yang didelegasikan harus terlebih dahulu memisahkan akun anggota, dan kemudian menghapusnya. Setelah ini, setiap akun anggota dapat menonaktifkan GuardDuty di akun mereka sendiri. Untuk informasi selengkapnya tentang melakukan tugas-tugas ini di organisasi Anda, lihat [Terus mengelola akun anggota Anda dalam GuardDuty](#).

Mengelola GuardDuty akun dengan AWS Organizations

Dalam suatu AWS organisasi, akun manajemen dapat menunjuk akun apa pun dalam organisasi ini sebagai akun GuardDuty administrator yang didelegasikan. Untuk akun administrator ini, GuardDuty akan diaktifkan secara otomatis hanya di saat ini Wilayah AWS. Secara default, akun administrator dapat mengaktifkan dan mengelola GuardDuty semua akun anggota di organisasi dalam Wilayah tersebut. Akun administrator dapat melihat dan menambahkan anggota ke AWS organisasi ini.

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

Daftar Isi

- [Pertimbangan dan rekomendasi untuk digunakan dengan GuardDuty AWS Organizations](#)
- [Izin yang diperlukan untuk menunjuk akun administrator yang didelegasikan GuardDuty](#)
- [Menunjuk akun administrator yang didelegasikan GuardDuty](#)
- [Menyetel preferensi aktifkan otomatis organisasi](#)
- [Menambahkan anggota ke organisasi](#)

- [\(Opsional\) Aktifkan paket perlindungan untuk akun anggota yang ada](#)
- [Terus mengelola akun anggota Anda dalam GuardDuty](#)
- [Penangguhan GuardDuty untuk akun anggota](#)
- [Memutuskan \(menghapus\) akun anggota dari akun administrator](#)
- [Menghapus akun anggota dari organisasi GuardDuty](#)
- [Mengubah akun GuardDuty administrator yang didelegasikan](#)

Pertimbangan dan rekomendasi untuk digunakan dengan GuardDuty AWS Organizations

Pertimbangan dan rekomendasi berikut dapat membantu Anda memahami cara operasi akun GuardDuty administrator yang didelegasikan: GuardDuty

Akun GuardDuty administrator yang didelegasikan dapat mengelola maksimal 50.000 anggota.

Ada batas 50.000 akun anggota per akun GuardDuty administrator yang didelegasikan. Ini termasuk akun anggota yang ditambahkan melalui AWS Organizations atau mereka yang menerima undangan akun GuardDuty administrator untuk bergabung dengan organisasi mereka. Namun, mungkin ada lebih dari 50.000 akun di AWS organisasi Anda.

Jika Anda melebihi batas 50.000 akun anggota, Anda akan menerima pemberitahuan dari CloudWatch, AWS Health Dashboard, dan email ke akun GuardDuty administrator yang didelegasikan yang ditunjuk.

Akun GuardDuty administrator yang didelegasikan adalah Regional.

Tidak seperti AWS Organizations, GuardDuty adalah layanan Regional. Akun GuardDuty administrator yang didelegasikan dan akun anggotanya harus ditambahkan AWS Organizations di setiap Wilayah yang diinginkan tempat Anda telah GuardDuty mengaktifkan. Jika akun manajemen organisasi menunjuk akun GuardDuty administrator yang didelegasikan hanya di AS Timur (Virginia N.), maka akun GuardDuty administrator yang didelegasikan hanya akan mengelola akun anggota yang ditambahkan ke organisasi di Wilayah tersebut. Untuk informasi selengkapnya tentang paritas fitur di Wilayah GuardDuty yang tersedia, lihat [Wilayah dan titik akhir](#).

Kasus khusus untuk Wilayah keikutsertaan

- Ketika akun GuardDuty administrator yang didelegasikan memilih keluar dari Wilayah keikutsertaan, meskipun organisasi Anda memiliki konfigurasi GuardDuty aktifkan otomatis

yang disetel ke akun anggota baru saja (NEW) atau semua akun anggota (ALL), GuardDuty tidak dapat diaktifkan untuk akun anggota mana pun di organisasi yang saat ini telah dinonaktifkan. GuardDuty Untuk informasi tentang konfigurasi akun anggota Anda, buka Akun di panel navigasi [GuardDuty konsol](#) atau gunakan [ListMembers](#) API.

- Saat bekerja dengan konfigurasi GuardDuty aktifkan otomatis yang disetel ke NEW, pastikan urutan berikut terpenuhi:
 1. Akun anggota ikut serta ke Wilayah keikutsertaan.
 2. Tambahkan akun anggota ke organisasi Anda di AWS Organizations.

Jika Anda mengubah urutan langkah-langkah ini, pengaturan GuardDuty aktifkan otomatis dengan tidak **NEW** akan berfungsi di Wilayah keikutsertaan tertentu karena akun anggota tidak lagi baru bagi organisasi. GuardDuty menyediakan dua solusi alternatif:

- Setel konfigurasi GuardDuty aktifkan otomatis ke ALL, yang mencakup akun anggota baru dan yang sudah ada. Dalam hal ini, urutan langkah-langkah ini tidak relevan.
- Jika akun anggota sudah menjadi bagian dari organisasi Anda, kelola GuardDuty konfigurasi untuk akun ini secara individual di Wilayah keikutsertaan tertentu dengan menggunakan GuardDuty konsol atau API.

Diperlukan agar AWS organisasi memiliki akun GuardDuty administrator yang didelegasikan yang sama di semua akun. Wilayah AWS

Anda harus menetapkan satu akun anggota sebagai akun GuardDuty administrator yang didelegasikan di semua Wilayah AWS tempat GuardDuty diaktifkan. 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 GuardDuty administrator yang didelegasikan di semua Wilayah lainnya.

Anda dapat menunjuk akun GuardDuty administrator yang didelegasikan baru kapan saja. Untuk informasi selengkapnya tentang menghapus akun GuardDuty administrator terdelegasi yang ada, lihat [Mengubah akun GuardDuty administrator yang didelegasikan](#).

Tidak disarankan untuk menetapkan akun manajemen organisasi Anda sebagai akun GuardDuty administrator yang didelegasikan.

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

Mengubah akun GuardDuty administrator yang didelegasikan tidak menonaktifkan GuardDuty akun anggota.

Jika Anda menghapus akun GuardDuty administrator yang didelegasikan, GuardDuty hapus semua akun anggota yang terkait dengan akun GuardDuty administrator yang didelegasikan ini. GuardDuty masih tetap diaktifkan untuk semua akun anggota ini.

Izin yang diperlukan untuk menunjuk akun administrator yang didelegasikan GuardDuty

Untuk mulai menggunakan Amazon GuardDuty dengan AWS Organizations, akun AWS Organizations manajemen untuk organisasi menetapkan akun sebagai akun GuardDuty administrator yang didelegasikan. Ini memungkinkan GuardDuty sebagai layanan tepercaya di AWS Organizations. Ini juga memungkinkan GuardDuty akun GuardDuty administrator yang didelegasikan dan juga memungkinkan akun administrator yang didelegasikan untuk mengaktifkan dan mengelola GuardDuty akun lain di organisasi di Wilayah saat ini. Untuk informasi tentang cara izin ini diberikan, lihat [Menggunakan AWS Organizations dengan AWS layanan lain](#).

Sebagai akun AWS Organizations manajemen, sebelum Anda menetapkan akun GuardDuty administrator yang didelegasikan untuk organisasi Anda, verifikasi bahwa Anda dapat melakukan GuardDuty tindakan berikut: `guardduty:EnableOrganizationAdminAccount` Tindakan ini memungkinkan Anda untuk menunjuk akun GuardDuty administrator yang didelegasikan untuk organisasi Anda dengan menggunakan. GuardDuty 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": "PermissionsForGuardDutyAdmin",
  "Effect": "Allow",
  "Action": [
    "guardduty:EnableOrganizationAdminAccount",
    "organizations:EnableAWSServiceAccess",
    "organizations:RegisterDelegatedAdministrator",
    "organizations:ListDelegatedAdministrators",
    "organizations:ListAWSServiceAccessForOrganization",
    "organizations:DescribeOrganizationalUnit",
```

```

    "organizations:DescribeAccount",
    "organizations:DescribeOrganization",
    "organizations:ListAccounts"
  ],
  "Resource": "*"
}
```

Jika Anda ingin menetapkan akun AWS Organizations manajemen Anda sebagai akun GuardDuty administrator yang didelegasikan, akun Anda juga akan memerlukan tindakan IAM: `CreateServiceLinkedRole`. Tindakan ini memungkinkan Anda untuk menginisialisasi GuardDuty untuk akun manajemen. Namun, tinjau [Pertimbangan dan rekomendasi untuk digunakan dengan GuardDuty AWS Organizations](#) sebelum Anda melanjutkan untuk menambahkan izin.

Untuk melanjutkan penunjukan akun manajemen sebagai akun GuardDuty administrator yang didelegasikan, tambahkan pernyataan berikut ke kebijakan IAM dan ganti **111122223333** dengan Akun AWS ID akun manajemen organisasi Anda:

```

{
  "Sid": "PermissionsToEnableGuardDuty"
  "Effect": "Allow",
  "Action": [
    "iam:CreateServiceLinkedRole"
  ],
  "Resource": "arn:aws:iam::111122223333:role/aws-service-role/guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty",
  "Condition": {
    "StringLike": {
      "iam:AWSServiceName": "guardduty.amazonaws.com"
    }
  }
}
```

Menunjuk akun administrator yang didelegasikan GuardDuty

Bagian ini menyediakan langkah-langkah untuk menunjuk administrator yang didelegasikan dalam organisasi. GuardDuty

Sebagai akun manajemen AWS organisasi, pastikan Anda membaca [Pertimbangan dan rekomendasi](#) tentang cara akun GuardDuty administrator yang didelegasikan beroperasi. Sebelum melanjutkan, pastikan Anda memilikinya [izin yang diperlukan untuk menunjuk akun administrator yang didelegasikan GuardDuty](#).

Pilih metode akses yang disukai untuk menunjuk akun GuardDuty administrator yang didelegasikan untuk organisasi Anda. Hanya akun manajemen yang dapat melakukan langkah ini.

Console

1. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.

Untuk masuk, gunakan kredensial akun manajemen untuk organisasi Anda AWS Organizations .

2. Dengan menggunakan Wilayah AWS pemilih di sudut kanan atas halaman, pilih Wilayah tempat Anda ingin menunjuk akun administrator yang didelegasikan GuardDuty untuk organisasi Anda.
3. Lakukan salah satu hal berikut, tergantung pada apakah GuardDuty diaktifkan untuk akun manajemen Anda di Wilayah saat ini:
 - Jika tidak GuardDuty diaktifkan, pilih Amazon GuardDuty - semua fitur dan pilih Memulai. Tindakan ini akan membawa Anda ke GuardDuty halaman Selamat Datang di.
 - Jika GuardDuty diaktifkan, pilih Pengaturan di panel navigasi.
4. Di bawah Administrator yang didelegasikan, masukkan Akun AWS ID 12 digit akun yang ingin Anda tetapkan sebagai akun GuardDuty administrator yang didelegasikan untuk organisasi.

Pastikan GuardDuty untuk mengaktifkan akun GuardDuty administrator delegasi yang baru ditunjuk, jika tidak maka tidak akan dapat mengambil tindakan apa pun.

5. Pilih Delegasikan.
6. (Disarankan) Ulangi langkah-langkah sebelumnya untuk menunjuk akun GuardDuty administrator yang didelegasikan di setiap Wilayah AWS tempat yang telah Anda aktifkan GuardDuty

API/CLI

1. Jalankan [enableOrganizationAdminAccount](#) menggunakan kredensi Akun AWS akun manajemen organisasi.
 - Atau, Anda dapat menggunakannya AWS Command Line Interface untuk melakukan ini. AWS CLI Perintah berikut menunjuk akun GuardDuty administrator yang didelegasikan untuk Wilayah Anda saat ini saja. Jalankan AWS CLI perintah berikut dan pastikan untuk mengganti **111111111111** dengan Akun AWS ID akun yang ingin Anda tetapkan sebagai akun GuardDuty administrator yang didelegasikan:

```
aws guardduty enable-organization-admin-account --admin-account-id 111111111111
```

Untuk menunjuk akun GuardDuty administrator yang didelegasikan untuk Wilayah lain, tentukan Wilayah dalam perintah. AWS CLI Contoh berikut menunjukkan cara mengaktifkan akun GuardDuty administrator yang didelegasikan di AS Barat (Oregon). Pastikan untuk mengganti *us-west-2* dengan Wilayah yang ingin Anda tetapkan akun GuardDuty administrator yang didelegasikan.

```
aws guardduty enable-organization-admin-account --admin-account-id 111111111111 --region us-west-2
```

Untuk informasi tentang Wilayah AWS tempat GuardDuty tersedia, lihat [Wilayah dan titik akhir](#).

Jika GuardDuty dinonaktifkan untuk akun GuardDuty administrator yang didelegasikan, akun tersebut tidak akan dapat mengambil tindakan apa pun. Jika belum dilakukan, pastikan GuardDuty untuk mengaktifkan akun GuardDuty administrator delegasi yang baru ditunjuk.

2. (Disarankan) ulangi langkah-langkah sebelumnya untuk menunjuk akun GuardDuty administrator yang didelegasikan di setiap Wilayah AWS tempat yang telah Anda aktifkan GuardDuty

Menyetel preferensi aktifkan otomatis organisasi

Fitur mengaktifkan otomatis organisasi di GuardDuty membantu Anda mengatur status paket perlindungan yang sama GuardDuty untuk akun ALL yang ada atau NEW anggota di organisasi Anda, dalam satu langkah. Demikian pula, Anda juga dapat menentukan kapan Anda tidak ingin mengambil tindakan apa pun pada akun anggota, dengan memilih NONE. Langkah-langkah berikut menjelaskan pengaturan ini dan juga menunjukkan kapan Anda ingin menggunakan pengaturan tertentu.

Note

Anda dapat mengatur preferensi aktifkan otomatis untuk semua paket perlindungan kecuali [Perlindungan Malware untuk S3](#).

Pilih metode akses yang disukai untuk memperbarui preferensi aktifkan otomatis untuk organisasi.

Console

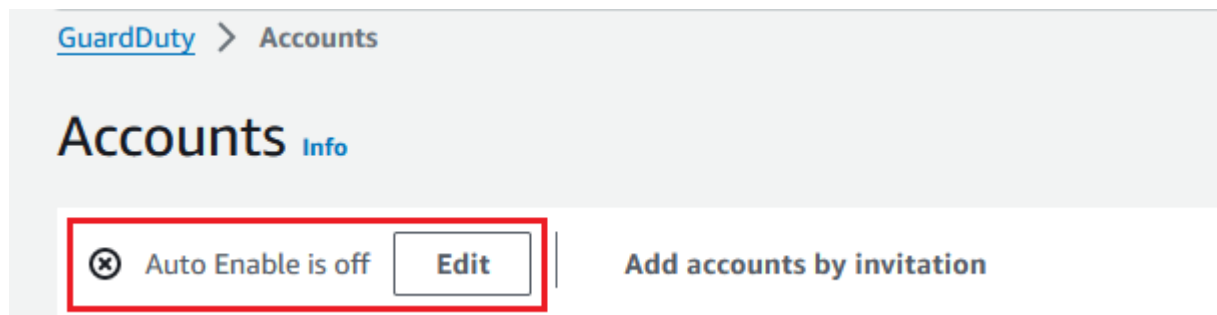
1. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.

Untuk masuk, gunakan GuardDuty kredensial akun administrator.

2. Di panel navigasi, pilih Akun.

Halaman Akun menyediakan opsi konfigurasi ke akun GuardDuty administrator untuk mengaktifkan otomatis GuardDuty dan paket perlindungan opsional atas nama akun anggota milik organisasi.

3. Untuk memperbarui pengaturan aktifkan otomatis yang ada, pilih Edit.



Dukungan ini tersedia untuk dikonfigurasi GuardDuty dan semua paket perlindungan opsional yang didukung di Anda Wilayah AWS. Anda dapat memilih salah satu opsi konfigurasi berikut untuk GuardDuty atas nama akun anggota Anda:

- Aktifkan untuk semua akun (**ALL**) — Pilih untuk mengaktifkan opsi yang sesuai untuk semua akun dalam suatu organisasi. Ini termasuk akun baru yang bergabung dengan organisasi dan akun yang mungkin telah ditangguhkan atau dihapus dari organisasi. Ini juga termasuk akun GuardDuty administrator yang didelegasikan.

Note

Diperlukan waktu hingga 24 jam untuk memperbarui konfigurasi untuk semua akun anggota.

- Aktifkan otomatis untuk akun baru (**NEW**) — Pilih untuk mengaktifkan GuardDuty atau paket perlindungan opsional hanya untuk akun anggota baru secara otomatis saat mereka bergabung dengan organisasi Anda.

- Jangan aktifkan (**NONE**) — Pilih untuk mencegah mengaktifkan opsi yang sesuai untuk akun baru di organisasi Anda. Dalam hal ini, akun GuardDuty administrator akan mengelola setiap akun secara individual.

Saat Anda memperbarui pengaturan aktifkan otomatis dari ALL atau NEW ke NONE, tindakan ini tidak menonaktifkan opsi yang sesuai untuk akun Anda yang ada. Konfigurasi ini akan berlaku untuk akun baru yang bergabung dengan organisasi. Setelah Anda memperbarui pengaturan aktifkan otomatis, tidak ada akun baru yang akan memiliki opsi yang sesuai sebagaimana diaktifkan.

 Note

Ketika akun GuardDuty administrator yang didelegasikan memilih keluar dari Wilayah keikutsertaan, meskipun organisasi Anda memiliki konfigurasi GuardDuty aktifkan otomatis yang disetel ke akun anggota baru saja (NEW) atau semua akun anggota (ALL), GuardDuty tidak dapat diaktifkan untuk akun anggota mana pun di organisasi yang saat ini telah dinonaktifkan. GuardDuty Untuk informasi tentang konfigurasi akun anggota Anda, buka Akun di panel navigasi [GuardDuty konsol](#) atau gunakan [ListMembers](#) API.

4. Pilih Simpan perubahan.
5. (Opsional) jika Anda ingin menggunakan preferensi yang sama di setiap Wilayah, perbarui preferensi Anda di setiap Wilayah yang didukung secara terpisah.

Beberapa paket perlindungan opsional mungkin tidak tersedia di semua Wilayah AWS tempat yang GuardDuty tersedia. Untuk informasi selengkapnya, lihat [Wilayah dan titik akhir](#).

API/CLI

1. Jalankan [UpdateOrganizationConfiguration](#) dengan menggunakan kredensial akun GuardDuty administrator yang didelegasikan, untuk secara otomatis mengonfigurasi GuardDuty dan rencana perlindungan opsional di Wilayah tersebut untuk organisasi Anda. [Untuk informasi tentang berbagai konfigurasi auto-enable, lihat `autoEnableOrganization Anggota`.](#)

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/> konsol, atau jalankan [ListDetectors](#) API. `detectorId`

Untuk mengatur preferensi aktifkan otomatis untuk salah satu paket perlindungan opsional yang didukung di Wilayah Anda, ikuti langkah-langkah yang disediakan di bagian dokumentasi terkait dari setiap paket perlindungan.

2. Anda dapat memvalidasi preferensi untuk organisasi Anda di Wilayah saat ini. Jalankan [describeOrganizationConfiguration](#). Pastikan untuk menentukan ID detektor dari akun GuardDuty administrator yang didelegasikan.

 Note

Mungkin diperlukan waktu hingga 24 jam untuk memperbarui konfigurasi untuk semua akun anggota.

3. Atau, jalankan AWS CLI perintah berikut untuk mengatur preferensi agar mengaktifkan atau menonaktifkan secara otomatis GuardDuty di Region untuk akun baru (NEW) yang bergabung dengan organisasi, semua akun (ALL), atau tidak ada akun (NONE) di organisasi. Untuk informasi selengkapnya, lihat [autoEnableOrganizationAnggota](#). Berdasarkan preferensi Anda, Anda mungkin perlu mengganti NEW dengan ALL atau NONE. Jika Anda mengonfigurasi paket perlindungan dengan ALL, paket perlindungan juga akan diaktifkan untuk akun GuardDuty administrator yang didelegasikan. Pastikan untuk menentukan ID detektor akun GuardDuty administrator yang didelegasikan yang mengelola konfigurasi organisasi.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/> konsol, atau jalankan [ListDetectors](#) API. `detectorId`

```
aws guardduty update-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0 --auto-enable-organization-members=NEW
```

4. Anda dapat memvalidasi preferensi untuk organisasi Anda di Wilayah saat ini. Jalankan AWS CLI perintah berikut dengan menggunakan ID detektor dari akun GuardDuty administrator yang didelegasikan.

```
aws guardduty describe-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0
```

(Disarankan) ulangi langkah sebelumnya di setiap Wilayah dengan menggunakan ID detektor akun GuardDuty administrator yang didelegasikan.

Note

Ketika akun GuardDuty administrator yang didelegasikan memilih keluar dari Wilayah keikutsertaan, meskipun organisasi Anda memiliki konfigurasi GuardDuty aktifkan otomatis yang disetel ke akun anggota baru saja (NEW) atau semua akun anggota (ALL), GuardDuty tidak dapat diaktifkan untuk akun anggota mana pun di organisasi yang saat ini telah dinonaktifkan. GuardDuty Untuk informasi tentang konfigurasi akun anggota Anda, buka Akun di panel navigasi [GuardDuty konsol](#) atau gunakan [ListMembersAPI](#).

Menambahkan anggota ke organisasi

Sebagai akun GuardDuty administrator yang didelegasikan, Anda dapat menambahkan satu atau lebih Akun AWS ke GuardDuty organisasi. Ketika Anda menambahkan akun sebagai GuardDuty anggota, itu akan secara otomatis GuardDuty diaktifkan di Wilayah itu. Ada pengecualian untuk akun manajemen organisasi. Sebelum akun manajemen ditambahkan sebagai GuardDuty anggota, itu harus GuardDuty diaktifkan.

Pilih metode yang disukai untuk menambahkan akun anggota ke GuardDuty organisasi Anda.

Console

1. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.

Untuk masuk, gunakan kredensial akun GuardDuty administrator yang didelegasikan.

2. Di panel navigasi, pilih Akun.

Tabel akun menampilkan semua akun anggota yang aktif (tidak ditangguhkan Akun AWS) dan mungkin terkait dengan akun GuardDuty administrator yang didelegasikan. Jika akun anggota dikaitkan dengan akun administrator organisasi, maka Type akan menjadi salah satu dari yang berikut: Via Organizations or By Invitation. Jika akun anggota tidak terkait dengan akun GuardDuty administrator organisasi, Jenis akun anggota ini bukan anggota.

3. Pilih satu atau beberapa akun IDs yang ingin Anda tambahkan sebagai anggota. Akun ini IDs harus memiliki Type as Via Organizations.

Akun yang ditambahkan melalui undangan bukan bagian dari organisasi Anda. Anda dapat mengelola akun tersebut secara individual. Untuk informasi selengkapnya, lihat [Mengelola akun dengan undangan](#).

4. Pilih dropdown Tindakan, lalu pilih Tambah anggota. Setelah Anda menambahkan akun ini sebagai anggota, GuardDuty konfigurasi auto-enable akan berlaku. Berdasarkan pengaturan di [Menyetel preferensi aktifkan otomatis organisasi](#), GuardDuty konfigurasi akun ini dapat berubah.
5. Anda dapat memilih panah bawah kolom Status untuk mengurutkan akun berdasarkan status Bukan anggota dan kemudian memilih setiap akun yang belum GuardDuty diaktifkan di Wilayah saat ini.

Jika tidak ada akun yang tercantum dalam tabel akun yang telah ditambahkan sebagai anggota, Anda dapat mengaktifkan GuardDuty di Wilayah saat ini untuk semua akun organisasi. Pilih Aktifkan di spanduk di bagian atas halaman. Tindakan ini secara otomatis mengaktifkan GuardDuty konfigurasi Auto-enable sehingga GuardDuty diaktifkan untuk setiap akun baru yang bergabung dengan organisasi.

6. Pilih Konfirmasi untuk menambahkan akun sebagai anggota. Tindakan ini juga memungkinkan GuardDuty untuk semua akun yang dipilih. Status akun akan berubah menjadi Diaktifkan.
7. (Disarankan) Ulangi langkah-langkah ini di masing-masing Wilayah AWS. Ini memastikan bahwa akun GuardDuty administrator yang didelegasikan dapat mengelola temuan dan konfigurasi lain untuk akun anggota di semua Wilayah yang telah GuardDuty Anda aktifkan.

Fitur auto-enable memungkinkan GuardDuty untuk semua anggota masa depan organisasi Anda. Ini memungkinkan akun GuardDuty administrator yang didelegasikan untuk mengelola anggota baru yang dibuat di dalam atau ditambahkan ke organisasi. Ketika jumlah akun anggota mencapai batas 50.000, fitur Auto-enable secara otomatis dimatikan. Jika Anda menghapus akun anggota dan jumlah total anggota berkurang menjadi kurang dari 50.000, fitur Auto-enable akan diaktifkan kembali.

API/CLI

- Jalankan [CreateMembers](#) dengan menggunakan kredensi akun administrator yang didelegasikan. GuardDuty

Anda harus menentukan ID detektor regional dari akun GuardDuty administrator yang didelegasikan dan detail akun (Akun AWS IDs dan alamat email yang sesuai) dari akun yang ingin Anda tambahkan sebagai GuardDuty anggota. Anda dapat membuat satu atau beberapa anggota dengan operasi API ini.

Ketika Anda menjalankan `CreateMembers` di organisasi Anda, preferensi mengaktifkan otomatis untuk anggota baru akan berlaku saat akun anggota baru bergabung dengan organisasi Anda. Ketika Anda menjalankan `CreateMembers` dengan akun anggota yang ada, konfigurasi organisasi juga akan berlaku untuk anggota yang ada. Ini mungkin mengubah konfigurasi akun anggota yang ada saat ini.

Jalankan [ListAccounts](#) di Referensi AWS Organizations API, untuk melihat semua akun di AWS organisasi.

- Atau, Anda dapat menggunakan AWS Command Line Interface. Jalankan AWS CLI perintah berikut dan pastikan untuk menggunakan ID detektor valid Anda sendiri, Akun AWS ID, dan alamat email yang terkait dengan ID akun.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan [ListDetectors](#) API. `detectorId`

```
aws guardduty create-members --detector-id 12abc34d567e8fa901bc2d34e56789f0
--account-details AccountId=111122223333,Email=guardduty-member-
name@amazon.com
```

Anda dapat melihat daftar semua anggota organisasi dengan menjalankan AWS CLI perintah berikut:

```
aws organizations list-accounts
```

Setelah Anda menambahkan akun ini sebagai anggota, GuardDuty konfigurasi auto-enable akan berlaku.

(Opsional) Aktifkan paket perlindungan untuk akun anggota yang ada

Prosedur berikut mencakup langkah-langkah untuk mengaktifkan rencana perlindungan untuk akun anggota yang ada dengan menggunakan halaman Akun. Untuk langkah-langkah untuk melakukan ini dengan menggunakan API atau AWS CLI, lihat dokumen yang terkait dengan rencana perlindungan tertentu.

Anda dapat mengaktifkan paket perlindungan untuk masing-masing akun melalui halaman Akun.

1. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.

Gunakan kredensi akun GuardDuty administrator yang didelegasikan.

2. Di panel navigasi, pilih Akun.
3. Pilih satu atau beberapa akun yang ingin Anda konfigurasi paket perlindungannya. Ulangi langkah-langkah berikut untuk setiap paket perlindungan yang ingin Anda konfigurasi:
 - a. Pilih Edit Paket Perlindungan.
 - b. Dari daftar rencana perlindungan, pilih satu paket perlindungan yang ingin Anda konfigurasi.
 - c. Pilih salah satu tindakan yang ingin Anda lakukan untuk paket perlindungan ini, lalu pilih Konfirmasi.
 - d. Untuk akun yang dipilih, kolom yang sesuai dengan paket perlindungan yang dikonfigurasi akan menampilkan konfigurasi yang diperbarui sebagai Diaktifkan atau Tidak diaktifkan.

Terus mengelola akun anggota Anda dalam GuardDuty

Sebagai akun GuardDuty administrator yang didelegasikan, Anda bertanggung jawab untuk menjaga konfigurasi GuardDuty dan rencana perlindungan opsionalnya untuk semua akun di organisasi Anda di setiap yang didukung Wilayah AWS. Bagian berikut memberikan opsi tentang mempertahankan status konfigurasi GuardDuty atau salah satu rencana perlindungan opsionalnya:

Untuk mempertahankan status konfigurasi seluruh organisasi Anda di setiap Wilayah

- Setel preferensi aktifkan otomatis untuk seluruh organisasi dengan menggunakan GuardDuty konsol — Anda dapat mengaktifkan GuardDuty secara otomatis untuk semua (ALL) anggota dalam organisasi atau anggota baru (NEW) yang bergabung dengan organisasi, atau memilih untuk tidak mengaktifkan secara otomatis salah satu anggota dalam organisasi. NONE

Anda juga dapat mengonfigurasi pengaturan yang sama atau berbeda untuk salah satu paket perlindungan di dalamnya GuardDuty.

Mungkin diperlukan waktu hingga 24 jam untuk memperbarui konfigurasi untuk semua akun anggota di organisasi.

- Perbarui preferensi aktifkan otomatis dengan menggunakan API — Jalankan [UpdateOrganizationConfiguration](#) untuk mengonfigurasi secara otomatis GuardDuty dan rencana perlindungan opsionalnya untuk organisasi. Ketika Anda menjalankan [CreateMembers](#) untuk

menambahkan akun anggota baru di organisasi Anda, pengaturan yang dikonfigurasi akan berlaku secara otomatis. Ketika Anda menjalankan `CreateMembers` dengan akun anggota yang ada, konfigurasi organisasi juga akan berlaku untuk anggota yang ada. Ini mungkin mengubah konfigurasi akun anggota yang ada saat ini.

Untuk melihat semua akun di organisasi Anda, jalankan [ListAccounts](#) di Referensi AWS Organizations API.

Untuk mempertahankan status konfigurasi untuk akun anggota secara individual di setiap Wilayah

- Untuk melihat semua akun di organisasi Anda, jalankan [ListAccounts](#) di Referensi AWS Organizations API.
- Jika Anda ingin akun anggota selektif memiliki status konfigurasi yang berbeda, jalankan [UpdateMemberDetectors](#) untuk setiap akun anggota satu per satu.

Anda dapat menggunakan GuardDuty konsol untuk melakukan tugas yang sama dengan menavigasi ke halaman Akun di GuardDuty konsol.

Untuk informasi tentang mengaktifkan paket perlindungan untuk masing-masing akun dengan menggunakan konsol atau API, lihat halaman konfigurasi untuk paket perlindungan terkait.

Penangguhan GuardDuty untuk akun anggota

Sebagai akun GuardDuty administrator yang didelegasikan, Anda dapat menangguhkan GuardDuty layanan untuk akun anggota di organisasi Anda. Jika Anda melakukan ini, akun anggota tetap berada di GuardDuty organisasi Anda. Anda juga dapat mengaktifkan kembali GuardDuty akun anggota ini di lain waktu. Namun, jika Anda akhirnya ingin memisahkan (menghapus) akun anggota ini, maka setelah mengikuti langkah-langkah di bagian ini, Anda harus mengikuti langkah-langkah di [Memutuskan \(menghapus\) akun anggota dari akun administrator](#).

Saat Anda menangguhkan GuardDuty akun anggota, Anda dapat mengharapkan perubahan berikut:

- GuardDuty tidak lagi memantau keamanan AWS lingkungan, atau menghasilkan temuan baru.
- Temuan yang ada di akun anggota tetap utuh.
- Akun anggota yang GuardDuty ditangguhkan tidak dikenakan biaya apa pun untuk. GuardDuty

Jika akun anggota telah mengaktifkan Perlindungan Malware untuk S3 untuk satu atau beberapa bucket di akun mereka, maka penangguhan GuardDuty tidak memengaruhi konfigurasi

Perlindungan Malware untuk S3. Akun anggota akan terus menimbulkan biaya penggunaan untuk Perlindungan Malware untuk S3. Agar akun anggota berhenti menggunakan Perlindungan Malware untuk S3, mereka harus menonaktifkan fitur ini untuk ember yang dilindungi. Untuk informasi selengkapnya, lihat [Menonaktifkan Perlindungan Malware untuk S3 untuk bucket yang dilindungi](#).

Pilih metode yang disukai GuardDuty untuk menangguhkan akun anggota di organisasi Anda.

Console

1. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.

Untuk masuk, gunakan kredensial akun administrator yang GuardDuty didelegasikan.

2. Di panel navigasi, pilih Akun.
3. Di halaman Akun, pilih satu atau beberapa akun yang ingin Anda tangguhkan GuardDuty.
4. Pilih menu tarik-turun Tindakan dan kemudian, pilih Tangguhkan. GuardDuty
5. Pilih Tangguhkan GuardDuty untuk mengonfirmasi pilihan.

Ini akan mengubah Status akun anggota menjadi Dinonaktifkan (ditangguhkan).

Ulangi langkah sebelumnya di setiap Wilayah tambahan di mana Anda ingin memisahkan atau menghapus akun anggota.

API

1. Untuk mengambil ID akun akun anggota yang ingin Anda tangguhkan GuardDuty, gunakan API. [ListMembers](#) Sertakan `OnlyAssociated` parameter dalam permintaan Anda. Jika Anda menetapkan nilai parameter `initrue`, GuardDuty mengembalikan `members` array yang memberikan rincian tentang hanya akun-akun yang saat ini menjadi GuardDuty anggota.

Atau, Anda dapat menggunakan AWS Command Line Interface (AWS CLI) untuk menjalankan perintah berikut:

```
aws guardduty list-members --only-associated true --region us-east-1
```

Ganti *us-east-1* dengan Wilayah tempat Anda ingin menangguhkan GuardDuty akun ini.

2. Untuk menangguhkan satu atau beberapa akun GuardDuty anggota, jalankan [StopMonitoringMembers](#) untuk menangguhkan GuardDuty akun anggota.

Atau, Anda dapat menggunakan AWS CLI untuk menjalankan perintah berikut:

```
aws guardduty stop-monitoring-members --detector-id  
12abc34d567e8fa901bc2d34EXAMPLE --account-ids 111122223333 --region us-east-1
```

Ganti *us-east-1* dengan Wilayah tempat Anda ingin menanggihkan akun ini. Jika Anda memiliki daftar akun IDs yang ingin Anda hapus, pisahkan dengan karakter spasi.

Jika Anda ingin memisahkan (menghapus) akun anggota ini, ikuti langkah-langkahnya. [Memutuskan \(menghapus\) akun anggota dari akun administrator](#)

Memutuskan (menghapus) akun anggota dari akun administrator

Saat Anda ingin berhenti mengonfigurasi GuardDuty pengaturan dan mengakses data dari akun anggota, hapus akun itu sebagai akun GuardDuty anggota. Anda dapat melakukannya dengan memisahkan (menghapus) akun itu dari akun GuardDuty administrator.

Saat Anda memisahkan akun GuardDuty anggota, GuardDuty tetap diaktifkan untuk akun di AWS Wilayah saat ini. Namun, akun tersebut dipisahkan dari akun GuardDuty administrator yang didelegasikan dan akun tersebut menjadi akun mandiri GuardDuty . Setelah Anda melepaskan akun anggota, akun tersebut terus ditampilkan di inventaris akun. GuardDuty tidak memberi tahu pemilik akun bahwa Anda memutuskan hubungan akun. Anda dapat menambahkan akun ke organisasi Anda lagi di lain waktu.

Pilih metode yang disukai untuk memisahkan (menghapus) akun anggota dari organisasi Anda.

Console

1. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.

Untuk masuk, gunakan kredensial akun administrator yang GuardDuty didelegasikan.

2. Di panel navigasi, pilih Akun.
3. Dalam tabel Akun, Anda dapat menghapus akun yang memiliki Type as Via Organizations and Status as Enabled.

Pilih satu atau beberapa akun dengan Jenis dan Status yang sama.

4. Dari menu tarik-turun Tindakan, pilih Putuskan akun.

5. Pilih Putuskan akun untuk mengonfirmasi pilihan Anda.
6. Nilai Status untuk akun yang dipilih akan berubah menjadi Bukan anggota. Jumlah Via Organizations (Active/All) di pojok kanan atas halaman Akun akan berubah untuk mencerminkan pembaruan.

Ulangi langkah sebelumnya di setiap Wilayah tambahan di mana Anda ingin memisahkan akun anggota.

API

1. Untuk mengambil ID akun untuk akun anggota yang ingin Anda hapus, gunakan [ListMembers](#) API. Sertakan `OnlyAssociated` parameter dalam permintaan Anda. Jika Anda menetapkan nilai parameter `init` true, GuardDuty mengembalikan `members` array yang memberikan rincian tentang hanya akun-akun yang saat ini menjadi GuardDuty anggota.

Atau, Anda dapat menggunakan AWS Command Line Interface (AWS CLI) untuk menjalankan perintah berikut:

```
aws guardduty list-members --only-associated true --region us-east-1
```

Ganti *us-east-1* dengan Wilayah tempat Anda ingin menghapus akun ini.

2. Untuk menghapus satu atau beberapa akun GuardDuty anggota, jalankan [DisassociateMembers](#) untuk menghapus akun anggota yang terkait dengan akun administrator.

Atau, Anda dapat menggunakan AWS CLI untuk menjalankan perintah berikut:

```
aws guardduty disassociate-members --detector-id 12abc34d567e8fa901bc2d34EXAMPLE  
--account-ids 111122223333 --region us-east-1
```

Ganti *us-east-1* dengan Wilayah tempat Anda ingin menghapus akun ini. Jika Anda memiliki daftar akun IDs yang ingin Anda hapus, pisahkan dengan karakter spasi.

Menghapus akun anggota dari organisasi GuardDuty

Sebagai akun GuardDuty administrator yang didelegasikan, setelah Anda melepaskan akun anggota dan Anda tidak ingin lagi menyimpan akun anggota tersebut di GuardDuty organisasi, Anda dapat

menghapus akun anggota tersebut dari organisasi Anda GuardDuty . Akun anggota ini tidak akan lagi muncul di inventaris akun Anda. Namun, jika tidak GuardDuty ditangguhkan di akun anggota ini, konfigurasi GuardDuty dan rencana perlindungan khusus tetap sama. Akun ini sekarang akan menjadi akun mandiri dan dapat [menonaktifkan GuardDuty](#) diri mereka sendiri.

Langkah ini tidak akan menghapus akun anggota dari AWS organisasi Anda.

Pilih metode yang diinginkan untuk menghapus akun anggota dari GuardDuty organisasi Anda.

Console

1. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.

Untuk masuk, gunakan kredensial akun administrator yang GuardDuty didelegasikan.

2. Di panel navigasi, pilih Akun.
3. Dalam tabel Akun, Anda dapat menghapus akun yang memiliki Type as Via Organizations and Status as Removed (disassociated).

Pilih satu atau beberapa akun dengan Jenis dan Status yang sama.

4. Dari menu tarik-turun Tindakan, pilih Hapus akun.
5. Pilih Hapus akun untuk mengonfirmasi pilihan Anda. Anggota akun yang dipilih tidak akan muncul lagi di tabel Akun Anda.

Ulangi langkah sebelumnya di setiap Wilayah tambahan tempat Anda ingin menghapus akun anggota ini.

API/CLI

1. Untuk mengambil ID akun untuk akun anggota yang ingin Anda hapus, gunakan [ListMembers](#) API. Sertakan `OnlyAssociated` parameter dalam permintaan Anda. Jika Anda menetapkan nilai parameter ini `false`, GuardDuty mengembalikan `members` larik yang memberikan rincian hanya tentang akun yang saat ini merupakan GuardDuty anggota yang tidak terkait.

Atau, Anda dapat menggunakan AWS Command Line Interface (AWS CLI) untuk menjalankan perintah berikut:

```
aws guardduty list-members --detector-id 12abc34d567e8fa901bc2d34EXAMPLE --only-associated="false" --region us-east-1
```

Ganti **12abc34d567e8fa901bc2d34EXAMPLE** dengan ID detektor akun GuardDuty administrator yang didelegasikan dan **us-east-1** dengan Wilayah tempat Anda ingin menghapus akun ini.

2. Untuk menghapus satu atau beberapa akun GuardDuty anggota, jalankan [DeleteMembers](#) untuk menghapus akun anggota dari GuardDuty organisasi.

Atau, Anda dapat menggunakan AWS CLI untuk menjalankan perintah berikut:

```
aws guardduty delete-members --detector-id 12abc34d567e8fa901bc2d34EXAMPLE --account-ids 111122223333 --region us-east-1
```

Ganti **12abc34d567e8fa901bc2d34EXAMPLE** dengan ID detektor akun GuardDuty administrator yang didelegasikan dan **us-east-1** dengan Wilayah tempat Anda ingin menghapus akun ini. Jika Anda memiliki daftar akun IDs yang ingin Anda hapus, pisahkan dengan karakter spasi.

Mengubah akun GuardDuty administrator yang didelegasikan

Anda dapat menghapus akun GuardDuty administrator yang didelegasikan untuk organisasi Anda di setiap Wilayah dan kemudian mendelegasikan administrator baru di setiap Wilayah. Untuk menjaga postur keamanan akun anggota organisasi Anda di Wilayah, Anda harus memiliki akun GuardDuty administrator yang didelegasikan di Wilayah tersebut.

Catatan

Sebelum menghapus akun GuardDuty administrator yang didelegasikan, Anda harus memisahkan semua akun anggota yang terkait dengan akun GuardDuty administrator yang didelegasikan, lalu menghapusnya dari organisasi. GuardDuty Untuk informasi selengkapnya tentang langkah-langkah ini, lihat dokumen berikut:

- [Memutuskan \(menghapus\) akun anggota dari akun administrator](#)
- [Menghapus akun anggota dari organisasi GuardDuty](#)

Menghapus akun GuardDuty administrator yang didelegasikan yang ada

Langkah 1 - Untuk menghapus akun GuardDuty administrator yang didelegasikan yang ada di setiap Wilayah

1. Sebagai akun GuardDuty administrator yang didelegasikan, cantumkan semua akun anggota yang terkait dengan akun administrator Anda. Jalankan [ListMembers](#) dengan `onlyAssociated=false`.
2. Jika preferensi aktifkan otomatis untuk GuardDuty atau salah satu paket perlindungan opsional disetel ke ALL, jalankan [UpdateOrganizationConfiguration](#) untuk memperbarui konfigurasi organisasi ke salah satu NEW atau NONE. Tindakan ini akan mencegah kesalahan saat Anda memisahkan semua akun anggota di langkah berikutnya.
3. Jalankan [DisassociateMembers](#) untuk memisahkan semua akun anggota yang terkait dengan akun administrator.
4. Jalankan [DeleteMembers](#) untuk menghapus asosiasi antara akun administrator dan akun anggota.
5. Sebagai akun manajemen organisasi, jalankan [DisableOrganizationAdminAccount](#) untuk menghapus akun GuardDuty administrator yang didelegasikan yang ada.
6. Ulangi langkah-langkah ini di setiap Wilayah AWS tempat Anda memiliki akun GuardDuty administrator yang didelegasikan ini.

Langkah 2 - Untuk membatalkan pendaftaran akun GuardDuty administrator yang didelegasikan yang ada di AWS Organizations (Tindakan global satu kali)

- Jalankan [DeregisterDelegatedAdministrator](#) di Referensi AWS Organizations API, untuk menghapus registrasi akun GuardDuty administrator yang sudah didelegasikan. AWS Organizations

Atau, Anda dapat menjalankan AWS CLI perintah berikut:

```
aws organizations deregister-delegated-administrator --account-id 111122223333 --  
service-principal guardduty.amazonaws.com
```

Pastikan untuk mengganti **111122223333** dengan akun GuardDuty administrator yang didelegasikan yang ada.

Setelah Anda membatalkan pendaftaran akun GuardDuty administrator lama yang didelegasikan, Anda dapat menambahkannya sebagai akun anggota ke akun administrator yang didelegasikan GuardDuty baru.

Menunjuk akun GuardDuty administrator baru yang didelegasikan di setiap Wilayah

1. Tentukan akun GuardDuty administrator baru yang didelegasikan di setiap Wilayah dengan menggunakan metode akses pilihan Anda - GuardDuty konsol, atau API atau AWS CLI Untuk informasi selengkapnya, lihat [Menunjuk akun administrator yang didelegasikan GuardDuty](#).
2. Jalankan [DescribeOrganizationConfiguration](#) untuk melihat konfigurasi aktifkan otomatis saat ini untuk organisasi Anda.

Important

Sebelum menambahkan anggota apa pun ke akun GuardDuty administrator yang didelegasikan baru, Anda harus memverifikasi konfigurasi aktifkan otomatis untuk organisasi Anda. Konfigurasi ini khusus untuk akun GuardDuty administrator yang didelegasikan baru dan Wilayah yang dipilih, dan tidak terkait AWS Organizations dengan. Saat Anda menambahkan akun anggota organisasi (baru atau yang sudah ada) di bawah akun GuardDuty administrator yang didelegasikan baru, konfigurasi aktifkan otomatis akun GuardDuty administrator yang didelegasikan akan berlaku pada saat mengaktifkan GuardDuty atau salah satu paket perlindungan opsionalnya.

Ubah konfigurasi organisasi untuk akun GuardDuty administrator baru yang didelegasikan dengan menggunakan metode akses pilihan Anda - GuardDuty konsol, atau API atau AWS CLI. Lihat informasi yang lebih lengkap di [Menyetel preferensi aktifkan otomatis organisasi](#).

Mengelola GuardDuty akun dengan undangan

Untuk mengelola akun di luar organisasi, Anda dapat menggunakan metode undangan lawas. Jika Anda menggunakan metode ini, akun Anda ditetapkan sebagai akun administrator saat akun lain menerima undangan Anda untuk menjadi akun anggota.

 Note

GuardDuty merekomendasikan menggunakan AWS Organizations alih-alih GuardDuty undangan, untuk mengelola akun anggota Anda. Untuk informasi selengkapnya, lihat [Mengelola akun dengan AWS Organizations](#).

Jika akun Anda bukan akun administrator, Anda dapat menerima undangan dari akun lain. Jika Anda menerima, akun Anda menjadi akun anggota. AWS Akun tidak dapat berupa akun GuardDuty administrator dan akun anggota secara bersamaan.

Ketika Anda menerima undangan dari satu akun, Anda tidak dapat menerima undangan dari akun lain. Untuk menerima undangan dari akun lain, Anda harus terlebih dahulu memisahkan akun Anda dari akun administrator yang ada. Atau, akun administrator juga dapat memisahkan dan menghapus akun Anda dari organisasi mereka.

Akun yang terkait dengan undangan memiliki account-to-member hubungan administrator keseluruhan yang sama dengan akun yang terkait dengan AWS Organizations, seperti yang dijelaskan dalam [Memahami hubungan antara akun GuardDuty administrator dan akun anggota](#). Namun, pengguna akun administrator undangan tidak dapat mengaktifkan GuardDuty atas nama akun anggota terkait atau melihat akun non-anggota lainnya dalam AWS Organizations organisasi mereka.

 Important

Transfer data lintas-regional dapat terjadi ketika GuardDuty membuat akun anggota menggunakan metode ini. Untuk memverifikasi alamat email akun anggota, GuardDuty gunakan layanan verifikasi email yang hanya beroperasi di Wilayah AS Timur (Virginia N.).

Topik

- [Menambahkan akun dengan undangan](#)
- [Mengkonsolidasikan akun GuardDuty administrator di bawah satu organisasi](#)

Menambahkan akun dengan undangan

Sebagai akun administrator yang telah GuardDuty diaktifkan, Anda dapat menambahkan anggota untuk mulai menggunakan GuardDuty. Setelah menambahkan anggota, Anda dapat mengundang mereka untuk bergabung GuardDuty, dan mereka dapat memilih untuk menanggapi undangan Anda.

Note

GuardDuty merekomendasikan menggunakan AWS Organizations alih-alih GuardDuty undangan, untuk mengelola akun anggota Anda. Untuk informasi selengkapnya, lihat [Mengelola akun dengan AWS Organizations](#).

Pilih metode akses yang disukai untuk menambahkan akun GuardDuty anggota sebagai akun GuardDuty administrator.

Console

Langkah 1 - Tambahkan akun

1. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.
2. Di panel navigasi, pilih Akun.
3. Pilih Tambahkan akun berdasarkan undangan di panel atas.
4. Pada halaman Tambahkan akun anggota, di bawah Masukkan detail akun, masukkan Akun AWS ID dan alamat email yang terkait dengan akun yang ingin Anda tambahkan.
5. Untuk menambahkan baris lain untuk memasukkan detail akun satu per satu, pilih Tambahkan akun lain. Anda juga dapat memilih Unggah file.csv dengan detail akun untuk menambahkan akun secara massal.

Important

Baris pertama file csv Anda harus berisi header, seperti yang digambarkan dalam contoh berikut —. Account ID,Email Setiap baris berikutnya harus berisi satu Akun AWS ID yang valid dan alamat email yang terkait. Format baris valid jika hanya berisi satu Akun AWS ID dan alamat email terkait dipisahkan oleh koma.

```
Account ID,Email
```

55555555555, user@example.com

6. Setelah Anda menambahkan semua detail akun, pilih Berikutnya. Anda dapat melihat akun yang baru ditambahkan di tabel Akun. Status akun ini akan menjadi Undangan tidak terkirim. Untuk informasi tentang mengirim undangan ke satu atau beberapa akun tambahan, lihat [Step 2 - Invite an account](#).

Langkah 2 - Undang akun

1. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.
2. Di panel navigasi, pilih Akun.
3. Pilih satu atau beberapa akun yang ingin Anda undang ke Amazon GuardDuty.
4. Pilih menu tarik-turun Tindakan dan kemudian pilih Undang.
5. Di kotak GuardDuty dialog Undangan ke, masukkan pesan undangan (opsional).

Jika akun yang diundang tidak memiliki akses ke email, pilih kotak centang Juga kirim pemberitahuan email ke pengguna root pada undangan Akun AWS dan buat peringatan di undangan. AWS Health Dashboard

6. Pilih Kirim undangan. Jika undangan memiliki akses ke alamat email yang ditentukan, mereka dapat melihat undangan dengan membuka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>
7. Saat undangan menerima undangan, nilai di kolom Status berubah menjadi Diundang. Untuk informasi tentang menerima undangan, lihat [Step 3 - Accept an invitation](#).

Langkah 3 - Terima undangan

1. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.

Important

Anda harus mengaktifkan GuardDuty sebelum Anda dapat melihat atau menerima undangan keanggotaan.

2. Lakukan hal berikut hanya jika Anda GuardDuty belum mengaktifkan; jika tidak, Anda dapat melewati langkah ini dan melanjutkan dengan langkah berikutnya.

Jika Anda belum mengaktifkan GuardDuty, pilih Memulai di GuardDuty halaman Amazon.

Pada GuardDuty halaman Selamat Datang di, pilih Aktifkan GuardDuty.

3. Setelah mengaktifkan GuardDuty akun Anda, gunakan langkah-langkah berikut untuk menerima undangan keanggotaan:
 - a. Pada panel navigasi, silakan pilih Pengaturan.
 - b. Pilih Akun .
 - c. Pada Akun, pastikan untuk memverifikasi pemilik akun tempat Anda menerima undangan. Aktifkan Terima untuk menerima undangan keanggotaan.
4. Setelah Anda menerima undangan, akun Anda menjadi akun GuardDuty anggota. Akun yang pemiliknya mengirim undangan menjadi akun GuardDuty administrator. Akun administrator akan tahu bahwa Anda telah menerima undangan. Tabel Akun di GuardDuty akun mereka akan diperbarui. Nilai di kolom Status yang sesuai dengan ID akun anggota Anda akan berubah menjadi Diaktifkan. Pemilik akun administrator sekarang dapat melihat GuardDuty dan mengelola serta konfigurasi paket perlindungan atas nama akun Anda. Akun administrator juga dapat melihat dan mengelola GuardDuty temuan yang dihasilkan untuk akun anggota Anda.

API/CLI

Anda dapat menunjuk akun GuardDuty administrator, dan membuat atau menambahkan akun GuardDuty anggota melalui undangan melalui operasi API. Jalankan operasi GuardDuty API berikut untuk menetapkan akun administrator dan akun anggota. GuardDuty

Selesaikan prosedur berikut menggunakan kredensi Akun AWS yang ingin Anda tetapkan sebagai akun administrator. GuardDuty

Membuat atau menambahkan akun anggota

1. Jalankan operasi [CreateMembers](#) API menggunakan kredensial AWS akun yang telah GuardDuty diaktifkan. Ini adalah akun yang Anda inginkan menjadi akun GuardDuty akun administrator.

Anda harus menentukan ID detektor AWS akun saat ini dan ID akun serta alamat email dari akun yang ingin Anda jadikan GuardDuty anggota. Anda dapat membuat satu atau beberapa anggota dengan operasi API ini.

Anda juga dapat menggunakan Alat Baris AWS Perintah untuk menunjuk akun administrator dengan menjalankan perintah CLI berikut. Pastikan untuk menggunakan ID pendeteksi, ID akun, dan email Anda sendiri yang valid.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan [ListDetectors](#) API. `detectorId`

```
aws guardduty create-members --detector-id 12abc34d567e8fa901bc2d34e56789f0 --  
account-details AccountId=111122223333,Email=guardduty-member@organization.com
```

2. Jalankan [InviteMembers](#) dengan menggunakan kredensi AWS akun yang telah GuardDuty diaktifkan. Ini adalah akun yang Anda inginkan menjadi akun GuardDuty akun administrator.

Anda harus menentukan ID detektor AWS akun saat ini dan akun IDs akun yang ingin Anda jadikan GuardDuty anggota. Anda dapat mengundang satu anggota atau lebih dengan operasi API ini.

Note

Anda juga dapat menentukan pesan undangan opsional dengan menggunakan parameter `message` permintaan.

Anda juga dapat menggunakan AWS Command Line Interface untuk menunjuk akun anggota dengan menjalankan perintah berikut. Pastikan untuk menggunakan ID detektor Anda sendiri yang valid dan akun yang valid IDs untuk akun yang ingin Anda undang.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan [ListDetectors](#) API. `detectorId`

```
aws guardduty invite-members --detector-id 12abc34d567e8fa901bc2d34e56789f0 --  
account-ids 111122223333
```

Menerima undangan

Selesaikan prosedur berikut menggunakan kredensi dari setiap AWS akun yang ingin Anda tetapkan sebagai GuardDuty akun anggota.

1. Jalankan operasi [CreateDetector](#) API untuk setiap AWS akun yang diundang untuk menjadi akun GuardDuty anggota dan Anda ingin menerima undangan.

Anda harus menentukan apakah sumber daya detektor akan diaktifkan menggunakan GuardDuty layanan. Detektor harus dibuat dan diaktifkan GuardDuty agar dapat beroperasi. Anda harus mengaktifkan terlebih dahulu GuardDuty sebelum menerima undangan.

Anda juga dapat melakukan ini dengan menggunakan AWS Command Line Tools menggunakan perintah CLI berikut.

```
aws guardduty create-detector --enable
```

2. Jalankan operasi [AcceptAdministratorInvitation](#) API untuk setiap AWS akun yang ingin Anda terima undangan keanggotaan, menggunakan kredensi akun tersebut.

Anda harus menentukan ID detektor AWS akun ini untuk akun anggota, ID akun akun administrator yang mengirim undangan, dan ID undangan undangan yang Anda terima. Anda dapat menemukan ID akun administrator di email undangan atau dengan menggunakan operasi API [ListInvitations](#).

Anda juga dapat menerima undangan menggunakan AWS Command Line Tools dengan menjalankan perintah CLI berikut. Pastikan Anda menggunakan ID detektor, ID akun administrator, dan ID undangan yang valid.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan [ListDetectors](#) API. `detectorId`

```
aws guardduty accept-invitation --detector-id 12abc34d567e8fa901bc2d34e56789f0  
--administrator-id 444455556666 --invitation-  
id 84b097800250d17d1872b34c4daadcf5
```

Mengkonsolidasikan akun GuardDuty administrator di bawah satu organisasi

GuardDuty merekomendasikan penggunaan asosiasi melalui AWS Organizations untuk mengelola akun anggota di bawah akun GuardDuty administrator yang didelegasikan. Anda dapat menggunakan contoh proses yang diuraikan di bawah ini untuk mengkonsolidasikan akun

administrator dan anggota yang terkait dengan undangan dalam organisasi di bawah satu akun administrator yang GuardDuty didelegasikan GuardDuty .

 Note

GuardDuty merekomendasikan menggunakan AWS Organizations alih-alih GuardDuty undangan, untuk mengelola akun anggota Anda. Untuk informasi selengkapnya, lihat [Mengelola akun dengan AWS Organizations](#).

Akun yang sudah dikelola oleh akun GuardDuty administrator yang didelegasikan, atau akun anggota aktif yang dikaitkan dengan akun administrator yang didelegasikan tidak dapat ditambahkan ke akun GuardDuty administrator yang didelegasikan lainnya GuardDuty . Setiap organisasi hanya dapat memiliki satu akun GuardDuty administrator yang didelegasikan per Wilayah, dan setiap akun anggota hanya dapat memiliki satu akun GuardDuty administrator yang didelegasikan.

Pilih metode akses yang disukai untuk mengkonsolidasikan akun GuardDuty administrator di bawah satu akun GuardDuty administrator yang didelegasikan.

Console

1. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.

Untuk masuk, gunakan kredensial akun manajemen organisasi.

2. Semua akun yang ingin Anda kelola GuardDuty harus menjadi bagian dari organisasi Anda. Untuk informasi tentang menambahkan akun ke organisasi Anda, lihat [Mengundang Akun AWS untuk bergabung dengan organisasi Anda](#).
3. Pastikan semua akun anggota dikaitkan dengan akun yang ingin Anda tetapkan sebagai akun GuardDuty administrator tunggal yang didelegasikan. Putuskan hubungan akun anggota yang masih terkait dengan akun administrator yang sudah ada sebelumnya.

Langkah-langkah berikut akan membantu Anda memisahkan akun anggota dari akun administrator yang sudah ada sebelumnya:

- a. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.
- b. Untuk masuk, gunakan kredensial akun administrator yang sudah ada sebelumnya.
- c. Di panel navigasi, pilih Akun.

- d. Pada halaman Akun, pilih satu atau beberapa akun yang ingin Anda pisahkan dari akun administrator.
 - e. Pilih Actions dan kemudian pilih Disassociate account.
 - f. Pilih Konfirmasi untuk menyelesaikan langkah.
4. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.

Untuk masuk, gunakan kredensial akun manajemen.

5. Pada panel navigasi, silakan pilih Pengaturan. Pada halaman Pengaturan, tentukan akun GuardDuty administrator yang didelegasikan untuk organisasi.
6. Masuk ke akun GuardDuty administrator yang didelegasikan yang ditunjuk.
7. Tambahkan anggota dari organisasi. Untuk informasi selengkapnya, lihat [Mengelola GuardDuty akun dengan AWS Organizations](#).

API/CLI

1. Semua akun yang ingin Anda kelola GuardDuty harus menjadi bagian dari organisasi Anda. Untuk informasi tentang menambahkan akun ke organisasi Anda, lihat [Mengundang Akun AWS untuk bergabung dengan organisasi Anda](#).
2. Pastikan semua akun anggota dikaitkan dengan akun yang ingin Anda tetapkan sebagai akun GuardDuty administrator tunggal yang didelegasikan.
 - a. Jalankan [DisassociateMembers](#) untuk memisahkan akun anggota yang masih terkait dengan akun administrator yang sudah ada sebelumnya.
 - b. Atau, Anda dapat menggunakan AWS Command Line Interface untuk menjalankan perintah berikut dan mengganti **777777777777** dengan ID detektor dari akun administrator yang sudah ada sebelumnya dari mana Anda ingin memisahkan akun anggota. Ganti **666666666666** dengan Akun AWS ID akun anggota yang ingin Anda pisahkan.

```
aws guardduty disassociate-members --detector-id 777777777777 --account-ids 666666666666
```

3. Jalankan [EnableOrganizationAdminAccount](#) untuk mendelegasikan akun GuardDuty administrator Akun AWS sebagai delegasi.

Atau, Anda dapat menggunakan AWS Command Line Interface untuk menjalankan perintah berikut untuk mendelegasikan akun GuardDuty administrator yang didelegasikan:

```
aws guardduty enable-organization-admin-account --admin-account-id 777777777777
```

4. Tambahkan anggota dari organisasi. Untuk informasi selengkapnya, lihat [Create or add member member accounts using API](#).

Important

Untuk memaksimalkan efektivitas GuardDuty, layanan regional, kami sarankan Anda menunjuk akun GuardDuty administrator yang didelegasikan dan menambahkan semua akun anggota Anda di setiap Wilayah.

GuardDuty pertimbangan untuk mengekspor detail akun anggota dalam format CSV

Sebagai akun GuardDuty administrator, Anda dapat mengekspor detail akun anggota dalam format CSV. Rincian ini mencakup ID akun anggota, nama, jenis (ditambahkan oleh AWS Organizations atau melalui undangan), dan status konfigurasi GuardDuty dan rencana perlindungan khusus.

Opsi Ekspor CSV ditampilkan di halaman GuardDuty Akun berdasarkan cara Anda mengelola beberapa akun anggota. Dengan menggunakan opsi Ekspor CSV, Anda dapat mengidentifikasi akun anggota mana yang mengaktifkan paket perlindungan tertentu.

Daftar berikut memberikan kriteria apakah CSV Ekspor akan tersedia di halaman GuardDuty Akun Anda atau tidak:

- Anda hanya menggunakan AWS Organizations untuk mengelola beberapa akun anggota dan jumlah total akun anggota di GuardDuty organisasi Anda hingga 5.000.
- Anda menggunakan metode keduanya AWS Organizations dan undangan, dan jumlah total akun anggota di GuardDuty organisasi Anda hingga 5.000.

Dalam skenario ini, CSV yang diekspor akan mencakup apakah akun anggota ditambahkan melalui AWS Organizations atau dengan menggunakan metode berbasis undangan.

- Jika Anda hanya menggunakan metode berbasis undangan untuk mengelola beberapa akun anggota, tidak ada opsi Ekspor CSV.

GuardDuty menemukan jenis

Temuan adalah pemberitahuan yang GuardDuty dihasilkan ketika mendeteksi indikasi aktivitas mencurigakan atau berbahaya di Anda. Akun AWS GuardDuty menghasilkan temuan di akun yang telah diaktifkan GuardDuty.

Untuk informasi tentang perubahan penting pada jenis GuardDuty temuan, termasuk jenis temuan yang baru ditambahkan atau yang sudah pensiun, lihat [Riwayat dokumen untuk Amazon GuardDuty](#).

Untuk informasi tentang menemukan jenis yang sekarang sudah pensiun, lihat [Tipe temuan yang sudah dihentikan](#).

GuardDuty EC2 menemukan jenis

Temuan berikut khusus untuk EC2 sumber daya Amazon dan selalu memiliki Jenis Sumber DayaInstance. Tingkat keparahan dan detail temuan berbeda berdasarkan Peran Sumber Daya, yang menunjukkan apakah EC2 sumber daya adalah target aktivitas yang mencurigakan atau aktor yang melakukan aktivitas tersebut.

Temuan yang tercantum di sini termasuk sumber data dan model yang digunakan untuk menghasilkan tipe temuan. Untuk informasi selengkapnya tentang sumber data dan model, lihat [GuardDuty sumber data dasar](#).

Catatan

- EC2 menemukan detail instance mungkin hilang jika instance sudah dihentikan, atau jika panggilan API yang mendasarinya berasal dari EC2 instance di Wilayah lain.
- EC2 Temuan yang menggunakan log aliran VPC sebagai sumber data tidak mendukung IPv6 lalu lintas.

Untuk semua EC2 temuan, disarankan agar Anda memeriksa sumber daya yang dimaksud untuk menentukan apakah itu berperilaku dengan cara yang diharapkan. Jika aktivitas diotorisasi, Anda dapat menggunakan Aturan Penekanan atau daftar IP Tepercaya untuk mencegah notifikasi positif palsu untuk sumber daya tersebut. Jika aktivitas tidak terduga, praktik keamanan terbaik adalah menganggap instans telah disusupi dan mengambil tindakan seperti yang diuraikan dalam [Memperbaiki instans Amazon yang berpotensi dikompromikan EC2](#).

Topik

- [Backdoor:EC2/C&CActivity.B](#)
- [Backdoor:EC2/C&CActivity.B!DNS](#)
- [Backdoor:EC2/DenialOfService.Dns](#)
- [Backdoor:EC2/DenialOfService.Tcp](#)
- [Backdoor:EC2/DenialOfService.Udp](#)
- [Backdoor:EC2/DenialOfService.UdpOnTcpPorts](#)
- [Backdoor:EC2/DenialOfService.UnusualProtocol](#)
- [Backdoor:EC2/Spambot](#)
- [Behavior:EC2/NetworkPortUnusual](#)
- [Behavior:EC2/TrafficVolumeUnusual](#)
- [CryptoCurrency:EC2/BitcoinTool.B](#)
- [CryptoCurrency:EC2/BitcoinTool.B!DNS](#)
- [DefenseEvasion:EC2/UnusualDNSResolver](#)
- [DefenseEvasion:EC2/UnusualDoHActivity](#)
- [DefenseEvasion:EC2/UnusualDoTActivity](#)
- [Impact:EC2/AbusedDomainRequest.Reputation](#)
- [Impact:EC2/BitcoinDomainRequest.Reputation](#)
- [Impact:EC2/MaliciousDomainRequest.Reputation](#)
- [Impact:EC2/PortSweep](#)
- [Impact:EC2/SuspiciousDomainRequest.Reputation](#)
- [Impact:EC2/WinRMBruteForce](#)
- [Recon:EC2/PortProbeEMRUnprotectedPort](#)
- [Recon:EC2/PortProbeUnprotectedPort](#)
- [Recon:EC2/Portscan](#)
- [Trojan:EC2/BlackholeTraffic](#)
- [Trojan:EC2/BlackholeTraffic!DNS](#)
- [Trojan:EC2/DGADomainRequest.B](#)

- [Trojan:EC2/DGADomainRequest.C!DNS](#)
- [Trojan:EC2/DNSDataExfiltration](#)
- [Trojan:EC2/DriveBySourceTraffic!DNS](#)
- [Trojan:EC2/DropPoint](#)
- [Trojan:EC2/DropPoint!DNS](#)
- [Trojan:EC2/PhishingDomainRequest!DNS](#)
- [UnauthorizedAccess:EC2/MaliciousIPCaller.Custom](#)
- [UnauthorizedAccess:EC2/MetadataDNSRebind](#)
- [UnauthorizedAccess:EC2/RDPBruteForce](#)
- [UnauthorizedAccess:EC2/SSHBruteForce](#)
- [UnauthorizedAccess:EC2/TorClient](#)
- [UnauthorizedAccess:EC2/TorRelay](#)

Backdoor:EC2/C&CActivity.B

Sebuah EC2 instance adalah query IP yang terkait dengan perintah yang dikenal dan server kontrol.

Tingkat keparahan default: Tinggi

- Sumber data: log alur VPC

Temuan ini menginformasikan bahwa instans yang tercantum dalam lingkungan AWS Anda menanyakan IP yang terkait dengan server perintah dan kontrol (C&C) yang dikenal. Instans yang tercantum mungkin disusupi. Server perintah dan kontrol adalah komputer yang mengeluarkan perintah untuk anggota botnet.

Botnet adalah kumpulan perangkat yang terhubung ke internet yang mungkin termasuk PCs, server, perangkat seluler, dan perangkat Internet of Things, yang terinfeksi dan dikendalikan oleh jenis malware yang umum. Botnet sering digunakan untuk mendistribusikan malware dan mengumpulkan informasi yang disalahgunakan, seperti nomor kartu kredit. Tergantung pada tujuan dan struktur botnet, server C&C mungkin juga mengeluarkan perintah untuk memulai serangan penolakan layanan (DDoS) terdistribusi.

Note

Jika IP yang ditanyakan terkait log4j, maka bidang temuan terkait akan mencakup nilai-nilai berikut:

- Service.additionalInfo. threatListName = Amazon
- Service.additionalInfo.ThreatName = Log4j Terkait

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, instans Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memperbaiki instans Amazon yang berpotensi dikompromikan EC2](#).

Backdoor:EC2/C&CAActivity.B!DNS

EC2 Instance adalah menanyakan nama domain yang dikaitkan dengan perintah dan server kontrol yang dikenal.

Tingkat keparahan default: Tinggi

- Sumber data: log DNS

Temuan ini menginformasikan bahwa instans yang tercantum dalam lingkungan AWS Anda menanyakan nama domain yang terkait dengan server perintah dan kontrol (C&C) yang dikenal. Instans yang tercantum mungkin disusupi. Server perintah dan kontrol adalah komputer yang mengeluarkan perintah untuk anggota botnet.

Botnet adalah kumpulan perangkat yang terhubung ke internet yang mungkin termasuk PCs, server, perangkat seluler, dan perangkat Internet of Things, yang terinfeksi dan dikendalikan oleh jenis malware yang umum. Botnet sering digunakan untuk mendistribusikan malware dan mengumpulkan informasi yang disalahgunakan, seperti nomor kartu kredit. Tergantung pada tujuan dan struktur botnet, server C&C mungkin juga mengeluarkan perintah untuk memulai serangan penolakan layanan (DDoS) terdistribusi.

 Note

Jika nama domain yang ditanyakan terkait log4j, maka bidang temuan terkait akan mencakup nilai-nilai berikut:

- `Service.additionalInfo.threatListName` = Amazon
- `Service.additionalInfo.ThreatName` = Log4j Terkait

 Note

Untuk menguji bagaimana GuardDuty menghasilkan jenis temuan ini, Anda dapat membuat permintaan DNS dari instance Anda (menggunakan `dig` untuk Linux atau `nslookup` untuk Windows) terhadap domain `guarddutyactivityb.com` pengujian.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, instans Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memperbaiki instans Amazon yang berpotensi dikompromikan EC2](#).

Backdoor:EC2/DenialOfService.Dns

Sebuah EC2 instance berperilaku dengan cara yang mungkin mengindikasikan sedang digunakan untuk melakukan serangan Denial of Service (DoS) menggunakan protokol DNS.

Tingkat keparahan default: Tinggi

- Sumber data: log alur VPC

Temuan ini memberi tahu Anda bahwa EC2 instance yang tercantum dalam AWS lingkungan Anda menghasilkan volume besar lalu lintas DNS keluar. Ini mungkin menunjukkan bahwa instance yang terdaftar dikompromikan dan digunakan untuk melakukan serangan denial-of-service (DoS) menggunakan protokol DNS.

Note

Temuan ini mendeteksi serangan DoS hanya terhadap alamat IP yang dapat dirutekan secara publik, yang merupakan target utama dari serangan DoS.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, instans Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memperbaiki instans Amazon yang berpotensi dikompromikan EC2](#).

Backdoor:EC2/DenialOfService.Tcp

Sebuah EC2 instance berperilaku dengan cara yang menunjukkan sedang digunakan untuk melakukan serangan Denial of Service (DoS) menggunakan protokol TCP.

Tingkat keparahan default: Tinggi

- Sumber data: log alur VPC

Temuan ini memberi tahu Anda bahwa EC2 instance yang tercantum dalam AWS lingkungan Anda menghasilkan volume besar lalu lintas TCP keluar. Ini mungkin menunjukkan bahwa instance dikompromikan dan digunakan untuk melakukan serangan denial-of-service (DoS) menggunakan protokol TCP.

Note

Temuan ini mendeteksi serangan DoS hanya terhadap alamat IP yang dapat dirutekan secara publik, yang merupakan target utama dari serangan DoS.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, instans Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memperbaiki instans Amazon yang berpotensi dikompromikan EC2](#).

Backdoor:EC2/DenialOfService.Udp

Sebuah EC2 instance berperilaku dengan cara yang menunjukkan sedang digunakan untuk melakukan serangan Denial of Service (DoS) menggunakan protokol UDP.

Tingkat keparahan default: Tinggi

- Sumber data: log alur VPC

Temuan ini memberi tahu Anda bahwa EC2 instance yang tercantum dalam AWS lingkungan Anda menghasilkan volume besar lalu lintas UDP keluar. Ini mungkin menunjukkan bahwa instance yang terdaftar dikompromikan dan digunakan untuk melakukan serangan denial-of-service (DoS) menggunakan protokol UDP.

Note

Temuan ini mendeteksi serangan DoS hanya terhadap alamat IP yang dapat dirutekan secara publik, yang merupakan target utama dari serangan DoS.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, instans Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memperbaiki instans Amazon yang berpotensi dikompromikan EC2](#).

Backdoor:EC2/DenialOfService.UdpOnTcpPorts

Sebuah EC2 instance berperilaku dengan cara yang mungkin mengindikasikan sedang digunakan untuk melakukan serangan Denial of Service (DoS) menggunakan protokol UDP pada port TCP.

Tingkat keparahan default: Tinggi

- Sumber data: log alur VPC

Temuan ini memberi tahu Anda bahwa EC2 instance yang tercantum dalam AWS lingkungan Anda menghasilkan volume besar lalu lintas UDP keluar yang ditargetkan ke port yang biasanya digunakan

untuk komunikasi TCP. Ini mungkin menunjukkan bahwa instance yang terdaftar dikompromikan dan digunakan untuk melakukan serangan denial-of-service (DoS) menggunakan protokol UDP pada port TCP.

 Note

Temuan ini mendeteksi serangan DoS hanya terhadap alamat IP yang dapat dirutekan secara publik, yang merupakan target utama dari serangan DoS.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, instans Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memperbaiki instans Amazon yang berpotensi dikompromikan EC2](#).

Backdoor:EC2/DenialOfService.UnusualProtocol

Sebuah EC2 instance berperilaku dengan cara yang mungkin mengindikasikan sedang digunakan untuk melakukan serangan Denial of Service (DoS) menggunakan protokol yang tidak biasa.

Tingkat keparahan default: Tinggi

- Sumber data: log alur VPC

Temuan ini memberi tahu Anda bahwa EC2 instance yang terdaftar di AWS lingkungan Anda menghasilkan volume besar lalu lintas keluar dari jenis protokol yang tidak biasa yang biasanya tidak digunakan oleh EC2 instance, seperti Internet Group Management Protocol. Ini mungkin menunjukkan bahwa instance dikompromikan dan sedang digunakan untuk melakukan serangan denial-of-service (DoS) menggunakan protokol yang tidak biasa. Temuan ini mendeteksi serangan DoS hanya terhadap alamat IP yang dapat dirutekan secara publik, yang merupakan target utama dari serangan DoS.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, instans Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memperbaiki instans Amazon yang berpotensi dikompromikan EC2](#).

Backdoor:EC2/Spambot

Sebuah EC2 instance menunjukkan perilaku yang tidak biasa dengan berkomunikasi dengan host jarak jauh di port 25.

Tingkat keparahan default: Sedang

- Sumber data: log alur VPC

Temuan ini memberi tahu Anda bahwa EC2 instance yang terdaftar di AWS lingkungan Anda berkomunikasi dengan host jarak jauh di port 25. Perilaku ini tidak biasa karena EC2 instance ini tidak memiliki riwayat komunikasi sebelumnya di port 25. Port 25 umumnya digunakan oleh server e-mail untuk komunikasi SMTP. Temuan ini menunjukkan EC2 instans Anda mungkin dikompromikan untuk digunakan dalam mengirimkan spam.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, instans Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memperbaiki instans Amazon yang berpotensi dikompromikan EC2](#).

Behavior:EC2/NetworkPortUnusual

Sebuah EC2 instance berkomunikasi dengan host jarak jauh pada port server yang tidak biasa.

Tingkat keparahan default: Sedang

- Sumber data: log alur VPC

Temuan ini memberi tahu Anda bahwa EC2 contoh yang tercantum di AWS lingkungan Anda berperilaku dengan cara yang menyimpang dari garis dasar yang ditetapkan. EC2 Instance ini tidak memiliki riwayat komunikasi sebelumnya di port jarak jauh ini.

Note

Jika EC2 instance dikomunikasikan pada port 389 atau port 1389, maka tingkat keparahan temuan terkait akan dimodifikasi menjadi Tinggi, dan bidang temuan akan mencakup nilai berikut:

- `Service.additionAlinfo.Context` = Kemungkinan panggilan balik log4j

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, instans Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memperbaiki instans Amazon yang berpotensi dikompromikan EC2](#).

Behavior:EC2/TrafficVolumeUnusual

Sebuah EC2 instance menghasilkan jumlah lalu lintas jaringan yang luar biasa besar ke host jarak jauh.

Tingkat keparahan default: Sedang

- Sumber data: log alur VPC

Temuan ini memberi tahu Anda bahwa EC2 contoh yang tercantum di AWS lingkungan Anda berperilaku dengan cara yang menyimpang dari garis dasar yang ditetapkan. EC2 Instance ini tidak memiliki riwayat sebelumnya dalam mengirimkan lalu lintas sebanyak ini ke host jarak jauh ini.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, instans Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memperbaiki instans Amazon yang berpotensi dikompromikan EC2](#).

CryptoCurrency:EC2/BitcoinTool.B

EC2 Instance adalah menanyakan alamat IP yang terkait dengan aktivitas terkait cryptocurrency.

Tingkat keparahan default: Tinggi

- Sumber data: log alur VPC

Temuan ini memberi tahu Anda bahwa EC2 instance yang terdaftar di AWS lingkungan Anda menanyakan Alamat IP yang terkait dengan Bitcoin atau aktivitas terkait cryptocurrency lainnya.

Bitcoin adalah cryptocurrency di seluruh dunia dan sistem pembayaran digital yang dapat ditukar dengan mata uang, produk, dan layanan lainnya. Bitcoin adalah hadiah untuk penambangan bitcoin dan sangat dicari oleh para pelaku ancaman.

Rekomendasi remediasi:

Jika Anda menggunakan EC2 instance ini untuk menambang atau mengelola cryptocurrency, atau instance ini terlibat dalam aktivitas blockchain, temuan ini dapat menjadi aktivitas yang diharapkan untuk lingkungan Anda. Jika hal ini dilakukan di lingkungan AWS Anda, kami menyarankan Anda untuk menetapkan aturan penekanan untuk temuan ini. Aturan penekanan harus terdiri dari dua kriteria filter. Kriteria pertama harus menggunakan atribut Tipe temuan dengan nilai `CryptoCurrency:EC2/BitcoinTool.B`. Kriteria filter kedua harus menggunakan ID Instans dari instans yang terlibat dalam aktivitas blockchain. Untuk mempelajari selengkapnya tentang cara membuat aturan penekanan, lihat [Aturan penindasan di GuardDuty](#).

Jika aktivitas ini tidak terduga, instans Anda kemungkinan disusupi, lihat [Memperbaiki instans Amazon yang berpotensi dikompromikan EC2](#).

CryptoCurrency:EC2/BitcoinTool.B!DNS

EC2 Instance adalah menanyakan nama domain yang terkait dengan aktivitas terkait cryptocurrency.

Tingkat keparahan default: Tinggi

- Sumber data: log DNS

Temuan ini memberi tahu Anda bahwa EC2 instance yang terdaftar di AWS lingkungan Anda menanyakan nama domain yang terkait dengan Bitcoin atau aktivitas terkait cryptocurrency lainnya. Bitcoin adalah cryptocurrency di seluruh dunia dan sistem pembayaran digital yang dapat ditukar dengan mata uang, produk, dan layanan lainnya. Bitcoin adalah hadiah untuk penambangan bitcoin dan sangat dicari oleh para pelaku ancaman.

Rekomendasi remediasi:

Jika Anda menggunakan EC2 instance ini untuk menambang atau mengelola cryptocurrency, atau instance ini terlibat dalam aktivitas blockchain, temuan ini dapat menjadi aktivitas yang diharapkan untuk lingkungan Anda. Jika hal ini dilakukan di lingkungan AWS Anda, kami menyarankan

Anda untuk menetapkan aturan penekanan untuk temuan ini. Aturan penekanan harus terdiri dari dua kriteria filter. Kriteria pertama harus menggunakan atribut Tipe temuan dengan nilai `CryptoCurrency:EC2/BitcoinTool.B!DNS`. Kriteria filter kedua harus menggunakan ID Instans dari instans yang terlibat dalam aktivitas blockchain. Untuk mempelajari selengkapnya tentang cara membuat aturan penekanan, lihat [Aturan penindasan di GuardDuty](#).

Jika aktivitas ini tidak terduga, instans Anda kemungkinan disusupi, lihat [Memperbaiki instans Amazon yang berpotensi dikompromikan EC2](#).

DefenseEvasion:EC2/UnusualDNSResolver

EC2Instans Amazon berkomunikasi dengan resolver DNS publik yang tidak biasa.

Tingkat keparahan default: Sedang

- Sumber data: log alur VPC

Temuan ini memberi tahu Anda bahwa EC2 instans Amazon yang terdaftar di AWS lingkungan Anda berperilaku dengan cara yang menyimpang dari perilaku dasar. EC2 Instance ini tidak memiliki riwayat komunikasi terbaru dengan resolver DNS publik ini. Bidang yang tidak biasa di panel detail pencarian di GuardDuty konsol dapat memberikan informasi tentang penyelesai DNS yang ditanyakan.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, instans Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memperbaiki instans Amazon yang berpotensi dikompromikan EC2](#).

DefenseEvasion:EC2/UnusualDoHActivity

EC2 Instans Amazon melakukan DNS yang tidak biasa melalui komunikasi HTTPS (DoH).

Tingkat keparahan default: Sedang

- Sumber data: log alur VPC

Temuan ini memberi tahu Anda bahwa EC2 instans Amazon yang terdaftar di AWS lingkungan Anda berperilaku dengan cara yang menyimpang dari garis dasar yang ditetapkan. EC2 Instance ini tidak memiliki riwayat DNS terbaru melalui komunikasi HTTPS (DoH) dengan server DoH publik ini. Bidang yang tidak biasa dalam rincian temuan dapat memberikan informasi tentang server DoH yang ditanyakan.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, instans Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memperbaiki instans Amazon yang berpotensi dikompromikan EC2](#).

DefenseEvasion:EC2/UnusualDoTActivity

EC2Instans Amazon melakukan komunikasi DNS yang tidak biasa melalui TLS (DoT).

Tingkat keparahan default: Sedang

- Sumber data: log alur VPC

Temuan ini memberi tahu Anda bahwa EC2 contoh yang tercantum di AWS lingkungan Anda berperilaku dengan cara yang menyimpang dari garis dasar yang ditetapkan. EC2 Instance ini tidak memiliki riwayat terbaru DNS melalui komunikasi TLS (DoT) dengan server DoT publik ini. Bidang yang tidak biasa di panel rincian temuan dapat memberikan informasi tentang server DoT yang ditanyakan.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, instans Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memperbaiki instans Amazon yang berpotensi dikompromikan EC2](#).

Impact:EC2/AbusedDomainRequest.Reputation

EC2Instance adalah menanyakan nama domain dengan reputasi rendah yang dikaitkan dengan domain yang disalahgunakan yang diketahui.

Tingkat keparahan default: Sedang

- Sumber data: log DNS

Temuan ini memberi tahu Anda bahwa EC2 instans Amazon yang terdaftar di AWS lingkungan Anda menanyakan nama domain dengan reputasi rendah yang terkait dengan domain atau alamat IP yang disalahgunakan yang diketahui. Contoh domain yang disalahgunakan adalah nama domain tingkat atas (TLDs) dan nama domain tingkat kedua (2LDs) yang menyediakan pendaftaran subdomain gratis serta penyedia DNS dinamis. Aktor ancaman cenderung menggunakan layanan ini untuk mendaftarkan domain secara gratis atau dengan biaya rendah. Domain bereputasi rendah dalam kategori ini mungkin juga merupakan domain kedaluwarsa yang mencari alamat IP parkir registrar dan oleh karena itu mungkin tidak lagi aktif. IP parkir adalah tempat registrar mengarahkan lalu lintas untuk domain yang belum ditautkan ke layanan apa pun. EC2 Instans Amazon yang terdaftar dapat dikompromikan karena pelaku ancaman biasanya menggunakan registrar atau layanan ini untuk distribusi C&C dan malware.

Domain reputasi rendah didasarkan pada model skor reputasi. Model ini mengevaluasi dan memberi peringkat karakteristik domain untuk menentukan kemungkinannya berbahaya.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, instans Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memperbaiki instans Amazon yang berpotensi dikompromikan EC2](#).

Impact:EC2/BitcoinDomainRequest.Reputation

Sebuah EC2 instance menanyakan nama domain dengan reputasi rendah yang terkait dengan aktivitas terkait cryptocurrency.

Tingkat keparahan default: Tinggi

- Sumber data: log DNS

Temuan ini memberi tahu Anda bahwa EC2 instans Amazon yang terdaftar di AWS lingkungan Anda menanyakan nama domain dengan reputasi rendah yang terkait dengan Bitcoin atau aktivitas terkait cryptocurrency lainnya. Bitcoin adalah cryptocurrency di seluruh dunia dan sistem pembayaran digital yang dapat ditukar dengan mata uang, produk, dan layanan lainnya. Bitcoin adalah hadiah untuk penambangan bitcoin dan sangat dicari oleh para pelaku ancaman.

Domain reputasi rendah didasarkan pada model skor reputasi. Model ini mengevaluasi dan memberi peringkat karakteristik domain untuk menentukan kemungkinannya berbahaya.

Rekomendasi remediasi:

Jika Anda menggunakan EC2 instance ini untuk menambang atau mengelola cryptocurrency, atau instance ini terlibat dalam aktivitas blockchain, temuan ini dapat mewakili aktivitas yang diharapkan untuk lingkungan Anda. Jika hal ini dilakukan di lingkungan AWS Anda, kami menyarankan Anda untuk menetapkan aturan penekanan untuk temuan ini. Aturan penekanan harus terdiri dari dua kriteria filter. Kriteria pertama harus menggunakan atribut Tipe temuan dengan nilai `Impact:EC2/BitcoinDomainRequest.Reputation`. Kriteria filter kedua harus menggunakan ID Instans dari instans yang terlibat dalam aktivitas blockchain. Untuk mempelajari selengkapnya tentang cara membuat aturan penekanan, lihat [Aturan penindasan di GuardDuty](#).

Jika aktivitas ini tidak terduga, instans Anda kemungkinan disusupi, lihat [Memperbaiki instans Amazon yang berpotensi dikompromikan EC2](#).

Impact:EC2/MaliciousDomainRequest.Reputation

Sebuah EC2 instans menanyakan domain dengan reputasi rendah yang dikaitkan dengan domain berbahaya yang diketahui.

Tingkat keparahan default: Tinggi

- Sumber data: log DNS

Temuan ini memberi tahu Anda bahwa EC2 instans Amazon yang terdaftar di AWS lingkungan Anda menanyakan nama domain dengan reputasi rendah yang terkait dengan domain berbahaya atau alamat IP yang diketahui. Misalnya, domain dapat dikaitkan dengan alamat IP sinkhole yang dikenal. Domain sinkhole adalah domain yang sebelumnya dikendalikan oleh aktor ancaman, dan permintaan yang dibuat untuk domain tersebut dapat menunjukkan bahwa instans disusupi. Domain ini juga dapat dikorelasikan dengan kampanye berbahaya atau algoritme pembuatan domain yang dikenal.

Domain reputasi rendah didasarkan pada model skor reputasi. Model ini mengevaluasi dan memberi peringkat karakteristik domain untuk menentukan kemungkinannya berbahaya.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, instans Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memperbaiki instans Amazon yang berpotensi dikompromikan EC2](#).

Impact:EC2/PortSweep

Sebuah EC2 instance sedang menyelidiki port pada sejumlah besar alamat IP.

Tingkat keparahan default: Tinggi

- Sumber data: log alur VPC

Temuan ini memberi tahu Anda bahwa EC2 instance yang terdaftar di AWS lingkungan Anda sedang menyelidiki port pada sejumlah besar alamat IP yang dapat dirutekan secara publik. Tipe aktivitas ini biasanya digunakan untuk menemukan host yang rentan untuk dieksploitasi. Di panel detail pencarian di GuardDuty konsol Anda, hanya alamat IP jarak jauh terbaru yang ditampilkan

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, instans Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memperbaiki instans Amazon yang berpotensi dikompromikan EC2](#).

Impact:EC2/SuspiciousDomainRequest.Reputation

Sebuah EC2 contoh adalah menanyakan nama domain dengan reputasi rendah yang mencurigakan karena usianya, atau popularitasnya yang rendah.

Tingkat keparahan default: Rendah

- Sumber data: log DNS

Temuan ini memberi tahu Anda bahwa EC2 instans Amazon yang terdaftar di AWS lingkungan Anda menanyakan nama domain dengan reputasi rendah yang diduga jahat. memperhatikan karakteristik domain ini yang konsisten dengan domain berbahaya yang diamati sebelumnya, namun, model reputasi kami tidak dapat secara definitif menghubungkannya dengan ancaman yang diketahui. Domain ini biasanya baru diamati atau menerima jumlah lalu lintas yang rendah.

Domain reputasi rendah didasarkan pada model skor reputasi. Model ini mengevaluasi dan memberi peringkat karakteristik domain untuk menentukan kemungkinannya berbahaya.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, instans Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memperbaiki instans Amazon yang berpotensi dikompromikan EC2](#).

Impact:EC2/WinRMBruteForce

Sebuah EC2 instance melakukan serangan brute force Windows Remote Management keluar.

Tingkat keparahan default: Rendah*

Note

Tingkat keparahan temuan ini rendah jika EC2 contoh Anda adalah target serangan brute force. Tingkat keparahan temuan ini tinggi jika EC2 contoh Anda adalah aktor yang digunakan untuk melakukan serangan brute force.

- Sumber data: log alur VPC

Temuan ini memberi tahu Anda bahwa EC2 instance yang terdaftar di AWS lingkungan Anda melakukan serangan brute force Windows Remote Management (WinRM) yang bertujuan untuk mendapatkan akses ke layanan Windows Remote Management pada sistem berbasis Windows.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, instans Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memperbaiki instans Amazon yang berpotensi dikompromikan EC2](#).

Recon:EC2/PortProbeEMRUnprotectedPort

Sebuah EC2 instance memiliki port terkait EMR yang tidak dilindungi yang sedang diselidiki oleh host jahat yang dikenal.

Tingkat keparahan default: Tinggi

- Sumber data: log alur VPC

Temuan ini memberi tahu Anda bahwa port sensitif terkait EMR pada instance yang EC2 terdaftar yang merupakan bagian dari cluster di lingkungan AWS Anda tidak diblokir oleh grup keamanan, daftar kontrol akses (ACL), atau firewall on-host seperti Linux. IPTables Temuan ini juga menginformasikan bahwa pemindai yang dikenal di Internet secara aktif menyelidiki port ini. Port yang dapat memicu temuan ini, seperti port 8088 (YARN Web UI port), berpotensi digunakan untuk eksekusi kode jarak jauh.

Rekomendasi remediasi:

Anda harus memblokir akses terbuka ke port pada klaster dari internet dan membatasi akses hanya ke alamat IP tertentu yang memerlukan akses ke port ini. Untuk informasi selengkapnya, lihat [Grup Keamanan untuk Klaster EMR](#).

Recon:EC2/PortProbeUnprotectedPort

Sebuah EC2 instance memiliki port yang tidak dilindungi yang sedang diselidiki oleh host jahat yang dikenal.

Tingkat keparahan default: Rendah*

Note

Tingkat kepelikan default temuan ini Rendah. Namun, jika port yang sedang diselidiki, digunakan oleh Elasticsearch (9200 atau 9300), tingkat keparahan temuannya Tinggi.

- Sumber data: log alur VPC

Temuan ini memberi tahu Anda bahwa port pada EC2 instance yang terdaftar di AWS lingkungan Anda tidak diblokir oleh grup keamanan, daftar kontrol akses (ACL), atau firewall on-host seperti Linux IPTables, dan pemindai yang dikenal di internet secara aktif menyelidikinya.

Jika port tidak terlindungi yang teridentifikasi adalah 22 atau 3389 dan Anda menggunakan port ini agar terhubung ke instans Anda, Anda masih dapat membatasi eksposur dengan mengizinkan akses ke port ini hanya untuk alamat IP dari ruang alamat IP jaringan perusahaan Anda. Untuk membatasi akses ke port 22 di Linux, lihat [Otorisasi Lalu Lintas Masuk untuk Instans Linux Anda](#).

Untuk membatasi akses ke port 3389 pada Windows, lihat [Otorisasi Lalu Lintas Masuk untuk Instans Windows Anda](#).

GuardDuty tidak menghasilkan temuan ini untuk port 443 dan 80.

Rekomendasi remediasi:

Mungkin terdapat kasus ketika instans sengaja diekspos, misalnya ketika instans menghosting server web. Jika ini terjadi di AWS lingkungan Anda, kami sarankan Anda membuat aturan penindasan untuk temuan ini. Aturan penekanan harus terdiri dari dua kriteria filter. Kriteria pertama harus menggunakan atribut Tipe temuan dengan nilai `Recon:EC2/PortProbeUnprotectedPort`. Kriteria filter kedua harus sesuai dengan instans yang berfungsi sebagai host bastion. Anda dapat menggunakan atribut ID gambar Instans atau atribut nilai Tanda, tergantung kriteria yang diidentifikasi dengan instans yang menghosting alat ini. Untuk informasi selengkapnya tentang cara membuat aturan penekanan, lihat [Aturan penindasan di GuardDuty](#).

Jika aktivitas ini tidak terduga, instans Anda kemungkinan disusupi, lihat [Memperbaiki instans Amazon yang berpotensi dikompromikan EC2](#).

Recon:EC2/Portscan

Sebuah EC2 instance melakukan pemindaian port keluar ke host jarak jauh.

Tingkat keparahan default: Sedang

- Sumber data: log alur VPC

Temuan ini memberi tahu Anda bahwa EC2 instance yang terdaftar di AWS lingkungan Anda terlibat dalam kemungkinan serangan pemindaian port karena mencoba terhubung ke beberapa port dalam waktu singkat. Tujuan serangan pemindaian port adalah untuk menemukan port terbuka guna menemukan layanan mana yang dijalankan mesin dan untuk mengidentifikasi sistem operasinya.

Rekomendasi remediasi:

Temuan ini bisa menjadi positif palsu ketika aplikasi penilaian kerentanan diterapkan pada EC2 instance di lingkungan Anda karena aplikasi ini melakukan pemindaian port untuk mengingatkan Anda tentang port terbuka yang salah konfigurasi. Jika ini terjadi di AWS lingkungan Anda, kami sarankan Anda membuat aturan penindasan untuk temuan ini. Aturan penekanan harus terdiri dari dua kriteria filter. Kriteria pertama harus menggunakan atribut Tipe temuan dengan nilai `Recon:EC2/`

Portscan. Kriteria filter kedua harus sesuai dengan instans yang menghosting alat penilaian kerentanan ini. Anda dapat menggunakan atribut ID gambar Instans atau atribut nilai Tanda, tergantung kriteria yang diidentifikasi dengan instans yang menghosting alat ini. Untuk informasi selengkapnya tentang cara membuat aturan penekanan, lihat [Aturan penindasan di GuardDuty](#).

Jika aktivitas ini tidak terduga, instans Anda kemungkinan disusupi, lihat [Memperbaiki instans Amazon yang berpotensi dikompromikan EC2](#).

Trojan:EC2/BlackholeTraffic

Sebuah EC2 contoh mencoba berkomunikasi dengan alamat IP dari host jarak jauh yang merupakan lubang hitam yang dikenal.

Tingkat keparahan default: Sedang

- Sumber data: log alur VPC

Temuan ini memberi tahu Anda bahwa EC2 instance yang terdaftar di AWS lingkungan Anda mungkin terganggu karena mencoba berkomunikasi dengan alamat IP lubang hitam (atau lubang wastafel). Lubang hitam adalah tempat di jaringan di mana lalu lintas masuk atau keluar dibuang secara diam-diam tanpa memberi tahu sumber bahwa data tidak mencapai penerima yang dituju. Alamat IP lubang hitam menentukan mesin host yang tidak berjalan atau alamat yang tidak ada host yang ditugaskan.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, instans Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memperbaiki instans Amazon yang berpotensi dikompromikan EC2](#).

Trojan:EC2/BlackholeTraffic!DNS

Sebuah EC2 instance menanyakan nama domain yang sedang dialihkan ke alamat IP lubang hitam.

Tingkat keparahan default: Sedang

- Sumber data: log DNS

Temuan ini memberi tahu Anda bahwa EC2 instance yang terdaftar di AWS lingkungan Anda mungkin terganggu karena menanyakan nama domain yang sedang dialihkan ke alamat IP lubang hitam. Lubang hitam adalah tempat di jaringan di mana lalu lintas masuk atau keluar dibuang secara diam-diam tanpa memberi tahu sumber bahwa data tidak mencapai penerima yang dituju.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, instans Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memperbaiki instans Amazon yang berpotensi dikompromikan EC2](#).

Trojan:EC2/DGADomainRequest.B

Sebuah EC2 instance menanyakan domain yang dihasilkan secara algoritmik. Domain semacam itu biasanya digunakan oleh malware dan bisa menjadi indikasi contoh yang dikompromikan EC2 .

Tingkat keparahan default: Tinggi

- Sumber data: log DNS

Temuan ini memberi tahu Anda bahwa EC2 instance yang terdaftar di AWS lingkungan Anda mencoba menanyakan domain algoritme pembuatan domain (DGA). EC2 Contoh Anda mungkin dikompromikan.

DGAs digunakan untuk secara berkala menghasilkan sejumlah besar nama domain yang dapat digunakan sebagai titik pertemuan dengan server perintah dan kontrol (C&C) mereka. Server perintah dan kontrol adalah komputer yang mengeluarkan perintah kepada anggota botnet, yang merupakan kumpulan perangkat yang terhubung ke internet yang terinfeksi dan dikendalikan oleh tipe malware yang umum. Banyaknya kemungkinan titik pertemuan menyulitkan untuk mematikan botnet secara efektif karena komputer yang terinfeksi berusaha menghubungi beberapa nama domain ini setiap hari untuk menerima pembaruan atau perintah.

Note

Temuan ini didasarkan pada analisis nama domain menggunakan heuristik lanjutan dan dapat mengidentifikasi domain DGA baru yang tidak terdapat dalam umpan intelijen ancaman.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, instans Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memperbaiki instans Amazon yang berpotensi dikompromikan EC2](#).

Trojan:EC2/DGADomainRequest.C!DNS

Sebuah EC2 instance menanyakan domain yang dihasilkan secara algoritmik. Domain semacam itu biasanya digunakan oleh malware dan bisa menjadi indikasi contoh yang dikompromikan EC2 .

Tingkat keparahan default: Tinggi

- Sumber data: log DNS

Temuan ini memberi tahu Anda bahwa EC2 instance yang terdaftar di AWS lingkungan Anda mencoba menanyakan domain algoritme pembuatan domain (DGA). EC2 Contoh Anda mungkin dikompromikan.

DGAs digunakan untuk secara berkala menghasilkan sejumlah besar nama domain yang dapat digunakan sebagai titik pertemuan dengan server perintah dan kontrol (C&C) mereka. Server perintah dan kontrol adalah komputer yang mengeluarkan perintah kepada anggota botnet, yang merupakan kumpulan perangkat yang terhubung ke internet yang terinfeksi dan dikendalikan oleh tipe malware yang umum. Banyaknya kemungkinan titik pertemuan menyulitkan untuk mematikan botnet secara efektif karena komputer yang terinfeksi berusaha menghubungi beberapa nama domain ini setiap hari untuk menerima pembaruan atau perintah.

Note

Temuan ini didasarkan pada domain DGA yang diketahui dari GuardDuty umpan intelijen ancaman.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, instans Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memperbaiki instans Amazon yang berpotensi dikompromikan EC2](#).

Trojan:EC2/DNSDataExfiltration

Sebuah EC2 instance mengekstraksi data melalui kueri DNS.

Tingkat keparahan default: Tinggi

- Sumber data: log DNS

Temuan ini memberi tahu Anda bahwa EC2 instance yang terdaftar di AWS lingkungan Anda menjalankan malware yang menggunakan kueri DNS untuk transfer data keluar. Tipe transfer data ini merupakan indikasi dari instans yang disusupi dan dapat mengakibatkan eksfiltrasi data. Lalu lintas DNS biasanya tidak diblokir oleh firewall. Misalnya, malware dalam EC2 contoh yang dikompromikan dapat menyandikan data, (seperti nomor kartu kredit Anda), ke dalam kueri DNS dan mengirimkannya ke server DNS jarak jauh yang dikendalikan oleh penyerang.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, instans Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memperbaiki instans Amazon yang berpotensi dikompromikan EC2](#).

Trojan:EC2/DriveBySourceTraffic!DNS

EC2 Instance adalah menanyakan nama domain dari host jarak jauh yang merupakan sumber serangan unduhan Drive-By yang dikenal.

Tingkat keparahan default: Tinggi

- Sumber data: log DNS

Temuan ini memberi tahu Anda bahwa EC2 instance yang terdaftar di AWS lingkungan Anda mungkin terganggu karena menanyakan nama domain host jarak jauh yang merupakan sumber serangan unduhan drive-by yang diketahui. Ini merupakan unduhan perangkat lunak komputer yang tidak diinginkan dari internet yang dapat memicu penginstalan virus, spyware, atau malware secara otomatis.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, instans Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memperbaiki instans Amazon yang berpotensi dikompromikan EC2](#).

Trojan:EC2/DropPoint

Sebuah EC2 contoh mencoba untuk berkomunikasi dengan alamat IP dari host jarak jauh yang diketahui memiliki kredensial dan data curian lainnya yang ditangkap oleh malware.

Tingkat keparahan default: Sedang

- Sumber data: log alur VPC

Temuan ini memberi tahu Anda bahwa sebuah EC2 instance di AWS lingkungan Anda mencoba berkomunikasi dengan alamat IP host jarak jauh yang diketahui memiliki kredensial dan data curian lainnya yang ditangkap oleh malware.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, instans Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memperbaiki instans Amazon yang berpotensi dikompromikan EC2](#).

Trojan:EC2/DropPoint!DNS

EC2 Instance adalah menanyakan nama domain dari host jarak jauh yang diketahui memiliki kredensial dan data curian lainnya yang ditangkap oleh malware.

Tingkat keparahan default: Sedang

- Sumber data: log DNS

Temuan ini memberi tahu Anda bahwa sebuah EC2 instance di AWS lingkungan Anda menanyakan nama domain dari host jarak jauh yang diketahui memiliki kredensial dan data curian lainnya yang ditangkap oleh malware.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, instans Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memperbaiki instans Amazon yang berpotensi dikompromikan EC2](#).

Trojan:EC2/PhishingDomainRequest!DNS

EC2 Instance adalah menanyakan domain yang terlibat dalam serangan phishing. EC2 Contoh Anda mungkin dikompromikan.

Tingkat keparahan default: Tinggi

- Sumber data: log DNS

Temuan ini memberi tahu Anda bahwa ada EC2 instance di AWS lingkungan Anda yang mencoba menanyakan domain yang terlibat dalam serangan phishing. Domain phishing dibuat oleh seseorang yang menyamar sebagai institusi yang sah untuk membujuk individu agar memberikan data sensitif, seperti informasi pengenalan pribadi, detail kartu kredit dan perbankan, serta kata sandi. EC2 Instans Anda mungkin mencoba mengambil data sensitif yang disimpan di situs web phishing, atau mungkin mencoba menyiapkan situs web phishing. EC2 Contoh Anda mungkin dikompromikan.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, instans Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memperbaiki instans Amazon yang berpotensi dikompromikan EC2](#).

UnauthorizedAccess:EC2/MaliciousIPCaller.Custom

Sebuah EC2 instans membuat koneksi ke alamat IP pada daftar ancaman khusus.

Tingkat keparahan default: Sedang

- Sumber data: log alur VPC

Temuan ini memberi tahu Anda bahwa sebuah EC2 instance di AWS lingkungan Anda berkomunikasi dengan alamat IP yang disertakan dalam daftar ancaman yang Anda unggah. Dalam GuardDuty, daftar ancaman terdiri dari alamat IP berbahaya yang diketahui. GuardDuty menghasilkan temuan berdasarkan daftar ancaman yang diunggah. Daftar ancaman yang digunakan untuk menghasilkan temuan ini akan tercantum dalam detail temuan.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, instans Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memperbaiki instans Amazon yang berpotensi dikompromikan EC2](#).

UnauthorizedAccess:EC2/MetadataDNSRebind

EC2Instance melakukan pencarian DNS yang menyelesaikan layanan metadata instance.

Tingkat keparahan default: Tinggi

- Sumber data: log DNS

Temuan ini memberi tahu Anda bahwa EC2 instance di AWS lingkungan Anda menanyakan domain yang menyelesaikan alamat IP EC2 metadata (169.254.169.254). Kueri DNS semacam ini dapat menunjukkan bahwa instans adalah target dari teknik rebinding DNS. Teknik ini dapat digunakan untuk mendapatkan metadata dari sebuah EC2 instance, termasuk kredensial IAM yang terkait dengan instance.

DNS rebinding melibatkan menipu aplikasi yang berjalan pada EC2 instance untuk memuat data yang dikembalikan dari URL, di mana nama domain di URL menyelesaikan ke alamat IP EC2 metadata (169.254.169.254). Ini menyebabkan aplikasi mengakses EC2 metadata dan mungkin membuatnya tersedia untuk penyerang.

Dimungkinkan untuk mengakses EC2 metadata menggunakan DNS rebinding hanya jika EC2 instance menjalankan aplikasi rentan yang memungkinkan injeksi URLs, atau jika seseorang mengakses URL di browser web yang berjalan pada instance. EC2

Rekomendasi remediasi:

Menanggapi temuan ini, Anda harus mengevaluasi apakah ada aplikasi rentan yang berjalan pada EC2 instance, atau jika seseorang menggunakan browser untuk mengakses domain yang diidentifikasi dalam temuan. Jika akar penyebabnya adalah aplikasi yang rentan, Anda harus memperbaiki kerentanannya. Jika seseorang menjelajahi domain yang diidentifikasi, Anda harus memblokir domain atau mencegah pengguna mengaksesnya. Jika Anda menentukan temuan ini terkait dengan kedua kasus di atas, [cabut sesi yang terkait dengan instance](#). EC2

Beberapa AWS pelanggan sengaja memetakan alamat IP metadata ke nama domain di server DNS otoritatif mereka. Jika hal ini dilakukan di lingkungan Anda, kami menyarankan Anda untuk

membuat aturan penekanan untuk temuan ini. Aturan penekanan harus terdiri dari dua kriteria filter. Kriteria pertama harus menggunakan atribut Tipe temuan dengan nilai `UnauthorizedAccess:EC2/MetaDataDNSRebind`. Kriteria filter kedua harus menggunakan Domain permintaan DNS dan nilainya harus sesuai dengan domain yang telah Anda petakan ke alamat IP (169.254.169.254) metadata. Untuk informasi selengkapnya tentang cara membuat aturan penekanan, lihat [Aturan penindasan di GuardDuty](#).

UnauthorizedAccess:EC2/RDPBruteForce

Sebuah EC2 contoh telah terlibat dalam serangan brute force RDP.

Tingkat keparahan default: Rendah*

Note

Tingkat keparahan temuan ini rendah jika EC2 contoh Anda adalah target serangan brute force. Tingkat keparahan temuan ini tinggi jika EC2 contoh Anda adalah aktor yang digunakan untuk melakukan serangan brute force.

- Sumber data: log alur VPC

Temuan ini memberi tahu Anda bahwa sebuah EC2 instance di AWS lingkungan Anda terlibat dalam serangan brute force yang bertujuan mendapatkan kata sandi untuk layanan RDP pada sistem berbasis Windows. Hal ini dapat mengindikasikan akses yang tidak sah ke sumber daya AWS Anda.

Rekomendasi remediasi:

Jika Peran Sumber Daya instans Anda adalah ACTOR, hal ini mengindikasikan bahwa instans Anda telah digunakan untuk melakukan serangan brute force RDP. Kecuali instans ini memiliki alasan yang sah untuk menghubungi alamat IP yang terdaftar sebagai Target, Anda disarankan untuk menganggap bahwa instans Anda telah disusupi dan mengambil tindakan yang tercantum di [Memperbaiki instans Amazon yang berpotensi dikompromikan EC2](#).

Jika Peran Sumber Daya instans Anda adalah TARGET, temuan ini dapat diperbaiki dengan mengamankan port RDP Anda agar hanya dipercaya IPs melalui Grup Keamanan,, ACLs atau firewall. Untuk informasi selengkapnya, lihat [Tips untuk mengamankan EC2 instans Anda \(Linux\)](#).

UnauthorizedAccess:EC2/SSHBruteForce

Sebuah EC2 contoh telah terlibat dalam serangan brute force SSH.

Tingkat keparahan default: Rendah*

Note

Tingkat keparahan temuan ini rendah jika serangan brute force ditujukan pada salah satu EC2 contoh Anda. Tingkat keparahan temuan ini tinggi jika EC2 instance Anda digunakan untuk melakukan serangan brute force.

- Sumber data: log alur VPC

Temuan ini memberi tahu Anda bahwa sebuah EC2 instance di AWS lingkungan Anda terlibat dalam serangan brute force yang bertujuan mendapatkan kata sandi ke layanan SSH pada sistem berbasis Linux. Hal ini dapat mengindikasikan akses yang tidak sah ke sumber daya AWS Anda.

Note

Temuan ini dihasilkan hanya melalui pemantauan lalu lintas pada port 22. Jika layanan SSH Anda dikonfigurasi untuk menggunakan port lain, temuan ini tidak dihasilkan.

Rekomendasi remediasi:

Jika target upaya brute force adalah host benteng, ini mungkin mewakili perilaku yang diharapkan untuk lingkungan Anda AWS . Jika demikian, kami menyarankan Anda untuk membuat aturan penekanan untuk temuan ini. Aturan penekanan harus terdiri dari dua kriteria filter. Kriteria pertama harus menggunakan atribut Tipe temuan dengan nilai `UnauthorizedAccess:EC2/SSHBruteForce`. Kriteria filter kedua harus sesuai dengan instans yang berfungsi sebagai host bastion. Anda dapat menggunakan atribut ID gambar Instans atau atribut nilai Tanda, tergantung kriteria yang diidentifikasi dengan instans yang menghosting alat ini. Untuk informasi selengkapnya tentang cara membuat aturan penekanan, lihat [Aturan penindasan di GuardDuty](#).

Jika aktivitas ini tidak diharapkan untuk lingkungan Anda dan Peran Sumber Daya instans Anda adalah TARGET, temuan ini dapat diperbaiki dengan mengamankan port SSH Anda agar hanya dipercaya IPs melalui Grup Keamanan ACLs, atau firewall. Untuk informasi selengkapnya, lihat [Tips untuk mengamankan EC2 instans Anda \(Linux\)](#).

Jika Peran Sumber Daya instans Anda adalah ACTOR, hal ini mengindikasikan bahwa instans telah digunakan untuk melakukan serangan brute force SSH. Kecuali instans ini memiliki alasan yang sah untuk menghubungi alamat IP yang terdaftar sebagai Target, Anda disarankan untuk menganggap bahwa instans Anda telah disusupi dan mengambil tindakan yang tercantum di [Memperbaiki instans Amazon yang berpotensi dikompromikan EC2](#).

UnauthorizedAccess:EC2/TorClient

EC2 Instance Anda membuat koneksi ke Tor Guard atau node Authority.

Tingkat keparahan default: Tinggi

- Sumber data: log alur VPC

Temuan ini memberi tahu Anda bahwa sebuah EC2 instance di AWS lingkungan Anda membuat koneksi ke Tor Guard atau node Authority. Tor adalah perangkat lunak untuk memungkinkan komunikasi anonim. Node Tor Guards dan Authority bertindak sebagai gateway awal ke dalam jaringan Tor. Lalu lintas ini dapat menunjukkan bahwa EC2 instance ini telah dikompromikan dan bertindak sebagai klien di jaringan Tor. Temuan ini mungkin menunjukkan akses tidak sah ke AWS sumber daya Anda dengan maksud menyembunyikan identitas asli penyerang.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, instans Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memperbaiki instans Amazon yang berpotensi dikompromikan EC2](#).

UnauthorizedAccess:EC2/TorRelay

EC2 Instance Anda membuat koneksi ke jaringan Tor sebagai relay Tor.

Tingkat keparahan default: Tinggi

- Sumber data: log alur VPC

Temuan ini memberi tahu Anda bahwa sebuah EC2 instance di AWS lingkungan Anda membuat koneksi ke jaringan Tor dengan cara yang menunjukkan bahwa itu bertindak sebagai relay Tor. Tor adalah perangkat lunak untuk memungkinkan komunikasi anonim. Tor meningkatkan anonimitas komunikasi dengan meneruskan lalu lintas klien yang kemungkinan terlarang dari satu relay Tor ke relay lainnya.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, instans Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memperbaiki instans Amazon yang berpotensi dikompromikan EC2](#).

GuardDuty Jenis pencarian IAM

Temuan berikut ini khusus untuk entitas IAM dan access key serta selalu memiliki Tipe Sumber Daya dari AccessKey. Tingkat kepelikan dan detail temuan berbeda berdasarkan tipe temuan.

Temuan yang tercantum di sini termasuk sumber data dan model yang digunakan untuk menghasilkan tipe temuan. Untuk informasi selengkapnya, lihat [GuardDuty sumber data dasar](#).

Untuk semua temuan terkait IAM, kami menyarankan Anda memeriksa entitas yang bersangkutan dan memastikan bahwa izin mereka mengikuti praktik terbaik dengan hak istimewa yang paling sedikit. Jika aktivitas tidak terduga, kredensial mungkin disusupi. Untuk informasi tentang remediasi temuan, lihat [Memulihkan kredensi yang berpotensi dikompromikan AWS](#).

Topik

- [CredentialAccess:IAMUser/AnomalousBehavior](#)
- [DefenseEvasion:IAMUser/AnomalousBehavior](#)
- [Discovery:IAMUser/AnomalousBehavior](#)
- [Exfiltration:IAMUser/AnomalousBehavior](#)
- [Impact:IAMUser/AnomalousBehavior](#)
- [InitialAccess:IAMUser/AnomalousBehavior](#)
- [PenTest:IAMUser/KaliLinux](#)
- [PenTest:IAMUser/ParrotLinux](#)
- [PenTest:IAMUser/PentoolLinux](#)

- [Persistence:IAMUser/AnomalousBehavior](#)
- [Policy:IAMUser/RootCredentialUsage](#)
- [Policy:IAMUser/ShortTermRootCredentialUsage](#)
- [PrivilegeEscalation:IAMUser/AnomalousBehavior](#)
- [Recon:IAMUser/MaliciousIPCaller](#)
- [Recon:IAMUser/MaliciousIPCaller.Custom](#)
- [Recon:IAMUser/TorIPCaller](#)
- [Stealth:IAMUser/CloudTrailLoggingDisabled](#)
- [Stealth:IAMUser/PasswordPolicyChange](#)
- [UnauthorizedAccess:IAMUser/ConsoleLoginSuccess.B](#)
- [UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS](#)
- [UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS](#)
- [UnauthorizedAccess:IAMUser/MaliciousIPCaller](#)
- [UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom](#)
- [UnauthorizedAccess:IAMUser/TorIPCaller](#)

CredentialAccess:IAMUser/AnomalousBehavior

API yang digunakan untuk mendapatkan akses ke AWS lingkungan dipanggil dengan cara yang anomali.

Tingkat keparahan default: Sedang

- Sumber data: acara CloudTrail manajemen

Temuan ini menginformasikan bahwa terdapat permintaan API anomali yang diamati di akun Anda. Temuan ini dapat mencakup satu permintaan API atau serangkaian permintaan API terkait yang dibuat di sekitar oleh satu [identitas pengguna](#). API yang diamati umumnya berkaitan dengan tahap akses kredensial serangan ketika musuh mencoba mengumpulkan kata sandi, nama pengguna, dan access key untuk lingkungan Anda. APIs Dalam kategori ini adalah `GetPasswordData`, `GetSecretValue`, `BatchGetSecretValue`, dan `GenerateDbAuthToken`.

Permintaan API ini diidentifikasi sebagai anomali oleh GuardDuty model pembelajaran mesin deteksi anomali (ML). Model ML mengevaluasi semua permintaan API di akun Anda dan mengidentifikasi peristiwa anomali yang terkait dengan teknik yang digunakan oleh musuh. Model ML melacak berbagai faktor permintaan API, seperti, pengguna yang membuat permintaan, lokasi tempat permintaan dibuat, dan API khusus yang diminta. Detail tentang faktor-faktor permintaan API yang tidak biasa untuk identitas pengguna yang memanggil permintaan dapat ditemukan di [detail temuan](#).

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, kredensi Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memulihkan kredensi yang berpotensi dikompromikan AWS](#).

DefenseEvasion:IAMUser/AnomalousBehavior

API yang digunakan untuk menghindari tindakan defensif dipanggil dengan cara yang anomali.

Tingkat keparahan default: Sedang

- Sumber data: acara CloudTrail manajemen

Temuan ini menginformasikan bahwa terdapat permintaan API anomali yang diamati di akun Anda. Temuan ini dapat mencakup satu permintaan API atau serangkaian permintaan API terkait yang dibuat di sekitar oleh satu [identitas pengguna](#). API yang diamati umumnya dikaitkan dengan taktik penghindaran pertahanan di mana musuh mencoba menutupi jejak mereka dan menghindari deteksi. APIs dalam kategori ini biasanya menghapus, menonaktifkan, atau menghentikan operasi, seperti, DeleteFlowLogs, DisableAlarmActions, atau StopLogging.

Permintaan API ini diidentifikasi sebagai anomali oleh GuardDuty model pembelajaran mesin deteksi anomali (ML). Model ML mengevaluasi semua permintaan API di akun Anda dan mengidentifikasi peristiwa anomali yang terkait dengan teknik yang digunakan oleh musuh. Model ML melacak berbagai faktor permintaan API, seperti, pengguna yang membuat permintaan, lokasi tempat permintaan dibuat, dan API khusus yang diminta. Detail tentang faktor-faktor permintaan API yang tidak biasa untuk identitas pengguna yang memanggil permintaan dapat ditemukan di [detail temuan](#).

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, kredensi Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memulihkan kredensi yang berpotensi dikompromikan AWS](#).

Discovery:IAMUser/AnomalousBehavior

API yang biasa digunakan untuk menemukan sumber daya dipanggil dengan cara yang anomali.

Tingkat keparahan default: Rendah

- Sumber data: acara CloudTrail manajemen

Temuan ini menginformasikan bahwa terdapat permintaan API anomali yang diamati di akun Anda. Temuan ini dapat mencakup satu permintaan API atau serangkaian permintaan API terkait yang dibuat di sekitar oleh satu [identitas pengguna](#). API yang diamati umumnya dikaitkan dengan tahap penemuan serangan ketika musuh mengumpulkan informasi untuk menentukan apakah AWS lingkungan Anda rentan terhadap serangan yang lebih luas. APIs dalam kategori ini biasanya mendapatkan, mendeskripsikan, atau daftar operasi, seperti, `DescribeInstances`, `GetRolePolicy`, atau `ListAccessKeys`.

Permintaan API ini diidentifikasi sebagai anomali oleh GuardDuty model pembelajaran mesin deteksi anomali (ML). Model ML mengevaluasi semua permintaan API di akun Anda dan mengidentifikasi peristiwa anomali yang terkait dengan teknik yang digunakan oleh musuh. Model ML melacak berbagai faktor permintaan API, seperti, pengguna yang membuat permintaan, lokasi tempat permintaan dibuat, dan API khusus yang diminta. Detail tentang faktor-faktor permintaan API yang tidak biasa untuk identitas pengguna yang memanggil permintaan dapat ditemukan di [detail temuan](#).

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, kredensi Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memulihkan kredensi yang berpotensi dikompromikan AWS](#).

Exfiltration:IAMUser/AnomalousBehavior

API yang biasa digunakan untuk mengumpulkan data dari AWS lingkungan dipanggil dengan cara yang anomali.

Tingkat keparahan default: Tinggi

- Sumber data: acara CloudTrail manajemen

Temuan ini menginformasikan bahwa terdapat permintaan API anomali yang diamati di akun Anda. Temuan ini dapat mencakup satu permintaan API atau serangkaian permintaan API terkait yang dibuat di sekitar oleh satu [identitas pengguna](#). API yang diamati umumnya dikaitkan dengan taktik eksfiltrasi di mana musuh mencoba mengumpulkan data dari jaringan Anda menggunakan pengemasan dan enkripsi untuk menghindari deteksi. APIs untuk jenis temuan ini hanya operasi manajemen (bidang kontrol) dan biasanya terkait dengan S3, snapshot, dan database, seperti,,, atau. PutBucketReplication CreateSnapshot RestoreDBInstanceFromDBSnapshot

Permintaan API ini diidentifikasi sebagai anomali oleh GuardDuty model pembelajaran mesin deteksi anomali (ML). Model ML mengevaluasi semua permintaan API di akun Anda dan mengidentifikasi peristiwa anomali yang terkait dengan teknik yang digunakan oleh musuh. Model ML melacak berbagai faktor permintaan API, seperti, pengguna yang membuat permintaan, lokasi tempat permintaan dibuat, dan API khusus yang diminta. Detail tentang faktor-faktor permintaan API yang tidak biasa untuk identitas pengguna yang memanggil permintaan dapat ditemukan di [detail temuan](#).

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, kredensi Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memulihkan kredensi yang berpotensi dikompromikan AWS](#).

Impact:IAMUser/AnomalousBehavior

API yang biasa digunakan untuk mengutak-atik data atau proses di AWS lingkungan dipanggil dengan cara yang anomali.

Tingkat keparahan default: Tinggi

- Sumber data: acara CloudTrail manajemen

Temuan ini menginformasikan bahwa terdapat permintaan API anomali yang diamati di akun Anda. Temuan ini dapat mencakup satu permintaan API atau serangkaian permintaan API terkait yang dibuat di sekitar oleh satu [identitas pengguna](#). API yang diamati umumnya dikaitkan dengan taktik dampak di mana musuh mencoba mengganggu operasi dan memanipulasi, mengganggu, atau menghancurkan data di akun Anda. APIs untuk jenis temuan ini biasanya menghapus, memperbarui, atau menempatkan operasi, seperti,DeleteSecurityGroup,UpdateUser, atauPutBucketPolicy.

Permintaan API ini diidentifikasi sebagai anomali oleh GuardDuty model pembelajaran mesin deteksi anomali (ML). Model ML mengevaluasi semua permintaan API di akun Anda dan mengidentifikasi peristiwa anomali yang terkait dengan teknik yang digunakan oleh musuh. Model ML melacak berbagai faktor permintaan API, seperti, pengguna yang membuat permintaan, lokasi tempat permintaan dibuat, dan API khusus yang diminta. Detail tentang faktor-faktor permintaan API yang tidak biasa untuk identitas pengguna yang memanggil permintaan dapat ditemukan di [detail temuan](#).

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, kredensi Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memulihkan kredensi yang berpotensi dikompromikan AWS](#).

InitialAccess:IAMUser/AnomalousBehavior

API yang biasa digunakan untuk mendapatkan akses tidak sah ke AWS lingkungan dipanggil dengan cara yang anomali.

Tingkat keparahan default: Sedang

- Sumber data: acara CloudTrail manajemen

Temuan ini menginformasikan bahwa terdapat permintaan API anomali yang diamati di akun Anda. Temuan ini dapat mencakup satu permintaan API atau serangkaian permintaan API terkait yang dibuat di sekitar oleh satu [identitas pengguna](#). API yang diamati umumnya dikaitkan dengan tahap akses awal serangan ketika musuh mencoba untuk membangun akses ke lingkungan Anda. APIs dalam kategori ini biasanya mendapatkan token, atau operasi sesi, seperti, `StartSession`, atau `GetAuthorizationToken`.

Permintaan API ini diidentifikasi sebagai anomali oleh GuardDuty model pembelajaran mesin deteksi anomali (ML). Model ML mengevaluasi semua permintaan API di akun Anda dan mengidentifikasi peristiwa anomali yang terkait dengan teknik yang digunakan oleh musuh. Model ML melacak berbagai faktor permintaan API, seperti, pengguna yang membuat permintaan, lokasi tempat permintaan dibuat, dan API khusus yang diminta. Detail tentang faktor-faktor permintaan API yang tidak biasa untuk identitas pengguna yang memanggil permintaan dapat ditemukan di [detail temuan](#).

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, kredensi Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memulihkan kredensi yang berpotensi dikompromikan AWS](#).

PenTest:IAMUser/KaliLinux

API dipanggil dari mesin Kali Linux.

Tingkat keparahan default: Sedang

- Sumber data: acara CloudTrail manajemen

Temuan ini memberi tahu Anda bahwa mesin yang menjalankan Kali Linux melakukan panggilan API menggunakan kredensial milik AWS akun yang terdaftar di lingkungan Anda. Kali Linux adalah alat pengujian penetrasi populer yang digunakan oleh para profesional keamanan untuk mengidentifikasi kelemahan dalam EC2 kasus yang memerlukan penambalan. Penyerang juga menggunakan alat ini untuk menemukan kelemahan EC2 konfigurasi dan mendapatkan akses tidak sah ke lingkungan Anda. AWS

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, kredensi Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memulihkan kredensi yang berpotensi dikompromikan AWS](#).

PenTest:IAMUser/ParrotLinux

API dipanggil dari mesin Parrot Security Linux.

Tingkat keparahan default: Sedang

- Sumber data: acara CloudTrail manajemen

Temuan ini memberi tahu Anda bahwa mesin yang menjalankan Parrot Security Linux melakukan panggilan API menggunakan kredensial milik AWS akun yang terdaftar di lingkungan Anda. Parrot Security Linux adalah alat pengujian penetrasi populer yang digunakan para profesional keamanan untuk mengidentifikasi kelemahan dalam EC2 kasus yang memerlukan penambalan. Penyerang juga menggunakan alat ini untuk menemukan kelemahan EC2 konfigurasi dan mendapatkan akses tidak sah ke lingkungan Anda. AWS

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, kredensi Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memulihkan kredensi yang berpotensi dikompromikan AWS](#).

PenTest:IAMUser/PentooLinux

API dipanggil dari mesin Pentoo Linux.

Tingkat keparahan default: Sedang

- Sumber data: acara CloudTrail manajemen

Temuan ini memberi tahu Anda bahwa mesin yang menjalankan Pentoo Linux melakukan panggilan API menggunakan kredensial milik AWS akun yang terdaftar di lingkungan Anda. Pentoo Linux adalah alat pengujian penetrasi populer yang digunakan oleh para profesional keamanan untuk mengidentifikasi kelemahan dalam EC2 kasus yang memerlukan penambalan. Penyerang juga menggunakan alat ini untuk menemukan kelemahan EC2 konfigurasi dan mendapatkan akses tidak sah ke lingkungan Anda. AWS

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, kredensi Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memulihkan kredensi yang berpotensi dikompromikan AWS](#).

Persistence:IAMUser/AnomalousBehavior

API yang biasa digunakan untuk mempertahankan akses tidak sah ke AWS lingkungan dipanggil dengan cara yang anomali.

Tingkat keparahan default: Sedang

- Sumber data: acara CloudTrail manajemen

Temuan ini menginformasikan bahwa terdapat permintaan API anomali yang diamati di akun Anda. Temuan ini dapat mencakup satu permintaan API atau serangkaian permintaan API terkait yang dibuat di sekitar oleh satu [identitas pengguna](#). API yang diamati umumnya dikaitkan dengan taktik persistensi di mana musuh telah mendapatkan akses ke lingkungan Anda dan berusaha mempertahankan akses itu. APIs dalam kategori ini biasanya membuat,

mengimpor, atau memodifikasi operasi, seperti `CreateAccessKey`, `ImportKeyPair`, atau `ModifyInstanceAttribute`.

Permintaan API ini diidentifikasi sebagai anomali oleh GuardDuty model pembelajaran mesin deteksi anomali (ML). Model ML mengevaluasi semua permintaan API di akun Anda dan mengidentifikasi peristiwa anomali yang terkait dengan teknik yang digunakan oleh musuh. Model ML melacak berbagai faktor permintaan API, seperti, pengguna yang membuat permintaan, lokasi tempat permintaan dibuat, dan API khusus yang diminta. Detail tentang faktor-faktor permintaan API yang tidak biasa untuk identitas pengguna yang memanggil permintaan dapat ditemukan di [detail temuan](#).

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, kredensi Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memulihkan kredensi yang berpotensi dikompromikan AWS](#).

Policy: IAMUser/RootCredentialUsage

API dipanggil menggunakan kredensial masuk pengguna root.

Tingkat keparahan default: Rendah

- Sumber data: peristiwa CloudTrail manajemen atau peristiwa CloudTrail data untuk S3

Temuan ini memberi tahu Anda bahwa kredensial masuk pengguna root dari yang tercantum Akun AWS di lingkungan Anda digunakan untuk membuat permintaan ke layanan. AWS Disarankan agar pengguna tidak pernah menggunakan kredensial masuk pengguna root untuk mengakses layanan. AWS Sebagai gantinya, AWS layanan harus diakses menggunakan kredensial sementara hak istimewa terkecil dari AWS Security Token Service (STS). Jika AWS STS tidak didukung, sebaiknya gunakan kredensial pengguna IAM. Untuk informasi selengkapnya, lihat [Praktik Terbaik IAM](#).

Note

Jika Perlindungan S3 diaktifkan untuk akun, maka temuan ini dapat dihasilkan sebagai tanggapan atas upaya untuk menjalankan operasi bidang data S3 di sumber daya Amazon S3 dengan menggunakan kredensial masuk pengguna root dari file. Akun AWS Panggilan API yang digunakan akan tercantum dalam detail temuan. Jika Perlindungan S3 tidak diaktifkan, maka temuan ini hanya dapat dipicu oleh log APIs Peristiwa. Untuk informasi lebih lanjut tentang Perlindungan S3, lihat [Perlindungan S3](#).

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, kredensi Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memulihkan kredensi yang berpotensi dikompromikan AWS](#).

Policy: IAMUser/ShortTermRootCredentialUsage

API dipanggil dengan menggunakan kredensial pengguna root terbatas.

Tingkat keparahan default: Rendah

- Sumber data: peristiwa AWS CloudTrail manajemen atau peristiwa AWS CloudTrail data untuk S3

Temuan ini memberi tahu Anda bahwa kredensi pengguna terbatas yang dibuat untuk yang terdaftar Akun AWS di lingkungan Anda, sedang digunakan untuk membuat permintaan. Layanan AWS Disarankan untuk menggunakan kredensi pengguna root hanya untuk [tugas-tugas yang memerlukan kredensi pengguna root](#).

Jika memungkinkan, akses peran IAM Layanan AWS dengan menggunakan hak istimewa terkecil dengan kredensi sementara dari (). AWS Security Token Service AWS STS Untuk skenario di AWS STS mana tidak didukung, praktik terbaik adalah menggunakan kredensial pengguna IAM. Untuk informasi selengkapnya, lihat [Praktik terbaik keamanan dalam praktik terbaik pengguna IAM dan Root untuk Anda Akun AWS](#) di Panduan Pengguna IAM.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, kredensi Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memulihkan kredensi yang berpotensi dikompromikan AWS](#).

PrivilegeEscalation: IAMUser/AnomalousBehavior

API yang biasa digunakan untuk mendapatkan izin tingkat tinggi ke AWS lingkungan dipanggil dengan cara yang anomali.

Tingkat keparahan default: Sedang

- Sumber data: acara CloudTrail manajemen

Temuan ini menginformasikan bahwa terdapat permintaan API anomali yang diamati di akun Anda. Temuan ini dapat mencakup satu permintaan API atau serangkaian permintaan API terkait yang dibuat di sekitar oleh satu [identitas pengguna](#). API yang diamati umumnya dikaitkan dengan taktik eskalasi hak istimewa di mana musuh berusaha mendapatkan izin tingkat yang lebih tinggi ke suatu lingkungan. APIs dalam kategori ini biasanya melibatkan operasi yang mengubah kebijakan, peran, dan pengguna IAM, seperti, `AssociateIamInstanceProfileAddUserToGroup`, atau `PutUserPolicy`.

Permintaan API ini diidentifikasi sebagai anomali oleh GuardDuty model pembelajaran mesin deteksi anomali (ML). Model ML mengevaluasi semua permintaan API di akun Anda dan mengidentifikasi peristiwa anomali yang terkait dengan teknik yang digunakan oleh musuh. Model ML melacak berbagai faktor permintaan API, seperti, pengguna yang membuat permintaan, lokasi tempat permintaan dibuat, dan API khusus yang diminta. Detail tentang faktor-faktor permintaan API yang tidak biasa untuk identitas pengguna yang memanggil permintaan dapat ditemukan di [detail temuan](#).

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, kredensi Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memulihkan kredensi yang berpotensi dikompromikan AWS](#).

Recon:IAMUser/MaliciousIPCaller

API dipanggil dari alamat IP berbahaya yang diketahui.

Tingkat keparahan default: Sedang

- Sumber data: acara CloudTrail manajemen

Temuan ini menginformasikan bahwa operasi API yang dapat mendaftarkan atau mendeskripsikan sumber daya AWS di akun dalam lingkungan Anda dipanggil dari alamat IP yang termasuk dalam daftar ancaman. Penyerang dapat menggunakan kredensial curian untuk melakukan jenis pengintaian AWS sumber daya Anda untuk menemukan kredensial yang lebih berharga atau menentukan kemampuan kredensial yang sudah mereka miliki.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, kredensi Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memulihkan kredensi yang berpotensi dikompromikan AWS](#).

Recon:IAMUser/MaliciousIPCaller.Custom

API dipanggil dari alamat IP berbahaya yang diketahui.

Tingkat keparahan default: Sedang

- Sumber data: acara CloudTrail manajemen

Temuan ini menginformasikan bahwa operasi API yang dapat mendaftarkan atau mendeskripsikan sumber daya AWS di akun dalam lingkungan Anda dipanggil dari alamat IP yang termasuk dalam daftar ancaman kustom. Daftar ancaman yang digunakan akan tercantum dalam detail temuan. Seorang penyerang mungkin menggunakan kredensial curian untuk melakukan jenis pengintaian AWS sumber daya Anda untuk menemukan kredensial yang lebih berharga atau menentukan kemampuan kredensial yang sudah mereka miliki.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, kredensi Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memulihkan kredensi yang berpotensi dikompromikan AWS](#).

Recon:IAMUser/TorIPCaller

API dipanggil dari alamat IP node keluar dari Tor.

Tingkat keparahan default: Sedang

- Sumber data: acara CloudTrail manajemen

Temuan ini menginformasikan bahwa operasi API yang dapat mendaftarkan atau mendeskripsikan sumber daya AWS di akun dalam lingkungan anda dipanggil dari alamat IP node keluar dari Tor. Tor adalah perangkat lunak untuk memungkinkan komunikasi anonim. Ini mengenkripsi dan secara acak mengalihkan komunikasi melalui relay antara serangkaian node jaringan. Node Tor terakhir disebut sebagai nod keluar. Penyerang akan menggunakan Tor untuk menutupi identitas mereka yang sebenarnya.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, kredensi Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memulihkan kredensi yang berpotensi dikompromikan AWS](#).

Stealth:IAMUser/CloudTrailLoggingDisabled

AWS CloudTrail logging dinonaktifkan.

Tingkat keparahan default: Rendah

- Sumber data: acara CloudTrail manajemen

Temuan ini memberi tahu Anda bahwa CloudTrail jejak di AWS lingkungan Anda dinonaktifkan. Ini bisa menjadi upaya penyerang untuk menonaktifkan pencatatan log untuk menutupi jejak mereka dengan menghilangkan jejak aktivitas mereka sekaligus mendapatkan akses ke sumber daya AWS Anda untuk tujuan berbahaya. Temuan ini dapat dipicu oleh penghapusan atau pembaruan jejak yang berhasil. Temuan ini juga dapat dipicu oleh penghapusan bucket S3 yang berhasil menyimpan log dari jejak yang terkait dengannya. GuardDuty

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, kredensi Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memulihkan kredensi yang berpotensi dikompromikan AWS](#).

Stealth:IAMUser/PasswordPolicyChange

Kebijakan kata sandi akun dilemahkan.

Tingkat keparahan default: Rendah*

Note

Tingkat keparahan temuan ini bisa Rendah, Sedang, atau Tinggi tergantung pada tingkat keparahan perubahan yang dibuat pada kebijakan kata sandi.

- Sumber data: acara CloudTrail manajemen

Kebijakan kata sandi AWS akun dilemahkan pada akun yang terdaftar di AWS lingkungan Anda. Misalnya, kata sandi dihapus atau diperbarui untuk memerlukan lebih sedikit karakter, tidak memerlukan simbol dan angka, atau diperlukan untuk memperpanjang masa kedaluwarsa kata sandi. Temuan ini juga dapat dipicu oleh upaya untuk memperbarui atau menghapus kebijakan kata sandi AWS akun Anda. Kebijakan kata sandi AWS akun mendefinisikan aturan yang mengatur jenis kata sandi apa yang dapat ditetapkan untuk pengguna IAM Anda. Kebijakan kata sandi yang lebih lemah memungkinkan pembuatan kata sandi yang mudah diingat dan berpotensi lebih mudah ditebak, sehingga menimbulkan risiko keamanan.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, kredensi Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memulihkan kredensi yang berpotensi dikompromikan AWS](#).

UnauthorizedAccess:IAMUser/ConsoleLoginSuccess.B

Beberapa login konsol yang berhasil di seluruh dunia diamati.

Tingkat keparahan default: Sedang

- Sumber data: acara CloudTrail manajemen

Temuan ini menginformasikan bahwa beberapa login konsol yang berhasil untuk pengguna IAM yang sama diamati pada waktu yang sama di berbagai lokasi geografis. Pola lokasi akses anomali dan berisiko seperti itu menunjukkan potensi akses tidak sah ke sumber daya Anda. AWS

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, kredensi Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memulihkan kredensi yang berpotensi dikompromikan AWS](#).

UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS

Kredensial yang dibuat secara eksklusif untuk sebuah EC2 instance melalui peran peluncuran Instance digunakan dari akun lain di dalamnya. AWS

Tingkat keparahan default: Tinggi*

 Note

Tingkat keparahan default temuan ini adalah Tinggi. Namun, jika API dipanggil oleh akun yang berafiliasi dengan AWS lingkungan Anda, tingkat keparahannya adalah Medium.

- Sumber data: peristiwa CloudTrail manajemen atau peristiwa CloudTrail data untuk S3

Temuan ini memberi tahu Anda kapan kredensi EC2 instans Amazon Anda digunakan untuk memanggil APIs dari alamat IP atau titik akhir VPC Amazon, yang dimiliki oleh akun yang berbeda dari AWS akun yang dijalankan instans Amazon terkait. EC2 Deteksi titik akhir VPC hanya tersedia untuk layanan yang mendukung peristiwa aktivitas jaringan untuk titik akhir VPC. Untuk informasi tentang layanan yang mendukung peristiwa aktivitas jaringan untuk titik akhir VPC, lihat [Mencatat peristiwa aktivitas jaringan di Panduan Pengguna AWS CloudTrail](#)

AWS tidak merekomendasikan untuk mendistribusikan ulang kredensi sementara di luar entitas yang membuatnya (misalnya AWS , aplikasi, Amazon EC2, atau). AWS Lambda Namun, pengguna yang berwenang dapat mengeksport kredensial dari EC2 instans Amazon mereka untuk melakukan panggilan API yang sah. Jika `remoteAccountDetails.Affiliated` bidangnya adalah `True` API dipanggil dari akun yang terkait dengan akun administrator yang sama. Untuk mengesampingkan potensi serangan dan memverifikasi legitimasi aktivitas, hubungi Akun AWS pemilik atau kepala IAM kepada siapa kredensi ini diberikan.

 Note

Jika GuardDuty mengamati aktivitas lanjutan dari akun jarak jauh, model pembelajaran mesin (ML) akan mengidentifikasi ini sebagai perilaku yang diharapkan. Oleh karena itu, GuardDuty akan berhenti menghasilkan temuan ini untuk aktivitas dari akun jarak jauh itu. GuardDuty akan terus menghasilkan temuan untuk perilaku baru dari akun jarak jauh lainnya dan akan mengevaluasi kembali akun jarak jauh yang dipelajari saat perilaku berubah seiring waktu.

Rekomendasi remediasi:

Temuan ini akan dihasilkan saat permintaan AWS API dibuat di dalam AWS melalui EC2 instance Amazon di luar instans Anda Akun AWS, dengan menggunakan kredensial sesi EC2 instans Amazon

Anda. Mungkin lazim, seperti untuk arsitektur Transit Gateway dalam konfigurasi [hub dan spoke](#), untuk merutekan lalu lintas melalui AWS VPC jalan keluar hub tunggal dengan titik akhir layanan. Jika perilaku ini diharapkan, maka GuardDuty sarankan Anda untuk menggunakan [Aturan penekanan](#) dan membuat aturan dengan kriteria dua filter. Kriteria pertama adalah tipe temuan, yang, dalam hal ini, adalah UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS. Kriteria filter kedua adalah ID akun jarak jauh dari detail akun jarak jauh.

Menanggapi temuan ini, Anda dapat menggunakan alur kerja berikut untuk menentukan tindakan:

1. Identifikasi akun jarak jauh yang terlibat dari `service.action.awsApiCallAction.remoteAccountDetails.accountId` lapangan.
2. Tentukan apakah akun itu berafiliasi dengan GuardDuty lingkungan Anda dari `service.action.awsApiCallAction.remoteAccountDetails.affiliated` lapangan.
3. Jika akun tersebut berafiliasi, hubungi pemilik akun jarak jauh dan pemilik kredensial EC2 instans Amazon untuk menyelidiki.

Jika akun tidak berafiliasi, maka langkah pertama adalah mengevaluasi apakah akun tersebut terkait dengan organisasi Anda tetapi bukan bagian dari pengaturan lingkungan beberapa GuardDuty akun Anda, atau jika GuardDuty belum diaktifkan di akun ini. Selanjutnya, hubungi pemilik kredensial EC2 instans Amazon untuk menentukan apakah ada kasus penggunaan untuk akun jarak jauh untuk menggunakan kredensial ini.

4. Jika pemilik kredensial tidak mengenali akun jarak jauh, kredensialnya mungkin telah dikompromikan oleh aktor ancaman yang beroperasi di dalamnya. AWS Anda harus mengambil langkah-langkah yang direkomendasikan [Memperbaiki instans Amazon yang berpotensi dikompromikan EC2](#), untuk mengamankan lingkungan Anda.

Selain itu, Anda dapat [mengirimkan laporan penyalahgunaan](#) ke tim AWS Trust and Safety untuk memulai penyelidikan ke akun jarak jauh. Saat mengirimkan laporan Anda ke AWS Trust and Safety, sertakan detail lengkap JSON dari temuan tersebut.

UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS

Kredensial yang dibuat secara eksklusif untuk sebuah EC2 instance melalui peran peluncuran Instance sedang digunakan dari alamat IP eksternal.

Tingkat keparahan default: Tinggi

- Sumber data: peristiwa CloudTrail manajemen atau peristiwa CloudTrail data untuk S3

Temuan ini memberi tahu Anda bahwa host di luar AWS telah mencoba menjalankan operasi AWS API menggunakan AWS kredensial sementara yang dibuat pada EC2 instance di lingkungan Anda. AWS EC2 Instance yang terdaftar mungkin dikompromikan, dan kredensial sementara dari instance ini mungkin telah diekstraksi ke host jarak jauh di luar. AWS tidak merekomendasikan untuk mendistribusikan ulang kredensial sementara di luar entitas yang membuatnya (misalnya, AWS aplikasi, EC2 atau Lambda). Namun, pengguna yang berwenang dapat mengeksport kredensial dari EC2 instans mereka untuk melakukan panggilan API yang sah. Untuk mengesampingkan potensi serangan dan memverifikasi legitimasi aktivitas, validasi jika penggunaan kredensial instance dari IP jarak jauh dalam temuan diharapkan.

Note

Jika GuardDuty mengamati aktivitas lanjutan dari akun jarak jauh, model pembelajaran mesin (ML) akan mengidentifikasi ini sebagai perilaku yang diharapkan. Oleh karena itu, GuardDuty akan berhenti menghasilkan temuan ini untuk aktivitas dari akun jarak jauh itu. GuardDuty akan terus menghasilkan temuan untuk perilaku baru dari akun jarak jauh lainnya dan akan mengevaluasi kembali akun jarak jauh yang dipelajari saat perilaku berubah seiring waktu.

Rekomendasi remediasi:

Temuan ini dibuat saat jaringan dikonfigurasi untuk merutekan lalu lintas internet sedemikian rupa sehingga keluar dari gateway on-premise, bukan dari Gateway Internet VPC (IGW). Konfigurasi umum, seperti penggunaan [AWS Outposts](#), atau koneksi VPN VPC, dapat mengakibatkan lalu lintas dirutekan dengan cara ini. Jika ini adalah perilaku yang diharapkan, kami sarankan Anda menggunakan aturan penekanan dan membuat aturan yang terdiri dari dua kriteria filter. Kriteria pertama adalah tipe temuan, yaitu `UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS`. Kriteria filter kedua adalah IPv4 Alamat pemanggil API dengan alamat IP atau rentang CIDR gateway internet lokal Anda. Untuk mempelajari selengkapnya tentang cara membuat aturan penekanan, lihat [Aturan penindasan di GuardDuty](#).

Note

Jika GuardDuty mengamati aktivitas lanjutan dari sumber eksternal, model pembelajaran mesinnya akan mengidentifikasi ini sebagai perilaku yang diharapkan dan berhenti menghasilkan temuan ini untuk aktivitas dari sumber itu. GuardDuty akan terus menghasilkan

temuan untuk perilaku baru dari sumber lain, dan akan mengevaluasi kembali sumber yang dipelajari saat perilaku berubah dari waktu ke waktu.

Jika aktivitas ini tidak terduga, kredensial Anda mungkin disusupi, lihat [Memulihkan kredensi yang berpotensi dikompromikan AWS](#).

UnauthorizedAccess:IAMUser/MaliciousIPCaller

API dipanggil dari alamat IP berbahaya yang diketahui.

Tingkat keparahan default: Sedang

- Sumber data: acara CloudTrail manajemen

Temuan ini memberi tahu Anda bahwa operasi API (misalnya, upaya untuk meluncurkan EC2 instance, membuat pengguna IAM baru, atau memodifikasi AWS hak istimewa Anda) dipanggil dari alamat IP berbahaya yang diketahui. Ini dapat menunjukkan akses tidak sah ke AWS sumber daya dalam lingkungan Anda.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, kredensi Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memulihkan kredensi yang berpotensi dikompromikan AWS](#).

UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom

API dipanggil dari alamat IP pada daftar ancaman kustom.

Tingkat keparahan default: Sedang

- Sumber data: acara CloudTrail manajemen

Temuan ini memberi tahu Anda bahwa operasi API (misalnya, upaya untuk meluncurkan EC2 instance, membuat pengguna IAM baru, atau memodifikasi AWS hak istimewa) dipanggil dari alamat IP yang disertakan pada daftar ancaman yang Anda unggah. Di , daftar ancaman terdiri dari alamat IP berbahaya yang diketahui. Ini dapat menunjukkan akses tidak sah ke AWS sumber daya dalam lingkungan Anda.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, kredensi Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memulihkan kredensi yang berpotensi dikompromikan AWS](#).

UnauthorizedAccess:IAMUser/TorIPCaller

API dipanggil dari alamat IP node keluar dari Tor.

Tingkat keparahan default: Sedang

- Sumber data: acara CloudTrail manajemen

Temuan ini memberi tahu Anda bahwa operasi API (misalnya, upaya untuk meluncurkan EC2 instance, membuat pengguna IAM baru, atau memodifikasi AWS hak istimewa Anda) dipanggil dari alamat IP node keluar Tor. Tor adalah perangkat lunak untuk memungkinkan komunikasi anonim. Ini mengenkripsi dan secara acak mengalihkan komunikasi melalui relay antara serangkaian node jaringan. Node Tor terakhir disebut sebagai nod keluar. Temuan ini mungkin mengindikasikan akses yang tidak sah ke sumber daya AWS Anda yang bertujuan untuk menyembunyikan identitas penyerang yang sebenarnya.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, kredensi Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memulihkan kredensi yang berpotensi dikompromikan AWS](#).

GuardDuty jenis pencarian urutan serangan

GuardDuty mendeteksi urutan serangan ketika urutan tertentu dari beberapa tindakan sejajar dengan aktivitas yang berpotensi mencurigakan. Urutan serangan mencakup sinyal seperti aktivitas dan GuardDuty temuan API. Ketika GuardDuty mengamati sekelompok sinyal dalam urutan tertentu yang menunjukkan ancaman keamanan yang sedang berlangsung, sedang berlangsung, atau baru-baru ini, GuardDuty menghasilkan temuan urutan serangan. GuardDuty menganggap aktivitas API individu [weak signals](#) karena mereka tidak menampilkan diri sebagai ancaman potensial.

Deteksi urutan serangan berfokus pada potensi kompromi data Amazon S3 (yang dapat menjadi bagian dari serangan ransomware yang lebih luas), AWS kredensi yang dikompromikan, dan kluster Amazon EKS yang dikompromikan. Bagian berikut memberikan rincian tentang masing-masing urutan serangan.

Topik

- [AttackSequence:EKS/CompromisedCluster](#)
- [AttackSequence:IAM/CompromisedCredentials](#)
- [AttackSequence:S3/CompromisedData](#)

AttackSequence:EKS/CompromisedCluster

Urutan tindakan mencurigakan yang dilakukan oleh cluster Amazon EKS yang berpotensi dikompromikan.

- Tingkat keparahan default: Kritis
- Sumber data:
 - [Kejadian log audit EKS](#)
 - [Pemantauan Runtime untuk Amazon EKS](#)
 - [Deteksi malware Amazon EKS untuk Amazon EC2](#)
 - [AWS CloudTrail peristiwa data untuk S3](#)
 - [AWS CloudTrail acara manajemen](#)
 - [Log Alur VPC](#)
 - [Log kueri DNS Route53 Resolver](#)

Temuan ini memberi tahu Anda bahwa GuardDuty mendeteksi urutan tindakan mencurigakan yang menunjukkan klaster Amazon EKS yang berpotensi dikompromikan di lingkungan Anda. Beberapa perilaku serangan yang mencurigakan dan anomali, seperti proses berbahaya atau koneksi dengan titik akhir berbahaya, diamati di cluster Amazon EKS yang sama.

GuardDuty menggunakan algoritma korelasi miliknya untuk mengamati dan mengidentifikasi urutan tindakan yang dilakukan dengan menggunakan kredensi IAM. GuardDuty mengevaluasi temuan di seluruh rencana perlindungan dan sumber sinyal lainnya untuk mengidentifikasi pola serangan yang umum dan muncul. GuardDuty menggunakan beberapa faktor untuk memunculkan ancaman, seperti reputasi IP, urutan API, konfigurasi pengguna, dan sumber daya yang berpotensi terkena dampak.

Tindakan remediasi: Jika perilaku ini tidak terduga di lingkungan Anda, maka klaster Amazon EKS Anda dapat dikompromikan. Untuk panduan remediasi yang komprehensif, lihat [Remediasi temuan Perlindungan EKS](#) dan [Remediasi temuan Runtime Monitoring](#).

Selain itu, karena AWS kredensial mungkin telah dikompromikan melalui kluster EKS, lihat.

[Memulihkan kredensi yang berpotensi dikompromikan AWS](#) Untuk langkah-langkah untuk memulihkan sumber daya lain yang mungkin berpotensi terkena dampak, lihat. [Memulihkan temuan GuardDuty keamanan yang terdeteksi](#)

AttackSequence:IAM/CompromisedCredentials

Urutan permintaan API yang dipanggil dengan menggunakan kredensial yang berpotensi dikompromikan AWS .

- Tingkat keparahan default: Kritis
- Sumber data: [AWS CloudTrail acara manajemen](#)

Temuan ini memberi tahu Anda bahwa GuardDuty mendeteksi serangkaian tindakan mencurigakan yang dilakukan dengan menggunakan AWS kredensial yang memengaruhi satu atau lebih sumber daya di lingkungan Anda. Beberapa perilaku serangan yang mencurigakan dan anomali diamati oleh kredensial yang sama, menghasilkan keyakinan yang lebih tinggi bahwa kredensial disalahgunakan.

GuardDuty menggunakan algoritma korelasi miliknya untuk mengamati dan mengidentifikasi urutan tindakan yang dilakukan dengan menggunakan kredensi IAM. GuardDuty mengevaluasi temuan di seluruh rencana perlindungan dan sumber sinyal lainnya untuk mengidentifikasi pola serangan yang umum dan muncul. GuardDuty menggunakan beberapa faktor untuk memunculkan ancaman, seperti reputasi IP, urutan API, konfigurasi pengguna, dan sumber daya yang berpotensi terkena dampak.

Tindakan remediasi: Jika perilaku ini tidak terduga di lingkungan Anda, maka AWS kredensial Anda mungkin telah dikompromikan. Untuk langkah-langkah untuk memperbaiki, lihat [Memulihkan kredensi yang berpotensi dikompromikan AWS](#). Kredensi yang disusupi mungkin telah digunakan untuk membuat atau memodifikasi sumber daya tambahan, seperti bucket Amazon S3, fungsi, atau instans Amazon AWS Lambda EC2 , di lingkungan Anda. Untuk langkah-langkah untuk memulihkan sumber daya lain yang mungkin berpotensi terkena dampak, lihat. [Memulihkan temuan GuardDuty keamanan yang terdeteksi](#)

AttackSequence:S3/CompromisedData

Urutan permintaan API dipanggil dalam upaya potensial untuk mengekstraksi atau menghancurkan data di Amazon S3.

- Tingkat keparahan default: Kritis

- Sumber data: [AWS CloudTrail peristiwa data untuk S3](#) dan [AWS CloudTrail acara manajemen](#)

Temuan ini memberi tahu Anda bahwa GuardDuty mendeteksi urutan tindakan mencurigakan yang menunjukkan kompromi data dalam satu atau beberapa bucket Amazon Simple Storage Service (Amazon S3), dengan menggunakan kredensial yang berpotensi dikompromikan. AWS Beberapa perilaku serangan yang mencurigakan dan anomali (permintaan API) diamati, menghasilkan kepercayaan yang lebih tinggi dari kredensial yang disalahgunakan.

GuardDuty menggunakan algoritma korelasinya untuk mengamati dan mengidentifikasi urutan tindakan yang dilakukan dengan menggunakan kredensi IAM. GuardDuty kemudian mengevaluasi temuan di seluruh rencana perlindungan dan sumber sinyal lainnya untuk mengidentifikasi pola serangan yang umum dan muncul. GuardDuty menggunakan beberapa faktor untuk memunculkan ancaman, seperti reputasi IP, urutan API, konfigurasi pengguna, dan sumber daya yang berpotensi terkena dampak.

Tindakan remediasi: Jika aktivitas ini tidak terduga di lingkungan Anda, AWS kredensial, atau data Amazon S3 Anda mungkin berpotensi diekstraksi atau dihancurkan. Untuk langkah-langkah untuk memulihkan, lihat [Memulihkan kredensi yang berpotensi dikompromikan AWS](#) dan [Memperbaiki bucket S3 yang berpotensi dikompromikan](#).

GuardDuty Jenis temuan Perlindungan S3

Temuan berikut khusus untuk sumber daya Amazon S3 dan akan memiliki Jenis Sumber Daya **S3Bucket** jika sumber data adalah peristiwa CloudTrail data untuk S3, atau **AccessKey** jika sumber data adalah CloudTrail peristiwa manajemen. Tingkat kepelikan dan detail temuan akan berbeda berdasarkan tipe temuan dan izin yang terkait dengan bucket.

Temuan yang tercantum di sini termasuk sumber data dan model yang digunakan untuk menghasilkan tipe temuan. Untuk informasi lebih lanjut sumber dan model data, lihat [GuardDuty sumber data dasar](#).

Important

Temuan dengan sumber data peristiwa CloudTrail data untuk S3 hanya dihasilkan jika Anda telah mengaktifkan Perlindungan S3. Secara default, setelah 31 Juli 2020, Perlindungan S3 diaktifkan saat akun diaktifkan GuardDuty untuk pertama kalinya, atau ketika akun GuardDuty administrator yang didelegasikan diaktifkan GuardDuty di akun anggota yang

ada. Namun, ketika anggota baru bergabung dengan GuardDuty organisasi, preferensi pengaktifan otomatis organisasi akan berlaku. Untuk informasi tentang preferensi aktifkan otomatis, lihat [Menyetel preferensi aktifkan otomatis organisasi](#). Untuk informasi tentang cara mengaktifkan Perlindungan S3, lihat [GuardDuty Perlindungan S3](#)

Untuk semua S3Bucket jenis temuan, Anda disarankan untuk memeriksa izin pada bucket yang bersangkutan dan izin dari setiap pengguna yang terlibat dalam temuan, jika aktivitas tidak terduga, lihat rekomendasi remediasi yang dirinci di [Memperbaiki bucket S3 yang berpotensi dikompromikan](#)

Topik

- [Discovery:S3/AnomalousBehavior](#)
- [Discovery:S3/MaliciousIPCaller](#)
- [Discovery:S3/MaliciousIPCaller.Custom](#)
- [Discovery:S3/TorIPCaller](#)
- [Exfiltration:S3/AnomalousBehavior](#)
- [Exfiltration:S3/MaliciousIPCaller](#)
- [Impact:S3/AnomalousBehavior.Delete](#)
- [Impact:S3/AnomalousBehavior.Permission](#)
- [Impact:S3/AnomalousBehavior.Write](#)
- [Impact:S3/MaliciousIPCaller](#)
- [PenTest:S3/KaliLinux](#)
- [PenTest:S3/ParrotLinux](#)
- [PenTest:S3/PentooLinux](#)
- [Policy:S3/AccountBlockPublicAccessDisabled](#)
- [Policy:S3/BucketAnonymousAccessGranted](#)
- [Policy:S3/BucketBlockPublicAccessDisabled](#)
- [Policy:S3/BucketPublicAccessGranted](#)
- [Stealth:S3/ServerAccessLoggingDisabled](#)
- [UnauthorizedAccess:S3/MaliciousIPCaller.Custom](#)
- [UnauthorizedAccess:S3/TorIPCaller](#)

Discovery:S3/AnomalousBehavior

API yang biasa digunakan untuk menemukan objek S3 dipanggil dengan cara yang anomali.

Tingkat keparahan default: Rendah

- Sumber data: peristiwa CloudTrail data untuk S3

Temuan ini menginformasikan bahwa entitas IAM telah memanggil API S3 untuk menemukan bucket S3 dalam lingkungan Anda, seperti `ListObjects`. Jenis aktivitas ini dikaitkan dengan tahap penemuan serangan di mana penyerang mengumpulkan informasi untuk menentukan apakah AWS lingkungan Anda rentan terhadap serangan yang lebih luas. Aktivitas ini mencurigakan karena entitas IAM memanggil API dengan cara yang tidak biasa. Misalnya, entitas IAM tanpa riwayat sebelumnya memanggil API S3, atau entitas IAM memanggil API S3 dari lokasi yang tidak biasa.

API ini diidentifikasi sebagai anomali oleh GuardDuty model pembelajaran mesin deteksi anomali (ML). Model ML mengevaluasi semua permintaan API di akun Anda dan mengidentifikasi kejadian anomali yang terkait dengan teknik yang digunakan oleh musuh. Ini melacak berbagai faktor permintaan API, seperti pengguna yang membuat permintaan, lokasi dari mana permintaan dibuat, API spesifik yang diminta, bucket yang diminta, dan jumlah panggilan API yang dibuat. Untuk informasi selengkapnya tentang faktor permintaan API yang tidak biasa untuk identitas pengguna yang memanggil permintaan, lihat [Menemukan detail](#).

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga untuk prinsipal terkait, ini mungkin menunjukkan bahwa kredensial telah diekspos atau izin S3 Anda tidak cukup membatasi. Untuk informasi selengkapnya, lihat [Memperbaiki bucket S3 yang berpotensi dikompromikan](#).

Discovery:S3/MaliciousIPCaller

API S3 yang biasa digunakan untuk menemukan sumber daya di AWS lingkungan dipanggil dari alamat IP berbahaya yang diketahui.

Tingkat keparahan default: Tinggi

- Sumber data: peristiwa CloudTrail data untuk S3

Temuan ini menginformasikan bahwa operasi API S3 dipanggil dari alamat IP yang terkait dengan aktivitas berbahaya yang diketahui. API yang diamati umumnya dikaitkan dengan tahap penemuan serangan ketika musuh mengumpulkan informasi tentang AWS lingkungan Anda. Contohnya termasuk `GetObjectAcl` dan `ListObjects`.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga untuk prinsipal terkait, ini mungkin menunjukkan bahwa kredensial telah diekspos atau izin S3 Anda tidak cukup membatasi. Untuk informasi selengkapnya, lihat [Memperbaiki bucket S3 yang berpotensi dikompromikan](#).

Discovery:S3/MaliciousIPCaller.Custom

API S3 dipanggil dari alamat IP yang termasuk dalam daftar ancaman kustom.

Tingkat keparahan default: Tinggi

- Sumber data: peristiwa CloudTrail data untuk S3

Temuan ini menginformasikan bahwa API S3, seperti `GetObjectAcl` atau `ListObjects`, dipanggil dari alamat IP yang termasuk dalam daftar ancaman yang Anda unggah. Daftar ancaman yang terkait dengan temuan ini tercantum di bagian Informasi tambahan dari detail temuan ini. Tipe aktivitas ini terkait dengan tahap penemuan serangan ketika penyerang mengumpulkan informasi untuk menentukan apakah lingkungan AWS Anda rentan terhadap serangan yang lebih luas.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga untuk prinsipal terkait, ini mungkin menunjukkan bahwa kredensial telah diekspos atau izin S3 Anda tidak cukup membatasi. Untuk informasi selengkapnya, lihat [Memperbaiki bucket S3 yang berpotensi dikompromikan](#).

Discovery:S3/TorIPCaller

API S3 dipanggil dari alamat IP node keluar Tor.

Tingkat keparahan default: Sedang

- Sumber data: peristiwa CloudTrail data untuk S3

Temuan ini menginformasikan bahwa API S3, seperti `GetObjectAcl` atau `ListObjects`, dipanggil dari alamat IP node keluar Tor. Jenis aktivitas ini dikaitkan dengan tahap penemuan serangan di mana penyerang mengumpulkan informasi untuk menentukan apakah AWS lingkungan Anda rentan terhadap serangan yang lebih luas. Tor adalah perangkat lunak untuk memungkinkan komunikasi anonim. Ini mengenkripsi dan secara acak mengalihkan komunikasi melalui relay antara serangkaian node jaringan. Node Tor terakhir disebut sebagai nod keluar. Ini dapat menunjukkan akses tidak sah ke AWS sumber daya Anda dengan maksud menyembunyikan identitas asli penyerang.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga untuk prinsipal terkait, ini mungkin menunjukkan bahwa kredensial telah diekspos atau izin S3 Anda tidak cukup membatasi. Untuk informasi selengkapnya, lihat [Memperbaiki bucket S3 yang berpotensi dikompromikan](#).

Exfiltration:S3/AnomalousBehavior

Entitas IAM memanggil API S3 dengan cara yang mencurigakan.

Tingkat keparahan default: Tinggi

- Sumber data: peristiwa CloudTrail data untuk S3

Temuan ini memberi tahu Anda bahwa entitas IAM melakukan panggilan API yang melibatkan bucket S3 dan aktivitas ini berbeda dari baseline yang ditetapkan entitas tersebut. Panggilan API yang digunakan dalam aktivitas ini dikaitkan dengan tahap eksfiltrasi serangan, di mana penyerang mencoba mengumpulkan data. Aktivitas ini mencurigakan karena entitas IAM memanggil API dengan cara yang tidak biasa. Misalnya, entitas IAM tanpa riwayat sebelumnya memanggil API S3, atau entitas IAM memanggil API S3 dari lokasi yang tidak biasa.

API ini diidentifikasi sebagai anomali oleh GuardDuty model pembelajaran mesin deteksi anomali (ML). Model ML mengevaluasi semua permintaan API di akun Anda dan mengidentifikasi kejadian anomali yang terkait dengan teknik yang digunakan oleh musuh. Ini melacak berbagai faktor permintaan API, seperti pengguna yang membuat permintaan, lokasi dari mana permintaan dibuat, API spesifik yang diminta, bucket yang diminta, dan jumlah panggilan API yang dibuat. Untuk informasi selengkapnya tentang faktor permintaan API yang tidak biasa untuk identitas pengguna yang memanggil permintaan, lihat [Menemukan detail](#).

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga untuk prinsipal terkait, ini mungkin menunjukkan bahwa kredensial telah diekspos atau izin S3 Anda tidak cukup membatasi. Untuk informasi selengkapnya, lihat [Memperbaiki bucket S3 yang berpotensi dikompromikan](#).

Exfiltration:S3/MaliciousIPCaller

API S3 yang biasa digunakan untuk mengumpulkan data dari AWS lingkungan dipanggil dari alamat IP berbahaya yang diketahui.

Tingkat keparahan default: Tinggi

- Sumber data: peristiwa CloudTrail data untuk S3

Temuan ini menginformasikan bahwa operasi API S3 dipanggil dari alamat IP yang terkait dengan aktivitas berbahaya yang diketahui. API yang diamati umumnya berkaitan dengan taktik eksfiltrasi ketika musuh mencoba mengumpulkan data dari jaringan Anda. Contohnya termasuk `GetObject` dan `CopyObject`.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga untuk prinsipal terkait, ini mungkin menunjukkan bahwa kredensial telah diekspos atau izin S3 Anda tidak cukup membatasi. Untuk informasi selengkapnya, lihat [Memperbaiki bucket S3 yang berpotensi dikompromikan](#).

Impact:S3/AnomalousBehavior.Delete

Entitas IAM memanggil API S3 yang mencoba menghapus data dengan cara yang mencurigakan.

Tingkat keparahan default: Tinggi

- Sumber data: peristiwa CloudTrail data untuk S3

Temuan ini memberi tahu Anda bahwa entitas IAM di AWS lingkungan Anda melakukan panggilan API yang melibatkan bucket S3, dan perilaku ini berbeda dari baseline yang ditetapkan entitas tersebut. Panggilan API yang digunakan dalam aktivitas ini dikaitkan dengan serangan yang

mencoba menghapus data. Aktivitas ini mencurigakan karena entitas IAM memanggil API dengan cara yang tidak biasa. Misalnya, entitas IAM tanpa riwayat sebelumnya memanggil API S3, atau entitas IAM memanggil API S3 dari lokasi yang tidak biasa.

API ini diidentifikasi sebagai anomali oleh GuardDuty model pembelajaran mesin deteksi anomali (ML). Model ML mengevaluasi semua permintaan API di akun Anda dan mengidentifikasi kejadian anomali yang terkait dengan teknik yang digunakan oleh musuh. Ini melacak berbagai faktor permintaan API, seperti pengguna yang membuat permintaan, lokasi dari mana permintaan dibuat, API spesifik yang diminta, bucket yang diminta, dan jumlah panggilan API yang dibuat. Untuk informasi selengkapnya tentang faktor permintaan API yang tidak biasa untuk identitas pengguna yang memanggil permintaan, lihat [Menemukan detail](#).

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga untuk prinsipal terkait, ini mungkin menunjukkan bahwa kredensial telah diekspos atau izin S3 Anda tidak cukup membatasi. Untuk informasi selengkapnya, lihat [Memperbaiki bucket S3 yang berpotensi dikompromikan](#).

Kami merekomendasikan audit konten bucket S3 Anda untuk menentukan apakah versi objek sebelumnya dapat atau harus dipulihkan.

Impact:S3/AnomalousBehavior.Permission

API yang biasa digunakan untuk mengatur izin daftar kontrol akses (ACL) dipanggil dengan cara yang tidak wajar.

Tingkat keparahan default: Tinggi

- Sumber data: peristiwa CloudTrail data untuk S3

Temuan ini memberi tahu Anda bahwa entitas IAM di AWS lingkungan Anda telah mengubah kebijakan bucket atau ACL pada bucket S3 yang terdaftar. Perubahan ini dapat mengekspos bucket S3 Anda secara publik ke semua pengguna yang diautentikasi. AWS

API ini diidentifikasi sebagai anomali oleh GuardDuty model pembelajaran mesin deteksi anomali (ML). Model ML mengevaluasi semua permintaan API di akun Anda dan mengidentifikasi kejadian anomali yang terkait dengan teknik yang digunakan oleh musuh. Ini melacak berbagai faktor permintaan API, seperti pengguna yang membuat permintaan, lokasi dari mana permintaan dibuat,

API spesifik yang diminta, bucket yang diminta, dan jumlah panggilan API yang dibuat. Untuk informasi selengkapnya tentang faktor permintaan API yang tidak biasa untuk identitas pengguna yang memanggil permintaan, lihat [Menemukan detail](#).

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga untuk prinsipal terkait, ini mungkin menunjukkan bahwa kredensial telah diekspos atau izin S3 Anda tidak cukup membatasi. Untuk informasi selengkapnya, lihat [Memperbaiki bucket S3 yang berpotensi dikompromikan](#).

Kami merekomendasikan audit konten bucket S3 Anda untuk memastikan bahwa tidak ada objek yang secara tidak terduga diizinkan untuk diakses secara publik.

Impact:S3/AnomalousBehavior.Write

Entitas IAM memanggil API S3 yang mencoba menulis data dengan cara yang mencurigakan.

Tingkat keparahan default: Sedang

- Sumber data: peristiwa CloudTrail data untuk S3

Temuan ini memberi tahu Anda bahwa entitas IAM di AWS lingkungan Anda melakukan panggilan API yang melibatkan bucket S3, dan perilaku ini berbeda dari baseline yang ditetapkan entitas tersebut. Panggilan API yang digunakan dalam aktivitas ini dikaitkan dengan serangan yang mencoba menulis data. Aktivitas ini mencurigakan karena entitas IAM memanggil API dengan cara yang tidak biasa. Misalnya, entitas IAM tanpa riwayat sebelumnya memanggil API S3, atau entitas IAM memanggil API S3 dari lokasi yang tidak biasa.

API ini diidentifikasi sebagai anomali oleh GuardDuty model pembelajaran mesin deteksi anomali (ML). Model ML mengevaluasi semua permintaan API di akun Anda dan mengidentifikasi kejadian anomali yang terkait dengan teknik yang digunakan oleh musuh. Ini melacak berbagai faktor permintaan API, seperti pengguna yang membuat permintaan, lokasi dari mana permintaan dibuat, API spesifik yang diminta, bucket yang diminta, dan jumlah panggilan API yang dibuat. Untuk informasi selengkapnya tentang faktor permintaan API yang tidak biasa untuk identitas pengguna yang memanggil permintaan, lihat [Menemukan detail](#).

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga untuk prinsipal terkait, ini mungkin menunjukkan bahwa kredensial telah diekspos atau izin S3 Anda tidak cukup membatasi. Untuk informasi selengkapnya, lihat [Memperbaiki bucket S3 yang berpotensi dikompromikan](#).

Kami merekomendasikan audit konten bucket S3 Anda untuk memastikan bahwa panggilan API ini tidak menulis data berbahaya atau tidak sah.

Impact:S3/MaliciousIPCaller

API S3 yang biasa digunakan untuk mengutak-atik data atau proses di AWS lingkungan dipanggil dari alamat IP berbahaya yang diketahui.

Tingkat keparahan default: Tinggi

- Sumber data: peristiwa CloudTrail data untuk S3

Temuan ini menginformasikan bahwa operasi API S3 dipanggil dari alamat IP yang terkait dengan aktivitas berbahaya yang diketahui. API yang diamati umumnya dikaitkan dengan taktik dampak di mana musuh mencoba memanipulasi, menyela, atau menghancurkan data dalam lingkungan Anda. AWS Contohnya termasuk PutObject dan PutObjectAcl.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga untuk prinsipal terkait, ini mungkin menunjukkan bahwa kredensial telah diekspos atau izin S3 Anda tidak cukup membatasi. Untuk informasi selengkapnya, lihat [Memperbaiki bucket S3 yang berpotensi dikompromikan](#).

PenTest:S3/KaliLinux

API S3 dipanggil dari mesin Kali Linux.

Tingkat keparahan default: Sedang

- Sumber data: peristiwa CloudTrail data untuk S3

Temuan ini memberi tahu Anda bahwa mesin yang menjalankan Kali Linux melakukan panggilan API S3 menggunakan kredensial milik akun Anda. AWS Kredensial Anda mungkin disusupi. Kali Linux adalah alat pengujian penetrasi populer yang digunakan oleh para profesional keamanan untuk

mengidentifikasi kelemahan dalam EC2 kasus yang memerlukan penambalan. Penyerang juga menggunakan alat ini untuk menemukan kelemahan EC2 konfigurasi dan mendapatkan akses tidak sah ke lingkungan Anda. AWS

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga untuk prinsipal terkait, ini mungkin menunjukkan bahwa kredensial telah diekspos atau izin S3 Anda tidak cukup membatasi. Untuk informasi selengkapnya, lihat [Memperbaiki bucket S3 yang berpotensi dikompromikan](#).

PenTest:S3/ParrotLinux

API S3 dipanggil dari mesin Parrot Security Linux.

Tingkat keparahan default: Sedang

- Sumber data: peristiwa CloudTrail data untuk S3

Temuan ini memberi tahu Anda bahwa mesin yang menjalankan Parrot Security Linux melakukan panggilan API S3 menggunakan kredensial milik akun Anda. AWS Kredensial Anda mungkin disusupi. Parrot Security Linux adalah alat pengujian penetrasi populer yang digunakan para profesional keamanan untuk mengidentifikasi kelemahan dalam EC2 kasus yang memerlukan penambalan. Penyerang juga menggunakan alat ini untuk menemukan kelemahan EC2 konfigurasi dan mendapatkan akses tidak sah ke lingkungan Anda. AWS

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga untuk prinsipal terkait, ini mungkin menunjukkan bahwa kredensial telah diekspos atau izin S3 Anda tidak cukup membatasi. Untuk informasi selengkapnya, lihat [Memperbaiki bucket S3 yang berpotensi dikompromikan](#).

PenTest:S3/PentooLinux

API S3 dipanggil dari mesin Pentoo Linux.

Tingkat keparahan default: Sedang

- Sumber data: peristiwa CloudTrail data untuk S3

Temuan ini memberi tahu Anda bahwa mesin yang menjalankan Pentoo Linux melakukan panggilan API S3 menggunakan kredensial milik akun Anda. AWS Kredensial Anda mungkin disusupi. Pentoo Linux adalah alat pengujian penetrasi populer yang digunakan oleh para profesional keamanan untuk mengidentifikasi kelemahan dalam EC2 kasus yang memerlukan penambalan. Penyerang juga menggunakan alat ini untuk menemukan kelemahan EC2 konfigurasi dan mendapatkan akses tidak sah ke lingkungan Anda. AWS

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga untuk prinsipal terkait, ini mungkin menunjukkan bahwa kredensial telah diekspos atau izin S3 Anda tidak cukup membatasi. Untuk informasi selengkapnya, lihat [Memperbaiki bucket S3 yang berpotensi dikompromikan](#).

Policy:S3/AccountBlockPublicAccessDisabled

Entitas IAM memanggil API yang digunakan untuk menonaktifkan S3 Block Public Access pada akun.

Tingkat keparahan default: Rendah

- Sumber data: acara CloudTrail manajemen

Temuan ini menginformasikan bahwa Blokir Akses Publik Amazon S3 dinonaktifkan pada tingkat akun. Ketika pengaturan Akses Publik Blok S3 diaktifkan, pengaturan tersebut digunakan untuk memfilter kebijakan atau daftar kontrol akses (ACLs) pada bucket sebagai langkah keamanan untuk mencegah paparan data publik yang tidak disengaja.

Biasanya, Blokir Akses Umum S3 dinonaktifkan pada akun untuk memungkinkan akses publik ke bucket atau ke objek dalam bucket. Saat S3 Block Public Access dinonaktifkan untuk sebuah akun, akses ke bucket Anda dikontrol oleh kebijakan ACLs, atau setelah Blokir Akses Publik tingkat ember yang diterapkan ke bucket individual Anda. Ini tidak berarti bahwa bucket dibagikan secara publik, tetapi bahwa Anda harus mengaudit izin yang diterapkan ke bucket untuk mengonfirmasi bahwa mereka menyediakan tingkat akses yang sesuai.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga untuk prinsipal terkait, ini mungkin menunjukkan bahwa kredensial telah diekspos atau izin S3 Anda tidak cukup membatasi. Untuk informasi selengkapnya, lihat [Memperbaiki bucket S3 yang berpotensi dikompromikan](#).

Policy:S3/BucketAnonymousAccessGranted

Prinsipal IAM telah memberikan akses ke bucket S3 ke internet dengan mengubah kebijakan bucket atau ACLs

Tingkat keparahan default: Tinggi

- Sumber data: acara CloudTrail manajemen

Temuan ini menginformasikan bahwa bucket S3 yang terdaftar telah dibuat agar dapat diakses secara publik di internet karena entitas IAM telah mengubah kebijakan bucket atau ACL pada bucket tersebut.

Setelah kebijakan atau perubahan ACL terdeteksi, GuardDuty gunakan penalaran otomatis yang didukung oleh [Zelkova](#), untuk menentukan apakah bucket dapat diakses publik.

Note

Jika kebijakan bucket ACLs atau bucket dikonfigurasi untuk secara eksplisit menolak atau menolak semuanya, temuan ini mungkin tidak mencerminkan status bucket saat ini. Temuan ini tidak akan mencerminkan pengaturan [Akses Publik Blok S3](#) yang mungkin telah diaktifkan untuk bucket S3 Anda. Dalam kasus seperti itu, effectivePermission nilai dalam temuan akan ditandai sebagai UNKNOWN.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga untuk prinsipal terkait, ini mungkin menunjukkan bahwa kredensial telah diekspos atau izin S3 Anda tidak cukup membatasi. Untuk informasi selengkapnya, lihat [Memperbaiki bucket S3 yang berpotensi dikompromikan](#).

Policy:S3/BucketBlockPublicAccessDisabled

Entitas IAM memanggil API yang digunakan untuk menonaktifkan S3 Block Public Access pada bucket.

Tingkat keparahan default: Rendah

- Sumber data: acara CloudTrail manajemen

Temuan ini menginformasikan bahwa Blokir Akses Publik dinonaktifkan untuk bucket S3 yang terdaftar. Saat diaktifkan, setelan Akses Publik Blok S3 digunakan untuk memfilter kebijakan atau daftar kontrol akses (ACLs) yang diterapkan ke bucket sebagai langkah keamanan untuk mencegah paparan data publik yang tidak disengaja.

Biasanya, Blokir Akses Publik S3 dinonaktifkan pada bucket untuk memungkinkan akses publik ke bucket atau ke objek di dalamnya. Jika S3 Block Public Access dinonaktifkan untuk bucket, akses ke bucket dikontrol oleh kebijakan atau ACLs diterapkan padanya. Ini tidak berarti bahwa bucket dibagikan secara publik, tetapi Anda harus mengaudit kebijakan dan ACLs diterapkan ke bucket untuk mengonfirmasi bahwa izin yang sesuai diterapkan.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga untuk prinsipal terkait, ini mungkin menunjukkan bahwa kredensial telah diekspos atau izin S3 Anda tidak cukup membatasi. Untuk informasi selengkapnya, lihat [Memperbaiki bucket S3 yang berpotensi dikompromikan](#).

Policy:S3/BucketPublicAccessGranted

Prinsipal IAM telah memberikan akses publik ke bucket S3 kepada semua AWS pengguna dengan mengubah kebijakan bucket atau ACLs

Tingkat keparahan default: Tinggi

- Sumber data: acara CloudTrail manajemen

Temuan ini memberi tahu Anda bahwa bucket S3 yang terdaftar telah diekspos secara publik ke semua AWS pengguna yang diautentikasi karena entitas IAM telah mengubah kebijakan bucket atau ACL pada bucket S3 tersebut.

Setelah kebijakan atau perubahan ACL terdeteksi, GuardDuty gunakan penalaran otomatis yang didukung oleh [Zelkova](#), untuk menentukan apakah bucket dapat diakses publik.

 Note

Jika kebijakan bucket ACLs atau bucket dikonfigurasi untuk secara eksplisit menolak atau menolak semuanya, temuan ini mungkin tidak mencerminkan status bucket saat ini. Temuan ini tidak akan mencerminkan pengaturan [Akses Publik Blok S3](#) yang mungkin telah diaktifkan untuk bucket S3 Anda. Dalam kasus seperti itu, `effectivePermission` nilai dalam temuan akan ditandai sebagai `UNKNOWN`.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga untuk prinsipal terkait, ini mungkin menunjukkan bahwa kredensial telah diekspos atau izin S3 Anda tidak cukup membatasi. Untuk informasi selengkapnya, lihat [Memperbaiki bucket S3 yang berpotensi dikompromikan](#).

Stealth:S3/ServerAccessLoggingDisabled

Pencatatan log akses server S3 dinonaktifkan untuk bucket.

Tingkat keparahan default: Rendah

- Sumber data: acara CloudTrail manajemen

Temuan ini memberi tahu Anda bahwa pencatatan akses server S3 dinonaktifkan untuk ember di lingkungan Anda AWS . Jika dinonaktifkan, tidak ada log permintaan web yang dibuat untuk setiap upaya mengakses bucket S3 yang diidentifikasi, namun, panggilan API manajemen S3 ke bucket, seperti [DeleteBucket](#), masih dilacak. Jika pencatatan peristiwa data S3 diaktifkan CloudTrail untuk bucket ini, permintaan web untuk objek di dalam bucket akan tetap dilacak. Menonaktifkan pencatatan log adalah teknik yang digunakan oleh pengguna yang tidak sah untuk menghindari deteksi. Untuk mempelajari selengkapnya tentang log S3, lihat [Pencatatan Log Akses Server S3](#) dan [Opsis Pencatatan Log S3](#).

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga untuk prinsipal terkait, ini mungkin menunjukkan bahwa kredensial telah diekspos atau izin S3 Anda tidak cukup membatasi. Untuk informasi selengkapnya, lihat [Memperbaiki bucket S3 yang berpotensi dikompromikan](#).

UnauthorizedAccess:S3/MaliciousIPCaller.Custom

API S3 dipanggil dari alamat IP yang termasuk dalam daftar ancaman kustom.

Tingkat keparahan default: Tinggi

- Sumber data: peristiwa CloudTrail data untuk S3

Temuan ini menginformasikan bahwa operasi API S3, seperti PutObject atau PutObjectAcl, dipanggil dari alamat IP yang termasuk dalam daftar ancaman yang Anda unggah. Daftar ancaman yang terkait dengan temuan ini tercantum di bagian Informasi tambahan dari detail temuan ini.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga untuk prinsipal terkait, ini mungkin menunjukkan bahwa kredensial telah diekspos atau izin S3 Anda tidak cukup membatasi. Untuk informasi selengkapnya, lihat [Memperbaiki bucket S3 yang berpotensi dikompromikan](#).

UnauthorizedAccess:S3/TorIPCaller

API S3 dipanggil dari alamat IP node keluar Tor.

Tingkat keparahan default: Tinggi

- Sumber data: peristiwa CloudTrail data untuk S3

Temuan ini menginformasikan bahwa operasi API S3, seperti PutObject atau PutObjectAcl, dipanggil dari alamat IP node keluar Tor. Tor adalah perangkat lunak yang memungkinkan komunikasi anonim. Ini mengenkripsi dan secara acak mengalihkan komunikasi melalui relay antara serangkaian node jaringan. Node Tor terakhir disebut sebagai nod keluar. Temuan ini dapat menunjukkan akses tidak sah ke AWS sumber daya Anda dengan maksud menyembunyikan identitas asli penyerang.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga untuk prinsipal terkait, ini mungkin menunjukkan bahwa kredensial telah diekspos atau izin S3 Anda tidak cukup membatasi. Lihat informasi yang lebih lengkap di [Memperbaiki bucket S3 yang berpotensi dikompromikan](#).

Jenis penemuan Perlindungan EKS

Temuan berikut khusus untuk sumber daya Amazon EKS dan memiliki `resource_type`. `EKSCluster` Tingkat keparahan dan detail temuan berbeda berdasarkan jenis temuan.

Untuk semua temuan jenis log audit EKS, kami sarankan Anda memeriksa sumber daya yang dimaksud untuk menentukan apakah aktivitas tersebut diharapkan atau berpotensi berbahaya. Untuk panduan tentang memulihkan sumber daya log audit EKS yang dikompromikan yang diidentifikasi oleh GuardDuty temuan, lihat. [Remediasi temuan Perlindungan EKS](#)

Note

Jika aktivitas yang menghasilkan temuan ini diharapkan, pertimbangkan [Aturan penindasan di GuardDuty](#) untuk menambahkan untuk mencegah peringatan di masa depan.

Topik

- [CredentialAccess:Kubernetes/MaliciousIPCaller](#)
- [CredentialAccess:Kubernetes/MaliciousIPCaller.Custom](#)
- [CredentialAccess:Kubernetes/SuccessfulAnonymousAccess](#)
- [CredentialAccess:Kubernetes/TorIPCaller](#)
- [DefenseEvasion:Kubernetes/MaliciousIPCaller](#)
- [DefenseEvasion:Kubernetes/MaliciousIPCaller.Custom](#)
- [DefenseEvasion:Kubernetes/SuccessfulAnonymousAccess](#)
- [DefenseEvasion:Kubernetes/TorIPCaller](#)
- [Discovery:Kubernetes/MaliciousIPCaller](#)
- [Discovery:Kubernetes/MaliciousIPCaller.Custom](#)
- [Discovery:Kubernetes/SuccessfulAnonymousAccess](#)
- [Discovery:Kubernetes/TorIPCaller](#)
- [Execution:Kubernetes/ExecInKubeSystemPod](#)
- [Impact:Kubernetes/MaliciousIPCaller](#)
- [Impact:Kubernetes/MaliciousIPCaller.Custom](#)

- [Impact:Kubernetes/SuccessfulAnonymousAccess](#)
- [Impact:Kubernetes/TorIPCaller](#)
- [Persistence:Kubernetes/ContainerWithSensitiveMount](#)
- [Persistence:Kubernetes/MaliciousIPCaller](#)
- [Persistence:Kubernetes/MaliciousIPCaller.Custom](#)
- [Persistence:Kubernetes/SuccessfulAnonymousAccess](#)
- [Persistence:Kubernetes/TorIPCaller](#)
- [Policy:Kubernetes/AdminAccessToDefaultServiceAccount](#)
- [Policy:Kubernetes/AnonymousAccessGranted](#)
- [Policy:Kubernetes/ExposedDashboard](#)
- [Policy:Kubernetes/KubeflowDashboardExposed](#)
- [PrivilegeEscalation:Kubernetes/PrivilegedContainer](#)
- [CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed](#)
- [PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated](#)
- [Execution:Kubernetes/AnomalousBehavior.ExecInPod](#)
- [PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer](#)
- [Persistence:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount](#)
- [Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed](#)
- [PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated](#)
- [Discovery:Kubernetes/AnomalousBehavior.PermissionChecked](#)

Note

Sebelum Kubernetes versi 1.14, `system:unauthenticated` grup ini dikaitkan dengan dan secara default. `system:discovery` `system:basic-user` ClusterRoles Asosiasi ini memungkinkan akses yang tidak diinginkan dari pengguna anonim. Pembaruan cluster tidak mencabut izin ini. Bahkan jika Anda memperbarui klaster Anda ke versi 1.14 atau lebih tinggi, izin ini mungkin masih diaktifkan. Kami menyarankan Anda untuk memisahkan izin ini dari grup. `system:unauthenticated` Untuk panduan tentang mencabut izin ini, lihat [Praktik terbaik keamanan untuk Amazon EKS](#) di Panduan Pengguna Amazon EKS.

CredentialAccess:Kubernetes/MaliciousIPCaller

API yang biasa digunakan untuk mengakses kredensi atau rahasia di klaster Kubernetes dipanggil dari alamat IP berbahaya yang diketahui.

Tingkat keparahan default: Tinggi

- Fitur: Log audit EKS

Temuan ini memberi tahu Anda bahwa operasi API dipanggil dari alamat IP yang terkait dengan aktivitas berbahaya yang diketahui. API yang diamati umumnya dikaitkan dengan taktik akses kredensial di mana musuh mencoba mengumpulkan kata sandi, nama pengguna, dan kunci akses untuk klaster Kubernetes Anda.

Rekomendasi remediasi:

Jika pengguna yang dilaporkan dalam temuan di bawah *KubernetesUserDetails* bagian ini adalah `system:anonymous`, selidiki mengapa pengguna anonim diizinkan untuk memanggil API dan mencabut izin, jika diperlukan, dengan mengikuti petunjuk dalam [Praktik terbaik Keamanan untuk Amazon EKS di Panduan Pengguna Amazon EKS](#). Jika pengguna adalah pengguna yang diautentikasi, selidiki untuk menentukan apakah aktivitas tersebut sah atau berbahaya. Jika aktivitas berbahaya, cabut akses pengguna dan balikkan perubahan apa pun yang dibuat oleh musuh ke klaster Anda. Untuk informasi selengkapnya, lihat [Remediasi temuan Perlindungan EKS](#).

CredentialAccess:Kubernetes/MaliciousIPCaller.Custom

API yang biasa digunakan untuk mengakses kredensi atau rahasia di klaster Kubernetes dipanggil dari alamat IP pada daftar ancaman kustom.

Tingkat keparahan default: Tinggi

- Fitur: Log audit EKS

Temuan ini memberi tahu Anda bahwa operasi API dipanggil dari alamat IP yang disertakan dalam daftar ancaman yang Anda unggah. Daftar ancaman yang terkait dengan temuan ini tercantum di bagian Informasi Tambahan dari detail temuan. API yang diamati umumnya dikaitkan dengan taktik

akses kredensial di mana musuh mencoba mengumpulkan kata sandi, nama pengguna, dan kunci akses untuk kluster Kubernetes Anda.

Rekomendasi remediasi:

Jika pengguna yang dilaporkan dalam temuan di bawah *KubernetesUserDetails* bagian ini adalah `system:anonymous`, selidiki mengapa pengguna anonim diizinkan untuk memanggil API dan mencabut izin, jika diperlukan, dengan mengikuti petunjuk dalam [Praktik terbaik Keamanan untuk Amazon EKS di Panduan Pengguna Amazon EKS](#). Jika pengguna adalah pengguna yang diautentikasi, selidiki untuk menentukan apakah aktivitas tersebut sah atau berbahaya. Jika aktivitas berbahaya, cabut akses pengguna dan balikkan perubahan apa pun yang dibuat oleh musuh ke kluster Anda. Untuk informasi selengkapnya, lihat [Remediasi temuan Perlindungan EKS](#).

CredentialAccess:Kubernetes/SuccessfulAnonymousAccess

API yang biasa digunakan untuk mengakses kredensial atau rahasia di kluster Kubernetes dipanggil oleh pengguna yang tidak diautentikasi.

Tingkat keparahan default: Tinggi

- Fitur: Log audit EKS

Temuan ini memberi tahu Anda bahwa operasi API berhasil dipanggil oleh pengguna `system:anonymous`. Panggilan API yang dibuat oleh `system:anonymous` tidak diautentikasi. API yang diamati biasanya dikaitkan dengan taktik akses kredensial di mana musuh mencoba mengumpulkan kata sandi, nama pengguna, dan kunci akses untuk kluster Kubernetes Anda. Aktivitas ini menunjukkan bahwa akses anonim atau tidak diautentikasi diizinkan pada tindakan API yang dilaporkan dalam temuan dan mungkin diizinkan pada tindakan lain. Jika perilaku ini tidak diharapkan, ini mungkin menunjukkan kesalahan konfigurasi atau kredensial Anda dikompromikan.

Rekomendasi remediasi:

Anda harus memeriksa izin yang telah diberikan kepada `system:anonymous` pengguna di kluster Anda dan memastikan bahwa semua izin diperlukan. Jika izin diberikan secara keliru atau jahat, Anda harus mencabut akses pengguna dan membalikkan setiap perubahan yang dibuat oleh musuh ke kluster Anda. Untuk informasi selengkapnya, lihat [Praktik terbaik keamanan untuk Amazon EKS di Panduan Pengguna Amazon EKS](#).

Untuk informasi selengkapnya, lihat [Remediasi temuan Perlindungan EKS](#).

CredentialAccess:Kubernetes/TorIPCaller

API yang biasa digunakan untuk mengakses kredensi atau rahasia di kluster Kubernetes dipanggil dari alamat IP node keluar Tor.

Tingkat keparahan default: Tinggi

- Fitur: Log audit EKS

Temuan ini memberi tahu Anda bahwa API dipanggil dari alamat IP node keluar Tor. API yang diamati umumnya dikaitkan dengan taktik akses kredensial di mana musuh mencoba mengumpulkan kata sandi, nama pengguna, dan kunci akses untuk kluster Kubernetes Anda. Tor adalah perangkat lunak untuk memungkinkan komunikasi anonim. Ini mengenkripsi dan secara acak mengalihkan komunikasi melalui relay antara serangkaian node jaringan. Node Tor terakhir disebut sebagai node keluar. Hal ini dapat menunjukkan akses tidak sah ke sumber daya kluster Kubernetes Anda dengan maksud menyembunyikan identitas asli penyerang.

Rekomendasi remediasi:

Jika pengguna yang dilaporkan dalam temuan di bawah *KubernetesUserDetails* bagian ini adalah `system:anonymous`, selidiki mengapa pengguna anonim diizinkan untuk memanggil API dan mencabut izin, jika diperlukan, dengan mengikuti petunjuk dalam [Praktik terbaik Keamanan untuk Amazon EKS di Panduan Pengguna Amazon EKS](#). Jika pengguna adalah pengguna yang diautentikasi, selidiki untuk menentukan apakah aktivitas tersebut sah atau berbahaya. Jika aktivitas berbahaya, cabut akses pengguna dan balikkan perubahan apa pun yang dibuat oleh musuh ke kluster Anda. Untuk informasi selengkapnya, lihat [Remediasi temuan Perlindungan EKS](#).

DefenseEvasion:Kubernetes/MaliciousIPCaller

API yang biasa digunakan untuk menghindari tindakan defensif dipanggil dari alamat IP berbahaya yang diketahui.

Tingkat keparahan default: Tinggi

- Fitur: Log audit EKS

Temuan ini memberi tahu Anda bahwa operasi API dipanggil dari alamat IP yang terkait dengan aktivitas berbahaya yang diketahui. API yang diamati umumnya dikaitkan dengan taktik penghindaran pertahanan di mana musuh mencoba menyembunyikan tindakan mereka untuk menghindari deteksi.

Rekomendasi remediasi:

Jika pengguna yang dilaporkan dalam temuan di bawah *KubernetesUserDetails* bagian ini adalah *system:anonymous*, selidiki mengapa pengguna anonim diizinkan untuk memanggil API dan mencabut izin, jika diperlukan, dengan mengikuti petunjuk dalam [Praktik terbaik Keamanan untuk Amazon EKS di Panduan Pengguna Amazon](#) EKS. Jika pengguna adalah pengguna yang diautentikasi, selidiki untuk menentukan apakah aktivitas tersebut sah atau berbahaya. Jika aktivitas berbahaya, cabut akses pengguna dan balikkan perubahan apa pun yang dibuat oleh musuh ke kluster Anda. Untuk informasi selengkapnya, lihat [Remediasi temuan Perlindungan EKS](#).

DefenseEvasion:Kubernetes/MaliciousIPCaller.Custom

API yang biasa digunakan untuk menghindari tindakan defensif dipanggil dari alamat IP pada daftar ancaman khusus.

Tingkat keparahan default: Tinggi

- Fitur: Log audit EKS

Temuan ini memberi tahu Anda bahwa operasi API dipanggil dari alamat IP yang disertakan dalam daftar ancaman yang Anda unggah. Daftar ancaman yang terkait dengan temuan ini tercantum di bagian Informasi Tambahan dari detail temuan. API yang diamati umumnya dikaitkan dengan taktik penghindaran pertahanan di mana musuh mencoba menyembunyikan tindakan mereka untuk menghindari deteksi.

Rekomendasi remediasi:

Jika pengguna yang dilaporkan dalam temuan di bawah *KubernetesUserDetails* bagian ini adalah *system:anonymous*, selidiki mengapa pengguna anonim diizinkan untuk memanggil API dan mencabut izin, jika diperlukan, dengan mengikuti petunjuk dalam [Praktik terbaik Keamanan untuk Amazon EKS di Panduan Pengguna Amazon](#) EKS. Jika pengguna adalah pengguna yang diautentikasi, selidiki untuk menentukan apakah aktivitas tersebut sah atau berbahaya. Jika aktivitas berbahaya, cabut akses pengguna dan balikkan perubahan apa pun yang dibuat oleh musuh ke kluster Anda. Untuk informasi selengkapnya, lihat [Remediasi temuan Perlindungan EKS](#).

DefenseEvasion:Kubernetes/SuccessfulAnonymousAccess

API yang biasa digunakan untuk menghindari tindakan defensif dipanggil oleh pengguna yang tidak diautentikasi.

Tingkat keparahan default: Tinggi

- Fitur: Log audit EKS

Temuan ini memberi tahu Anda bahwa operasi API berhasil dipanggil oleh pengguna. `system:anonymous` Panggilan API yang dibuat oleh tidak `system:anonymous` diautentikasi. API yang diamati umumnya dikaitkan dengan taktik penghindaran pertahanan di mana musuh mencoba menyembunyikan tindakan mereka untuk menghindari deteksi. Aktivitas ini menunjukkan bahwa akses anonim atau tidak diautentikasi diizinkan pada tindakan API yang dilaporkan dalam temuan dan mungkin diizinkan pada tindakan lain. Jika perilaku ini tidak diharapkan, ini mungkin menunjukkan kesalahan konfigurasi atau kredensial Anda dikompromikan.

Rekomendasi remediasi:

Anda harus memeriksa izin yang telah diberikan kepada `system:anonymous` pengguna di kluster Anda dan memastikan bahwa semua izin diperlukan. Jika izin diberikan secara keliru atau jahat, Anda harus mencabut akses pengguna dan membalikkan setiap perubahan yang dibuat oleh musuh ke kluster Anda. Untuk informasi selengkapnya, lihat [Praktik terbaik keamanan untuk Amazon EKS](#) di Panduan Pengguna Amazon EKS.

Untuk informasi selengkapnya, lihat [Remediasi temuan Perlindungan EKS](#).

DefenseEvasion:Kubernetes/TorIPCaller

API yang biasa digunakan untuk menghindari tindakan defensif dipanggil dari alamat IP node keluar Tor.

Tingkat keparahan default: Tinggi

- Fitur: Log audit EKS

Temuan ini memberi tahu Anda bahwa API dipanggil dari alamat IP node keluar Tor. API yang diamati umumnya dikaitkan dengan taktik penghindaran pertahanan di mana musuh mencoba

menyembunyikan tindakan mereka untuk menghindari deteksi. Tor adalah perangkat lunak untuk memungkinkan komunikasi anonim. Ini mengenkripsi dan secara acak mengalihkan komunikasi melalui relay antara serangkaian node jaringan. Node Tor terakhir disebut sebagai nod keluar. Hal ini dapat menunjukkan akses tidak sah ke klaster Kubernetes Anda dengan maksud menyembunyikan identitas asli musuh.

Rekomendasi remediasi:

Jika pengguna yang dilaporkan dalam temuan di bawah *KubernetesUserDetails* bagian ini adalah `system:anonymous`, selidiki mengapa pengguna anonim diizinkan untuk memanggil API dan mencabut izin, jika diperlukan, dengan mengikuti petunjuk dalam [Praktik terbaik Keamanan untuk Amazon EKS di Panduan Pengguna Amazon EKS](#). Jika pengguna adalah pengguna yang diautentikasi, selidiki untuk menentukan apakah aktivitas tersebut sah atau berbahaya. Jika aktivitas berbahaya, cabut akses pengguna dan balikkan perubahan apa pun yang dibuat oleh musuh ke klaster Anda. Untuk informasi selengkapnya, lihat [Remediasi temuan Perlindungan EKS](#).

Discovery:Kubernetes/MaliciousIPCaller

API yang biasa digunakan untuk menemukan sumber daya di klaster Kubernetes dipanggil dari alamat IP.

Tingkat keparahan default: Sedang

- Fitur: Log audit EKS

Temuan ini memberi tahu Anda bahwa operasi API dipanggil dari alamat IP yang terkait dengan aktivitas berbahaya yang diketahui. API yang diamati biasanya digunakan dengan tahap penemuan serangan di mana penyerang mengumpulkan informasi untuk menentukan apakah cluster Kubernetes Anda rentan terhadap serangan yang lebih luas.

Untuk akses yang tidak diautentikasi

MaliciousIPCaller temuan tidak dihasilkan untuk akses yang tidak diautentikasi.

SuccessfulAnonymousAccess Temuan dihasilkan untuk akses yang tidak diautentikasi atau anonim.

Rekomendasi remediasi:

Jika pengguna yang dilaporkan dalam temuan di bawah *KubernetesUserDetails* bagian ini adalah *system:anonymous*, selidiki mengapa pengguna anonim diizinkan untuk memanggil API dan mencabut izin, jika diperlukan, dengan mengikuti petunjuk dalam [Praktik terbaik Keamanan untuk Amazon EKS di Panduan Pengguna Amazon EKS](#). Jika pengguna adalah pengguna yang diautentikasi, selidiki untuk menentukan apakah aktivitas tersebut sah atau berbahaya. Jika aktivitas berbahaya, cabut akses pengguna dan balikkan perubahan apa pun yang dibuat oleh musuh ke klaster Anda. Untuk informasi selengkapnya, lihat [Remediasi temuan Perlindungan EKS](#).

Discovery:Kubernetes/MaliciousIPCaller.Custom

API yang biasa digunakan untuk menemukan sumber daya di klaster Kubernetes dipanggil dari alamat IP pada daftar ancaman khusus.

Tingkat keparahan default: Sedang

- Fitur: Log audit EKS

Temuan ini memberi tahu Anda bahwa API dipanggil dari alamat IP yang disertakan dalam daftar ancaman yang Anda unggah. Daftar ancaman yang terkait dengan temuan ini tercantum di bagian Informasi Tambahan dari detail temuan. API yang diamati biasanya digunakan dengan tahap penemuan serangan di mana penyerang mengumpulkan informasi untuk menentukan apakah cluster Kubernetes Anda rentan terhadap serangan yang lebih luas.

Rekomendasi remediasi:

Jika pengguna yang dilaporkan dalam temuan di bawah *KubernetesUserDetails* bagian ini adalah *system:anonymous*, selidiki mengapa pengguna anonim diizinkan untuk memanggil API dan mencabut izin, jika diperlukan, dengan mengikuti petunjuk dalam [Praktik terbaik Keamanan untuk Amazon EKS di Panduan Pengguna Amazon EKS](#). Jika pengguna adalah pengguna yang diautentikasi, selidiki untuk menentukan apakah aktivitas tersebut sah atau berbahaya. Jika aktivitas berbahaya, cabut akses pengguna dan balikkan perubahan apa pun yang dibuat oleh musuh ke klaster Anda. Untuk informasi selengkapnya, lihat [Remediasi temuan Perlindungan EKS](#).

Discovery:Kubernetes/SuccessfulAnonymousAccess

API yang biasa digunakan untuk menemukan sumber daya di klaster Kubernetes dipanggil oleh pengguna yang tidak diautentikasi.

Tingkat keparahan default: Sedang

- Fitur: Log audit EKS

Temuan ini memberi tahu Anda bahwa operasi API berhasil dipanggil oleh pengguna. `system:anonymous` Panggilan API yang dibuat oleh `system:anonymous` diautentikasi. API yang diamati biasanya dikaitkan dengan tahap penemuan serangan ketika musuh mengumpulkan informasi di cluster Kubernetes Anda. Aktivitas ini menunjukkan bahwa akses anonim atau tidak diautentikasi diizinkan pada tindakan API yang dilaporkan dalam temuan dan mungkin diizinkan pada tindakan lain. Jika perilaku ini tidak diharapkan, ini mungkin menunjukkan kesalahan konfigurasi atau kredensial Anda dikompromikan.

Jenis temuan ini mengecualikan titik akhir API pemeriksaan kesehatan seperti `/healthz`, `/livez/readyz`, dan `/version`

Rekomendasi remediasi:

Anda harus memeriksa izin yang telah diberikan kepada `system:anonymous` pengguna di klaster Anda dan memastikan bahwa semua izin diperlukan. Jika izin diberikan secara keliru atau jahat, Anda harus mencabut akses pengguna dan membalikkan setiap perubahan yang dibuat oleh musuh ke klaster Anda. Untuk informasi selengkapnya, lihat [Praktik terbaik keamanan untuk Amazon EKS](#) di Panduan Pengguna Amazon EKS.

Untuk informasi selengkapnya, lihat [Remediasi temuan Perlindungan EKS](#).

Discovery:Kubernetes/TorIPCaller

API yang biasa digunakan untuk menemukan sumber daya dalam klaster Kubernetes dipanggil dari alamat IP node keluar Tor.

Tingkat keparahan default: Sedang

- Fitur: Log audit EKS

Temuan ini memberi tahu Anda bahwa API dipanggil dari alamat IP node keluar Tor. API yang diamati biasanya digunakan dengan tahap penemuan serangan di mana penyerang mengumpulkan informasi untuk menentukan apakah cluster Kubernetes Anda rentan terhadap serangan yang lebih luas. Tor adalah perangkat lunak untuk memungkinkan komunikasi anonim. Ini mengenkripsi dan

secara acak mengalihkan komunikasi melalui relay antara serangkaian node jaringan. Node Tor terakhir disebut sebagai nod keluar. Hal ini dapat menunjukkan akses tidak sah ke klaster Kubernetes Anda dengan maksud menyembunyikan identitas asli musuh.

Rekomendasi remediasi:

Jika pengguna yang dilaporkan dalam temuan di bawah *KubernetesUserDetails* bagian ini adalah `system:anonymous`, selidiki mengapa pengguna anonim diizinkan untuk memanggil API dan pencabutan izin, jika diperlukan, dengan mengikuti petunjuk dalam [Praktik terbaik Keamanan untuk Amazon EKS di Panduan Pengguna Amazon EKS](#). Jika pengguna adalah pengguna yang diautentikasi, selidiki untuk menentukan apakah aktivitas tersebut sah atau berbahaya. Jika aktivitas berbahaya, cabut akses pengguna dan balikkan perubahan apa pun yang dibuat oleh musuh ke klaster Anda. Untuk informasi selengkapnya, lihat [Remediasi temuan Perlindungan EKS](#).

Execution:Kubernetes/ExecInKubeSystemPod

Sebuah perintah dieksekusi di dalam pod di dalam **kube-system** namespace

Tingkat keparahan default: Sedang

- Fitur: Log audit EKS

Temuan ini memberi tahu Anda bahwa sebuah perintah telah dijalankan di sebuah pod di dalam kube-system namespace menggunakan Kubernetes exec API. kube-system namespace adalah ruang nama default, yang terutama digunakan untuk komponen tingkat sistem seperti kube-dns kube-proxy. Sangat jarang untuk mengeksekusi perintah di dalam pod atau kontainer di bawah kube-system namespace dan mungkin menunjukkan aktivitas yang mencurigakan.

Rekomendasi remediasi:

Jika eksekusi perintah ini tidak terduga, kredensi identitas pengguna yang digunakan untuk menjalankan perintah dapat dikompromikan. Cabut akses pengguna dan balikkan perubahan apa pun yang dibuat oleh musuh ke klaster Anda. Untuk informasi selengkapnya, lihat [Remediasi temuan Perlindungan EKS](#).

Impact:Kubernetes/MaliciousIPCaller

API yang biasa digunakan untuk mengutak-atik sumber daya di klaster Kubernetes dipanggil dari alamat IP berbahaya yang diketahui.

Tingkat keparahan default: Tinggi

- Fitur: Log audit EKS

Temuan ini memberi tahu Anda bahwa operasi API dipanggil dari alamat IP yang terkait dengan aktivitas berbahaya yang diketahui. API yang diamati umumnya dikaitkan dengan taktik dampak di mana musuh mencoba memanipulasi, mengganggu, atau menghancurkan data dalam lingkungan Anda. AWS

Rekomendasi remediasi:

Jika pengguna yang dilaporkan dalam temuan di bawah *KubernetesUserDetails* bagian ini adalah *system:anonymous*, selidiki mengapa pengguna anonim diizinkan untuk memanggil API dan mencabut izin, jika diperlukan, dengan mengikuti petunjuk dalam [Praktik terbaik Keamanan untuk Amazon EKS di Panduan Pengguna Amazon EKS](#). Jika pengguna adalah pengguna yang diautentikasi, selidiki untuk menentukan apakah aktivitas tersebut sah atau berbahaya. Jika aktivitas berbahaya, cabut akses pengguna dan balikkan perubahan apa pun yang dibuat oleh musuh ke kluster Anda. Untuk informasi selengkapnya, lihat [Remediasi temuan Perlindungan EKS](#).

Impact:Kubernetes/MaliciousIPCaller.Custom

API yang biasa digunakan untuk mengutak-atik sumber daya di kluster Kubernetes dipanggil dari alamat IP pada daftar ancaman khusus.

Tingkat keparahan default: Tinggi

- Fitur: Log audit EKS

Temuan ini memberi tahu Anda bahwa operasi API dipanggil dari alamat IP yang disertakan dalam daftar ancaman yang Anda unggah. Daftar ancaman yang terkait dengan temuan ini tercantum di bagian Informasi Tambahan dari detail temuan. API yang diamati umumnya dikaitkan dengan taktik dampak di mana musuh mencoba memanipulasi, mengganggu, atau menghancurkan data dalam lingkungan Anda. AWS

Rekomendasi remediasi:

Jika pengguna yang dilaporkan dalam temuan di bawah *KubernetesUserDetails* bagian ini adalah *system:anonymous*, selidiki mengapa pengguna anonim diizinkan untuk memanggil API

dan mencabut izin, jika diperlukan, dengan mengikuti petunjuk dalam [Praktik terbaik Keamanan untuk Amazon EKS di Panduan Pengguna Amazon EKS](#). Jika pengguna adalah pengguna yang diautentikasi, selidiki untuk menentukan apakah aktivitas tersebut sah atau berbahaya. Jika aktivitas berbahaya, cabut akses pengguna dan balikkan perubahan apa pun yang dibuat oleh musuh ke kluster Anda. Untuk informasi selengkapnya, lihat [Remediasi temuan Perlindungan EKS](#).

Impact:Kubernetes/SuccessfulAnonymousAccess

API yang biasa digunakan untuk mengutak-atik sumber daya di kluster Kubernetes dipanggil oleh pengguna yang tidak diautentikasi.

Tingkat keparahan default: Tinggi

- Fitur: Log audit EKS

Temuan ini memberi tahu Anda bahwa operasi API berhasil dipanggil oleh pengguna. `system:anonymous` Panggilan API yang dibuat oleh tidak `system:anonymous` diautentikasi. API yang diamati umumnya dikaitkan dengan tahap dampak serangan saat musuh merusak sumber daya di cluster Anda. Aktivitas ini menunjukkan bahwa akses anonim atau tidak diautentikasi diizinkan pada tindakan API yang dilaporkan dalam temuan dan mungkin diizinkan pada tindakan lain. Jika perilaku ini tidak diharapkan, ini mungkin menunjukkan kesalahan konfigurasi atau kredensial Anda dikompromikan.

Rekomendasi remediasi:

Anda harus memeriksa izin yang telah diberikan kepada `system:anonymous` pengguna di kluster Anda dan memastikan bahwa semua izin diperlukan. Jika izin diberikan secara keliru atau jahat, Anda harus mencabut akses pengguna dan membalikkan setiap perubahan yang dibuat oleh musuh ke kluster Anda. Untuk informasi selengkapnya, lihat [Praktik terbaik keamanan untuk Amazon EKS](#) di Panduan Pengguna Amazon EKS.

Untuk informasi selengkapnya, lihat [Remediasi temuan Perlindungan EKS](#).

Impact:Kubernetes/TorIPCaller

API yang biasa digunakan untuk mengutak-atik sumber daya di kluster Kubernetes dipanggil dari alamat IP node keluar Tor.

Tingkat keparahan default: Tinggi

- Fitur: Log audit EKS

Temuan ini memberi tahu Anda bahwa API dipanggil dari alamat IP node keluar Tor. API yang diamati umumnya dikaitkan dengan taktik dampak di mana musuh mencoba memanipulasi, mengganggu, atau menghancurkan data dalam lingkungan Anda. AWS Tor adalah perangkat lunak untuk memungkinkan komunikasi anonim. Ini mengenkripsi dan secara acak mengalihkan komunikasi melalui relay antara serangkaian node jaringan. Node Tor terakhir disebut sebagai nod keluar. Hal ini dapat menunjukkan akses tidak sah ke kluster Kubernetes Anda dengan maksud menyembunyikan identitas asli musuh.

Rekomendasi remediasi:

Jika pengguna yang dilaporkan dalam temuan di bawah *KubernetesUserDetails* bagian ini adalah `system:anonymous`, selidiki mengapa pengguna anonim diizinkan untuk memanggil API dan mencabut izin, jika diperlukan, dengan mengikuti petunjuk dalam [Praktik terbaik Keamanan untuk Amazon EKS di Panduan Pengguna Amazon EKS](#). Jika pengguna adalah pengguna yang diautentikasi, selidiki untuk menentukan apakah aktivitas tersebut sah atau berbahaya. Jika aktivitas berbahaya, cabut akses pengguna dan balikkan perubahan apa pun yang dibuat oleh musuh ke kluster Anda. Untuk informasi selengkapnya, lihat [Remediasi temuan Perlindungan EKS](#).

Persistence:Kubernetes/ContainerWithSensitiveMount

Sebuah wadah diluncurkan dengan jalur host eksternal sensitif yang dipasang di dalamnya.

Tingkat keparahan default: Sedang

- Fitur: Log audit EKS

Temuan ini memberi tahu Anda bahwa wadah diluncurkan dengan konfigurasi yang menyertakan jalur host sensitif dengan akses tulis di `volumeMounts` bagian tersebut. Ini membuat jalur host sensitif dapat diakses dan dapat ditulis dari dalam wadah. Teknik ini biasanya digunakan oleh musuh untuk mendapatkan akses ke sistem file host.

Rekomendasi remediasi:

Jika peluncuran kontainer ini tidak terduga, kredensial identitas pengguna yang digunakan untuk meluncurkan penampung dapat dikompromikan. Cabut akses pengguna dan balikkan perubahan apa

pun yang dibuat oleh musuh ke klaster Anda. Untuk informasi selengkapnya, lihat [Remediasi temuan Perlindungan EKS](#).

Jika peluncuran kontainer ini diharapkan, Anda disarankan untuk menggunakan aturan penekanan yang terdiri dari kriteria filter berdasarkan `resource.KubernetesDetails.KubernetesWorkloadDetails.containers.imagePrefix` bidang. Dalam kriteria filter `imagePrefix` bidang harus sama dengan yang `imagePrefix` ditentukan dalam temuan. Untuk mempelajari selengkapnya tentang cara membuat aturan penekanan, lihat [Aturan penekanan](#).

Persistence:Kubernetes/MaliciousIPCaller

API yang biasa digunakan untuk mendapatkan akses persisten ke klaster Kubernetes dipanggil dari alamat IP berbahaya yang diketahui.

Tingkat keparahan default: Sedang

- Fitur: Log audit EKS

Temuan ini memberi tahu Anda bahwa operasi API dipanggil dari alamat IP yang terkait dengan aktivitas berbahaya yang diketahui. API yang diamati umumnya dikaitkan dengan taktik persistensi di mana musuh telah memperoleh akses ke klaster Kubernetes Anda dan berusaha mempertahankan akses tersebut.

Rekomendasi remediasi:

Jika pengguna yang dilaporkan dalam temuan di bawah *KubernetesUserDetails* bagian ini adalah `system:anonymous`, selidiki mengapa pengguna anonim diizinkan untuk memanggil API dan mencabut izin, jika diperlukan, dengan mengikuti petunjuk dalam [Praktik terbaik Keamanan untuk Amazon EKS di Panduan Pengguna Amazon EKS](#). Jika pengguna adalah pengguna yang diautentikasi, selidiki untuk menentukan apakah aktivitas tersebut sah atau berbahaya. Jika aktivitas berbahaya, cabut akses pengguna dan balikkan perubahan apa pun yang dibuat oleh musuh ke klaster Anda. Untuk informasi selengkapnya, lihat [Remediasi temuan Perlindungan EKS](#).

Persistence:Kubernetes/MaliciousIPCaller.Custom

API yang biasa digunakan untuk mendapatkan akses persisten ke klaster Kubernetes dipanggil dari alamat IP pada daftar ancaman khusus.

Tingkat keparahan default: Sedang

- Fitur: Log audit EKS

Temuan ini memberi tahu Anda bahwa operasi API dipanggil dari alamat IP yang disertakan dalam daftar ancaman yang Anda unggah. Daftar ancaman yang terkait dengan temuan ini tercantum di bagian Informasi Tambahan dari detail temuan. API yang diamati umumnya dikaitkan dengan taktik persistensi di mana musuh telah memperoleh akses ke kluster Kubernetes Anda dan berusaha mempertahankan akses tersebut.

Rekomendasi remediasi:

Jika pengguna yang dilaporkan dalam temuan di bawah *KubernetesUserDetails* bagian ini adalah `system:anonymous`, selidiki mengapa pengguna anonim diizinkan untuk memanggil API dan mencabut izin, jika diperlukan, dengan mengikuti petunjuk dalam [Praktik terbaik Keamanan untuk Amazon EKS di Panduan Pengguna Amazon EKS](#). Jika pengguna adalah pengguna yang diautentikasi, selidiki untuk menentukan apakah aktivitas tersebut sah atau berbahaya. Jika aktivitas berbahaya, cabut akses pengguna dan balikkan perubahan apa pun yang dibuat oleh musuh ke kluster Anda. Untuk informasi selengkapnya, lihat [Remediasi temuan Perlindungan EKS](#).

Persistence:Kubernetes/SuccessfulAnonymousAccess

API yang biasa digunakan untuk mendapatkan izin tingkat tinggi ke kluster Kubernetes dipanggil oleh pengguna yang tidak diautentikasi.

Tingkat keparahan default: Tinggi

- Fitur: Log audit EKS

Temuan ini memberi tahu Anda bahwa operasi API berhasil dipanggil oleh pengguna. `system:anonymous` Panggilan API yang dibuat oleh tidak `system:anonymous` diautentikasi. API yang diamati umumnya dikaitkan dengan taktik persistensi di mana musuh telah mendapatkan akses ke cluster Anda dan berusaha mempertahankan akses itu. Aktivitas ini menunjukkan bahwa akses anonim atau tidak diautentikasi diizinkan pada tindakan API yang dilaporkan dalam temuan dan mungkin diizinkan pada tindakan lain. Jika perilaku ini tidak diharapkan, ini mungkin menunjukkan kesalahan konfigurasi atau kredensial Anda dikompromikan.

Rekomendasi remediasi:

Anda harus memeriksa izin yang telah diberikan kepada `system:anonymous` pengguna di klaster Anda dan memastikan bahwa semua izin diperlukan. Jika izin diberikan secara keliru atau jahat, Anda harus mencabut akses pengguna dan membalikkan setiap perubahan yang dibuat oleh musuh ke klaster Anda. Untuk informasi selengkapnya, lihat [Praktik terbaik keamanan untuk Amazon EKS](#) di Panduan Pengguna Amazon EKS.

Untuk informasi selengkapnya, lihat [Remediasi temuan Perlindungan EKS](#).

Persistence:Kubernetes/TorIPCaller

API yang biasa digunakan untuk mendapatkan akses persisten ke klaster Kubernetes dipanggil dari alamat IP node keluar Tor.

Tingkat keparahan default: Sedang

- Fitur: Log audit EKS

Temuan ini memberi tahu Anda bahwa API dipanggil dari alamat IP node keluar Tor. API yang diamati umumnya dikaitkan dengan taktik persistensi di mana musuh telah memperoleh akses ke klaster Kubernetes Anda dan berusaha mempertahankan akses tersebut. Tor adalah perangkat lunak untuk memungkinkan komunikasi anonim. Ini mengenkripsi dan secara acak mengalihkan komunikasi melalui relay antara serangkaian node jaringan. Node Tor terakhir disebut sebagai node keluar. Ini dapat menunjukkan akses tidak sah ke AWS sumber daya Anda dengan maksud menyembunyikan identitas asli penyerang.

Rekomendasi remediasi:

Jika pengguna yang dilaporkan dalam temuan di bawah *KubernetesUserDetails* bagian ini adalah `system:anonymous`, selidiki mengapa pengguna anonim diizinkan untuk memanggil API dan mencabut izin, jika diperlukan, dengan mengikuti petunjuk dalam [Praktik terbaik Keamanan untuk Amazon EKS di Panduan Pengguna Amazon EKS](#). Jika pengguna adalah pengguna yang diautentikasi, selidiki untuk menentukan apakah aktivitas tersebut sah atau berbahaya. Jika aktivitas berbahaya, cabut akses pengguna dan balikkan perubahan apa pun yang dibuat oleh musuh ke klaster Anda. Untuk informasi selengkapnya, lihat [Remediasi temuan Perlindungan EKS](#).

Policy:Kubernetes/AdminAccessToDefaultServiceAccount

Akun layanan default diberikan hak istimewa admin pada klaster Kubernetes.

Tingkat keparahan default: Tinggi

- Fitur: Log audit EKS

Temuan ini memberi tahu Anda bahwa akun layanan default untuk namespace di kluster Kubernetes Anda telah diberikan hak istimewa admin. Kubernetes membuat akun layanan default untuk semua namespace di cluster. Ini secara otomatis menetapkan akun layanan default sebagai identitas ke pod yang belum secara eksplisit dikaitkan dengan akun layanan lain. Jika akun layanan default memiliki hak istimewa admin, hal itu dapat mengakibatkan pod diluncurkan secara tidak sengaja dengan hak istimewa admin. Jika perilaku ini tidak diharapkan, ini mungkin menunjukkan kesalahan konfigurasi atau kredensial Anda dikompromikan.

Rekomendasi remediasi:

Anda tidak boleh menggunakan akun layanan default untuk memberikan izin ke Pod. Sebagai gantinya, Anda harus membuat akun layanan khusus untuk setiap beban kerja dan memberikan izin ke akun tersebut berdasarkan kebutuhan. Untuk memperbaiki masalah ini, Anda harus membuat akun layanan khusus untuk semua pod dan beban kerja Anda dan memperbarui pod dan beban kerja untuk bermigrasi dari akun layanan default ke akun khusus mereka. Maka Anda harus menghapus izin admin dari akun layanan default. Untuk informasi selengkapnya, lihat [Remediasi temuan Perlindungan EKS](#).

Policy:Kubernetes/AnonymousAccessGranted

system:anonymous Pengguna diberikan izin API pada kluster Kubernetes.

Tingkat keparahan default: Tinggi

- Fitur: Log audit EKS

Temuan ini memberi tahu Anda bahwa pengguna di kluster Kubernetes Anda berhasil membuat ClusterRoleBinding atau mengikat pengguna RoleBinding ke peran. `system:anonymous` Ini memungkinkan akses tidak terautentikasi ke operasi API yang diizinkan oleh peran. Jika perilaku ini tidak diharapkan, ini mungkin menunjukkan kesalahan konfigurasi atau kredensi Anda dikompromikan

Rekomendasi remediasi:

Anda harus memeriksa izin yang telah diberikan kepada `system:anonymous` pengguna atau `system:unauthenticated` grup di klaster Anda dan mencabut akses anonim yang tidak perlu. Untuk informasi selengkapnya, lihat [Praktik terbaik keamanan untuk Amazon EKS](#) di Panduan Pengguna Amazon EKS. Jika izin diberikan secara berbahaya, Anda harus mencabut akses pengguna yang memberikan izin dan membalikkan perubahan apa pun yang dibuat oleh musuh ke klaster Anda. Untuk informasi selengkapnya, lihat [Remediasi temuan Perlindungan EKS](#).

Policy:Kubernetes/ExposedDashboard

Dasbor untuk cluster Kubernetes terpapar ke internet

Tingkat keparahan default: Sedang

- Fitur: Log audit EKS

Temuan ini memberi tahu Anda bahwa dasbor Kubernetes untuk klaster Anda diekspos ke internet oleh layanan Load Balancer. Dasbor yang terbuka membuat antarmuka manajemen cluster Anda dapat diakses dari internet dan memungkinkan musuh untuk mengeksploitasi kesenjangan otentikasi dan kontrol akses apa pun yang mungkin ada.

Rekomendasi remediasi:

Anda harus memastikan bahwa otentikasi dan otorisasi yang kuat diberlakukan di Dasbor Kubernetes. Anda juga harus menerapkan kontrol akses jaringan untuk membatasi akses ke dasbor dari alamat IP tertentu.

Untuk informasi selengkapnya, lihat [Remediasi temuan Perlindungan EKS](#).

Policy:Kubernetes/KubeflowDashboardExposed

Dasbor Kubeflow untuk cluster Kubernetes diekspos ke Internet

Tingkat keparahan default: Sedang

- Fitur: Log audit EKS

Temuan ini memberi tahu Anda bahwa dasbor Kubeflow untuk klaster Anda diekspos ke Internet oleh layanan Load Balancer. Dasbor Kubeflow yang terbuka membuat antarmuka manajemen lingkungan

Kubeflow Anda dapat diakses dari Internet dan memungkinkan musuh untuk mengeksploitasi celah otentikasi dan kontrol akses apa pun yang mungkin ada.

Rekomendasi remediasi:

Anda harus memastikan bahwa otentikasi dan otorisasi yang kuat diberlakukan di Dasbor Kubeflow. Anda juga harus menerapkan kontrol akses jaringan untuk membatasi akses ke dasbor dari alamat IP tertentu.

Untuk informasi selengkapnya, lihat [Remediasi temuan Perlindungan EKS](#).

PrivilegeEscalation:Kubernetes/PrivilegedContainer

Kontainer istimewa dengan akses tingkat root diluncurkan di klaster Kubernetes Anda.

Tingkat keparahan default: Sedang

- Fitur: Log audit EKS

Temuan ini memberi tahu Anda bahwa kontainer istimewa diluncurkan di klaster Kubernetes Anda menggunakan gambar yang belum pernah digunakan sebelumnya untuk meluncurkan kontainer istimewa di klaster Anda. Wadah istimewa memiliki akses tingkat root ke host. Musuh dapat meluncurkan wadah istimewa sebagai taktik eskalasi hak istimewa untuk mendapatkan akses ke dan kemudian membahayakan tuan rumah.

Rekomendasi remediasi:

Jika peluncuran kontainer ini tidak terduga, kredensial identitas pengguna yang digunakan untuk meluncurkan penampung dapat dikompromikan. Cabut akses pengguna dan balikkan perubahan apa pun yang dibuat oleh musuh ke klaster Anda. Untuk informasi selengkapnya, lihat [Remediasi temuan Perlindungan EKS](#).

CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed

API Kubernetes yang biasa digunakan untuk mengakses rahasia dipanggil dengan cara yang anomali.

Tingkat keparahan default: Sedang

- Fitur: Log audit EKS

Temuan ini memberi tahu Anda bahwa operasi API anomali untuk mengambil rahasia kluster sensitif telah dipanggil oleh pengguna Kubernetes di kluster Anda. API yang diamati umumnya dikaitkan dengan taktik akses kredensial yang dapat menyebabkan eskalasi istimewa dan akses lebih lanjut dalam kluster Anda. Jika perilaku ini tidak diharapkan, ini mungkin menunjukkan kesalahan konfigurasi atau AWS kredensial Anda dikompromikan.

API yang diamati diidentifikasi sebagai anomali oleh model pembelajaran mesin deteksi GuardDuty anomali (ML). Model ML mengevaluasi semua aktivitas API pengguna dalam kluster EKS Anda dan mengidentifikasi kejadian anomali yang terkait dengan teknik yang digunakan oleh pengguna yang tidak sah. Model ML melacak beberapa faktor operasi API seperti pengguna yang membuat permintaan, lokasi permintaan dibuat, agen pengguna yang digunakan, dan namespace yang dioperasikan pengguna. Anda dapat menemukan detail permintaan API yang tidak biasa, di panel detail pencarian di GuardDuty konsol.

Rekomendasi remediasi:

Periksa izin yang diberikan kepada pengguna Kubernetes di kluster Anda dan pastikan bahwa semua izin ini diperlukan. Jika izin diberikan secara keliru atau jahat, cabut akses pengguna dan balikkan perubahan apa pun yang dibuat oleh pengguna yang tidak sah ke kluster Anda. Untuk informasi selengkapnya, lihat [Remediasi temuan Perlindungan EKS](#).

Jika AWS kredensialmu dikompromikan, lihat. [Memulihkan kredensi yang berpotensi dikompromikan AWS](#)

PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated

Sebuah RoleBinding atau ClusterRoleBinding ke peran yang terlalu permisif atau namespace yang sensitif telah dibuat atau dimodifikasi di kluster Kubernetes Anda.

Tingkat keparahan default: Medium*

Note

Tingkat keparahan default temuan ini adalah Medium. Namun, jika RoleBinding atau ClusterRoleBinding melibatkan ClusterRoles `admin` atau `cluster-admin`, tingkat keparahannya Tinggi.

- Fitur: Log audit EKS

Temuan ini memberi tahu Anda bahwa pengguna di kluster Kubernetes Anda membuat `RoleBinding` atau `ClusterRoleBinding` untuk mengikat pengguna ke peran dengan izin admin atau ruang nama sensitif. Jika perilaku ini tidak diharapkan, ini mungkin menunjukkan kesalahan konfigurasi atau AWS kredensial Anda dikompromikan.

API yang diamati diidentifikasi sebagai anomali oleh model pembelajaran mesin deteksi GuardDuty anomali (ML). Model ML mengevaluasi semua aktivitas API pengguna dalam kluster EKS Anda. Model ML ini juga mengidentifikasi peristiwa anomali yang terkait dengan teknik yang digunakan oleh pengguna yang tidak sah. Model ML juga melacak beberapa faktor operasi API, seperti pengguna yang membuat permintaan, lokasi permintaan dibuat, agen pengguna yang digunakan, dan namespace yang dioperasikan pengguna. Anda dapat menemukan detail permintaan API yang tidak biasa, di panel detail pencarian di GuardDuty konsol.

Rekomendasi remediasi:

Periksa izin yang diberikan kepada pengguna Kubernetes. Izin ini didefinisikan dalam peran dan subjek yang terlibat dalam `RoleBinding` dan `ClusterRoleBinding`. Jika izin diberikan secara keliru atau jahat, cabut akses pengguna dan balikkan perubahan apa pun yang dibuat oleh pengguna yang tidak sah ke kluster Anda. Untuk informasi selengkapnya, lihat [Remediasi temuan Perlindungan EKS](#).

Jika AWS kredensialmu dikompromikan, lihat. [Memulihkan kredensi yang berpotensi dikompromikan AWS](#)

Execution:Kubernetes/AnomalousBehavior.ExecInPod

Sebuah perintah dieksekusi di dalam pod dengan cara yang anomali.

Tingkat keparahan default: Sedang

- Fitur: Log audit EKS

Temuan ini memberi tahu Anda bahwa sebuah perintah dieksekusi di sebuah pod menggunakan API `exec` Kubernetes. `Exec` API Kubernetes memungkinkan menjalankan perintah arbitrer dalam sebuah pod. Jika perilaku ini tidak diharapkan untuk pengguna, namespace, atau pod, ini mungkin menunjukkan kesalahan konfigurasi atau AWS kredensialmu disusupi.

API yang diamati diidentifikasi sebagai anomali oleh model pembelajaran mesin deteksi GuardDuty anomali (ML). Model ML mengevaluasi semua aktivitas API pengguna dalam kluster EKS Anda. Model ML ini juga mengidentifikasi peristiwa anomali yang terkait dengan teknik yang digunakan oleh pengguna yang tidak sah. Model ML juga melacak beberapa faktor operasi API, seperti pengguna yang membuat permintaan, lokasi permintaan dibuat, agen pengguna yang digunakan, dan namespace yang dioperasikan pengguna. Anda dapat menemukan detail permintaan API yang tidak biasa, di panel detail pencarian di GuardDuty konsol.

Rekomendasi remediasi:

Jika eksekusi perintah ini tidak terduga, kredensial identitas pengguna yang digunakan untuk menjalankan perintah mungkin telah dikompromikan. Cabut akses pengguna dan balikkan perubahan apa pun yang dibuat oleh pengguna yang tidak sah ke kluster Anda. Untuk informasi selengkapnya, lihat [Remediasi temuan Perlindungan EKS](#).

Jika AWS kredensialmu dikompromikan, lihat. [Memulihkan kredensi yang berpotensi dikompromikan AWS](#)

PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer

Beban kerja diluncurkan dengan wadah istimewa dengan cara yang anomali.

Tingkat keparahan default: Tinggi

- Fitur: Log audit EKS

Temuan ini memberi tahu Anda bahwa beban kerja diluncurkan dengan wadah istimewa di kluster Amazon EKS Anda. Wadah istimewa memiliki akses tingkat root ke host. Pengguna yang tidak sah dapat meluncurkan kontainer istimewa sebagai taktik eskalasi hak istimewa untuk terlebih dahulu mendapatkan akses ke host dan kemudian mengkompromikannya.

Pembuatan atau modifikasi wadah yang diamati diidentifikasi sebagai anomali oleh model pembelajaran mesin deteksi GuardDuty anomali (ML). Model ML mengevaluasi semua API pengguna dan aktivitas image container dalam kluster EKS Anda. Model ML ini juga mengidentifikasi peristiwa anomali yang terkait dengan teknik yang digunakan oleh pengguna yang tidak sah. Model ML juga melacak beberapa faktor operasi API, seperti pengguna yang membuat permintaan, lokasi permintaan dibuat, agen pengguna yang digunakan, gambar kontainer yang diamati di akun Anda,

dan namespace yang dioperasikan pengguna. Anda dapat menemukan detail permintaan API yang tidak biasa, di panel detail pencarian di GuardDuty konsol.

Rekomendasi remediasi:

Jika peluncuran kontainer ini tidak terduga, kredensial identitas pengguna yang digunakan untuk meluncurkan penampung mungkin telah disusupi. Cabut akses pengguna dan balikkan perubahan apa pun yang dibuat oleh pengguna yang tidak sah ke kluster Anda. Untuk informasi selengkapnya, lihat [Remediasi temuan Perlindungan EKS](#).

Jika AWS kredensialmu dikompromikan, lihat. [Memulihkan kredensi yang berpotensi dikompromikan AWS](#)

Jika peluncuran kontainer ini diharapkan, Anda disarankan untuk menggunakan aturan penekanan dengan kriteria filter berdasarkan `resource.KubernetesDetails.KubernetesWorkloadDetails.containers.imagePrefix` bidang. Dalam kriteria filter, `imagePrefix` bidang harus memiliki nilai yang sama dengan `imagePrefix` bidang yang ditentukan dalam temuan. Untuk informasi selengkapnya, lihat [Aturan penindasan di GuardDuty](#).

Persistence:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount

Beban kerja diterapkan dengan cara yang anomali, dengan jalur host sensitif dipasang di dalam beban kerja.

Tingkat keparahan default: Tinggi

- Fitur: Log audit EKS

Temuan ini memberi tahu Anda bahwa beban kerja diluncurkan dengan wadah yang menyertakan jalur host sensitif di bagian tersebut `volumeMounts`. Ini berpotensi membuat jalur host sensitif dapat diakses dan dapat ditulis dari dalam wadah. Teknik ini biasanya digunakan oleh pengguna yang tidak sah untuk mendapatkan akses ke sistem file host.

Pembuatan atau modifikasi wadah yang diamati diidentifikasi sebagai anomali oleh model pembelajaran mesin deteksi GuardDuty anomali (ML). Model ML mengevaluasi semua API pengguna dan aktivitas image container dalam kluster EKS Anda. Model ML ini juga mengidentifikasi peristiwa

anomali yang terkait dengan teknik yang digunakan oleh pengguna yang tidak sah. Model ML juga melacak beberapa faktor operasi API, seperti pengguna yang membuat permintaan, lokasi permintaan dibuat, agen pengguna yang digunakan, gambar kontainer yang diamati di akun Anda, dan namespace yang dioperasikan pengguna. Anda dapat menemukan detail permintaan API yang tidak biasa, di panel detail pencarian di GuardDuty konsol.

Rekomendasi remediasi:

Jika peluncuran kontainer ini tidak terduga, kredensial identitas pengguna yang digunakan untuk meluncurkan penampung mungkin telah disusupi. Cabut akses pengguna dan balikkan perubahan apa pun yang dibuat oleh pengguna yang tidak sah ke kluster Anda. Untuk informasi selengkapnya, lihat [Remediasi temuan Perlindungan EKS](#).

Jika AWS kredensi Anda dikompromikan, lihat. [Memulihkan kredensi yang berpotensi dikompromikan AWS](#)

Jika peluncuran kontainer ini diharapkan, Anda disarankan untuk menggunakan aturan penekanan dengan kriteria filter berdasarkan `resource.KubernetesDetails.KubernetesWorkloadDetails.containers.imagePrefix` bidang. Dalam kriteria filter, `imagePrefix` bidang harus memiliki nilai yang sama dengan `imagePrefix` bidang yang ditentukan dalam temuan. Untuk informasi selengkapnya, lihat [Aturan penindasan di GuardDuty](#).

Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed

Beban kerja diluncurkan dengan cara yang anomali.

Tingkat keparahan default: Rendah*

Note

Tingkat keparahan default adalah Rendah. Namun, jika beban kerja berisi nama gambar yang berpotensi mencurigakan, seperti alat pentest yang dikenal, atau wadah yang menjalankan perintah yang berpotensi mencurigakan saat peluncuran, seperti perintah shell terbalik, maka tingkat keparahan jenis temuan ini akan dianggap sebagai Medium.

- Fitur: Log audit EKS

Temuan ini memberi tahu Anda bahwa beban kerja Kubernetes dibuat atau dimodifikasi secara anomali, seperti aktivitas API, image container baru, atau konfigurasi beban kerja berisiko, di dalam kluster Amazon EKS Anda. Pengguna yang tidak sah dapat meluncurkan kontainer sebagai taktik untuk mengeksekusi kode arbitrer untuk terlebih dahulu mendapatkan akses ke host dan kemudian mengkompromikannya.

Pembuatan atau modifikasi wadah yang diamati diidentifikasi sebagai anomali oleh model pembelajaran mesin deteksi GuardDuty anomali (ML). Model ML mengevaluasi semua API pengguna dan aktivitas image container dalam kluster EKS Anda. Model ML ini juga mengidentifikasi peristiwa anomali yang terkait dengan teknik yang digunakan oleh pengguna yang tidak sah. Model ML juga melacak beberapa faktor operasi API, seperti pengguna yang membuat permintaan, lokasi permintaan dibuat, agen pengguna yang digunakan, gambar kontainer yang diamati di akun Anda, dan namespace yang dioperasikan pengguna. Anda dapat menemukan detail permintaan API yang tidak biasa, di panel detail pencarian di GuardDuty konsol.

Rekomendasi remediasi:

Jika peluncuran kontainer ini tidak terduga, kredensial identitas pengguna yang digunakan untuk meluncurkan penampung mungkin telah disusupi. Cabut akses pengguna dan balikkan perubahan apa pun yang dibuat oleh pengguna yang tidak sah ke kluster Anda. Untuk informasi selengkapnya, lihat [Remediasi temuan Perlindungan EKS](#).

Jika AWS kredensi Anda dikompromikan, lihat. [Memulihkan kredensi yang berpotensi dikompromikan AWS](#)

Jika peluncuran kontainer ini diharapkan, Anda disarankan untuk menggunakan aturan penekanan dengan kriteria filter berdasarkan `resource.KubernetesDetails.KubernetesWorkloadDetails.containers.imagePrefix` bidang. Dalam kriteria filter, `imagePrefix` bidang harus memiliki nilai yang sama dengan `imagePrefix` bidang yang ditentukan dalam temuan. Untuk informasi selengkapnya, lihat [Aturan penindasan di GuardDuty](#).

PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated

Peran yang sangat permisif atau ClusterRole diciptakan atau dimodifikasi dengan cara yang anomali.

Tingkat keparahan default: Rendah

- Fitur: Log audit EKS

Temuan ini memberi tahu Anda bahwa operasi API anomali untuk membuat Role atau ClusterRole dengan izin berlebihan dipanggil oleh pengguna Kubernetes di cluster Amazon EKS Anda. Aktor dapat menggunakan pembuatan peran dengan izin yang kuat untuk menghindari penggunaan peran mirip admin bawaan dan menghindari deteksi. Izin yang berlebihan dapat menyebabkan eskalasi istimewa, eksekusi kode jarak jauh, dan berpotensi mengontrol namespace atau cluster. Jika perilaku ini tidak diharapkan, ini mungkin menunjukkan kesalahan konfigurasi atau kredensial Anda dikompromikan.

API yang diamati diidentifikasi sebagai anomali oleh model pembelajaran mesin deteksi GuardDuty anomali (ML). Model ML mengevaluasi semua aktivitas API pengguna dalam kluster Amazon EKS Anda dan mengidentifikasi kejadian anomali yang terkait dengan teknik yang digunakan oleh pengguna yang tidak sah. Model ML juga melacak beberapa faktor operasi API, seperti pengguna yang membuat permintaan, lokasi permintaan dibuat, agen pengguna yang digunakan, gambar kontainer yang diamati di akun Anda, dan namespace yang dioperasikan pengguna. Anda dapat menemukan detail permintaan API yang tidak biasa, di panel detail pencarian di GuardDuty konsol.

Rekomendasi remediasi:

Periksa izin yang ditentukan dalam Role atau ClusterRole untuk memastikan bahwa semua izin diperlukan dan ikuti prinsip hak istimewa paling sedikit. Jika izin diberikan secara keliru atau jahat, cabut akses pengguna dan balikkan perubahan apa pun yang dibuat oleh pengguna yang tidak sah ke kluster Anda. Untuk informasi selengkapnya, lihat [Remediasi temuan Perlindungan EKS](#).

Jika AWS kredensi Anda dikompromikan, lihat. [Memulihkan kredensi yang berpotensi dikompromikan AWS](#)

Discovery:Kubernetes/AnomalousBehavior.PermissionChecked

Seorang pengguna memeriksa izin akses mereka dengan cara yang tidak wajar.

Tingkat keparahan default: Rendah

- Fitur: Log audit EKS

Temuan ini memberi tahu Anda bahwa pengguna di kluster Kubernetes Anda berhasil memeriksa apakah izin kuat yang diketahui yang dapat menyebabkan eskalasi istimewa dan eksekusi kode jarak jauh, diizinkan atau tidak. Misalnya, perintah umum yang digunakan untuk memeriksa izin

bagi pengguna adalah `kubectl auth can-i`. Jika perilaku ini tidak diharapkan, ini mungkin menunjukkan kesalahan konfigurasi atau kredensial Anda telah disusupi.

API yang diamati diidentifikasi sebagai anomali oleh model pembelajaran mesin deteksi GuardDuty anomali (ML). Model ML mengevaluasi semua aktivitas API pengguna dalam kluster Amazon EKS Anda dan mengidentifikasi kejadian anomali yang terkait dengan teknik yang digunakan oleh pengguna yang tidak sah. Model ML juga melacak beberapa faktor operasi API, seperti pengguna yang membuat permintaan, lokasi permintaan dibuat, izin diperiksa, dan namespace yang dioperasikan pengguna. Anda dapat menemukan detail permintaan API yang tidak biasa, di panel detail pencarian di GuardDuty konsol.

Rekomendasi remediasi:

Periksa izin yang diberikan kepada pengguna Kubernetes untuk memastikan bahwa semua izin diperlukan. Jika izin diberikan secara keliru atau jahat, cabut akses pengguna dan balikkan perubahan apa pun yang dibuat oleh pengguna yang tidak sah ke kluster Anda. Untuk informasi selengkapnya, lihat [Remediasi temuan Perlindungan EKS](#).

Jika AWS kredensi Anda dikompromikan, lihat [Memulihkan kredensi yang berpotensi dikompromikan AWS](#)

GuardDuty Jenis penemuan Runtime Monitoring

Amazon GuardDuty menghasilkan temuan Runtime Monitoring berikut untuk menunjukkan potensi ancaman berdasarkan perilaku tingkat sistem operasi dari EC2 host dan container Amazon di kluster Amazon EKS, beban kerja Fargate dan Amazon ECS, serta instans Amazon. EC2

Note

Jenis pencarian Runtime Monitoring didasarkan pada log runtime yang dikumpulkan dari host. Log berisi bidang seperti jalur file yang dapat dikontrol oleh aktor jahat. Bidang ini juga termasuk dalam GuardDuty temuan untuk memberikan konteks runtime. Saat memproses temuan Runtime Monitoring di luar GuardDuty konsol, Anda harus membersihkan bidang pencarian. Misalnya, Anda dapat menyandikan HTML bidang pencarian saat menampilkannya di halaman web.

Topik

- [CryptoCurrency:Runtime/BitcoinTool.B](#)

- [Backdoor:Runtime/C&CActivity.B](#)
- [UnauthorizedAccess:Runtime/TorRelay](#)
- [UnauthorizedAccess:Runtime/TorClient](#)
- [Trojan:Runtime/BlackholeTraffic](#)
- [Trojan:Runtime/DropPoint](#)
- [CryptoCurrency:Runtime/BitcoinTool.B!DNS](#)
- [Backdoor:Runtime/C&CActivity.B!DNS](#)
- [Trojan:Runtime/BlackholeTraffic!DNS](#)
- [Trojan:Runtime/DropPoint!DNS](#)
- [Trojan:Runtime/DGADomainRequest.C!DNS](#)
- [Trojan:Runtime/DriveBySourceTraffic!DNS](#)
- [Trojan:Runtime/PhishingDomainRequest!DNS](#)
- [Impact:Runtime/AbusedDomainRequest.Reputation](#)
- [Impact:Runtime/BitcoinDomainRequest.Reputation](#)
- [Impact:Runtime/MaliciousDomainRequest.Reputation](#)
- [Impact:Runtime/SuspiciousDomainRequest.Reputation](#)
- [UnauthorizedAccess:Runtime/MetadataDNSRebind](#)
- [Execution:Runtime/NewBinaryExecuted](#)
- [PrivilegeEscalation:Runtime/DockerSocketAccessed](#)
- [PrivilegeEscalation:Runtime/RuncContainerEscape](#)
- [PrivilegeEscalation:Runtime/CGroupsReleaseAgentModified](#)
- [DefenseEvasion:Runtime/ProcessInjection.Proc](#)
- [DefenseEvasion:Runtime/ProcessInjection.Ptrace](#)
- [DefenseEvasion:Runtime/ProcessInjection.VirtualMemoryWrite](#)
- [Execution:Runtime/ReverseShell](#)
- [DefenseEvasion:Runtime/FilelessExecution](#)
- [Impact:Runtime/CryptoMinerExecuted](#)
- [Execution:Runtime/NewLibraryLoaded](#)
- [PrivilegeEscalation:Runtime/ContainerMountsHostDirectory](#)
- [PrivilegeEscalation:Runtime/UserfaultfdUsage](#)

- [Execution:Runtime/SuspiciousTool](#)
- [Execution:Runtime/SuspiciousCommand](#)
- [DefenseEvasion:Runtime/SuspiciousCommand](#)
- [DefenseEvasion:Runtime/PtraceAntiDebugging](#)
- [Execution:Runtime/MaliciousFileExecuted](#)
- [Execution:Runtime/SuspiciousShellCreated](#)
- [PrivilegeEscalation:Runtime/ElevationToRoot](#)
- [Discovery:Runtime/SuspiciousCommand](#)
- [Persistence:Runtime/SuspiciousCommand](#)
- [PrivilegeEscalation:Runtime/SuspiciousCommand](#)

CryptoCurrency:Runtime/BitcoinTool.B

EC2 Instance Amazon atau container menanyakan alamat IP yang terkait dengan aktivitas terkait cryptocurrency.

Tingkat keparahan default: Tinggi

- Fitur: Pemantauan Runtime

Temuan ini memberi tahu Anda bahwa proses yang berjalan pada EC2 instance yang terdaftar atau wadah di AWS lingkungan Anda menanyakan alamat IP yang terkait dengan aktivitas terkait cryptocurrency. Aktor ancaman mungkin berusaha untuk mengambil kendali atas sumber daya komputasi untuk menggunakannya kembali secara jahat untuk penambangan cryptocurrency yang tidak sah.

Agan GuardDuty runtime memantau peristiwa dari beberapa jenis sumber daya. Untuk mengidentifikasi sumber daya yang berpotensi dikompromikan, lihat Jenis sumber daya di panel temuan di GuardDuty konsol. Konteks tambahan, termasuk informasi garis keturunan proses dan proses, tersedia dalam temuan untuk penyelidikan lebih lanjut.

Rekomendasi remediasi:

Jika Anda menggunakan EC2 instance ini atau wadah untuk menambang atau mengelola cryptocurrency, atau salah satu dari ini terlibat dalam aktivitas blockchain, CryptoCurrency:Runtime/

BitcoinTool.B temuan dapat mewakili aktivitas yang diharapkan untuk lingkungan Anda. Jika ini terjadi di AWS lingkungan Anda, kami sarankan Anda membuat aturan penindasan untuk temuan ini. Aturan penekanan harus terdiri dari dua kriteria filter. Kriteria filter pertama harus menggunakan atribut Finding type dengan nilai. `CryptoCurrency:Runtime/BitcoinTool.B` Kriteria filter kedua harus berupa ID Instance dari instance atau Container Image ID dari container yang terlibat dalam cryptocurrency atau aktivitas terkait blockchain. Untuk informasi selengkapnya, lihat [Aturan penindasan](#).

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat [Remediasi temuan Runtime Monitoring](#).

Backdoor:Runtime/C&CActivity.B

EC2 Instance Amazon atau container menanyakan IP yang terkait dengan server perintah dan kontrol yang dikenal.

Tingkat keparahan default: Tinggi

- Fitur: Pemantauan Runtime

Temuan ini memberi tahu Anda bahwa proses yang berjalan pada EC2 instance yang terdaftar atau wadah dalam AWS lingkungan Anda menanyakan alamat IP yang terkait dengan server perintah dan kontrol (C&C) yang dikenal. Instance atau wadah yang terdaftar mungkin berpotensi dikompromikan. Server perintah dan kontrol adalah komputer yang mengeluarkan perintah untuk anggota botnet.

Botnet adalah kumpulan perangkat yang terhubung ke internet yang mungkin termasuk PCs, server, perangkat seluler, dan perangkat Internet of Things, yang terinfeksi dan dikendalikan oleh jenis malware yang umum. Botnet sering digunakan untuk mendistribusikan malware dan mengumpulkan informasi yang disalahgunakan, seperti nomor kartu kredit. Tergantung pada tujuan dan struktur botnet, server C&C mungkin juga mengeluarkan perintah untuk memulai serangan penolakan layanan (DDoS) terdistribusi.

Note

Jika IP yang ditanyakan terkait log4j, maka bidang temuan terkait akan mencakup nilai-nilai berikut:

- `service.additionalInfo.threatListName = Amazon`

- `service.additionalInfo.threatName = Log4j Related`

Agan GuardDuty runtime memantau peristiwa dari beberapa jenis sumber daya. Untuk mengidentifikasi sumber daya yang berpotensi dikompromikan, lihat Jenis sumber daya di panel temuan di GuardDuty konsol. Konteks tambahan, termasuk informasi garis keturunan proses dan proses, tersedia dalam temuan untuk penyelidikan lebih lanjut.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat [Remediasi temuan Runtime Monitoring](#).

UnauthorizedAccess:Runtime/TorRelay

EC2 Instance Amazon Anda atau wadah membuat koneksi ke jaringan Tor sebagai relay Tor.

Tingkat keparahan default: Tinggi

- Fitur: Pemantauan Runtime

Temuan ini memberi tahu Anda bahwa proses yang berjalan pada EC2 instance yang terdaftar atau wadah di AWS lingkungan Anda membuat koneksi ke jaringan Tor dengan cara yang menunjukkan bahwa itu bertindak sebagai relay Tor. Tor adalah perangkat lunak untuk memungkinkan komunikasi anonim. Tor meningkatkan anonimitas komunikasi dengan meneruskan lalu lintas klien yang kemungkinan terlarang dari satu relay Tor ke relay lainnya.

Agan GuardDuty runtime memantau peristiwa dari beberapa jenis sumber daya. Untuk mengidentifikasi sumber daya yang berpotensi dikompromikan, lihat Jenis sumber daya di panel temuan di GuardDuty konsol.

Agan GuardDuty runtime memantau peristiwa dari beberapa jenis sumber daya. Untuk mengidentifikasi sumber daya yang berpotensi dikompromikan, lihat Jenis sumber daya di panel temuan di GuardDuty konsol. Konteks tambahan, termasuk informasi garis keturunan proses dan proses, tersedia dalam temuan untuk penyelidikan lebih lanjut.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat [Remediasi temuan Runtime Monitoring](#).

UnauthorizedAccess:Runtime/TorClient

EC2 Instance Amazon atau container Anda membuat koneksi ke Tor Guard atau node Authority.

Tingkat keparahan default: Tinggi

- Fitur: Pemantauan Runtime

Temuan ini memberi tahu Anda bahwa proses yang berjalan pada EC2 instance yang terdaftar atau wadah di AWS lingkungan Anda membuat koneksi ke Tor Guard atau node Authority. Tor adalah perangkat lunak untuk memungkinkan komunikasi anonim. Node Tor Guards dan Authority bertindak sebagai gateway awal ke dalam jaringan Tor. Lalu lintas ini dapat menunjukkan bahwa EC2 instance ini atau wadah telah berpotensi dikompromikan dan bertindak sebagai klien pada jaringan Tor. Temuan ini mungkin menunjukkan akses tidak sah ke AWS sumber daya Anda dengan maksud menyembunyikan identitas asli penyerang.

Agan GuardDuty runtime memantau peristiwa dari beberapa jenis sumber daya. Untuk mengidentifikasi sumber daya yang berpotensi dikompromikan, lihat Jenis sumber daya di panel temuan di GuardDuty konsol.

Agan GuardDuty runtime memantau peristiwa dari beberapa jenis sumber daya. Untuk mengidentifikasi sumber daya yang berpotensi dikompromikan, lihat Jenis sumber daya di panel temuan di GuardDuty konsol. Konteks tambahan, termasuk informasi garis keturunan proses dan proses, tersedia dalam temuan untuk penyelidikan lebih lanjut.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat [Remediasi temuan Runtime Monitoring](#).

Trojan:Runtime/BlackholeTraffic

EC2 Instance Amazon atau wadah mencoba berkomunikasi dengan alamat IP host jarak jauh yang merupakan lubang hitam yang dikenal.

Tingkat keparahan default: Sedang

- Fitur: Pemantauan Runtime

Temuan ini memberi tahu Anda bahwa proses yang berjalan pada EC2 instance yang terdaftar atau wadah di AWS lingkungan Anda mungkin terganggu karena mencoba berkomunikasi dengan alamat IP lubang hitam (atau lubang wastafel). Lubang hitam adalah tempat di jaringan di mana lalu lintas masuk atau keluar dibuang secara diam-diam tanpa memberi tahu sumber bahwa data tidak mencapai penerima yang dituju. Alamat IP lubang hitam menentukan mesin host yang tidak berjalan atau alamat yang tidak ada host yang ditugaskan.

Agan GuardDuty runtime memantau peristiwa dari beberapa jenis sumber daya. Untuk mengidentifikasi sumber daya yang berpotensi dikompromikan, lihat Jenis sumber daya di panel temuan di GuardDuty konsol. Konteks tambahan, termasuk informasi garis keturunan proses dan proses, tersedia dalam temuan untuk penyelidikan lebih lanjut.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat [Remediasi temuan Runtime Monitoring](#).

Trojan:Runtime/DropPoint

EC2 Instans Amazon atau wadah mencoba berkomunikasi dengan alamat IP dari host jarak jauh yang diketahui memiliki kredensi dan data curian lainnya yang ditangkap oleh malware.

Tingkat keparahan default: Sedang

- Fitur: Pemantauan Runtime

Temuan ini memberi tahu Anda bahwa proses yang berjalan pada EC2 instance yang terdaftar atau wadah di AWS lingkungan Anda mencoba berkomunikasi dengan alamat IP host jarak jauh yang diketahui menyimpan kredensyal dan data curian lainnya yang ditangkap oleh malware.

Agan GuardDuty runtime memantau peristiwa dari beberapa jenis sumber daya. Untuk mengidentifikasi sumber daya yang berpotensi dikompromikan, lihat Jenis sumber daya di panel

temuan di GuardDuty konsol. Konteks tambahan, termasuk informasi garis keturunan proses dan proses, tersedia dalam temuan untuk penyelidikan lebih lanjut.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat [Remediasi temuan Runtime Monitoring](#).

CryptoCurrency:Runtime/BitcoinTool.B!DNS

EC2 Instance Amazon atau container menanyakan nama domain yang terkait dengan aktivitas cryptocurrency.

Tingkat keparahan default: Tinggi

- Fitur: Pemantauan Runtime

Temuan ini memberi tahu Anda bahwa proses yang berjalan pada EC2 instance yang terdaftar atau wadah di AWS lingkungan Anda sedang menanyakan nama domain yang terkait dengan Bitcoin atau aktivitas terkait cryptocurrency lainnya. Aktor ancaman mungkin berusaha untuk mengambil kendali atas sumber daya komputasi untuk menggunakannya kembali secara jahat untuk penambangan cryptocurrency yang tidak sah.

Agan GuardDuty runtime memantau peristiwa dari beberapa jenis sumber daya. Untuk mengidentifikasi sumber daya yang berpotensi dikompromikan, lihat Jenis sumber daya di panel temuan di GuardDuty konsol. Konteks tambahan, termasuk informasi garis keturunan proses dan proses, tersedia dalam temuan untuk penyelidikan lebih lanjut.

Rekomendasi remediasi:

Jika Anda menggunakan EC2 instance atau wadah ini untuk menambang atau mengelola cryptocurrency, atau salah satu dari ini terlibat dalam aktivitas blockchain, CryptoCurrency:Runtime/BitcoinTool.B!DNS temuan bisa menjadi kegiatan yang diharapkan untuk lingkungan Anda. Jika ini terjadi di AWS lingkungan Anda, kami sarankan Anda membuat aturan penindasan untuk temuan ini. Aturan penekanan harus terdiri dari dua kriteria filter. Kriteria pertama harus menggunakan atribut Tipe temuan dengan nilai `CryptoCurrency:Runtime/BitcoinTool.B!DNS`. Kriteria filter kedua harus berupa ID Instance dari instance atau Container Image ID dari container yang terlibat dalam aktivitas cryptocurrency atau blockchain. Untuk informasi selengkapnya, lihat [Aturan Penindasan](#).

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat [Remediasi temuan Runtime Monitoring](#).

Backdoor:Runtime/C&CActivity.B!DNS

EC2 Instance Amazon atau container menanyakan nama domain yang dikaitkan dengan server perintah dan kontrol yang dikenal.

Tingkat keparahan default: Tinggi

- Fitur: Pemantauan Runtime

Temuan ini memberi tahu Anda bahwa proses yang berjalan pada EC2 instance yang terdaftar atau wadah dalam AWS lingkungan Anda sedang menanyakan nama domain yang terkait dengan server perintah dan kontrol (C&C) yang dikenal. EC2 Instance yang terdaftar atau wadah mungkin dikompromikan. Server perintah dan kontrol adalah komputer yang mengeluarkan perintah untuk anggota botnet.

Botnet adalah kumpulan perangkat yang terhubung ke internet yang mungkin termasuk PCs, server, perangkat seluler, dan perangkat Internet of Things, yang terinfeksi dan dikendalikan oleh jenis malware yang umum. Botnet sering digunakan untuk mendistribusikan malware dan mengumpulkan informasi yang disalahgunakan, seperti nomor kartu kredit. Tergantung pada tujuan dan struktur botnet, server C&C mungkin juga mengeluarkan perintah untuk memulai serangan penolakan layanan (DDoS) terdistribusi.

Note

Jika nama domain yang ditanyakan terkait log4j, maka bidang temuan terkait akan mencakup nilai-nilai berikut:

- `service.additionalInfo.threatListName` = Amazon
- `service.additionalInfo.threatName` = Log4j Related

 Note

Untuk menguji bagaimana GuardDuty menghasilkan jenis temuan ini, Anda dapat membuat permintaan DNS dari instance Anda (menggunakan `dig` untuk Linux atau `nslookup` untuk Windows) terhadap domain `guarddutyactivityb.com` pengujian.

Agen GuardDuty runtime memantau peristiwa dari beberapa jenis sumber daya. Untuk mengidentifikasi sumber daya yang berpotensi dikompromikan, lihat Jenis sumber daya di panel temuan di GuardDuty konsol. Konteks tambahan, termasuk informasi garis keturunan proses dan proses, tersedia dalam temuan untuk penyelidikan lebih lanjut.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat [Remediasi temuan Runtime Monitoring](#).

Trojan:Runtime/BlackholeTraffic!DNS

EC2 Instance Amazon atau wadah menanyakan nama domain yang sedang dialihkan ke alamat IP lubang hitam.

Tingkat keparahan default: Sedang

- Fitur: Pemantauan Runtime

Temuan ini memberi tahu Anda bahwa proses yang berjalan pada EC2 instance yang terdaftar atau wadah di AWS lingkungan Anda mungkin terganggu karena menanyakan nama domain yang sedang dialihkan ke alamat IP lubang hitam. Lubang hitam adalah tempat di jaringan di mana lalu lintas masuk atau keluar dibuang secara diam-diam tanpa memberi tahu sumber bahwa data tidak mencapai penerima yang dituju.

Agen GuardDuty runtime memantau peristiwa dari beberapa jenis sumber daya. Untuk mengidentifikasi sumber daya yang berpotensi dikompromikan, lihat Jenis sumber daya di panel temuan di GuardDuty konsol. Konteks tambahan, termasuk informasi garis keturunan proses dan proses, tersedia dalam temuan untuk penyelidikan lebih lanjut.

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat [Remediasi temuan Runtime Monitoring](#).

Trojan:Runtime/DropPoint!DNS

EC2 Instance Amazon atau kontainer menanyakan nama domain host jarak jauh yang diketahui memiliki kredensi dan data curian lainnya yang ditangkap oleh malware.

Tingkat keparahan default: Sedang

- Fitur: Pemantauan Runtime

Temuan ini memberi tahu Anda bahwa proses yang berjalan pada EC2 instance yang terdaftar atau wadah di AWS lingkungan Anda menanyakan nama domain host jarak jauh yang diketahui menyimpan kredensyal dan data curian lainnya yang ditangkap oleh malware.

Agen GuardDuty runtime memantau peristiwa dari beberapa jenis sumber daya. Untuk mengidentifikasi sumber daya yang berpotensi dikompromikan, lihat Jenis sumber daya di panel temuan di GuardDuty konsol. Konteks tambahan, termasuk informasi garis keturunan proses dan proses, tersedia dalam temuan untuk penyelidikan lebih lanjut.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat [Remediasi temuan Runtime Monitoring](#).

Trojan:Runtime/DGADomainRequest.C!DNS

EC2 Instance Amazon atau container menanyakan domain yang dihasilkan secara algoritmik. Domain semacam itu biasanya digunakan oleh malware dan bisa menjadi indikasi EC2 instance yang dikompromikan atau wadah.

Tingkat keparahan default: Tinggi

- Fitur: Pemantauan Runtime

Temuan ini memberi tahu Anda bahwa proses yang berjalan pada EC2 instance yang terdaftar atau wadah di AWS lingkungan Anda mencoba menanyakan domain algoritma pembuatan domain (DGA). Sumber daya Anda mungkin telah dikompromikan.

DGAs digunakan untuk secara berkala menghasilkan sejumlah besar nama domain yang dapat digunakan sebagai titik pertemuan dengan server perintah dan kontrol (C&C) mereka. Server perintah dan kontrol adalah komputer yang mengeluarkan perintah kepada anggota botnet, yang merupakan kumpulan perangkat yang terhubung ke internet yang terinfeksi dan dikendalikan oleh tipe malware yang umum. Banyaknya kemungkinan titik pertemuan menyulitkan untuk mematikan botnet secara efektif karena komputer yang terinfeksi berusaha menghubungi beberapa nama domain ini setiap hari untuk menerima pembaruan atau perintah.

Note

Temuan ini didasarkan pada domain DGA yang diketahui dari umpan intelijen GuardDuty ancaman.

Agan GuardDuty runtime memantau peristiwa dari beberapa jenis sumber daya. Untuk mengidentifikasi sumber daya yang berpotensi dikompromikan, lihat Jenis sumber daya di panel temuan di GuardDuty konsol. Konteks tambahan, termasuk informasi garis keturunan proses dan proses, tersedia dalam temuan untuk penyelidikan lebih lanjut.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat [Remediasi temuan Runtime Monitoring](#).

Trojan:Runtime/DriveBySourceTraffic!DNS

EC2 Instance Amazon atau container menanyakan nama domain dari host jarak jauh yang merupakan sumber serangan unduhan Drive-By yang diketahui.

Tingkat keparahan default: Tinggi

- Fitur: Pemantauan Runtime

Temuan ini memberi tahu Anda bahwa proses yang berjalan pada EC2 instance yang terdaftar atau wadah di AWS lingkungan Anda mungkin terganggu karena menanyakan nama domain host jarak jauh yang merupakan sumber serangan unduhan drive-by yang diketahui. Ini adalah unduhan perangkat lunak komputer yang tidak diinginkan dari internet yang dapat memulai instalasi otomatis virus, spyware, atau malware.

Agan GuardDuty runtime memantau peristiwa dari beberapa jenis sumber daya. Untuk mengidentifikasi sumber daya yang berpotensi dikompromikan, lihat Jenis sumber daya di panel temuan di GuardDuty konsol. Konteks tambahan, termasuk informasi garis keturunan proses dan proses, tersedia dalam temuan untuk penyelidikan lebih lanjut.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat [Remediasi temuan Runtime Monitoring](#).

Trojan:Runtime/PhishingDomainRequest!DNS

EC2 Instance Amazon atau container menanyakan domain yang terlibat dalam serangan phishing.

Tingkat keparahan default: Tinggi

- Fitur: Pemantauan Runtime

Temuan ini memberi tahu Anda bahwa proses yang berjalan pada EC2 instance yang terdaftar atau wadah di AWS lingkungan Anda mencoba menanyakan domain yang terlibat dalam serangan phishing. Domain phishing dibuat oleh seseorang yang menyamar sebagai institusi yang sah untuk membujuk individu agar memberikan data sensitif, seperti informasi pengenalan pribadi, detail kartu kredit dan perbankan, serta kata sandi. EC2 Instance atau wadah Anda mungkin mencoba mengambil data sensitif yang disimpan di situs web phishing, atau mungkin mencoba menyiapkan situs web phishing. EC2Instance Anda atau wadah mungkin dikompromikan.

Agan GuardDuty runtime memantau peristiwa dari beberapa jenis sumber daya. Untuk mengidentifikasi sumber daya yang berpotensi dikompromikan, lihat Jenis sumber daya di panel temuan di GuardDuty konsol. Konteks tambahan, termasuk informasi garis keturunan proses dan proses, tersedia dalam temuan untuk penyelidikan lebih lanjut.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat [Remediasi temuan Runtime Monitoring](#).

Impact:Runtime/AbusedDomainRequest.Reputation

EC2 Instance Amazon atau container menanyakan nama domain dengan reputasi rendah yang dikaitkan dengan domain yang disalahgunakan yang diketahui.

Tingkat keparahan default: Sedang

- Fitur: Pemantauan Runtime

Temuan ini memberi tahu Anda bahwa proses yang berjalan pada EC2 instance yang terdaftar atau wadah dalam AWS lingkungan Anda menanyakan nama domain dengan reputasi rendah yang terkait dengan domain atau alamat IP yang disalahgunakan yang diketahui. Contoh domain yang disalahgunakan adalah nama domain tingkat atas (TLDs) dan nama domain tingkat kedua (2LDs) yang menyediakan pendaftaran subdomain gratis serta penyedia DNS dinamis. Aktor ancaman cenderung menggunakan layanan ini untuk mendaftarkan domain secara gratis atau dengan biaya rendah. Domain bereputasi rendah dalam kategori ini mungkin juga merupakan domain kedaluwarsa yang mencari alamat IP parkir registrar dan oleh karena itu mungkin tidak lagi aktif. IP parkir adalah tempat registrar mengarahkan lalu lintas untuk domain yang belum ditautkan ke layanan apa pun. EC2 Instans Amazon yang terdaftar atau wadah dapat dikompromikan karena pelaku ancaman biasanya menggunakan registrar atau layanan ini untuk distribusi C&C dan malware.

Domain reputasi rendah didasarkan pada model skor reputasi. Model ini mengevaluasi dan memberi peringkat karakteristik domain untuk menentukan kemungkinannya berbahaya.

Agan GuardDuty runtime memantau peristiwa dari beberapa jenis sumber daya. Untuk mengidentifikasi sumber daya yang berpotensi dikompromikan, lihat Jenis sumber daya di panel temuan di GuardDuty konsol. Konteks tambahan, termasuk informasi garis keturunan proses dan proses, tersedia dalam temuan untuk penyelidikan lebih lanjut.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat [Remediasi temuan Runtime Monitoring](#).

Impact:Runtime/BitcoinDomainRequest.Reputation

EC2 Instance Amazon atau container menanyakan nama domain dengan reputasi rendah yang terkait dengan aktivitas terkait cryptocurrency.

Tingkat keparahan default: Tinggi

- Fitur: Pemantauan Runtime

Temuan ini memberi tahu Anda bahwa proses yang berjalan pada EC2 instance yang terdaftar atau wadah di AWS lingkungan Anda menanyakan nama domain dengan reputasi rendah yang terkait dengan Bitcoin atau aktivitas terkait cryptocurrency lainnya. Aktor ancaman mungkin berusaha untuk mengambil kendali atas sumber daya komputasi untuk menggunakannya kembali secara jahat untuk penambangan cryptocurrency yang tidak sah.

Domain reputasi rendah didasarkan pada model skor reputasi. Model ini mengevaluasi dan memberi peringkat karakteristik domain untuk menentukan kemungkinannya berbahaya.

Agan GuardDuty runtime memantau peristiwa dari beberapa jenis sumber daya. Untuk mengidentifikasi sumber daya yang berpotensi dikompromikan, lihat Jenis sumber daya di panel temuan di GuardDuty konsol. Konteks tambahan, termasuk informasi garis keturunan proses dan proses, tersedia dalam temuan untuk penyelidikan lebih lanjut.

Rekomendasi remediasi:

Jika Anda menggunakan EC2 instance ini atau wadah untuk menambang atau mengelola cryptocurrency, atau jika sumber daya ini terlibat dalam aktivitas blockchain, temuan ini dapat mewakili aktivitas yang diharapkan untuk lingkungan Anda. Jika ini terjadi di AWS lingkungan Anda, kami sarankan Anda membuat aturan penindasan untuk temuan ini. Aturan penekanan harus terdiri dari dua kriteria filter. Kriteria filter pertama harus menggunakan atribut Finding type dengan nilai `Impact:Runtime/BitcoinDomainRequest.Reputation`. Kriteria filter kedua harus berupa ID Instance dari instance atau ID Gambar Kontainer dari container terlibat dalam aktivitas terkait cryptocurrency atau blockchain. Untuk informasi selengkapnya, lihat [Aturan penindasan](#).

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat [Remediasi temuan Runtime Monitoring](#).

Impact:Runtime/MaliciousDomainRequest.Reputation

EC2 Instance Amazon atau container menanyakan domain dengan reputasi rendah yang dikaitkan dengan domain berbahaya yang diketahui.

Tingkat keparahan default: Tinggi

- Fitur: Pemantauan Runtime

Temuan ini memberi tahu Anda bahwa proses yang berjalan pada EC2 instance yang terdaftar atau wadah di AWS lingkungan Anda menanyakan nama domain dengan reputasi rendah yang terkait dengan domain berbahaya atau alamat IP yang diketahui. Misalnya, domain dapat dikaitkan dengan alamat IP sinkhole yang dikenal. Domain sinkhole adalah domain yang sebelumnya dikendalikan oleh aktor ancaman, dan permintaan yang dibuat untuk domain tersebut dapat menunjukkan bahwa instans disusupi. Domain ini juga dapat dikorelasikan dengan kampanye berbahaya atau algoritme pembuatan domain yang dikenal.

Domain reputasi rendah didasarkan pada model skor reputasi. Model ini mengevaluasi dan memberi peringkat karakteristik domain untuk menentukan kemungkinannya berbahaya.

Agen GuardDuty runtime memantau peristiwa dari beberapa jenis sumber daya. Untuk mengidentifikasi sumber daya yang berpotensi dikompromikan, lihat Jenis sumber daya di panel temuan di GuardDuty konsol. Konteks tambahan, termasuk informasi garis keturunan proses dan proses, tersedia dalam temuan untuk penyelidikan lebih lanjut.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat [Remediasi temuan Runtime Monitoring](#).

Impact:Runtime/SuspiciousDomainRequest.Reputation

EC2 Instance Amazon atau container menanyakan nama domain dengan reputasi rendah yang mencurigakan karena usianya, atau popularitasnya yang rendah.

Tingkat keparahan default: Rendah

- Fitur: Pemantauan Runtime

Temuan ini memberi tahu Anda bahwa proses yang berjalan pada EC2 instance yang terdaftar atau wadah di AWS lingkungan Anda menanyakan nama domain dengan reputasi rendah yang diduga berbahaya. Karakteristik yang diamati dari domain ini konsisten dengan domain berbahaya yang diamati sebelumnya. Namun, model reputasi kami tidak dapat secara definitif menghubungkannya

dengan ancaman yang diketahui. Domain ini biasanya baru diamati atau menerima jumlah lalu lintas yang rendah.

Domain reputasi rendah didasarkan pada model skor reputasi. Model ini mengevaluasi dan memberi peringkat karakteristik domain untuk menentukan kemungkinannya berbahaya.

Agan GuardDuty runtime memantau peristiwa dari beberapa jenis sumber daya. Untuk mengidentifikasi sumber daya yang berpotensi dikompromikan, lihat Jenis sumber daya di panel temuan di GuardDuty konsol. Konteks tambahan, termasuk informasi garis keturunan proses dan proses, tersedia dalam temuan untuk penyelidikan lebih lanjut.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat [Remediasi temuan Runtime Monitoring](#).

UnauthorizedAccess:Runtime/MetadataDNSRebind

EC2 Instance Amazon atau container melakukan pencarian DNS yang menyelesaikan layanan metadata instance.

Tingkat keparahan default: Tinggi

- Fitur: Pemantauan Runtime

Note

Saat ini, jenis temuan ini hanya didukung untuk AMD64 arsitektur.

Temuan ini memberi tahu Anda bahwa proses yang berjalan pada EC2 instance yang terdaftar atau wadah di AWS lingkungan Anda sedang menanyakan domain yang menyelesaikan ke alamat IP EC2 metadata (169.254.169.254). Kueri DNS semacam ini dapat menunjukkan bahwa instans adalah target dari teknik rebinding DNS. Teknik ini dapat digunakan untuk mendapatkan metadata dari sebuah EC2 instance, termasuk kredensyal IAM yang terkait dengan instance.

DNS rebinding melibatkan menipu aplikasi yang berjalan pada EC2 instance untuk memuat data yang dikembalikan dari URL, di mana nama domain di URL menyelesaikan ke alamat IP EC2

metadata (). 169.254.169.254 Ini menyebabkan aplikasi mengakses EC2 metadata dan mungkin membuatnya tersedia untuk penyerang.

Dimungkinkan untuk mengakses EC2 metadata menggunakan DNS rebinding hanya jika EC2 instance menjalankan aplikasi rentan yang memungkinkan injeksi URLs, atau jika seseorang mengakses URL di browser web yang berjalan pada instance. EC2

Agen GuardDuty runtime memantau peristiwa dari beberapa jenis sumber daya. Untuk mengidentifikasi sumber daya yang berpotensi dikompromikan, lihat Jenis sumber daya di panel temuan di GuardDuty konsol. Konteks tambahan, termasuk informasi garis keturunan proses dan proses, tersedia dalam temuan untuk penyelidikan lebih lanjut.

Rekomendasi remediasi:

Menanggapi temuan ini, Anda harus mengevaluasi apakah ada aplikasi rentan yang berjalan pada EC2 instance atau pada wadah, atau jika seseorang menggunakan browser untuk mengakses domain yang diidentifikasi dalam temuan. Jika akar penyebabnya adalah aplikasi yang rentan, perbaiki kerentanan. Jika seseorang menelusuri domain yang diidentifikasi, blokir domain atau cegah pengguna mengaksesnya. Jika Anda menentukan temuan ini terkait dengan kedua kasus di atas, [Cabut sesi yang terkait dengan instance](#). EC2

Beberapa AWS pelanggan sengaja memetakan alamat IP metadata ke nama domain di server DNS otoritatif mereka. Jika hal ini dilakukan di lingkungan Anda, kami menyarankan Anda untuk membuat aturan penekanan untuk temuan ini. Aturan penekanan harus terdiri dari dua kriteria filter. Kriteria filter pertama harus menggunakan atribut Finding type dengan nilai. UnauthorizedAccess:Runtime/MetaDataDNSRebind Kriteria filter kedua harus domain permintaan DNS atau ID Gambar Kontainer dari wadah. Nilai domain permintaan DNS harus sesuai dengan domain yang telah Anda petakan ke alamat IP metadata (). 169.254.169.254 Untuk informasi tentang membuat aturan penindasan, lihat Aturan [penindasan](#).

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat [Remediasi temuan Runtime Monitoring](#).

Execution:Runtime/NewBinaryExecuted

File biner yang baru dibuat atau baru dimodifikasi dalam wadah telah dieksekusi.

Tingkat keparahan default: Sedang

- Fitur: Pemantauan Runtime

Temuan ini memberi tahu Anda bahwa file biner yang baru dibuat atau yang baru saja dimodifikasi, dalam wadah telah dieksekusi. Ini adalah praktik terbaik untuk menjaga kontainer tetap tidak berubah saat runtime, dan file biner, skrip, atau pustaka tidak boleh dibuat atau dimodifikasi selama masa pakai penampung. Perilaku ini menunjukkan bahwa aktor jahat yang telah memperoleh akses ke wadah, telah mengunduh, dan mengeksekusi malware atau perangkat lunak lain sebagai bagian dari potensi kompromi. Meskipun jenis aktivitas ini bisa menjadi indikasi kompromi, ini juga merupakan pola penggunaan yang umum. Oleh karena itu, GuardDuty gunakan mekanisme untuk mengidentifikasi contoh mencurigakan dari aktivitas ini dan menghasilkan jenis temuan ini hanya untuk contoh yang mencurigakan.

Agen GuardDuty runtime memantau peristiwa dari beberapa jenis sumber daya. Untuk mengidentifikasi sumber daya yang berpotensi dikompromikan, lihat Jenis sumber daya di panel temuan di GuardDuty konsol. Untuk mengidentifikasi proses modifikasi dan biner baru, lihat detail proses Modifikasi dan detail Proses

Rincian proses modifikasi termasuk dalam `service.runtimeDetails.context.modifyingProcess` bidang penemuan JSON, atau di bawah Proses Memodifikasi di panel rincian temuan. Untuk jenis temuan ini, proses modifikasi adalah `/usr/bin/dpkg`, seperti yang diidentifikasi oleh `service.runtimeDetails.context.modifyingProcess.executablePath` bidang temuan JSON, atau sebagai bagian dari Proses Memodifikasi di panel rincian temuan.

Rincian biner baru atau modifikasi yang dieksekusi disertakan dalam JSON temuan, atau bagian Proses di bawah rincian Runtime. `service.runtimeDetails.process` Untuk jenis temuan ini, biner baru atau yang dimodifikasi adalah `/usr/bin/python3.8`, seperti yang ditunjukkan oleh bidang `service.runtimeDetails.process.executablePath` (Jalur yang dapat dieksekusi).

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat [Remediasi temuan Runtime Monitoring](#).

PrivilegeEscalation:Runtime/DockerSocketAccessed

Sebuah proses di dalam wadah berkomunikasi dengan daemon Docker menggunakan soket Docker.

Tingkat keparahan default: Sedang

- Fitur: Pemantauan Runtime

Soket Docker adalah Unix Domain Socket yang digunakan Docker daemon (`dockerd`) untuk berkomunikasi dengan kliennya. Klien dapat melakukan berbagai tindakan, seperti membuat kontainer dengan berkomunikasi dengan daemon Docker melalui soket Docker. Sangat mencurigakan jika proses penampung mengakses soket Docker. Proses kontainer dapat keluar dari wadah dan mendapatkan akses tingkat host dengan berkomunikasi dengan soket Docker dan membuat wadah istimewa.

Agen GuardDuty runtime memantau peristiwa dari beberapa jenis sumber daya. Untuk mengidentifikasi sumber daya yang berpotensi dikompromikan, lihat Jenis sumber daya di panel temuan di GuardDuty konsol. Konteks tambahan, termasuk informasi garis keturunan proses dan proses, tersedia dalam temuan untuk penyelidikan lebih lanjut.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat [Remediasi temuan Runtime Monitoring](#).

PrivilegeEscalation:Runtime/RuncContainerEscape

Upaya pelarian kontainer melalui runC terdeteksi.

Tingkat keparahan default: Tinggi

- Fitur: Pemantauan Runtime

runC adalah runtime kontainer tingkat rendah yang digunakan runtime kontainer tingkat tinggi, seperti Docker dan Containerd untuk menelurkan dan menjalankan container. RunC selalu dijalankan dengan hak akses root karena perlu melakukan tugas tingkat rendah untuk membuat wadah. Aktor ancaman dapat memperoleh akses tingkat host dengan memodifikasi atau mengeksploitasi kerentanan dalam biner runC.

Temuan ini mendeteksi modifikasi biner runC dan upaya potensial untuk mengeksploitasi kerentanan RuNC berikut:

- [CVE-2019-5736](#)— Eksploitasi CVE-2019-5736 melibatkan penimpaan biner runC dari dalam wadah. Temuan ini dipanggil ketika biner runC dimodifikasi oleh proses di dalam wadah.

- [CVE-2024-21626](#)— Eksploitasi CVE-2024-21626 melibatkan pengaturan direktori kerja saat ini (CWD) atau wadah ke deskriptor file terbuka. `/proc/self/fd/FileDescriptor` Temuan ini dipanggil ketika proses kontainer dengan direktori kerja saat ini di bawah `/proc/self/fd/` terdeteksi, misalnya, `/proc/self/fd/7`.

Temuan ini mungkin menunjukkan bahwa aktor jahat telah berusaha melakukan eksploitasi di salah satu jenis kontainer berikut:

- Wadah baru dengan gambar yang dikendalikan penyerang.
- Wadah yang ada yang dapat diakses oleh aktor dengan izin menulis pada biner runC tingkat host.

Agan GuardDuty runtime memantau peristiwa dari beberapa jenis sumber daya. Untuk mengidentifikasi sumber daya yang berpotensi dikompromikan, lihat Jenis sumber daya di panel temuan di GuardDuty konsol.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat [Remediasi temuan Runtime Monitoring](#).

PrivilegeEscalation:Runtime/CGroupsReleaseAgentModified

Upaya pelarian kontainer melalui agen CGroups rilis terdeteksi.

Tingkat keparahan default: Tinggi

- Fitur: Pemantauan Runtime

Temuan ini memberi tahu Anda bahwa upaya untuk memodifikasi file agen rilis grup kontrol (cgroup) telah terdeteksi. Linux menggunakan kelompok kontrol (cgroups) untuk membatasi, memperhitungkan, dan mengisolasi penggunaan sumber daya dari kumpulan proses. Setiap cgroup memiliki file agen rilis (`release_agent`), skrip yang dijalankan Linux ketika proses apa pun di dalam cgroup berakhir. File agen rilis selalu dijalankan di tingkat host. Aktor ancaman di dalam wadah dapat melarikan diri ke host dengan menulis perintah arbitrer ke file agen rilis milik cgroup. Ketika proses di dalam cgroup itu berakhir, perintah yang ditulis oleh aktor dieksekusi.

Agan GuardDuty runtime memantau peristiwa dari beberapa jenis sumber daya. Untuk mengidentifikasi sumber daya yang berpotensi dikompromikan, lihat Jenis sumber daya di panel temuan di GuardDuty konsol.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat [Remediasi temuan Runtime Monitoring](#).

DefenseEvasion:Runtime/ProcessInjection.Proc

Injeksi proses menggunakan sistem file proc terdeteksi dalam wadah atau instance Amazon. EC2

Tingkat keparahan default: Tinggi

- Fitur: Pemantauan Runtime

Injeksi proses adalah teknik yang digunakan aktor ancaman untuk menyuntikkan kode ke dalam proses untuk menghindari pertahanan dan berpotensi meningkatkan hak istimewa. Proc filesystem (procfs) adalah filesystem khusus di Linux yang menyajikan memori virtual proses sebagai file. Jalur file itu adalah `/proc/PID/mem`, di mana PID ID unik dari proses tersebut. Seorang aktor ancaman dapat menulis ke file ini untuk menyuntikkan kode ke dalam proses. Temuan ini mengidentifikasi upaya potensial untuk menulis ke file ini.

Agan GuardDuty runtime memantau peristiwa dari beberapa jenis sumber daya. Untuk mengidentifikasi sumber daya yang berpotensi dikompromikan, lihat Jenis sumber daya di panel temuan di GuardDuty konsol. Konteks tambahan, termasuk informasi garis keturunan proses dan proses, tersedia dalam temuan untuk penyelidikan lebih lanjut.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, jenis sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat [Remediasi temuan Runtime Monitoring](#).

DefenseEvasion:Runtime/ProcessInjection.Ptrace

Injeksi proses menggunakan panggilan sistem ptrace terdeteksi dalam wadah atau EC2 instance Amazon.

Tingkat keparahan default: Sedang

- Fitur: Pemantauan Runtime

Injeksi proses adalah teknik yang digunakan aktor ancaman untuk menyuntikkan kode ke dalam proses untuk menghindari pertahanan dan berpotensi meningkatkan hak istimewa. Suatu proses dapat menggunakan panggilan sistem `ptrace` untuk menyuntikkan kode ke proses lain. Temuan ini mengidentifikasi upaya potensial untuk menyuntikkan kode ke dalam proses menggunakan panggilan sistem `ptrace`.

Agen GuardDuty runtime memantau peristiwa dari beberapa jenis sumber daya. Untuk mengidentifikasi sumber daya yang berpotensi dikompromikan, lihat Jenis sumber daya di panel temuan di GuardDuty konsol. Konteks tambahan, termasuk informasi garis keturunan proses dan proses, tersedia dalam temuan untuk penyelidikan lebih lanjut.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, jenis sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat [Remediasi temuan Runtime Monitoring](#).

DefenseEvasion:Runtime/ProcessInjection.VirtualMemoryWrite

Injeksi proses melalui penulisan langsung ke memori virtual terdeteksi dalam wadah atau EC2 instance Amazon.

Tingkat keparahan default: Tinggi

- Fitur: Pemantauan Runtime

Injeksi proses adalah teknik yang digunakan aktor ancaman untuk menyuntikkan kode ke dalam proses untuk menghindari pertahanan dan berpotensi meningkatkan hak istimewa. Suatu proses dapat menggunakan panggilan sistem seperti `process_vm_writev` untuk langsung menyuntikkan kode ke memori virtual proses lain. Temuan ini mengidentifikasi upaya potensial untuk menyuntikkan kode ke dalam proses menggunakan panggilan sistem untuk menulis ke memori virtual dari proses tersebut.

Agen GuardDuty runtime memantau peristiwa dari beberapa jenis sumber daya. Untuk mengidentifikasi sumber daya yang berpotensi dikompromikan, lihat Jenis sumber daya di panel

temuan di GuardDuty konsol. Konteks tambahan, termasuk informasi garis keturunan proses dan proses, tersedia dalam temuan untuk penyelidikan lebih lanjut.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, jenis sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat [Remediasi temuan Runtime Monitoring](#).

Execution:Runtime/ReverseShell

Proses dalam wadah atau EC2 instance Amazon telah membuat shell terbalik.

Tingkat keparahan default: Tinggi

- Fitur: Pemantauan Runtime

Shell terbalik adalah sesi shell yang dibuat pada koneksi yang dimulai dari host target ke host aktor. Ini berlawanan dengan cangkang normal yang dimulai dari host aktor ke host target. Aktor ancaman membuat shell terbalik untuk menjalankan perintah pada target setelah mendapatkan akses awal ke target. Temuan ini mengidentifikasi koneksi shell terbalik yang berpotensi mencurigakan.

GuardDuty memeriksa aktivitas dan konteks runtime terkait, dan menghasilkan jenis temuan ini hanya jika aktivitas dan konteks terkait ditemukan tidak biasa atau mencurigakan. Konteks tambahan, termasuk informasi garis keturunan proses dan proses, tersedia dalam temuan untuk penyelidikan lebih lanjut.

Rekomendasi remediasi:

Agen GuardDuty keamanan memantau peristiwa dari berbagai sumber. Untuk mengidentifikasi sumber daya yang terkena dampak, lihat Jenis sumber daya di detail temuan di GuardDuty konsol. Jika aktivitas ini tidak terduga, jenis sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat [Remediasi temuan Runtime Monitoring](#).

DefenseEvasion:Runtime/FilelessExecution

Proses dalam wadah atau EC2 instance Amazon mengeksekusi kode dari memori.

Tingkat keparahan default: Sedang

- Fitur: Pemantauan Runtime

Temuan ini memberi tahu Anda ketika suatu proses dijalankan menggunakan file yang dapat dieksekusi dalam memori pada disk. Ini adalah teknik penghindaran pertahanan umum yang menghindari penulisan executable berbahaya ke disk untuk menghindari deteksi berbasis pemindaian sistem file. Meskipun teknik ini digunakan oleh malware, ia juga memiliki beberapa kasus penggunaan yang sah. Salah satu contohnya adalah compiler just-in-time (JIT) yang menulis kode dikompilasi ke memori dan mengeksekusinya dari memori.

Agan GuardDuty runtime memantau peristiwa dari beberapa jenis sumber daya. Untuk mengidentifikasi sumber daya yang berpotensi dikompromikan, lihat Jenis sumber daya di panel temuan di GuardDuty konsol. Konteks tambahan, termasuk informasi garis keturunan proses dan proses, tersedia dalam temuan untuk penyelidikan lebih lanjut.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat [Remediasi temuan Runtime Monitoring](#).

Impact:Runtime/CryptoMinerExecuted

Sebuah wadah atau EC2 instans Amazon mengeksekusi file biner yang terkait dengan aktivitas penambangan cryptocurrency.

Tingkat keparahan default: Tinggi

- Fitur: Pemantauan Runtime

Temuan ini memberi tahu Anda bahwa proses yang berjalan pada EC2 instance atau wadah yang terdaftar di AWS lingkungan Anda mengeksekusi file biner yang terkait dengan aktivitas penambangan cryptocurrency. Aktor ancaman mungkin berusaha untuk mengambil kendali atas sumber daya komputasi untuk menggunakannya kembali secara jahat untuk penambangan cryptocurrency yang tidak sah.

Agan GuardDuty runtime memantau peristiwa dari beberapa jenis sumber daya. Untuk mengidentifikasi sumber daya yang berpotensi dikompromikan, lihat Jenis sumber daya di panel temuan di GuardDuty konsol. Konteks tambahan, termasuk informasi garis keturunan proses dan proses, tersedia dalam temuan untuk penyelidikan lebih lanjut.

Rekomendasi remediasi:

Agan GuardDuty runtime memantau peristiwa dari berbagai sumber daya. Untuk mengidentifikasi sumber daya yang terpengaruh, lihat Jenis sumber daya dalam detail temuan di GuardDuty konsol dan lihat [Remediasi temuan Runtime Monitoring](#).

Execution:Runtime/NewLibraryLoaded

Pustaka yang baru dibuat atau yang baru dimodifikasi dimuat oleh proses di dalam wadah.

Tingkat keparahan default: Sedang

- Fitur: Pemantauan Runtime

Temuan ini memberi tahu Anda bahwa pustaka dibuat atau dimodifikasi di dalam wadah selama runtime dan dimuat oleh proses yang berjalan di dalam wadah. Praktik terbaik adalah menjaga kontainer tetap tidak berubah saat runtime, dan tidak membuat atau memodifikasi file biner, skrip, atau pustaka selama masa pakai penampung. Memuat pustaka yang baru dibuat atau dimodifikasi dalam wadah dapat menunjukkan aktivitas yang mencurigakan. Perilaku ini menunjukkan bahwa aktor jahat berpotensi memperoleh akses ke wadah, telah mengunduh, dan mengeksekusi malware atau perangkat lunak lain sebagai bagian dari potensi kompromi. Meskipun jenis aktivitas ini bisa menjadi indikasi kompromi, ini juga merupakan pola penggunaan yang umum. Oleh karena itu, GuardDuty gunakan mekanisme untuk mengidentifikasi contoh mencurigakan dari aktivitas ini dan menghasilkan jenis temuan ini hanya untuk contoh yang mencurigakan.

Agan GuardDuty runtime memantau peristiwa dari berbagai sumber daya. Untuk mengidentifikasi sumber daya yang terpengaruh, lihat Jenis sumber daya dalam detail temuan di GuardDuty konsol. Konteks tambahan, termasuk informasi garis keturunan proses dan proses, tersedia dalam temuan untuk penyelidikan lebih lanjut.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat [Remediasi temuan Runtime Monitoring](#).

PrivilegeEscalation:Runtime/ContainerMountsHostDirectory

Sebuah proses di dalam wadah memasang sistem file host saat runtime.

Tingkat keparahan default: Sedang

- Fitur: Pemantauan Runtime

Beberapa teknik pelarian kontainer melibatkan pemasangan sistem file host di dalam wadah saat runtime. Temuan ini memberi tahu Anda bahwa proses di dalam wadah berpotensi mencoba memasang sistem file host, yang mungkin menunjukkan upaya untuk melarikan diri ke host.

Agen GuardDuty runtime memantau peristiwa dari berbagai sumber daya. Untuk mengidentifikasi sumber daya yang terpengaruh, lihat Jenis sumber daya dalam detail temuan di GuardDuty konsol. Konteks tambahan, termasuk informasi garis keturunan proses dan proses, tersedia dalam temuan untuk penyelidikan lebih lanjut.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat [Remediasi temuan Runtime Monitoring](#).

PrivilegeEscalation:Runtime/UserfaultfdUsage

Sebuah proses yang digunakan **userfaultfd** sistem panggilan untuk menangani kesalahan halaman dalam ruang pengguna.

Tingkat keparahan default: Sedang

- Fitur: Pemantauan Runtime

Biasanya, kesalahan halaman ditangani oleh kernel di ruang kernel. Namun, panggilan `userfaultfd` sistem memungkinkan proses untuk menangani kesalahan halaman pada sistem file di ruang pengguna. Ini adalah fitur berguna yang memungkinkan implementasi sistem file ruang pengguna. Di sisi lain, ini juga dapat digunakan oleh proses yang berpotensi berbahaya untuk mengganggu kernel dari ruang pengguna. Menginterupsi kernel dengan menggunakan panggilan `userfaultfd` sistem adalah teknik eksploitasi umum untuk memperluas jendela balapan selama eksploitasi kondisi ras kernel. Penggunaan `userfaultfd` dapat menunjukkan aktivitas mencurigakan di instans Amazon Elastic Compute Cloud EC2 (Amazon).

Agen GuardDuty runtime memantau peristiwa dari berbagai sumber daya. Untuk mengidentifikasi sumber daya yang terpengaruh, lihat Jenis sumber daya dalam detail temuan di GuardDuty konsol.

Konteks tambahan, termasuk informasi garis keturunan proses dan proses, tersedia dalam temuan untuk penyelidikan lebih lanjut.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat [Remediasi temuan Runtime Monitoring](#).

Execution:Runtime/SuspiciousTool

Container atau EC2 instance Amazon menjalankan file biner atau skrip yang sering digunakan dalam skenario keamanan ofensif seperti keterlibatan pentesting.

Tingkat keparahan default: Variabel

Tingkat keparahan temuan ini bisa tinggi atau rendah, tergantung pada apakah alat mencurigakan yang terdeteksi dianggap penggunaan ganda atau hanya untuk penggunaan ofensif.

- Fitur: Pemantauan Runtime

Temuan ini memberi tahu Anda bahwa alat yang mencurigakan telah dieksekusi pada EC2 instance atau wadah di lingkungan Anda AWS . Ini termasuk alat yang digunakan dalam keterlibatan pentesting, juga dikenal sebagai alat backdoor, pemindai jaringan, dan sniffer jaringan. Semua alat ini dapat digunakan dalam konteks jinak tetapi juga sering digunakan oleh pelaku ancaman dengan niat jahat. Mengamati alat keamanan ofensif dapat menunjukkan bahwa EC2 contoh atau wadah terkait telah dikompromikan.

GuardDuty memeriksa aktivitas dan konteks runtime terkait sehingga menghasilkan temuan ini hanya ketika aktivitas dan konteks terkait berpotensi mencurigakan.

Agen GuardDuty runtime memantau peristiwa dari berbagai sumber daya. Untuk mengidentifikasi sumber daya yang terpengaruh, lihat Jenis sumber daya dalam detail temuan di GuardDuty konsol. Bila berlaku, konteks tambahan, termasuk informasi garis keturunan proses dan proses, tersedia dalam temuan untuk penyelidikan lebih lanjut.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat [Remediasi temuan Runtime Monitoring](#).

Execution:Runtime/SuspiciousCommand

Perintah mencurigakan telah dijalankan pada EC2 instance Amazon atau wadah yang menunjukkan kompromi.

Tingkat keparahan default: Variabel

Bergantung pada dampak dari pola berbahaya yang diamati, tingkat keparahan jenis temuan ini bisa rendah, sedang, atau tinggi.

- Fitur: Pemantauan Runtime

Temuan ini memberi tahu Anda bahwa perintah mencurigakan telah dijalankan dan ini menunjukkan bahwa EC2 instance Amazon atau wadah di AWS lingkungan Anda telah disusupi. Ini mungkin berarti bahwa file diunduh dari sumber yang mencurigakan dan kemudian dieksekusi, atau proses yang berjalan menampilkan pola berbahaya yang diketahui di baris perintahnya. Ini lebih lanjut menunjukkan bahwa malware berjalan di sistem.

GuardDuty memeriksa aktivitas dan konteks runtime terkait sehingga menghasilkan temuan ini hanya ketika aktivitas dan konteks terkait berpotensi mencurigakan.

Agen GuardDuty runtime memantau peristiwa dari berbagai sumber daya. Untuk mengidentifikasi sumber daya yang terpengaruh, lihat Jenis sumber daya dalam detail temuan di GuardDuty konsol. Bila berlaku, konteks tambahan, termasuk informasi garis keturunan proses dan proses, tersedia dalam temuan untuk penyelidikan lebih lanjut.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat [Remediasi temuan Runtime Monitoring](#).

DefenseEvasion:Runtime/SuspiciousCommand

Sebuah perintah telah dijalankan pada EC2 instance Amazon yang terdaftar atau wadah, ia mencoba untuk memodifikasi atau menonaktifkan mekanisme pertahanan Linux, seperti firewall atau layanan sistem penting.

Tingkat keparahan default: Variabel

Bergantung pada mekanisme pertahanan mana yang telah dimodifikasi atau dinonaktifkan, tingkat keparahan jenis temuan ini bisa tinggi, sedang, atau rendah.

- Fitur: Pemantauan Runtime

Temuan ini memberi tahu Anda bahwa perintah yang mencoba menyembunyikan serangan dari layanan keamanan sistem lokal, telah dieksekusi. Ini termasuk tindakan seperti menonaktifkan firewall Unix, memodifikasi tabel IP lokal, menghapus crontab entri, menonaktifkan layanan lokal, atau mengambil alih fungsi. `LDPreLoad` Modifikasi apa pun sangat mencurigakan dan merupakan indikator kompromi yang potensial. Oleh karena itu, mekanisme ini mendeteksi atau mencegah kompromi lebih lanjut dari sistem.

GuardDuty memeriksa aktivitas dan konteks runtime terkait sehingga menghasilkan temuan ini hanya ketika aktivitas dan konteks terkait berpotensi mencurigakan.

Agen GuardDuty runtime memantau peristiwa dari berbagai sumber daya. Untuk mengidentifikasi sumber daya yang berpotensi dikompromikan, lihat Jenis sumber daya dalam detail temuan di GuardDuty konsol. Bila berlaku, konteks tambahan, termasuk informasi garis keturunan proses dan proses, tersedia dalam temuan untuk penyelidikan lebih lanjut.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat [Remediasi temuan Runtime Monitoring](#).

DefenseEvasion:Runtime/PtraceAntiDebugging

Proses dalam wadah atau EC2 instans Amazon telah menjalankan tindakan anti-debugging menggunakan panggilan sistem `ptrace`.

Tingkat keparahan default: Rendah

- Fitur: Pemantauan Runtime

Temuan ini menunjukkan bahwa proses yang berjalan pada EC2 instance Amazon yang terdaftar atau wadah dalam AWS lingkungan Anda telah menggunakan panggilan sistem `ptrace` dengan `PTRACE_TRACEME` opsi tersebut. Aktivitas ini akan menyebabkan debugger terlampir terlepas

dari proses yang sedang berjalan. Jika tidak ada debugger yang terpasang, itu tidak berpengaruh. Namun, aktivitas itu sendiri menimbulkan kecurigaan. Ini mungkin menunjukkan bahwa malware berjalan di sistem. Malware sering menggunakan teknik anti-debugging untuk menghindari analisis, dan teknik ini dapat dideteksi saat runtime.

GuardDuty memeriksa aktivitas dan konteks runtime terkait sehingga menghasilkan temuan ini hanya ketika aktivitas dan konteks terkait berpotensi mencurigakan.

Agen GuardDuty runtime memantau peristiwa dari berbagai sumber daya. Untuk mengidentifikasi sumber daya yang terpengaruh, lihat Jenis sumber daya dalam detail temuan di GuardDuty konsol. Konteks tambahan, termasuk informasi garis keturunan proses dan proses, tersedia dalam temuan untuk penyelidikan lebih lanjut.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat [Remediasi temuan Runtime Monitoring](#).

Execution:Runtime/MaliciousFileExecuted

File executable berbahaya yang diketahui telah dieksekusi pada EC2 instance Amazon atau wadah.

Tingkat keparahan default: Tinggi

- Fitur: Pemantauan Runtime

Temuan ini memberi tahu Anda bahwa executable berbahaya yang diketahui telah dieksekusi di EC2 instans Amazon atau wadah di lingkungan Anda. AWS Ini adalah indikator kuat bahwa instance atau wadah berpotensi dikompromikan dan malware telah dieksekusi.

GuardDuty memeriksa aktivitas dan konteks runtime terkait sehingga menghasilkan temuan ini hanya ketika aktivitas dan konteks terkait berpotensi mencurigakan.

Agen GuardDuty runtime memantau peristiwa dari berbagai sumber daya. Untuk mengidentifikasi sumber daya yang terpengaruh, lihat Jenis sumber daya dalam detail temuan di GuardDuty konsol. Bila berlaku, konteks tambahan, termasuk informasi garis keturunan proses dan proses, tersedia dalam temuan untuk penyelidikan lebih lanjut.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat [Remediasi temuan Runtime Monitoring](#).

Execution:Runtime/SuspiciousShellCreated

Layanan jaringan atau proses yang dapat diakses jaringan pada EC2 instans Amazon, atau dalam wadah telah memulai proses shell interaktif.

Tingkat keparahan default: Rendah

- Fitur: Pemantauan Runtime

Temuan ini memberi tahu Anda bahwa layanan yang dapat diakses jaringan pada EC2 instans Amazon atau dalam wadah di AWS lingkungan Anda telah meluncurkan shell interaktif. Dalam keadaan tertentu, skenario ini dapat mengindikasikan perilaku pasca-eksploitasi. Shell interaktif memungkinkan penyerang untuk mengeksekusi perintah arbitrer pada instance atau wadah yang dikompromikan.

Agen GuardDuty runtime memantau peristiwa dari berbagai sumber daya. Untuk mengidentifikasi sumber daya yang terpengaruh, lihat Jenis sumber daya dalam detail temuan di GuardDuty konsol. Konteks tambahan, termasuk informasi garis keturunan proses dan proses, tersedia dalam temuan untuk penyelidikan lebih lanjut. Anda dapat melihat informasi proses yang dapat diakses jaringan di detail proses induk.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat [Remediasi temuan Runtime Monitoring](#).

PrivilegeEscalation:Runtime/ElevationToRoot

Proses yang berjalan pada EC2 instans atau penampung Amazon yang terdaftar telah mengasumsikan hak akses root.

Tingkat keparahan default: Sedang

- Fitur: Pemantauan Runtime

Temuan ini memberi tahu Anda bahwa proses yang berjalan di Amazon yang terdaftar EC2 atau dalam wadah yang terdaftar di AWS lingkungan Anda telah mengasumsikan hak akses root melalui eksekusi biner yang tidak biasa atau mencurigakansetuid. Ini menunjukkan bahwa proses yang sedang berjalan berpotensi dikompromikan, EC2 misalnya melalui eksploitasi, atau melalui setuid eksploitasi. Dengan menggunakan hak akses root, penyerang berpotensi mengeksekusi perintah pada instance atau container.

Meskipun GuardDuty dirancang untuk tidak menghasilkan jenis temuan ini untuk aktivitas yang melibatkan penggunaan sudo perintah secara teratur, itu akan menghasilkan temuan ini ketika mengidentifikasi aktivitas sebagai tidak biasa atau mencurigakan.

GuardDuty memeriksa aktivitas dan konteks runtime terkait, dan menghasilkan jenis temuan ini hanya jika aktivitas dan konteks terkait tidak biasa atau mencurigakan.

Agen GuardDuty runtime memantau peristiwa dari berbagai sumber daya. Untuk mengidentifikasi sumber daya yang terpengaruh, lihat Jenis sumber daya dalam detail temuan di GuardDuty konsol. Konteks tambahan, termasuk informasi garis keturunan proses dan proses, tersedia dalam temuan untuk penyelidikan lebih lanjut.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat [Remediasi temuan Runtime Monitoring](#).

Discovery:Runtime/SuspiciousCommand

Perintah mencurigakan telah dijalankan pada EC2 instans Amazon atau dalam wadah, yang memungkinkan penyerang untuk mendapatkan informasi tentang sistem lokal, AWS infrastruktur sekitarnya, atau infrastruktur kontainer.

Tingkat keparahan default: Rendah

Fitur: Pemantauan Runtime

Temuan ini memberi tahu Anda bahwa proses yang berjalan pada EC2 instans atau wadah Amazon yang terdaftar di AWS lingkungan Anda telah menjalankan perintah yang mungkin memberi penyerang informasi penting untuk berpotensi memajukan serangan. Informasi berikut mungkin telah diambil:

- Sistem lokal seperti konfigurasi pengguna atau jaringan,
- AWS Sumber daya dan izin lain yang tersedia, atau
- Infrastruktur Kubernetes seperti layanan dan pod.

EC2 Instance Amazon atau wadah yang tercantum dalam detail temuan mungkin telah disusupi.

Agen GuardDuty runtime memantau peristiwa dari beberapa jenis sumber daya. Untuk mengidentifikasi sumber daya yang berpotensi dikompromikan, lihat Jenis sumber daya dalam detail temuan di GuardDuty konsol. Anda dapat menemukan detail tentang perintah mencurigakan di `service.runtimeDetails.context` bidang penemuan JSON. Konteks tambahan, termasuk informasi garis keturunan proses dan proses, tersedia dalam temuan untuk penyelidikan lebih lanjut.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat [Remediasi temuan Runtime Monitoring](#).

Persistence:Runtime/SuspiciousCommand

Perintah mencurigakan telah dijalankan pada EC2 instans Amazon atau dalam wadah, yang memungkinkan penyerang untuk mempertahankan akses dan kontrol di lingkungan Anda. AWS

Tingkat keparahan default: Sedang

- Fitur: Pemantauan Runtime

Temuan ini memberi tahu Anda bahwa proses yang berjalan pada EC2 instance Amazon yang terdaftar atau dalam wadah di AWS lingkungan Anda telah menjalankan perintah yang mencurigakan. Perintah ini menginstal metode persistensi yang memungkinkan malware berjalan tanpa gangguan, atau memungkinkan penyerang untuk terus mengakses instance atau tipe sumber daya kontainer yang berpotensi dikompromikan. Ini berpotensi berarti bahwa layanan sistem telah diinstal atau dimodifikasi, `crontab` telah dimodifikasi, atau pengguna baru telah ditambahkan ke konfigurasi sistem.

GuardDuty memeriksa aktivitas dan konteks runtime terkait, dan menghasilkan jenis temuan ini hanya jika aktivitas dan konteks terkait tidak biasa atau mencurigakan.

EC2 Instance Amazon atau wadah yang tercantum dalam detail temuan mungkin telah disusupi.

Agen GuardDuty runtime memantau peristiwa dari berbagai sumber daya. Untuk mengidentifikasi sumber daya yang berpotensi dikompromikan, lihat Jenis sumber daya dalam detail temuan di GuardDuty konsol. Anda dapat menemukan detail tentang perintah mencurigakan di `service.runtimeDetails.context` bidang penemuan JSON. Bila berlaku, konteks tambahan, termasuk informasi garis keturunan proses dan proses, tersedia dalam temuan untuk penyelidikan lebih lanjut.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat [Remediasi temuan Runtime Monitoring](#).

PrivilegeEscalation:Runtime/SuspiciousCommand

Perintah mencurigakan telah dijalankan pada EC2 instance Amazon atau dalam wadah, yang memungkinkan penyerang untuk meningkatkan hak istimewa.

Tingkat keparahan default: Sedang

- Fitur: Pemantauan Runtime

Temuan ini memberi tahu Anda bahwa proses yang berjalan pada EC2 instance Amazon yang terdaftar atau dalam wadah di AWS lingkungan Anda telah menjalankan perintah yang mencurigakan. Perintah mencoba untuk melakukan eskalasi hak istimewa, yang memungkinkan musuh untuk melakukan tugas-tugas hak istimewa yang tinggi.

GuardDuty memeriksa aktivitas dan konteks runtime terkait, dan menghasilkan jenis temuan ini hanya jika aktivitas dan konteks terkait tidak biasa atau mencurigakan.

EC2 Instance Amazon atau wadah yang tercantum dalam detail temuan mungkin telah disusupi.

Agen GuardDuty runtime memantau peristiwa dari berbagai sumber daya. Untuk mengidentifikasi sumber daya yang terpengaruh, lihat Jenis sumber daya dalam detail temuan di GuardDuty konsol. Bila berlaku, konteks tambahan, termasuk informasi garis keturunan proses dan proses, tersedia dalam temuan untuk penyelidikan lebih lanjut.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Lihat informasi yang lebih lengkap di [Remediasi temuan Runtime Monitoring](#).

Perlindungan Malware untuk EC2 menemukan jenis

GuardDuty Perlindungan Malware untuk EC2 menyediakan Perlindungan Malware tunggal untuk EC2 menemukan semua ancaman yang terdeteksi selama pemindaian EC2 instance atau beban kerja kontainer. Temuan ini mencakup jumlah total deteksi yang dilakukan selama pemindaian, dan berdasarkan tingkat keparahannya, memberikan rincian untuk 32 ancaman teratas yang dideteksi. Tidak seperti GuardDuty temuan lain, Perlindungan Malware untuk EC2 temuan tidak diperbarui ketika EC2 instance atau beban kerja kontainer yang sama dipindai lagi.

Perlindungan Malware baru untuk EC2 penemuan dihasilkan untuk setiap pemindaian yang mendeteksi malware. Perlindungan Malware untuk EC2 temuan mencakup informasi tentang pemindaian yang sesuai yang menghasilkan temuan serta GuardDuty temuan yang memulai pemindaian ini. Ini membuatnya lebih mudah untuk menghubungkan perilaku mencurigakan dengan malware yang terdeteksi.

Note

Saat GuardDuty mendeteksi aktivitas berbahaya pada beban kerja kontainer, Perlindungan Malware for EC2 tidak menghasilkan temuan EC2 level.

Temuan berikut khusus untuk Perlindungan GuardDuty Malware untuk EC2.

Topik

- [Execution:EC2/MaliciousFile](#)
- [Execution:ECS/MaliciousFile](#)
- [Execution:Kubernetes/MaliciousFile](#)
- [Execution:Container/MaliciousFile](#)
- [Execution:EC2/SuspiciousFile](#)
- [Execution:ECS/SuspiciousFile](#)
- [Execution:Kubernetes/SuspiciousFile](#)
- [Execution:Container/SuspiciousFile](#)

Execution:EC2/MaliciousFile

File berbahaya telah terdeteksi pada sebuah EC2 instance.

Tingkat keparahan default: Bervariasi tergantung pada ancaman yang terdeteksi.

- Fitur: Perlindungan Malware EBS

Temuan ini menunjukkan bahwa Perlindungan GuardDuty Malware untuk EC2 pemindaian telah mendeteksi satu atau lebih file berbahaya pada EC2 instance yang terdaftar di AWS lingkungan Anda. Contoh yang terdaftar ini mungkin dikompromikan. Untuk informasi selengkapnya, lihat bagian Terdeteksi ancaman di detail temuan.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, instans Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memperbaiki instans Amazon yang berpotensi dikompromikan EC2](#).

Execution:ECS/MaliciousFile

File berbahaya telah terdeteksi pada cluster ECS.

Tingkat keparahan default: Bervariasi tergantung pada ancaman yang terdeteksi.

- Fitur: Perlindungan Malware EBS

Temuan ini menunjukkan bahwa Perlindungan GuardDuty Malware untuk EC2 pemindaian telah mendeteksi satu atau lebih file berbahaya pada beban kerja kontainer milik cluster ECS. Untuk informasi selengkapnya, lihat bagian Terdeteksi ancaman di detail temuan.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, kontainer milik klaster ECS dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memulihkan cluster ECS yang berpotensi dikompromikan](#).

Execution:Kubernetes/MaliciousFile

File berbahaya telah terdeteksi di klaster Kubernetes.

Tingkat keparahan default: Bervariasi tergantung pada ancaman yang terdeteksi.

- Fitur: Perlindungan Malware EBS

Temuan ini menunjukkan bahwa Perlindungan GuardDuty Malware untuk EC2 pemindaian telah mendeteksi satu atau lebih file berbahaya pada beban kerja kontainer milik cluster Kubernetes. Jika ini adalah cluster yang dikelola EKS, detail temuan akan memberikan informasi tambahan tentang sumber daya EKS yang terkena dampak. Untuk informasi selengkapnya, lihat bagian Terdeteksi ancaman di detail temuan.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, beban kerja kontainer Anda mungkin terganggu. Untuk informasi selengkapnya, lihat [Remediasi temuan Perlindungan EKS](#).

Execution:Container/MaliciousFile

File berbahaya telah terdeteksi pada wadah mandiri.

Tingkat keparahan default: Bervariasi tergantung pada ancaman yang terdeteksi.

- Fitur: Perlindungan Malware EBS

Temuan ini menunjukkan bahwa Perlindungan GuardDuty Malware untuk EC2 pemindaian telah mendeteksi satu atau lebih file berbahaya pada beban kerja kontainer dan tidak ada informasi cluster yang diidentifikasi. Untuk informasi selengkapnya, lihat bagian Terdeteksi ancaman di detail temuan.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, beban kerja kontainer Anda mungkin terganggu. Untuk informasi selengkapnya, lihat [Memulihkan wadah mandiri yang berpotensi dikompromikan](#).

Execution:EC2/SuspiciousFile

File yang mencurigakan telah terdeteksi pada sebuah EC2 instance.

Tingkat keparahan default: Bervariasi tergantung pada ancaman yang terdeteksi.

- Fitur: Perlindungan Malware EBS

Temuan ini menunjukkan bahwa Perlindungan GuardDuty Malware untuk EC2 pemindaian telah mendeteksi satu atau lebih file yang mencurigakan pada sebuah EC2 instance. Untuk informasi selengkapnya, lihat bagian Terdeteksi ancaman di detail temuan.

SuspiciousFileDeteksi jenis menunjukkan bahwa program yang berpotensi tidak diinginkan seperti adware, spyware, atau alat penggunaan ganda hadir pada sumber daya yang terkena dampak. Program-program ini dapat memiliki dampak negatif pada sumber daya Anda, atau digunakan oleh penyerang untuk tujuan jahat. Misalnya, alat jaringan dapat digunakan secara sah atau jahat oleh musuh sebagai alat hack untuk mencoba dan mengkompromikan sumber daya.

Ketika file mencurigakan telah terdeteksi, evaluasi apakah Anda berharap untuk melihat file yang terdeteksi di AWS lingkungan Anda. Jika file tidak terduga, ikuti rekomendasi remediasi yang disediakan di bagian selanjutnya.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, instans Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memperbaiki instans Amazon yang berpotensi dikompromikan EC2](#).

Execution:ECS/SuspiciousFile

File mencurigakan telah terdeteksi pada cluster ECS.

Tingkat keparahan default: Bervariasi tergantung pada ancaman yang terdeteksi.

- Fitur: Perlindungan Malware EBS

Temuan ini menunjukkan bahwa Perlindungan GuardDuty Malware untuk EC2 pemindaian telah mendeteksi satu atau lebih file mencurigakan pada wadah milik cluster ECS. Untuk informasi selengkapnya, lihat bagian Terdeteksi ancaman di detail temuan.

SuspiciousFileDeteksi jenis menunjukkan bahwa program yang berpotensi tidak diinginkan seperti adware, spyware, atau alat penggunaan ganda hadir pada sumber daya yang terkena dampak. Program-program ini dapat memiliki dampak negatif pada sumber daya Anda, atau

digunakan oleh penyerang untuk tujuan jahat. Misalnya, alat jaringan dapat digunakan secara sah atau jahat oleh musuh sebagai alat hack untuk mencoba dan mengkompromikan sumber daya.

Ketika file mencurigakan telah terdeteksi, evaluasi apakah Anda berharap untuk melihat file yang terdeteksi di AWS lingkungan Anda. Jika file tidak terduga, ikuti rekomendasi remediasi yang disediakan di bagian selanjutnya.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, kontainer milik kluster ECS dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memulihkan cluster ECS yang berpotensi dikompromikan](#).

Execution:Kubernetes/SuspiciousFile

Sebuah file mencurigakan telah terdeteksi pada kluster Kubernetes.

Tingkat keparahan default: Bervariasi tergantung pada ancaman yang terdeteksi.

- Fitur: Perlindungan Malware EBS

Temuan ini menunjukkan bahwa Perlindungan GuardDuty Malware untuk EC2 pemindaian telah mendeteksi satu atau lebih file mencurigakan pada wadah milik cluster Kubernetes. Jika ini adalah cluster yang dikelola EKS, detail temuan akan memberikan informasi tambahan tentang EKS yang terkena dampak. Untuk informasi selengkapnya, lihat bagian Terdeteksi ancaman di detail temuan.

SuspiciousFileDeteksi jenis menunjukkan bahwa program yang berpotensi tidak diinginkan seperti adware, spyware, atau alat penggunaan ganda hadir pada sumber daya yang terkena dampak. Program-program ini dapat memiliki dampak negatif pada sumber daya Anda, atau digunakan oleh penyerang untuk tujuan jahat. Misalnya, alat jaringan dapat digunakan secara sah atau jahat oleh musuh sebagai alat hack untuk mencoba dan mengkompromikan sumber daya.

Ketika file mencurigakan telah terdeteksi, evaluasi apakah Anda berharap untuk melihat file yang terdeteksi di AWS lingkungan Anda. Jika file tidak terduga, ikuti rekomendasi remediasi yang disediakan di bagian selanjutnya.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, beban kerja kontainer Anda mungkin terganggu. Untuk informasi selengkapnya, lihat [Remediasi temuan Perlindungan EKS](#).

Execution:Container/SuspiciousFile

File mencurigakan telah terdeteksi pada wadah mandiri.

Tingkat keparahan default: Bervariasi tergantung pada ancaman yang terdeteksi.

- Fitur: Perlindungan Malware EBS

Temuan ini menunjukkan bahwa Perlindungan GuardDuty Malware untuk EC2 pemindaian telah mendeteksi satu atau lebih file mencurigakan pada wadah tanpa informasi cluster. Untuk informasi selengkapnya, lihat bagian Terdeteksi ancaman di detail temuan.

SuspiciousFileDeteksi jenis menunjukkan bahwa program yang berpotensi tidak diinginkan seperti adware, spyware, atau alat penggunaan ganda hadir pada sumber daya yang terkena dampak. Program-program ini dapat memiliki dampak negatif pada sumber daya Anda, atau digunakan oleh penyerang untuk tujuan jahat. Misalnya, alat jaringan dapat digunakan secara sah atau jahat oleh musuh sebagai alat hack untuk mencoba dan mengkompromikan sumber daya.

Ketika file mencurigakan telah terdeteksi, evaluasi apakah Anda berharap untuk melihat file yang terdeteksi di AWS lingkungan Anda. Jika file tidak terduga, ikuti rekomendasi remediasi yang disediakan di bagian selanjutnya.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, beban kerja kontainer Anda mungkin terganggu. Untuk informasi selengkapnya, lihat [Memulihkan wadah mandiri yang berpotensi dikompromikan](#).

Perlindungan Malware untuk tipe pencarian S3

GuardDuty menghasilkan temuan hanya ketika mendeteksi potensi ancaman keamanan di Anda Akun AWS. Perlindungan Malware untuk temuan S3 menunjukkan bahwa objek yang diunggah yang memulai pemindaian malware berisi file yang berpotensi berbahaya.

GuardDuty Agar Amazon dapat menghasilkan temuan di Anda Akun AWS, aktifkan keduanya GuardDuty dan Perlindungan Malware untuk S3. Praktik terbaik adalah mengaktifkan terlebih dahulu GuardDuty dan kemudian Perlindungan Malware untuk S3. Jika pesanan ini berbeda untuk Anda, pastikan untuk mengaktifkan GuardDuty sebelum objek S3 diunggah ke bucket Anda yang dilindungi.

 Note

GuardDuty tidak dapat menghasilkan temuan untuk objek S3 yang dipindai sebelum Anda mengaktifkan. GuardDuty Untuk memindai objek S3 yang ada, Anda dapat mengunggahnya lagi.

Object:S3/MaliciousFile

File berbahaya telah terdeteksi pada objek S3 yang dipindai.

Tingkat keparahan default: Tinggi

- Fitur: Perlindungan Malware untuk S3

Temuan ini menunjukkan bahwa pemindaian malware telah mendeteksi objek S3 yang terdaftar sebagai berbahaya. Untuk informasi selengkapnya, lihat bagian Ancaman terdeteksi di panel rincian pencarian.

Remediasi rekomendasi:

Jika temuan ini tidak terduga, objek S3 berpotensi berbahaya. Untuk informasi tentang langkah-langkah remediasi yang direkomendasikan, lihat [Memperbaiki objek S3 yang berpotensi berbahaya](#).

GuardDuty Jenis temuan Perlindungan RDS

GuardDuty RDS Protection mendeteksi perilaku login anomali pada instance database Anda.

Temuan berikut khusus untuk [Basis data Amazon Aurora, Amazon RDS, dan Aurora Limitless yang didukung](#) dan akan memiliki Jenis Sumber Daya RDSDBInstance atau RDSLimitlessDB. Tingkat keparahan dan detail temuan akan berbeda berdasarkan jenis temuan.

Topik

- [CredentialAccess:RDS/AnomalousBehavior.SuccessfulLogin](#)
- [CredentialAccess:RDS/AnomalousBehavior.FailedLogin](#)
- [CredentialAccess:RDS/AnomalousBehavior.SuccessfulBruteForce](#)
- [CredentialAccess:RDS/MaliciousIPCaller.SuccessfulLogin](#)

- [CredentialAccess:RDS/MaliciousIPCaller.FailedLogin](#)
- [Discovery:RDS/MaliciousIPCaller](#)
- [CredentialAccess:RDS/TorIPCaller.SuccessfulLogin](#)
- [CredentialAccess:RDS/TorIPCaller.FailedLogin](#)
- [Discovery:RDS/TorIPCaller](#)

CredentialAccess:RDS/AnomalousBehavior.SuccessfulLogin

Seorang pengguna berhasil masuk ke database RDS di akun Anda dengan cara yang anomali.

Tingkat keparahan default: Variabel

Note

Bergantung pada perilaku anomali yang terkait dengan temuan ini, tingkat keparahan default dapat Rendah, Sedang, dan Tinggi.

- Rendah — Jika nama pengguna yang terkait dengan temuan ini masuk dari alamat IP yang terkait dengan jaringan pribadi.
- Medium — Jika nama pengguna yang terkait dengan temuan ini masuk dari alamat IP publik.
- Tinggi — Jika ada pola yang konsisten dari upaya login yang gagal dari alamat IP publik yang menunjukkan kebijakan akses yang terlalu permisif.

- Fitur: Pemantauan aktivitas login RDS

Temuan ini memberi tahu Anda bahwa login yang berhasil anomali diamati pada database RDS di lingkungan Anda. AWS Ini mungkin menunjukkan bahwa pengguna tak terlihat sebelumnya masuk ke database RDS untuk pertama kalinya. Skenario umum adalah pengguna internal yang masuk ke database yang diakses secara terprogram oleh aplikasi dan bukan oleh pengguna individu.

Login yang berhasil ini diidentifikasi sebagai anomali oleh model pembelajaran mesin deteksi GuardDuty anomali (ML). Model ML mengevaluasi semua peristiwa login database di Anda [Basis](#)

[data Amazon Aurora, Amazon RDS, dan Aurora Limitless yang didukung](#) dan mengidentifikasi peristiwa anomali yang terkait dengan teknik yang digunakan oleh musuh. Model ML melacak berbagai faktor aktivitas login RDS seperti pengguna yang membuat permintaan, lokasi permintaan dibuat, dan detail koneksi database spesifik yang digunakan. Untuk informasi tentang peristiwa login yang berpotensi tidak biasa, lihat [Anomali berbasis aktivitas login RDS](#).

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga untuk database terkait, disarankan untuk mengubah kata sandi pengguna database terkait, dan meninjau log audit yang tersedia untuk aktivitas yang dilakukan oleh pengguna anomali. Temuan tingkat keparahan sedang dan tinggi dapat mengindikasikan bahwa ada kebijakan akses yang terlalu permisif ke database, dan kredensial pengguna mungkin telah terpapar atau dikompromikan. Disarankan untuk menempatkan database di VPC pribadi, dan membatasi aturan grup keamanan untuk mengizinkan lalu lintas hanya dari sumber yang diperlukan. Untuk informasi selengkapnya, lihat [Memulihkan database yang berpotensi dikompromikan dengan peristiwa login yang berhasil](#).

CredentialAccess:RDS/AnomalousBehavior.FailedLogin

Satu atau lebih upaya login gagal yang tidak biasa diamati pada database RDS di akun Anda.

Tingkat keparahan default: Rendah

- Fitur: Pemantauan aktivitas login RDS

Temuan ini memberi tahu Anda bahwa satu atau lebih login gagal anomali diamati pada database RDS di lingkungan Anda. AWS Upaya login yang gagal dari alamat IP publik dapat mengindikasikan bahwa database RDS di akun Anda telah mengalami percobaan serangan brute force oleh aktor yang berpotensi jahat.

Login yang gagal ini diidentifikasi sebagai anomali oleh model pembelajaran mesin deteksi GuardDuty anomali (ML). Model ML mengevaluasi semua peristiwa login database di Anda [Basis data Amazon Aurora, Amazon RDS, dan Aurora Limitless yang didukung](#) dan mengidentifikasi peristiwa anomali yang terkait dengan teknik yang digunakan oleh musuh. Model ML melacak berbagai faktor aktivitas login RDS seperti pengguna yang membuat permintaan, lokasi permintaan dibuat, dan detail koneksi database spesifik yang digunakan. Untuk informasi tentang aktivitas login RDS yang berpotensi tidak biasa, lihat [Anomali berbasis aktivitas login RDS](#).

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga untuk database terkait, ini mungkin mengindikasikan bahwa database diekspos secara publik atau ada kebijakan akses yang terlalu permisif ke database. Disarankan untuk menempatkan database di VPC pribadi, dan membatasi aturan grup keamanan untuk mengizinkan lalu lintas hanya dari sumber yang diperlukan. Untuk informasi selengkapnya, lihat [Memulihkan database yang berpotensi dikompromikan dengan peristiwa login yang gagal](#).

CredentialAccess:RDS/AnomalousBehavior.SuccessfulBruteForce

Seorang pengguna berhasil masuk ke database RDS di akun Anda dari alamat IP publik dengan cara anomali setelah pola konsisten dari upaya login gagal yang tidak biasa.

Tingkat keparahan default: Tinggi

- Fitur: Pemantauan aktivitas login RDS

Temuan ini memberi tahu Anda bahwa indikasi login anomali dari kekuatan kasar yang berhasil diamati pada database RDS di lingkungan Anda. AWS Sebelum login berhasil anomali, pola konsisten dari upaya login gagal yang tidak biasa diamati. Ini menunjukkan bahwa pengguna dan kata sandi yang terkait dengan database RDS di akun Anda mungkin telah disusupi, dan database RDS mungkin telah diakses oleh aktor yang berpotensi jahat.

Login brute force yang berhasil ini diidentifikasi sebagai anomali oleh model pembelajaran mesin deteksi GuardDuty anomali (ML). Model ML mengevaluasi semua peristiwa login database di Anda [Basis data Amazon Aurora, Amazon RDS, dan Aurora Limitless yang didukung](#) dan mengidentifikasi peristiwa anomali yang terkait dengan teknik yang digunakan oleh musuh. Model ML melacak berbagai faktor aktivitas login RDS seperti pengguna yang membuat permintaan, lokasi permintaan dibuat, dan detail koneksi database spesifik yang digunakan. Untuk informasi tentang aktivitas login RDS yang berpotensi tidak biasa, lihat [Anomali berbasis aktivitas login RDS](#).

Rekomendasi remediasi:

Aktivitas ini menunjukkan bahwa kredensial database mungkin telah diekspos atau dikompromikan. Disarankan untuk mengubah kata sandi pengguna database terkait, dan meninjau log audit yang tersedia untuk aktivitas yang dilakukan oleh pengguna yang berpotensi disusupi. Pola konsisten dari

upaya login gagal yang tidak biasa menunjukkan kebijakan akses yang terlalu permisif ke database atau database mungkin juga telah diekspos publik. Disarankan untuk menempatkan database di VPC pribadi, dan membatasi aturan grup keamanan untuk mengizinkan lalu lintas hanya dari sumber yang diperlukan. Untuk informasi selengkapnya, lihat [Memulihkan database yang berpotensi dikompromikan dengan peristiwa login yang berhasil](#).

CredentialAccess:RDS/MaliciousIPCaller.SuccessfulLogin

Seorang pengguna berhasil masuk ke database RDS di akun Anda dari alamat IP berbahaya yang diketahui.

Tingkat keparahan default: Tinggi

- Fitur: Pemantauan aktivitas login RDS

Temuan ini memberi tahu Anda bahwa aktivitas login RDS yang berhasil terjadi dari alamat IP yang dikaitkan dengan aktivitas berbahaya yang diketahui di lingkungan Anda AWS . Ini menunjukkan bahwa pengguna dan kata sandi yang terkait dengan database RDS di akun Anda mungkin telah disusupi, dan database RDS mungkin telah diakses oleh aktor yang berpotensi jahat.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga untuk database terkait, ini mungkin menunjukkan bahwa kredensial pengguna mungkin telah diekspos atau disusupi. Disarankan untuk mengubah kata sandi pengguna database terkait, dan meninjau log audit yang tersedia untuk aktivitas yang dilakukan oleh pengguna yang disusupi. Aktivitas ini juga dapat menunjukkan bahwa ada kebijakan akses yang terlalu permisif ke database atau database diekspos secara publik. Disarankan untuk menempatkan database di VPC pribadi, dan membatasi aturan grup keamanan untuk mengizinkan lalu lintas hanya dari sumber yang diperlukan. Untuk informasi selengkapnya, lihat [Memulihkan database yang berpotensi dikompromikan dengan peristiwa login yang berhasil](#).

CredentialAccess:RDS/MaliciousIPCaller.FailedLogin

Alamat IP yang dikaitkan dengan aktivitas berbahaya yang diketahui tidak berhasil mencoba masuk ke database RDS di akun Anda.

Tingkat keparahan default: Sedang

- Fitur: Pemantauan aktivitas login RDS

Temuan ini memberi tahu Anda bahwa alamat IP yang terkait dengan aktivitas berbahaya yang diketahui mencoba masuk ke database RDS di AWS lingkungan Anda, tetapi gagal memberikan nama pengguna atau kata sandi yang benar. Ini menunjukkan bahwa aktor yang berpotensi jahat mungkin mencoba untuk mengkompromikan database RDS di akun Anda.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga untuk database terkait, ini mungkin menunjukkan bahwa ada kebijakan akses yang terlalu permisif ke database atau database diekspos secara publik. Disarankan untuk menempatkan database di VPC pribadi, dan membatasi aturan grup keamanan untuk mengizinkan lalu lintas hanya dari sumber yang diperlukan. Untuk informasi selengkapnya, lihat [Memulihkan database yang berpotensi dikompromikan dengan peristiwa login yang gagal](#).

Discovery:RDS/MaliciousIPCaller

Alamat IP yang dikaitkan dengan aktivitas berbahaya yang diketahui memeriksa database RDS di akun Anda; tidak ada upaya otentikasi yang dilakukan.

Tingkat keparahan default: Sedang

- Fitur: Pemantauan aktivitas login RDS

Temuan ini memberi tahu Anda bahwa alamat IP yang terkait dengan aktivitas berbahaya yang diketahui menyelidiki database RDS di AWS lingkungan Anda, meskipun tidak ada upaya login yang dilakukan. Ini mungkin menunjukkan bahwa aktor yang berpotensi jahat sedang mencoba memindai infrastruktur yang dapat diakses publik.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga untuk database terkait, ini mungkin menunjukkan bahwa ada kebijakan akses yang terlalu permisif ke database atau database diekspos secara publik. Disarankan untuk menempatkan database di VPC pribadi, dan membatasi aturan grup keamanan untuk mengizinkan lalu lintas hanya dari sumber yang diperlukan. Untuk informasi selengkapnya, lihat [Memulihkan database yang berpotensi dikompromikan dengan peristiwa login yang gagal](#).

CredentialAccess:RDS/TorIPCaller.SuccessfulLogin

Seorang pengguna berhasil masuk ke database RDS di akun Anda dari alamat IP node keluar Tor.

Tingkat keparahan default: Tinggi

- Fitur: Pemantauan aktivitas login RDS

Temuan ini memberi tahu Anda bahwa pengguna berhasil masuk ke database RDS di AWS lingkungan Anda, dari alamat IP node keluar Tor. Tor adalah perangkat lunak untuk memungkinkan komunikasi anonim. Ini mengenkripsi dan secara acak mengalihkan komunikasi melalui relay antara serangkaian node jaringan. Node Tor terakhir disebut sebagai node keluar. Ini dapat menunjukkan akses tidak sah ke sumber daya RDS di akun Anda, dengan maksud menyembunyikan identitas asli pengguna anonim.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga untuk database terkait, ini mungkin menunjukkan bahwa kredensial pengguna mungkin telah diekspos atau disusupi. Disarankan untuk mengubah kata sandi pengguna database terkait, dan meninjau log audit yang tersedia untuk aktivitas yang dilakukan oleh pengguna yang disusupi. Aktivitas ini juga dapat menunjukkan bahwa ada kebijakan akses yang terlalu permisif ke database atau database diekspos secara publik. Disarankan untuk menempatkan database di VPC pribadi, dan membatasi aturan grup keamanan untuk mengizinkan lalu lintas hanya dari sumber yang diperlukan. Untuk informasi selengkapnya, lihat [Memulihkan database yang berpotensi dikompromikan dengan peristiwa login yang berhasil](#).

CredentialAccess:RDS/TorIPCaller.FailedLogin

Alamat IP Tor mencoba untuk tidak berhasil masuk ke database RDS di akun Anda.

Tingkat keparahan default: Sedang

- Fitur: Pemantauan aktivitas login RDS

Temuan ini memberi tahu Anda bahwa alamat IP node keluar Tor mencoba masuk ke database RDS di AWS lingkungan Anda, tetapi gagal memberikan nama pengguna atau kata sandi yang benar. Tor

adalah perangkat lunak untuk memungkinkan komunikasi anonim. Ini mengenkripsi dan secara acak mengalihkan komunikasi melalui relay antara serangkaian node jaringan. Node Tor terakhir disebut sebagai nod keluar. Ini dapat menunjukkan akses tidak sah ke sumber daya RDS di akun Anda, dengan maksud menyembunyikan identitas asli pengguna anonim.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga untuk database terkait, ini mungkin menunjukkan bahwa ada kebijakan akses yang terlalu permisif ke database atau database diekspos secara publik. Disarankan untuk menempatkan database di VPC pribadi, dan membatasi aturan grup keamanan untuk mengizinkan lalu lintas hanya dari sumber yang diperlukan. Untuk informasi selengkapnya, lihat [Memulihkan database yang berpotensi dikompromikan dengan peristiwa login yang gagal](#).

Discovery:RDS/TorIPCaller

Alamat IP node keluar Tor memeriksa database RDS di akun Anda, tidak ada upaya otentikasi yang dilakukan.

Tingkat keparahan default: Sedang

- Fitur: Pemantauan aktivitas login RDS

Temuan ini memberi tahu Anda bahwa alamat IP node keluar Tor memeriksa database RDS di AWS lingkungan Anda, meskipun tidak ada upaya login yang dilakukan. Ini mungkin menunjukkan bahwa aktor yang berpotensi jahat sedang mencoba memindai infrastruktur yang dapat diakses publik. Tor adalah perangkat lunak untuk memungkinkan komunikasi anonim. Ini mengenkripsi dan memantulkan komunikasi melalui relay antara serangkaian node jaringan. Node Tor terakhir disebut sebagai nod keluar. Ini dapat menunjukkan akses tidak sah ke sumber daya RDS di akun Anda, dengan maksud menyembunyikan identitas asli aktor yang berpotensi jahat.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga untuk database terkait, ini mungkin menunjukkan bahwa ada kebijakan akses yang terlalu permisif ke database atau database diekspos secara publik. Disarankan untuk menempatkan database di VPC pribadi, dan membatasi aturan grup keamanan untuk mengizinkan lalu lintas hanya dari sumber yang diperlukan. Lihat informasi yang lebih lengkap di [Memulihkan database yang berpotensi dikompromikan dengan peristiwa login yang gagal](#).

Jenis temuan Perlindungan Lambda

Bagian ini menjelaskan jenis temuan yang spesifik untuk AWS Lambda sumber daya Anda dan memiliki yang `resourceType` terdaftar sebagai Lambda. Untuk semua temuan Lambda, kami sarankan Anda memeriksa sumber daya yang dimaksud dan menentukan apakah itu berperilaku dengan cara yang diharapkan. Jika aktivitas diotorisasi, Anda dapat menggunakan [aturan Suppression](#) atau [IP Tepercaya dan daftar ancaman](#) untuk mencegah pemberitahuan positif palsu untuk sumber daya tersebut.

Jika aktivitasnya tidak terduga, praktik terbaik keamanan adalah mengasumsikan bahwa Lambda berpotensi dikompromikan dan mengikuti rekomendasi remediasi.

Topik

- [Backdoor:Lambda/C&CActivity.B](#)
- [CryptoCurrency:Lambda/BitcoinTool.B](#)
- [Trojan:Lambda/BlackholeTraffic](#)
- [Trojan:Lambda/DropPoint](#)
- [UnauthorizedAccess:Lambda/MaliciousIPCaller.Custom](#)
- [UnauthorizedAccess:Lambda/TorClient](#)
- [UnauthorizedAccess:Lambda/TorRelay](#)

Backdoor:Lambda/C&CActivity.B

Fungsi Lambda adalah menanyakan alamat IP yang terkait dengan server perintah dan kontrol yang dikenal.

Tingkat keparahan default: Tinggi

- Fitur: Pemantauan Aktivitas Jaringan Lambda

Temuan ini memberi tahu Anda bahwa fungsi Lambda yang terdaftar di lingkungan AWS Anda menanyakan alamat IP yang terkait dengan server perintah dan kontrol (C&C) yang dikenal. Fungsi Lambda yang terkait dengan temuan yang dihasilkan berpotensi dikompromikan. Server C&C adalah komputer yang mengeluarkan perintah kepada anggota botnet.

Botnet adalah kumpulan perangkat yang terhubung ke internet, yang mungkin termasuk PCs, server, perangkat seluler, dan perangkat Internet of Things, yang terinfeksi dan dikendalikan oleh jenis malware yang umum. Botnet sering digunakan untuk mendistribusikan malware dan mengumpulkan informasi yang disalahgunakan, seperti nomor kartu kredit. Tergantung pada tujuan dan struktur botnet, server C&C mungkin juga mengeluarkan perintah untuk memulai penolakan layanan terdistribusi.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, fungsi Lambda Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memperbaiki fungsi Lambda yang berpotensi dikompromikan](#).

CryptoCurrency:Lambda/BitcoinTool.B

Fungsi Lambda adalah menanyakan alamat IP yang terkait dengan aktivitas terkait cryptocurrency.

Tingkat keparahan default: Tinggi

- Fitur: Pemantauan Aktivitas Jaringan Lambda

Temuan ini memberi tahu Anda bahwa fungsi Lambda yang terdaftar di lingkungan AWS Anda menanyakan alamat IP yang terkait dengan Bitcoin atau aktivitas terkait cryptocurrency lainnya. Aktor ancaman mungkin berusaha untuk mengambil kendali atas fungsi Lambda untuk menggunakannya kembali dengan jahat untuk penambangan cryptocurrency yang tidak sah.

Rekomendasi remediasi:

Jika Anda menggunakan fungsi Lambda ini untuk menambang atau mengelola cryptocurrency, atau fungsi ini terlibat dalam aktivitas blockchain, ini berpotensi menjadi aktivitas yang diharapkan untuk lingkungan Anda. Jika ini terjadi di AWS lingkungan Anda, kami sarankan Anda membuat aturan penindasan untuk temuan ini. Aturan penekanan harus terdiri dari dua kriteria filter. Kriteria pertama harus menggunakan atribut tipe temuan dengan nilai CryptoCurrency:Lambda/BitcoinTool.B. Kriteria filter kedua harus menjadi nama fungsi Lambda dari fungsi yang terlibat dalam aktivitas blockchain. Untuk informasi tentang membuat aturan penindasan, lihat Aturan [penindasan](#).

Jika aktivitas ini tidak terduga, fungsi Lambda Anda berpotensi dikompromikan. Untuk informasi selengkapnya, lihat [Memperbaiki fungsi Lambda yang berpotensi dikompromikan](#).

Trojan:Lambda/BlackholeTraffic

Fungsi Lambda mencoba berkomunikasi dengan alamat IP host jarak jauh yang merupakan lubang hitam yang dikenal.

Tingkat keparahan default: Sedang

- Fitur: Pemantauan Aktivitas Jaringan Lambda

Temuan ini memberi tahu Anda bahwa fungsi Lambda yang terdaftar di lingkungan AWS Anda mencoba berkomunikasi dengan alamat IP lubang hitam (atau lubang wastafel). Lubang hitam adalah tempat di jaringan di mana lalu lintas masuk atau keluar dibuang secara diam-diam tanpa memberi tahu sumber bahwa data tidak mencapai penerima yang dituju. Alamat IP lubang hitam menentukan mesin host yang tidak berjalan atau alamat yang tidak ada host yang ditugaskan. Fungsi Lambda yang terdaftar berpotensi dikompromikan.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, fungsi Lambda Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memperbaiki fungsi Lambda yang berpotensi dikompromikan](#).

Trojan:Lambda/DropPoint

Fungsi Lambda mencoba berkomunikasi dengan alamat IP dari host jarak jauh yang diketahui memiliki kredensi dan data curian lainnya yang ditangkap oleh malware.

Tingkat keparahan default: Sedang

- Fitur: Pemantauan Aktivitas Jaringan Lambda

Temuan ini memberi tahu Anda bahwa fungsi Lambda yang terdaftar di lingkungan AWS Anda mencoba berkomunikasi dengan alamat IP host jarak jauh yang diketahui menyimpan kredensial dan data curian lainnya yang ditangkap oleh malware.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, fungsi Lambda Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memperbaiki fungsi Lambda yang berpotensi dikompromikan](#).

UnauthorizedAccess:Lambda/MaliciousIPCaller.Custom

Fungsi Lambda membuat koneksi ke alamat IP pada daftar ancaman khusus.

Tingkat keparahan default: Sedang

- Fitur: Pemantauan Aktivitas Jaringan Lambda

Temuan ini memberi tahu Anda bahwa fungsi Lambda di lingkungan AWS Anda berkomunikasi dengan alamat IP yang disertakan dalam daftar ancaman yang Anda unggah. Dalam GuardDuty, [daftar ancaman](#) terdiri dari alamat IP berbahaya yang diketahui. GuardDuty menghasilkan temuan berdasarkan daftar ancaman yang diunggah. Anda dapat melihat detail daftar ancaman di detail temuan di GuardDuty konsol.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, fungsi Lambda Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memperbaiki fungsi Lambda yang berpotensi dikompromikan](#).

UnauthorizedAccess:Lambda/TorClient

Fungsi Lambda adalah membuat koneksi ke Tor Guard atau node Authority.

Tingkat keparahan default: Tinggi

- Fitur: Pemantauan Aktivitas Jaringan Lambda

Temuan ini memberi tahu Anda bahwa fungsi Lambda di lingkungan AWS Anda membuat koneksi ke Tor Guard atau node Authority. Tor adalah perangkat lunak untuk memungkinkan komunikasi anonim. Tor Guards dan Authority node bertindak sebagai gateway awal ke dalam jaringan Tor. Lalu lintas ini dapat menunjukkan bahwa fungsi Lambda ini berpotensi dikompromikan. Sekarang bertindak sebagai klien di jaringan Tor.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, fungsi Lambda Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memperbaiki fungsi Lambda yang berpotensi dikompromikan](#).

UnauthorizedAccess:Lambda/TorRelay

Fungsi Lambda adalah membuat koneksi ke jaringan Tor sebagai relay Tor.

Tingkat keparahan default: Tinggi

- Fitur: Pemantauan Aktivitas Jaringan Lambda

Temuan ini memberi tahu Anda bahwa fungsi Lambda di lingkungan AWS Anda membuat koneksi ke jaringan Tor dengan cara yang menunjukkan bahwa itu bertindak sebagai relai Tor. Tor adalah perangkat lunak untuk memungkinkan komunikasi anonim. Tor memungkinkan komunikasi anonim dengan meneruskan lalu lintas berpotensi ilegal klien dari satu relay Tor ke yang lain.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, fungsi Lambda Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memperbaiki fungsi Lambda yang berpotensi dikompromikan](#).

Tipe temuan yang sudah dihentikan

Temuan adalah pemberitahuan yang berisi rincian tentang potensi masalah keamanan yang GuardDuty ditemukan. Untuk informasi tentang perubahan penting pada jenis GuardDuty temuan, termasuk jenis temuan yang baru ditambahkan atau yang sudah pensiun, lihat [Riwayat dokumen untuk Amazon GuardDuty](#).

Jenis temuan berikut sudah pensiun dan tidak lagi dihasilkan oleh GuardDuty.

Important

Anda tidak dapat mengaktifkan kembali tipe GuardDuty temuan yang sudah pensiun.

Topik

- [Exfiltration:S3/ObjectRead.Unusual](#)
- [Impact:S3/PermissionsModification.Unusual](#)
- [Impact:S3/ObjectDelete.Unusual](#)

- [Discovery:S3/BucketEnumeration.Unusual](#)
- [Persistence:IAMUser/NetworkPermissions](#)
- [Persistence:IAMUser/ResourcePermissions](#)
- [Persistence:IAMUser/UserPermissions](#)
- [PrivilegeEscalation:IAMUser/AdministrativePermissions](#)
- [Recon:IAMUser/NetworkPermissions](#)
- [Recon:IAMUser/ResourcePermissions](#)
- [Recon:IAMUser/UserPermissions](#)
- [ResourceConsumption:IAMUser/ComputeResources](#)
- [Stealth:IAMUser/LoggingConfigurationModified](#)
- [UnauthorizedAccess:IAMUser/ConsoleLogin](#)
- [UnauthorizedAccess:EC2/TorIPCaller](#)
- [Backdoor:EC2/XORDDOS](#)
- [Behavior:IAMUser/InstanceLaunchUnusual](#)
- [CryptoCurrency:EC2/BitcoinTool.A](#)
- [UnauthorizedAccess:IAMUser/UnusualASNCaller](#)

Exfiltration:S3/ObjectRead.Unusual

Entitas IAM memanggil API S3 dengan cara yang mencurigakan.

Tingkat keparahan default: Sedang*

Note

Tingkat kepelikan default temuan ini adalah Medium. Namun, jika API dipanggil menggunakan AWS kredensial sementara yang dibuat pada sebuah instance, tingkat keparahan temuannya adalah Tinggi.

- Sumber data: peristiwa CloudTrail data untuk S3

Temuan ini memberi tahu Anda bahwa entitas IAM di AWS lingkungan Anda melakukan panggilan API yang melibatkan bucket S3 dan yang berbeda dari baseline yang ditetapkan entitas tersebut. Panggilan API yang digunakan dalam aktivitas ini dikaitkan dengan tahap eksfiltrasi serangan, ketika penyerang sedang mencoba untuk mengumpulkan data. Aktivitas ini mencurigakan karena cara entitas IAM memanggil API tidak biasa. Misalnya, entitas IAM ini sebelumnya tidak memiliki riwayat memanggil tipe API ini, atau API dipanggil dari lokasi yang tidak biasa.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga untuk prinsipal terkait, ini mungkin menunjukkan bahwa kredensial telah diekspos atau izin S3 Anda tidak cukup membatasi. Untuk informasi selengkapnya, lihat [Memperbaiki bucket S3 yang berpotensi dikompromikan](#).

Impact:S3/PermissionsModification.Unusual

Entitas IAM memanggil API untuk mengubah izin pada satu sumber daya S3 atau lebih.

Tingkat keparahan default: Sedang*

Note

Tingkat kepelikan default temuan ini adalah Medium. Namun, jika API dipanggil menggunakan AWS kredensial sementara yang dibuat pada sebuah instance, tingkat keparahan temuannya adalah Tinggi.

Temuan ini menginformasikan bahwa entitas IAM membuat panggilan API yang dirancang untuk mengubah izin pada satu atau lebih bucket atau objek di lingkungan AWS Anda. Tindakan ini dapat dilakukan oleh penyerang untuk memungkinkan informasi dibagikan di luar akun. Aktivitas ini mencurigakan karena cara entitas IAM memanggil API tidak biasa. Misalnya, entitas IAM ini sebelumnya tidak memiliki riwayat memanggil tipe API ini, atau API dipanggil dari lokasi yang tidak biasa.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga untuk prinsipal terkait, ini mungkin menunjukkan bahwa kredensial telah diekspos atau izin S3 Anda tidak cukup membatasi. Untuk informasi selengkapnya, lihat [Memperbaiki bucket S3 yang berpotensi dikompromikan](#).

Impact:S3/ObjectDelete.Unusual

Entitas IAM memanggil API yang digunakan untuk menghapus data dalam bucket S3.

Tingkat keparahan default: Sedang*

Note

Tingkat kepelikan default temuan ini adalah Medium. Namun, jika API dipanggil menggunakan AWS kredensial sementara yang dibuat pada sebuah instance, tingkat keparahan temuannya adalah Tinggi.

Temuan ini memberi tahu Anda bahwa entitas IAM tertentu di AWS lingkungan Anda membuat panggilan API yang dirancang untuk menghapus data di bucket S3 yang terdaftar dengan menghapus bucket itu sendiri. Aktivitas ini mencurigakan karena cara entitas IAM memanggil API tidak biasa. Misalnya, entitas IAM ini sebelumnya tidak memiliki riwayat memanggil tipe API ini, atau API dipanggil dari lokasi yang tidak biasa.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga untuk prinsipal terkait, ini mungkin menunjukkan bahwa kredensial telah diekspos atau izin S3 Anda tidak cukup membatasi. Untuk informasi selengkapnya, lihat [Memperbaiki bucket S3 yang berpotensi dikompromikan](#).

Discovery:S3/BucketEnumeration.Unusual

Entitas IAM memanggil API S3 yang digunakan untuk menemukan bucket S3 dalam jaringan Anda.

Tingkat keparahan default: Sedang*

Note

Tingkat kepelikan default temuan ini adalah Medium. Namun, jika API dipanggil menggunakan AWS kredensial sementara yang dibuat pada sebuah instance, tingkat keparahan temuannya adalah Tinggi.

Temuan ini menginformasikan bahwa entitas IAM telah memanggil API S3 untuk menemukan bucket S3 dalam lingkungan Anda, seperti `ListBuckets`. Jenis aktivitas ini dikaitkan dengan tahap penemuan serangan di mana penyerang mengumpulkan informasi untuk menentukan apakah AWS lingkungan Anda rentan terhadap serangan yang lebih luas. Aktivitas ini mencurigakan karena cara entitas IAM memanggil API tidak biasa. Misalnya, entitas IAM ini sebelumnya tidak memiliki riwayat memanggil tipe API ini, atau API dipanggil dari lokasi yang tidak biasa.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga untuk prinsipal terkait, ini mungkin menunjukkan bahwa kredensial telah diekspos atau izin S3 Anda tidak cukup membatasi. Untuk informasi selengkapnya, lihat [Memperbaiki bucket S3 yang berpotensi dikompromikan](#).

Persistence:IAMUser/NetworkPermissions

Entitas IAM memanggil API yang biasa digunakan untuk mengubah izin akses jaringan untuk grup keamanan, rute, dan ACLs di akun Anda. AWS

Tingkat keparahan default: Sedang*

Note

Tingkat kepelikan default temuan ini adalah Medium. Namun, jika API dipanggil menggunakan AWS kredensial sementara yang dibuat pada sebuah instance, tingkat keparahan temuannya adalah Tinggi.

Temuan ini menunjukkan bahwa prinsipal tertentu (Pengguna root akun AWS, peran IAM, atau pengguna) di AWS lingkungan Anda menunjukkan perilaku yang berbeda dari baseline yang ditetapkan. Prinsipal ini sebelumnya tidak memiliki riwayat memanggil API ini.

Temuan ini dipicu ketika pengaturan konfigurasi jaringan berubah dalam keadaan yang mencurigakan, seperti ketika prinsipal memanggil API `CreateSecurityGroup` tanpa riwayat sebelumnya. Penyerang sering mencoba untuk mengubah kelompok keamanan untuk memungkinkan lalu lintas masuk tertentu di berbagai port untuk meningkatkan kemampuan mereka untuk mengakses sebuah EC2 instance.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, kredensi Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memulihkan kredensi yang berpotensi dikompromikan AWS](#).

Persistence:IAMUser/ResourcePermissions

Seorang prinsipal memanggil API yang biasa digunakan untuk mengubah kebijakan akses keamanan berbagai sumber daya di Akun AWS.

Tingkat keparahan default: Sedang*

Note

Tingkat keparahan default temuan ini adalah Medium. Namun, jika API yang dipanggil menggunakan AWS kredensial sementara yang dibuat pada sebuah instance, tingkat keparahan temuannya adalah Tinggi.

Temuan ini menunjukkan bahwa prinsipal tertentu (Pengguna root akun AWS, peran IAM, atau pengguna) di AWS lingkungan Anda menunjukkan perilaku yang berbeda dari baseline yang ditetapkan. Prinsipal ini sebelumnya tidak memiliki riwayat memanggil API ini.

Temuan ini dipicu ketika perubahan terdeteksi pada kebijakan atau izin yang dilampirkan ke AWS sumber daya, seperti ketika prinsipal di AWS lingkungan Anda memanggil PutBucketPolicy API tanpa riwayat sebelumnya untuk melakukannya. Beberapa layanan, seperti Amazon S3, mendukung izin yang melekat pada sumber daya yang memberikan satu akses utama atau lebih ke sumber daya. Dengan kredensial curian, penyerang dapat mengubah kebijakan yang melekat pada sumber daya untuk memperoleh akses ke sumber daya tersebut.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, kredensi Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memulihkan kredensi yang berpotensi dikompromikan AWS](#).

Persistence:IAMUser/UserPermissions

Prinsipal memanggil API yang biasa digunakan untuk menambah, memodifikasi, atau menghapus pengguna, grup, atau kebijakan IAM di akun Anda AWS .

Tingkat keparahan default: Sedang*

Note

Tingkat kepelikan default temuan ini adalah Medium. Namun, jika API dipanggil menggunakan AWS kredensial sementara yang dibuat pada sebuah instance, tingkat keparahan temuannya adalah Tinggi.

Temuan ini menunjukkan bahwa prinsipal tertentu (Pengguna root akun AWS, peran IAM, atau pengguna) di AWS lingkungan Anda menunjukkan perilaku yang berbeda dari baseline yang ditetapkan. Prinsipal ini sebelumnya tidak memiliki riwayat memanggil API ini.

Temuan ini dipicu oleh perubahan mencurigakan pada izin terkait pengguna di AWS lingkungan Anda, seperti saat prinsipal di AWS lingkungan Anda memanggil `AttachUserPolicy` API tanpa riwayat sebelumnya untuk melakukannya. Penyerang dapat menggunakan kredensial curian untuk membuat pengguna baru, menambahkan kebijakan akses ke pengguna yang ada, atau membuat kunci akses untuk memaksimalkan akses mereka ke akun, bahkan jika titik akses asli mereka ditutup. Misalnya, pemilik akun mungkin memperhatikan bahwa pengguna atau kata sandi IAM tertentu telah dicuri dan menghapusnya dari akun. Namun, mereka mungkin tidak menghapus pengguna lain yang dibuat oleh kepala admin yang dibuat secara curang, sehingga AWS akun mereka dapat diakses oleh penyerang.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, kredensi Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memulihkan kredensi yang berpotensi dikompromikan AWS](#).

PrivilegeEscalation:IAMUser/AdministrativePermissions

Prinsipal telah berusaha untuk menetapkan kebijakan yang sangat permisif untuk diri mereka sendiri.

Tingkat keparahan default: Rendah*

Note

Tingkat kepelikan temuan ini Rendah jika upaya eskalasi hak istimewa tidak berhasil, dan Medium jika upaya eskalasi hak istimewa berhasil.

Temuan ini menunjukkan bahwa entitas IAM tertentu di AWS lingkungan Anda menunjukkan perilaku yang dapat menjadi indikasi serangan eskalasi hak istimewa. Temuan ini dipicu ketika pengguna atau IAM role mencoba untuk menetapkan kebijakan yang sangat permisif untuk diri mereka sendiri. Jika pengguna atau peran yang dimaksud tidak dimaksudkan untuk memiliki hak administratif, kredensial pengguna dapat disusupi atau izin peran mungkin tidak dikonfigurasi dengan benar.

Penyerang akan menggunakan kredensial curian untuk membuat pengguna baru, menambahkan kebijakan akses ke pengguna yang ada, atau membuat kunci akses untuk memaksimalkan akses mereka ke akun bahkan jika titik akses asli mereka ditutup. Misalnya, pemilik akun mungkin memperhatikan bahwa kredensi masuk pengguna IAM tertentu dicuri dan dihapus dari akun, tetapi mungkin tidak menghapus pengguna lain yang dibuat oleh kepala admin yang dibuat secara curang, sehingga AWS akun mereka masih dapat diakses oleh penyerang.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, kredensi Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memulihkan kredensi yang berpotensi dikompromikan AWS](#).

Recon:IAMUser/NetworkPermissions

Prinsipal memanggil API yang biasa digunakan untuk mengubah izin akses jaringan untuk grup keamanan, rute, dan ACLs di akun Anda AWS .

Tingkat keparahan default: Sedang*

Note

Tingkat kepelikan default temuan ini adalah Medium. Namun, jika API dipanggil menggunakan AWS kredensial sementara yang dibuat pada sebuah instance, tingkat keparahan temuannya adalah Tinggi.

Temuan ini menunjukkan bahwa prinsipal tertentu (Pengguna root akun AWS, peran IAM, atau pengguna) di AWS lingkungan Anda menunjukkan perilaku yang berbeda dari baseline yang ditetapkan. Prinsipal ini sebelumnya tidak memiliki riwayat memanggil API ini.

Temuan ini dipicu ketika izin akses sumber daya di akun AWS Anda diperiksa dalam keadaan yang mencurigakan. Misalnya, jika prinsipal memanggil API `DescribeInstances` tanpa riwayat

sebelumnya. Seorang penyerang mungkin menggunakan kredensial curian untuk melakukan jenis pengintaian AWS sumber daya Anda untuk menemukan kredensial yang lebih berharga atau menentukan kemampuan kredensial yang sudah mereka miliki.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, kredensi Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memulihkan kredensi yang berpotensi dikompromikan AWS](#).

Recon:IAMUser/ResourcePermissions

Seorang prinsipal memanggil API yang biasa digunakan untuk mengubah kebijakan akses keamanan berbagai sumber daya di AWS akun Anda.

Tingkat keparahan default: Sedang*

Note

Tingkat keparahan default temuan ini adalah Medium. Namun, jika API dipanggil menggunakan AWS kredensial sementara yang dibuat pada sebuah instance, tingkat keparahan temuannya adalah Tinggi.

Temuan ini menunjukkan bahwa prinsipal tertentu (Pengguna root akun AWS, peran IAM, atau pengguna) di AWS lingkungan Anda menunjukkan perilaku yang berbeda dari baseline yang ditetapkan. Prinsipal ini sebelumnya tidak memiliki riwayat memanggil API ini.

Temuan ini dipicu ketika izin akses sumber daya di akun AWS Anda diperiksa dalam keadaan yang mencurigakan. Misalnya, jika prinsipal memanggil API `DescribeInstances` tanpa riwayat sebelumnya. Seorang penyerang mungkin menggunakan kredensial curian untuk melakukan jenis pengintaian AWS sumber daya Anda untuk menemukan kredensial yang lebih berharga atau menentukan kemampuan kredensial yang sudah mereka miliki.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, kredensi Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memulihkan kredensi yang berpotensi dikompromikan AWS](#).

Recon:IAMUser/UserPermissions

Prinsipal memanggil API yang biasa digunakan untuk menambah, mengubah, atau menghapus pengguna, grup, atau kebijakan IAM di akun AWS Anda.

Tingkat keparahan default: Sedang*

Note

Tingkat kepelikan default temuan ini adalah Medium. Namun, jika API dipanggil menggunakan AWS kredensial sementara yang dibuat pada sebuah instance, tingkat keparahan temuannya adalah Tinggi.

Temuan ini dipicu ketika izin pengguna di AWS lingkungan Anda diselidiki dalam keadaan yang mencurigakan. Misalnya, jika prinsipal (Pengguna root akun AWS, peran IAM, atau pengguna IAM) memanggil `ListInstanceProfilesForRole` API tanpa riwayat sebelumnya untuk melakukannya. Seorang penyerang mungkin menggunakan kredensial curian untuk melakukan jenis pengintaian AWS sumber daya Anda untuk menemukan kredensial yang lebih berharga atau menentukan kemampuan kredensial yang sudah mereka miliki.

Temuan ini menunjukkan bahwa prinsip tertentu di AWS lingkungan Anda menunjukkan perilaku yang berbeda dari garis dasar yang ditetapkan. Prinsipal ini sebelumnya tidak memiliki riwayat memanggil API ini dengan cara ini.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, kredensi Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memulihkan kredensi yang berpotensi dikompromikan AWS](#).

ResourceConsumption:IAMUser/ComputeResources

Seorang prinsipal memanggil API yang biasa digunakan untuk meluncurkan sumber daya Komputasi seperti EC2 Instans.

Tingkat keparahan default: Sedang*

Note

Tingkat kepelikan default temuan ini adalah Medium. Namun, jika API dipanggil menggunakan AWS kredensial sementara yang dibuat pada sebuah instance, tingkat keparahan temuannya adalah Tinggi.

Temuan ini dipicu ketika EC2 instance di akun yang terdaftar di AWS lingkungan Anda diluncurkan dalam keadaan yang mencurigakan. Temuan ini menunjukkan bahwa prinsip tertentu di AWS lingkungan Anda menunjukkan perilaku yang berbeda dari baseline yang ditetapkan; misalnya, jika prinsipal (, peran IAM Pengguna root akun AWS, atau pengguna IAM) memanggil RunInstances API tanpa riwayat sebelumnya untuk melakukannya. Ini mungkin merupakan indikasi penyerang menggunakan kredensial curian untuk mencuri waktu komputasi (mungkin untuk penambangan mata uang kripto atau peretasan kata sandi). Ini juga bisa menjadi indikasi penyerang menggunakan EC2 instance di AWS lingkungan Anda dan kredensialnya untuk mempertahankan akses ke akun Anda.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, kredensi Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memulihkan kredensi yang berpotensi dikompromikan AWS](#).

Stealth:IAMUser/LoggingConfigurationModified

Prinsipal memanggil API yang biasa digunakan untuk menghentikan CloudTrail Logging, menghapus log yang ada, dan menghilangkan jejak aktivitas di AWS akun Anda.

Tingkat keparahan default: Sedang*

Note

Tingkat kepelikan default temuan ini adalah Medium. Namun, jika API dipanggil menggunakan AWS kredensial sementara yang dibuat pada sebuah instance, tingkat keparahan temuannya adalah Tinggi.

Temuan ini dipicu ketika konfigurasi pencatatan log di akun AWS yang terdaftar dalam lingkungan Anda diubah dalam keadaan yang mencurigakan. Temuan ini memberi tahu Anda bahwa prinsip tertentu di AWS lingkungan Anda menunjukkan perilaku yang berbeda dari garis dasar yang ditetapkan; misalnya, jika prinsipal (, peran IAM Pengguna root akun AWS, atau pengguna IAM) memanggil API tanpa riwayat sebelumnya untuk melakukannya. StopLogging Ini bisa menjadi indikasi penyerang yang mencoba menutupi jejak mereka dengan menghilangkan jejak aktivitas mereka.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, kredensi Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memulihkan kredensi yang berpotensi dikompromikan AWS](#).

UnauthorizedAccess:IAMUser/ConsoleLogin

Login konsol yang tidak biasa oleh kepala sekolah di AWS akun Anda diamati.

Tingkat keparahan default: Sedang*

Note

Tingkat keparahan default temuan ini adalah Medium. Namun, jika API dipanggil menggunakan AWS kredensial sementara yang dibuat pada sebuah instance, tingkat keparahan temuannya adalah Tinggi.

Temuan ini dipicu ketika login konsol terdeteksi dalam keadaan yang mencurigakan. Misalnya, jika prinsipal tanpa riwayat sebelumnya melakukannya, memanggil ConsoleLogin API dari never-before-used klien atau lokasi yang tidak biasa. Ini bisa menjadi indikasi kredensial curian yang digunakan untuk mendapatkan akses ke AWS akun Anda, atau pengguna yang valid mengakses akun dengan cara yang tidak valid atau kurang aman (misalnya, tidak melalui VPN yang disetujui).

Temuan ini memberi tahu Anda bahwa prinsip tertentu di AWS lingkungan Anda menunjukkan perilaku yang berbeda dari garis dasar yang ditetapkan. Prinsipal ini tidak memiliki riwayat aktivitas login sebelumnya menggunakan aplikasi klien ini dari lokasi spesifik ini.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, kredensi Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memulihkan kredensi yang berpotensi dikompromikan AWS](#).

UnauthorizedAccess:EC2/TorIPCaller

EC2 Instance Anda menerima koneksi masuk dari node keluar Tor.

Tingkat keparahan default: Sedang

Temuan ini memberi tahu Anda bahwa sebuah EC2 instance di AWS lingkungan Anda menerima koneksi masuk dari node keluar Tor. Tor adalah perangkat lunak untuk memungkinkan komunikasi anonim. Ini mengenkripsi dan secara acak mengalihkan komunikasi melalui relay antara serangkaian node jaringan. Node Tor terakhir disebut sebagai node keluar. Temuan ini dapat menunjukkan akses tidak sah ke AWS sumber daya Anda dengan maksud menyembunyikan identitas asli penyerang.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, instans Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memperbaiki instans Amazon yang berpotensi dikompromikan EC2](#).

Backdoor:EC2/XORDDOS

Sebuah EC2 instance mencoba berkomunikasi dengan alamat IP yang terkait dengan malware XOR DDoS.

Tingkat keparahan default: Tinggi

Temuan ini memberi tahu Anda bahwa sebuah EC2 instance di AWS lingkungan Anda mencoba berkomunikasi dengan alamat IP yang terkait dengan malware XOR DDoS. EC2 Contoh ini mungkin dikompromikan. XOR DDoS adalah malware Trojan yang membajak sistem Linux. Untuk mendapatkan akses ke sistem, malware ini meluncurkan serangan brute force untuk memperoleh kata sandi ke layanan Secure Shell (SSH) di Linux. Setelah kredensi SSH diperoleh dan login berhasil, ia menggunakan hak pengguna root untuk menjalankan skrip yang mengunduh dan menginstal XOR DDoS. Malware ini kemudian digunakan sebagai bagian dari botnet untuk meluncurkan serangan penolakan layanan terdistribusi (DDoS) terhadap target lain.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, instans Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memperbaiki instans Amazon yang berpotensi dikompromikan EC2](#).

Behavior:IAMUser/InstanceLaunchUnusual

Seorang pengguna meluncurkan EC2 instance dari tipe yang tidak biasa.

Tingkat keparahan default: Tinggi

Temuan ini memberi tahu Anda bahwa pengguna tertentu di AWS lingkungan Anda menunjukkan perilaku yang berbeda dari baseline yang ditetapkan. Pengguna ini tidak memiliki riwayat peluncuran EC2 instance jenis ini sebelumnya. Kredensi masuk Anda mungkin terganggu.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, kredensi Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memulihkan kredensi yang berpotensi dikompromikan AWS](#).

CryptoCurrency:EC2/BitcoinTool.A

EC2 misalnya berkomunikasi dengan kolam penambangan Bitcoin.

Tingkat keparahan default: Tinggi

Temuan ini memberi tahu Anda bahwa sebuah EC2 contoh di AWS lingkungan Anda berkomunikasi dengan kumpulan penambangan Bitcoin. Di bidang penambangan mata uang kripto, kolam penambangan adalah kolam sumber daya penambang yang berbagi kekuatan pemrosesan mereka melalui jaringan untuk membagi hadiah sesuai dengan jumlah pekerjaan yang mereka kontribusikan untuk memecahkan blok. Kecuali Anda menggunakan EC2 contoh ini untuk penambangan Bitcoin, EC2 instans Anda mungkin dikompromikan.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, instans Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memperbaiki instans Amazon yang berpotensi dikompromikan EC2](#).

UnauthorizedAccess:IAMUser/UnusualASNCaller

API dipanggil dari alamat IP dari jaringan yang tidak biasa.

Tingkat keparahan default: Tinggi

Temuan ini menginformasikan bahwa aktivitas tertentu dipanggil dari alamat IP dari jaringan yang tidak biasa. Jaringan ini tidak pernah diamati di seluruh riwayat penggunaan AWS dari pengguna yang dimaksud. Aktivitas ini dapat mencakup login konsol, upaya untuk meluncurkan EC2 instance, membuat pengguna IAM baru, memodifikasi AWS hak istimewa Anda, dll. Ini dapat menunjukkan akses tidak sah ke AWS sumber daya Anda.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, kredensi Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memulihkan kredensi yang berpotensi dikompromikan AWS](#).

GuardDuty menemukan jenis dengan sumber daya yang berpotensi terkena dampak

Halaman-halaman berikut dikategorikan berdasarkan jenis sumber daya yang berpotensi terkena dampak yang terkait dengan GuardDuty temuan:

- [EC2 menemukan jenis](#)
- [Tipe temuan IAM](#)
- [Jenis pencarian urutan serangan](#)
- [Jenis temuan Perlindungan S3](#)
- [Jenis penemuan Perlindungan EKS](#)
- [Jenis penemuan Runtime Monitoring](#)
- [Perlindungan Malware untuk EC2 menemukan jenis](#)
- [Perlindungan Malware untuk tipe pencarian S3](#)
- [Jenis temuan Perlindungan RDS](#)
- [Jenis temuan Perlindungan Lambda](#)

GuardDuty jenis temuan aktif

Tabel berikut menunjukkan semua jenis temuan aktif yang diurutkan berdasarkan sumber atau fitur data dasar, sebagaimana berlaku. Dalam tabel berikut, beberapa temuan memiliki nilai kolom Finding severity yang ditandai dengan tanda bintang (*) atau tanda plus (+):

* Jenis temuan ini memiliki tingkat keparahan yang bervariasi. Temuan jenis tertentu mungkin memiliki tingkat keparahan yang berbeda tergantung pada konteks khusus untuk temuan tersebut. Untuk informasi selengkapnya tentang jenis temuan, lihat deskripsi detailnya.

+ EC2 temuan yang menggunakan log aliran VPC sebagai sumber data tidak mendukung IPv6 lalu lintas.

Tipe temuan	Jenis sumber daya	Sumber/fitur data dasar	Menemukan tingkat keparahan
Discovery:S3/AnomalousBehavior	Amazon S3	CloudTrail peristiwa data untuk S3	Rendah
Discovery:S3/MaliciousIPCaller	Amazon S3	CloudTrail peristiwa data untuk S3	Tinggi
Discovery:S3/MaliciousIPCaller.Custom	Amazon S3	CloudTrail peristiwa data untuk S3	Tinggi
Discovery:S3/TorIPCaller	Amazon S3	CloudTrail peristiwa data untuk S3	Sedang
Exfiltration:S3/AnomalousBehavior	Amazon S3	CloudTrail peristiwa data untuk S3	Tinggi
Exfiltration:S3/MaliciousIPCaller	Amazon S3	CloudTrail peristiwa data untuk S3	Tinggi
Impact:S3/AnomalousBehavior.Delete	Amazon S3	CloudTrail peristiwa data untuk S3	Tinggi
Impact:S3/AnomalousBehavior.Permission	Amazon S3	CloudTrail peristiwa data untuk S3	Tinggi
Impact:S3/AnomalousBehavior.Write	Amazon S3	CloudTrail peristiwa data untuk S3	Sedang
Impact:S3/MaliciousIPCaller	Amazon S3	CloudTrail peristiwa data untuk S3	Tinggi
PenTest:S3/KaliLinux	Amazon S3	CloudTrail peristiwa data untuk S3	Sedang
PenTest:S3/ParrotLinux	Amazon S3	CloudTrail peristiwa data untuk S3	Sedang

Tipe temuan	Jenis sumber daya	Sumber/fitur data dasar	Menemukan tingkat keparahan
PenTest:S3/PentoolLinux	Amazon S3	CloudTrail peristiwa data untuk S3	Sedang
UnauthorizedAccess:S3/TorIPCaller	Amazon S3	CloudTrail peristiwa data untuk S3	Tinggi
UnauthorizedAccess:S3/MaliciousIPCaller.Custom	Amazon S3	CloudTrail peristiwa data untuk S3	Tinggi
CredentialAccess:IAMUser/AnomalousBehavior	IAM	CloudTrail acara manajemen	Sedang
DefenseEvasion:IAMUser/AnomalousBehavior	IAM	CloudTrail acara manajemen	Sedang
Discovery:IAMUser/AnomalousBehavior	IAM	CloudTrail acara manajemen	Rendah
Exfiltration:IAMUser/AnomalousBehavior	IAM	CloudTrail acara manajemen	Tinggi
Impact:IAMUser/AnomalousBehavior	IAM	CloudTrail acara manajemen	Tinggi
InitialAccess:IAMUser/AnomalousBehavior	IAM	CloudTrail acara manajemen	Sedang
PenTest:IAMUser/KaliLinux	IAM	CloudTrail acara manajemen	Sedang
PenTest:IAMUser/ParrrotLinux	IAM	CloudTrail acara manajemen	Sedang

Tipe temuan	Jenis sumber daya	Sumber/fitur data dasar	Menemukan tingkat keparahan
PenTest:IAMUser/Pe ntoolLinux	IAM	CloudTrail acara manajemen	Sedang
Persistence:IAMUser/ AnomalousBehavior	IAM	CloudTrail acara manajemen	Sedang
Stealth:IAMUser/Pa sswordPolicyChange	IAM	CloudTrail acara manajemen	Rendah [*] __
UnauthorizedAccess :IAMUser/InstanceC redentialExfiltrat ion.InsideAWS	IAM	CloudTrail acara manajemen	Tinggi [*] __
Policy:S3/AccountB lockPublicAccessDi sabled	Amazon S3	CloudTrail acara manajemen	Rendah
Policy:S3/BucketAn onymousAccessGrant ed	Amazon S3	CloudTrail acara manajemen	Tinggi
Policy:S3/BucketBl ockPublicAccessDis abled	Amazon S3	CloudTrail acara manajemen	Rendah
Policy:S3/BucketPu blicAccessGranted	Amazon S3	CloudTrail acara manajemen	Tinggi
PrivilegeEscalatio n:IAMUser/Anomalou sBehavior	IAM	CloudTrail acara manajemen	Sedang
Recon:IAMUser/Mali ciousIPCaller	IAM	CloudTrail acara manajemen	Sedang

Tipe temuan	Jenis sumber daya	Sumber/fitur data dasar	Menemukan tingkat keparahan
Recon:IAMUser/MaliciousIPCaller.Custom	IAM	CloudTrail acara manajemen	Sedang
Recon:IAMUser/TorIPCaller	IAM	CloudTrail acara manajemen	Sedang
Stealth:IAMUser/CloudTrailLoggingDisabled	IAM	CloudTrail acara manajemen	Rendah
Stealth:S3/ServerAccessLoggingDisabled	Amazon S3	CloudTrail acara manajemen	Rendah
UnauthorizedAccess:IAMUser/ConsoleLoginSuccess.B	IAM	CloudTrail acara manajemen	Sedang
UnauthorizedAccess:IAMUser/MaliciousIPCaller	IAM	CloudTrail acara manajemen	Sedang
UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom	IAM	CloudTrail acara manajemen	Sedang
UnauthorizedAccess:IAMUser/TorIPCaller	IAM	CloudTrail acara manajemen	Sedang
Policy:IAMUser/RootCredentialUsage	IAM	CloudTrail peristiwa manajemen atau peristiwa CloudTrail data untuk S3	Rendah

Tipe temuan	Jenis sumber daya	Sumber/fitur data dasar	Menemukan tingkat keparahan
Policy:IAMUser/ShortTermRootCredentialUsage	IAM	CloudTrail peristiwa manajemen atau peristiwa CloudTrail data untuk S3	Rendah
UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS	IAM	CloudTrail peristiwa manajemen atau peristiwa CloudTrail data untuk S3	Tinggi
AttackSequence:EKS/CompromisedCluster	Sumber daya yang terlibat dalam urutan serangan	• Acara log audit EKS • Pemantauan Runtime untuk Amazon EKS • Deteksi malware Amazon EKS untuk Amazon EC2 • AWS CloudTrail peristiwa data untuk S3 • AWS CloudTrail acara manajemen • Log Alur VPC • Log kueri DNS Route53 Resolver	Kritis
AttackSequence:IAM/CompromisedCredentials	Sumber daya yang terlibat dalam urutan serangan	CloudTrail acara manajemen	Kritis

Tipe temuan	Jenis sumber daya	Sumber/fitur data dasar	Menemukan tingkat keparahan
AttackSequence:S3/CompromisedData	Sumber daya yang terlibat dalam urutan serangan	CloudTrail acara manajemen dan peristiwa CloudTrail data untuk S3	Kritis
Backdoor:EC2/C&CActivity.B!DNS	Amazon EC2	Log DNS	Tinggi
CryptoCurrency:EC2/BitcoinTool.B!DNS	Amazon EC2	Log DNS	Tinggi
Impact:EC2/AbusedDomainRequest.Reputation	Amazon EC2	Log DNS	Sedang
Impact:EC2/BitcoinDomainRequest.Reputation	Amazon EC2	Log DNS	Tinggi
Impact:EC2/MaliciousDomainRequest.Reputation	Amazon EC2	Log DNS	Tinggi
Impact:EC2/SuspiciousDomainRequest.Reputation	Amazon EC2	Log DNS	Rendah
Trojan:EC2/BlackholeTraffic!DNS	Amazon EC2	Log DNS	Sedang
Trojan:EC2/DGADomainRequest.B	Amazon EC2	Log DNS	Tinggi

Tipe temuan	Jenis sumber daya	Sumber/fitur data dasar	Menemukan tingkat keparahan
Trojan:EC2/DGADomainRequest.C!DNS	Amazon EC2	Log DNS	Tinggi
Trojan:EC2/DNSDataExfiltration	Amazon EC2	Log DNS	Tinggi
Trojan:EC2/DriveBySourceTraffic!DNS	Amazon EC2	Log DNS	Tinggi
Trojan:EC2/DropPoint!DNS	Amazon EC2	Log DNS	Sedang
Trojan:EC2/PhishingDomainRequest!DNS	Amazon EC2	Log DNS	Tinggi
UnauthorizedAccess:EC2/MetadataDNSRebind	Amazon EC2	Log DNS	Tinggi
Execution:Container/MaliciousFile	Kontainer	Perlindungan Malware EBS	Bervariasi tergantung pada ancaman yang terdeteksi
Execution:Container/SuspiciousFile	Kontainer	Perlindungan Malware EBS	Bervariasi tergantung pada ancaman yang terdeteksi
Execution:EC2/MaliciousFile	Amazon EC2	Perlindungan Malware EBS	Bervariasi tergantung pada ancaman yang terdeteksi
Execution:EC2/SuspiciousFile	Amazon EC2	Perlindungan Malware EBS	Bervariasi tergantung pada ancaman yang terdeteksi

Tipe temuan	Jenis sumber daya	Sumber/fitur data dasar	Menemukan tingkat keparahan
Execution:ECS/MaliciousFile	ECS	Perlindungan Malware EBS	Bervariasi tergantung pada ancaman yang terdeteksi
Execution:ECS/SuspiciousFile	ECS	Perlindungan Malware EBS	Bervariasi tergantung pada ancaman yang terdeteksi
Execution:Kubernetes/MaliciousFile	Kubernetes	Perlindungan Malware EBS	Bervariasi tergantung pada ancaman yang terdeteksi
Execution:Kubernetes/SuspiciousFile	Kubernetes	Perlindungan Malware EBS	Bervariasi tergantung pada ancaman yang terdeteksi
CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed	Kubernetes	Log audit EKS	Sedang
CredentialAccess:Kubernetes/MaliciousIPCaller	Kubernetes	Log audit EKS	Tinggi
CredentialAccess:Kubernetes/MaliciousIPCaller.Custom	Kubernetes	Log audit EKS	Tinggi
CredentialAccess:Kubernetes/SuccessfulAnonymousAccess	Kubernetes	Log audit EKS	Tinggi
CredentialAccess:Kubernetes/TorIPCaller	Kubernetes	Log audit EKS	Tinggi

Tipe temuan	Jenis sumber daya	Sumber/fitur data dasar	Menemukan tingkat keparahan
DefenseEvasion:Kubernetes/MaliciousIPCaller	Kubernetes	Log audit EKS	Tinggi
DefenseEvasion:Kubernetes/MaliciousIPCaller.Custom	Kubernetes	Log audit EKS	Tinggi
DefenseEvasion:Kubernetes/SuccessfulAnonymousAccess	Kubernetes	Log audit EKS	Tinggi
DefenseEvasion:Kubernetes/TorIPCaller	Kubernetes	Log audit EKS	Tinggi
Discovery:Kubernetes/AnomalousBehavior.PermissionChecked	Kubernetes	Log audit EKS	Rendah
Discovery:Kubernetes/MaliciousIPCaller	Kubernetes	Log audit EKS	Sedang
Discovery:Kubernetes/MaliciousIPCaller.Custom	Kubernetes	Log audit EKS	Sedang
Discovery:Kubernetes/SuccessfulAnonymousAccess	Kubernetes	Log audit EKS	Sedang
Discovery:Kubernetes/TorIPCaller	Kubernetes	Log audit EKS	Sedang

Tipe temuan	Jenis sumber daya	Sumber/fitur data dasar	Menemukan tingkat keparahan
Execution:Kubernetes/ExecInKubeSystemPod	Kubernetes	Log audit EKS	Sedang
Execution:Kubernetes/AnomalousBehavior.ExecInPod	Kubernetes	Log audit EKS	Sedang
Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed	Kubernetes	Log audit EKS	Rendah
Impact:Kubernetes/MaliciousIPCaller	Kubernetes	Log audit EKS	Tinggi
Impact:Kubernetes/MaliciousIPCaller.Custom	Kubernetes	Log audit EKS	Tinggi
Impact:Kubernetes/SuccessfulAnonymousAccess	Kubernetes	Log audit EKS	Tinggi
Impact:Kubernetes/TorIPCaller	Kubernetes	Log audit EKS	Tinggi
Persistence:Kubernetes/ContainerWithSensitiveMount	Kubernetes	Log audit EKS	Sedang
Persistence:Kubernetes/MaliciousIPCaller	Kubernetes	Log audit EKS	Sedang
Persistence:Kubernetes/MaliciousIPCaller.Custom	Kubernetes	Log audit EKS	Sedang

Tipe temuan	Jenis sumber daya	Sumber/fitur data dasar	Menemukan tingkat keparahan
Persistence:Kubernetes/SuccessfulAnonymousAccess	Kubernetes	Log audit EKS	Tinggi
Persistence:Kubernetes/TorIPCaller	Kubernetes	Log audit EKS	Sedang
Policy:Kubernetes/AdminAccessToDefaultServiceAccount	Kubernetes	Log audit EKS	Tinggi
Policy:Kubernetes/AnonymousAccessGranted	Kubernetes	Log audit EKS	Tinggi
Policy:Kubernetes/KubeflowDashboardExposed	Kubernetes	Log audit EKS	Sedang
Policy:Kubernetes/ExposedDashboard	Kubernetes	Log audit EKS	Sedang
PrivilegeEscalation:Kubernetes/AnonymousBehavior.RoleBindingCreated	Kubernetes	Log audit EKS	Sedang [*]
PrivilegeEscalation:Kubernetes/AnonymousBehavior.RoleCreated	Kubernetes	Log audit EKS	Rendah

Tipe temuan	Jenis sumber daya	Sumber/fitur data dasar	Menemukan tingkat keparahan
Persistence:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount	Kubernetes	Log audit EKS	Tinggi
PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer	Kubernetes	Log audit EKS	Tinggi
PrivilegeEscalation:Kubernetes/PrivilegedContainer	Kubernetes	Log audit EKS	Sedang
Backdoor:Lambda/C&CAActivity.B	Lambda	Pemantauan Aktivitas Jaringan Lambda	Tinggi
CryptoCurrency:Lambda/BitcoinTool.B	Lambda	Pemantauan Aktivitas Jaringan Lambda	Tinggi
Trojan:Lambda/BlackholeTraffic	Lambda	Pemantauan Aktivitas Jaringan Lambda	Sedang
Trojan:Lambda/DropPoint	Lambda	Pemantauan Aktivitas Jaringan Lambda	Sedang
UnauthorizedAccess:Lambda/MaliciousIPCaller.Custom	Lambda	Pemantauan Aktivitas Jaringan Lambda	Sedang
UnauthorizedAccess:Lambda/TorClient	Lambda	Pemantauan Aktivitas Jaringan Lambda	Tinggi

Tipe temuan	Jenis sumber daya	Sumber/fitur data dasar	Menemukan tingkat keparahan
UnauthorizedAccess:Lambda/TorRelay	Lambda	Pemantauan Aktivitas Jaringan Lambda	Tinggi
Object:S3/MaliciousFile	S3Object	Perlindungan Malware untuk S3	Tinggi
CredentialAccess:RDS/AnomalousBehavior.FailedLogin	Basis data Amazon Aurora, Amazon RDS, dan Aurora Limitless yang didukung	Pemantauan Aktivitas Login RDS	Rendah
CredentialAccess:RDS/AnomalousBehavior.SuccessfulBruteForce	Basis data Amazon Aurora, Amazon RDS, dan Aurora Limitless yang didukung	Pemantauan Aktivitas Login RDS	Tinggi
CredentialAccess:RDS/AnomalousBehavior.SuccessfulLogin	Basis data Amazon Aurora, Amazon RDS, dan Aurora Limitless yang didukung	Pemantauan Aktivitas Login RDS	Variabel [*]
CredentialAccess:RDS/MaliciousIPCaller.FailedLogin	Basis data Amazon Aurora, Amazon RDS, dan Aurora Limitless yang didukung	Pemantauan Aktivitas Login RDS	Sedang
CredentialAccess:RDS/MaliciousIPCaller.SuccessfulLogin	Basis data Amazon Aurora, Amazon RDS, dan Aurora Limitless yang didukung	Pemantauan Aktivitas Login RDS	Tinggi
CredentialAccess:RDS/TorIPCaller.FailedLogin	Basis data Amazon Aurora, Amazon RDS, dan Aurora Limitless yang didukung	Pemantauan Aktivitas Login RDS	Sedang

Tipe temuan	Jenis sumber daya	Sumber/fitur data dasar	Menemukan tingkat keparahan
CredentialAccess:RDS/TorIPCaller.SuccessfulLogin	Basis data Amazon Aurora, Amazon RDS, dan Aurora Limitless yang didukung	Pemantauan Aktivitas Login RDS	Tinggi
Discovery:RDS/MaliciousIPCaller	Basis data Amazon Aurora, Amazon RDS, dan Aurora Limitless yang didukung	Pemantauan Aktivitas Login RDS	Sedang
Discovery:RDS/TorIPCaller	Basis data Amazon Aurora, Amazon RDS, dan Aurora Limitless yang didukung	Pemantauan Aktivitas Login RDS	Sedang
Backdoor:Runtime/C&CActivity.B	Instance, kluster EKS, cluster ECS, atau wadah	Pemantauan Runtime	Tinggi
Backdoor:Runtime/C&CActivity.B!DNS	Instance, kluster EKS, cluster ECS, atau wadah	Pemantauan Runtime	Tinggi
CryptoCurrency:Runtime/BitcoinTool.B	Instance, kluster EKS, cluster ECS, atau wadah	Pemantauan Runtime	Tinggi
CryptoCurrency:Runtime/BitcoinTool.B!DNS	Instance, kluster EKS, cluster ECS, atau wadah	Pemantauan Runtime	Tinggi
DefenseEvasion:Runtime/FilelessExecution	Instance, kluster EKS, cluster ECS, atau wadah	Pemantauan Runtime	Sedang

Tipe temuan	Jenis sumber daya	Sumber/fitur data dasar	Menemukan tingkat keparahan
DefenseEvasion:Runtime/ProcessInjection.Proc	Instance, kluster EKS, cluster ECS, atau wadah	Pemantauan Runtime	Tinggi
DefenseEvasion:Runtime/ProcessInjection.Ptrace	Instance, kluster EKS, cluster ECS, atau wadah	Pemantauan Runtime	Sedang
DefenseEvasion:Runtime/ProcessInjection.VirtualMemoryWrite	Instance, kluster EKS, cluster ECS, atau wadah	Pemantauan Runtime	Tinggi
DefenseEvasion:Runtime/PtraceAntiDebugging	Instance, kluster EKS, cluster ECS, atau wadah	Pemantauan Runtime	Rendah
DefenseEvasion:Runtime/SuspiciousCommand	Instance, kluster EKS, cluster ECS, atau wadah	Pemantauan Runtime	Tinggi
Discovery:Runtime/SuspiciousCommand	Instance, kluster EKS, cluster ECS, atau wadah	Pemantauan Runtime	Rendah
Execution:Runtime/MaliciousFileExecuted	Instance, kluster EKS, cluster ECS, atau wadah	Pemantauan Runtime	Tinggi
Execution:Runtime/NewBinaryExecuted	Instance, kluster EKS, cluster ECS, atau wadah	Pemantauan Runtime	Sedang
Execution:Runtime/NewLibraryLoaded	Instance, kluster EKS, cluster ECS, atau wadah	Pemantauan Runtime	Sedang

Tipe temuan	Jenis sumber daya	Sumber/fitur data dasar	Menemukan tingkat keparahan
Execution:Runtime/SuspiciousCommand	Instance, kluster EKS, cluster ECS, atau wadah	Pemantauan Runtime	Variabel
Execution:Runtime/SuspiciousShellCreated	Instance, kluster EKS, cluster ECS, atau wadah	Pemantauan Runtime	Rendah
Execution:Runtime/SuspiciousTool	Instance, kluster EKS, cluster ECS, atau wadah	Pemantauan Runtime	Variabel
Execution:Runtime/ReverseShell	Instance, kluster EKS, cluster ECS, atau wadah	Pemantauan Runtime	Tinggi
Impact:Runtime/AbusedDomainRequest.Reputation	Instance, kluster EKS, cluster ECS, atau kontainer	Pemantauan Runtime	Sedang
Impact:Runtime/BitcoinDomainRequest.Reputation	Instance, kluster EKS, cluster ECS, atau kontainer	Pemantauan Runtime	Tinggi
Impact:Runtime/CryptoMinerExecuted	Instance, kluster EKS, cluster ECS, atau kontainer	Pemantauan Runtime	Tinggi
Impact:Runtime/MaliciousDomainRequest.Reputation	Instance, kluster EKS, cluster ECS, atau kontainer	Pemantauan Runtime	Sedang
Impact:Runtime/SuspiciousDomainRequest.Reputation	Instance, kluster EKS, cluster ECS, atau kontainer	Pemantauan Runtime	Rendah

Tipe temuan	Jenis sumber daya	Sumber/fitur data dasar	Menemukan tingkat keparahan
Persistence:Runtime/SuspiciousCommand	Instance, kluster EKS, cluster ECS, atau kontainer	Pemantauan Runtime	Sedang
PrivilegeEscalation:Runtime/CGroupsReleaseAgentModified	Instance, kluster EKS, cluster ECS, atau kontainer	Pemantauan Runtime	Tinggi
PrivilegeEscalation:Runtime/ContainerMountsHostDirectory	Instance, kluster EKS, cluster ECS, atau kontainer	Pemantauan Runtime	Sedang
PrivilegeEscalation:Runtime/DockerSocketAccessed	Instance, kluster EKS, cluster ECS, atau kontainer	Pemantauan Runtime	Sedang
PrivilegeEscalation:Runtime/ElevationToRoot	Instance, kluster EKS, cluster ECS, atau kontainer	Pemantauan Runtime	Sedang
PrivilegeEscalation:Runtime/RuncContainerEscape	Instance, kluster EKS, cluster ECS, atau kontainer	Pemantauan Runtime	Tinggi
PrivilegeEscalation:Runtime/SuspiciousCommand	Instance, kluster EKS, cluster ECS, atau kontainer	Pemantauan Runtime	Sedang
PrivilegeEscalation:Runtime/UserfaultfdUsage	Instance, kluster EKS, cluster ECS, atau kontainer	Pemantauan Runtime	Sedang
Trojan:Runtime/BlackholeTraffic	Instance, kluster EKS, cluster ECS, atau kontainer	Pemantauan Runtime	Sedang

Tipe temuan	Jenis sumber daya	Sumber/fitur data dasar	Menemukan tingkat keparahan
Trojan:Runtime/Bla ckholeTraffic!DNS	Instance, kluster EKS, cluster ECS, atau kontainer	Pemantauan Runtime	Sedang
Trojan:Runtime/Dro pPoint	Instance, kluster EKS, cluster ECS, atau kontainer	Pemantauan Runtime	Sedang
Trojan:Runtime/DGA DomainRequest.C!DN S	Instance, kluster EKS, cluster ECS, atau kontainer	Pemantauan Runtime	Tinggi
Trojan:Runtime/Dri veBySourceTraffic! DNS	Instance, kluster EKS, cluster ECS, atau kontainer	Pemantauan Runtime	Tinggi
Trojan:Runtime/Dro pPoint!DNS	Instance, kluster EKS, cluster ECS, atau kontainer	Pemantauan Runtime	Sedang
Trojan:Runtime/Phi shingDomainRequest !DNS	Instance, kluster EKS, cluster ECS, atau kontainer	Pemantauan Runtime	Tinggi
UnauthorizedAccess :Runtime/MetadataD NSRebind	Instance, kluster EKS, cluster ECS, atau kontainer	Pemantauan Runtime	Tinggi
UnauthorizedAccess :Runtime/TorClient	Instance, kluster EKS, cluster ECS, atau kontainer	Pemantauan Runtime	Tinggi
UnauthorizedAccess :Runtime/TorRelay	Instance, kluster EKS, cluster ECS, atau kontainer	Pemantauan Runtime	Tinggi

Tipe temuan	Jenis sumber daya	Sumber/fitur data dasar	Menemukan tingkat keparahan
Backdoor:EC2/C&CAActivity.B	Amazon EC2	Log aliran VPC ⁺	Tinggi
Backdoor:EC2/DeniaIOfService.Dns	Amazon EC2	Log aliran VPC ⁺	Tinggi
Backdoor:EC2/DeniaIOfService.Tcp	Amazon EC2	Log aliran VPC ⁺	Tinggi
Backdoor:EC2/DeniaIOfService.Udp	Amazon EC2	Log aliran VPC ⁺	Tinggi
Backdoor:EC2/DeniaIOfService.UdpOnTcpPorts	Amazon EC2	Log aliran VPC ⁺	Tinggi
Backdoor:EC2/DeniaIOfService.UnusualProtocol	Amazon EC2	Log aliran VPC ⁺	Tinggi
Backdoor:EC2/Spambot	Amazon EC2	Log aliran VPC ⁺	Sedang
Behavior:EC2/NetworkPortUnusual	Amazon EC2	Log aliran VPC ⁺	Sedang
Behavior:EC2/TrafficVolumeUnusual	Amazon EC2	Log aliran VPC ⁺	Sedang
CryptoCurrency:EC2/BitcoinTool.B	Amazon EC2	Log aliran VPC ⁺	Tinggi
DefenseEvasion:EC2/UnusualDNSResolver	Amazon EC2	Log aliran VPC ⁺	Sedang

Tipe temuan	Jenis sumber daya	Sumber/fitur data dasar	Menemukan tingkat keparahan
DefenseEvasion:EC2/UnusualDoHActivity	Amazon EC2	Log aliran VPC ⁺	Sedang
DefenseEvasion:EC2/UnusualDoTActivity	Amazon EC2	Log aliran VPC ⁺	Sedang
Impact:EC2/PortSweep	Amazon EC2	Log aliran VPC ⁺	Tinggi
Impact:EC2/WinRMBruteForce	Amazon EC2	Log aliran VPC ⁺	Rendah [*]
Recon:EC2/PortProbeEMRUnprotectedPort	Amazon EC2	Log aliran VPC ⁺	Tinggi
Recon:EC2/PortProbeUnprotectedPort	Amazon EC2	Log aliran VPC ⁺	Rendah [*]
Recon:EC2/Portscan	Amazon EC2	Log aliran VPC ⁺	Sedang
Trojan:EC2/BlackholeTraffic	Amazon EC2	Log aliran VPC ⁺	Sedang
Trojan:EC2/DropPoint	Amazon EC2	Log aliran VPC ⁺	Sedang
UnauthorizedAccess:EC2/MaliciousIPCaller.Custom	Amazon EC2	Log aliran VPC ⁺	Sedang
UnauthorizedAccess:EC2/RDPBruteForce	Amazon EC2	Log aliran VPC ⁺	Rendah [*]
UnauthorizedAccess:EC2/SSHBruteForce	Amazon EC2	Log aliran VPC ⁺	Rendah [*]

Tipe temuan	Jenis sumber daya	Sumber/fitur data dasar	Menemukan tingkat keparahan
UnauthorizedAccess:EC2/TorClient	Amazon EC2	Log aliran VPC ⁺	Tinggi
UnauthorizedAccess:EC2/TorRelay	Amazon EC2	Log aliran VPC ⁺	Tinggi

Memahami dan menghasilkan GuardDuty temuan Amazon

GuardDuty Temuan mewakili masalah keamanan potensial yang terdeteksi di dalam Akun AWS, beban kerja, dan data. GuardDuty menghasilkan temuan setiap kali mendeteksi aktivitas tak terduga dan berpotensi berbahaya di AWS lingkungan Anda.

Anda dapat melihat dan mengelola GuardDuty temuan Anda di halaman Temuan di GuardDuty konsol, atau dengan menggunakan operasi AWS CLI atau API. Untuk informasi tentang bagaimana Anda dapat mengelola GuardDuty temuan, lihat [Mengelola GuardDuty temuan Amazon](#).

Topik:

[GuardDuty menemukan format](#)

Memahami format GuardDuty menemukan jenis dan tujuan ancaman yang berbeda yang GuardDuty melacak.

[Sampel temuan](#)

Hasilkan temuan sampel di GuardDuty konsol, atau dengan menggunakan GuardDuty API atau AWS CLI perintah. Temuan sampel yang dihasilkan mencakup detail fiktif untuk membantu Anda memahami detail temuan yang terkait dengan setiap GuardDuty temuan. Temuan ini ditandai dengan awalan [SAMPEL].

[GuardDuty Temuan uji di akun khusus](#)

Anda dapat menguji GuardDuty temuan spesifik di lingkungan Anda. Jalankan `guardduty-tester` skrip dalam non-produksi Akun AWS khusus. GuardDuty Untuk mendeteksi dan mensimulasikan temuan, itu akan menyebarkan sumber daya tertentu di lingkungan Anda. Pengalaman ini berbeda dengan menghasilkan temuan sampel.

[Melihat temuan yang dihasilkan di GuardDuty konsol](#)

Pelajari cara meninjau temuan yang dihasilkan di GuardDuty konsol.

[Tingkat keparahan GuardDuty temuan](#)

Setiap GuardDuty temuan memiliki tingkat keparahan terkait yang mencerminkan potensi risiko di AWS lingkungan Anda. Bagian ini menjelaskan apa arti setiap tingkat keparahan.

[Detail temuan](#)

Pelajari detail yang terkait dengan GuardDuty temuan yang dihasilkan di akun Anda. Topik ini mencakup detail yang terkait dengan deteksi ancaman dasar, Deteksi Ancaman Diperpanjang, dan rencana perlindungan khusus di GuardDuty.

[GuardDuty menemukan agregasi](#)

Pelajari cara GuardDuty menangani beberapa kejadian dari jenis temuan yang sama. Dengan menggabungkan jenis temuan yang sama yang terdeteksi, GuardDuty memperbarui jenis temuan asli dengan detail terbaru.

[GuardDuty menemukan jenis](#)

Bagian ini mendaftarkan jenis GuardDuty pencarian berdasarkan yang terkait [Sumber data dasar](#) atau [Fitur yang dipetakan GuardDuty](#). Untuk mempelajari tentang setiap jenis temuan, pilih temuan itu untuk detail lebih lanjut, seperti deskripsi dan langkah-langkah potensial untuk memulihkan temuan tersebut.

GuardDuty menemukan format

Ketika GuardDuty mendeteksi perilaku mencurigakan atau tidak terduga di AWS lingkungan Anda, itu menghasilkan temuan. Temuan adalah pemberitahuan yang berisi rincian tentang potensi masalah keamanan yang GuardDuty ditemukan. [Melihat temuan yang dihasilkan di GuardDuty konsol](#) Termasuk informasi tentang apa yang terjadi, AWS sumber daya mana yang terlibat dalam aktivitas mencurigakan, kapan kegiatan ini berlangsung, dan informasi terkait yang dapat membantu Anda memahami akar penyebabnya.

Salah satu bagian informasi yang paling berguna dalam detail temuan adalah jenis temuan. Tujuan dari jenis temuan adalah untuk memberikan deskripsi ringkas namun dapat dibaca tentang potensi masalah keamanan. Misalnya, tipe PortProbeUnprotectedPort pencarian GuardDuty Recon:EC2/dengan cepat memberi tahu Anda bahwa di suatu tempat di AWS lingkungan Anda, sebuah EC2 instance memiliki port yang tidak dilindungi yang sedang diselidiki oleh penyerang potensial.

GuardDuty menggunakan format berikut untuk menamai berbagai jenis temuan yang dihasilkannya:

ThreatPurpose:ResourceTypeAffected/ThreatFamilyName. DetectionMechanism! Artifak

Setiap bagian dari format ini mewakili aspek dari jenis temuan. Aspek-aspek ini memiliki penjelasan sebagai berikut:

- **ThreatPurpose**- menggambarkan tujuan utama dari ancaman, jenis serangan atau tahap serangan potensial. Lihat bagian berikut untuk daftar lengkap tujuan GuardDuty ancaman.
- **ResourceTypeAffected**- menjelaskan jenis AWS sumber daya mana yang diidentifikasi dalam temuan ini sebagai target potensial musuh. Saat ini, GuardDuty dapat menghasilkan temuan untuk jenis sumber daya yang tercantum dalam [GuardDuty jenis temuan aktif](#).
- **ThreatFamilyName**- menggambarkan ancaman keseluruhan atau potensi aktivitas jahat GuardDuty yang mendeteksi. Misalnya, nilai `NetworkPortUnusual` menunjukkan bahwa EC2 instance yang diidentifikasi dalam GuardDuty temuan tidak memiliki riwayat komunikasi sebelumnya pada port jarak jauh tertentu yang juga diidentifikasi dalam temuan tersebut.
- **DetectionMechanism**- menjelaskan metode di mana GuardDuty mendeteksi temuan. Ini dapat digunakan untuk menunjukkan variasi pada jenis temuan umum atau temuan yang GuardDuty menggunakan mekanisme khusus untuk mendeteksi. Misalnya, `Backdoor:EC2/DenialOfService.Tcp` menunjukkan penolakan layanan (DoS) terdeteksi melalui TCP. Varian UDP adalah `Backdoor:EC2/DenialOfService.Udp`.

Nilai `.Custom` menunjukkan bahwa GuardDuty mendeteksi temuan berdasarkan daftar ancaman kustom Anda. Untuk informasi selengkapnya, lihat [Daftar IP terpercaya dan daftar ancaman](#).

Nilai `.Reputation` menunjukkan bahwa GuardDuty mendeteksi temuan menggunakan model skor reputasi domain. Untuk informasi selengkapnya, lihat [Cara AWS melacak ancaman keamanan terbesar cloud dan membantu mematikannya](#).

- **Artifact** - menjelaskan sumber daya tertentu yang dimiliki oleh alat yang digunakan dalam aktivitas berbahaya. Misalnya, DNS dalam tipe temuan `CryptoCurrency:EC2/BitcoinTool.B!DNS` menunjukkan bahwa EC2 instance Amazon berkomunikasi dengan domain terkait Bitcoin yang diketahui.

Note

Artifak bersifat opsional dan mungkin tidak tersedia untuk semua jenis GuardDuty temuan.

Tujuan Ancaman

Dalam tujuan GuardDuty ancaman menggambarkan tujuan utama dari ancaman, jenis serangan, atau tahap serangan potensial. Misalnya, beberapa tujuan ancaman, seperti `Backdoor`, menunjukkan jenis serangan. Namun, beberapa tujuan ancaman, seperti `Impact` sejajar dengan [taktik MITRE](#)

[ATT&CK](#). Taktik MITRE ATT&CK menunjukkan fase yang berbeda dalam siklus serangan musuh. Dalam rilis saat ini GuardDuty, ThreatPurpose dapat memiliki nilai-nilai berikut:

Pintu Belakang

Nilai ini menunjukkan bahwa musuh telah mengkompromikan AWS sumber daya dan mengubah sumber daya sehingga mampu menghubungi server home command and control (C&C) untuk menerima instruksi lebih lanjut untuk aktivitas berbahaya.

Perilaku

Nilai ini menunjukkan bahwa GuardDuty telah mendeteksi aktivitas atau pola aktivitas yang berbeda dari garis dasar yang ditetapkan untuk AWS sumber daya yang terlibat.

CredentialAccess

Nilai ini menunjukkan bahwa GuardDuty telah mendeteksi pola aktivitas yang mungkin digunakan musuh untuk mencuri kredensial, seperti kata sandi, nama pengguna, dan kunci akses, dari lingkungan Anda. Tujuan ancaman ini didasarkan pada [taktik MITRE ATT&CK](#).

Cryptocurrency

Nilai ini menunjukkan bahwa GuardDuty telah mendeteksi bahwa AWS sumber daya di lingkungan Anda adalah perangkat lunak hosting yang terkait dengan cryptocurrency (misalnya, Bitcoin).

DefenseEvasion

Nilai ini menunjukkan bahwa GuardDuty telah mendeteksi aktivitas atau pola aktivitas yang mungkin digunakan musuh untuk menghindari deteksi saat menyusup ke lingkungan Anda. Tujuan ancaman ini didasarkan pada [taktik MITRE ATT&CK](#).

Penemuan

Nilai ini menunjukkan bahwa GuardDuty telah mendeteksi aktivitas atau pola aktivitas yang dapat digunakan musuh untuk memperluas pengetahuan mereka tentang sistem dan jaringan internal Anda. Tujuan ancaman ini didasarkan pada [taktik MITRE ATT&CK](#).

Eksekusi

Nilai ini menunjukkan bahwa GuardDuty telah mendeteksi bahwa musuh dapat mencoba menjalankan atau telah menjalankan kode berbahaya untuk menjelajahi AWS lingkungan, atau mencuri data. Tujuan ancaman ini didasarkan pada [taktik MITRE ATT&CK](#).

Ekfiltrasi

Nilai ini menunjukkan bahwa GuardDuty telah mendeteksi aktivitas atau pola aktivitas yang mungkin digunakan musuh saat mencoba mencuri data dari lingkungan Anda. Tujuan ancaman ini didasarkan pada [taktik MITRE ATT&CK](#).

Dampak

Nilai ini menunjukkan bahwa GuardDuty telah mendeteksi aktivitas atau pola aktivitas yang menunjukkan bahwa musuh sedang mencoba memanipulasi, mengganggu, atau menghancurkan sistem dan data Anda. Tujuan ancaman ini didasarkan pada [taktik MITRE ATT&CK](#).

InitialAccess

Nilai ini umumnya dikaitkan dengan tahap akses awal serangan ketika musuh mencoba untuk membangun akses ke lingkungan Anda. Tujuan ancaman ini didasarkan pada [taktik MITRE ATT&CK](#).

Pentest

Terkadang pemilik AWS sumber daya atau perwakilan resmi mereka sengaja menjalankan tes terhadap AWS aplikasi untuk menemukan kerentanan, seperti grup keamanan terbuka atau kunci akses yang terlalu permisif. Uji penetrasi ini dilakukan dalam upaya untuk mengidentifikasi dan mengunci sumber daya yang rentan sebelum ditemukan oleh musuh. Namun, beberapa alat yang digunakan oleh penguji penetrasi resmi tersedia secara bebas dan oleh karena itu dapat digunakan oleh pengguna yang tidak sah atau musuh untuk menjalankan uji probing. Meskipun tidak GuardDuty dapat mengidentifikasi tujuan sebenarnya di balik aktivitas tersebut, nilai Pentest menunjukkan bahwa GuardDuty mendeteksi aktivitas tersebut, bahwa itu mirip dengan aktivitas yang dihasilkan oleh alat pengujian pena yang diketahui, dan bahwa itu dapat menunjukkan penyelidikan berbahaya pada jaringan Anda.

Kegigihan

Nilai ini menunjukkan bahwa GuardDuty telah mendeteksi aktivitas atau pola aktivitas yang dapat digunakan musuh untuk mencoba dan mempertahankan akses ke sistem Anda bahkan jika rute akses awal mereka terputus. Misalnya, ini dapat termasuk membuat pengguna IAM baru setelah mendapatkan akses menggunakan kredensial pengguna yang ada. Ketika kredensial pengguna yang ada dihapus, musuh akan mempertahankan akses pada pengguna baru yang tidak terdeteksi sebagai bagian dari peristiwa asli. Tujuan ancaman ini didasarkan pada [taktik MITRE ATT&CK](#).

Kebijakan

Nilai ini menunjukkan bahwa Anda Akun AWS menunjukkan perilaku yang bertentangan dengan praktik terbaik keamanan yang direkomendasikan. Misalnya, modifikasi kebijakan izin yang tidak disengaja yang terkait dengan AWS sumber daya atau lingkungan Anda, dan penggunaan akun istimewa yang seharusnya memiliki sedikit atau tidak ada penggunaan.

PrivilegeEscalation

Nilai ini menginformasikan bahwa prinsipal yang terlibat dalam lingkungan AWS Anda menunjukkan perilaku yang mungkin digunakan musuh untuk mendapatkan izin dengan tingkat yang lebih tinggi ke jaringan Anda. Tujuan ancaman ini didasarkan pada [taktik MITRE ATT&CK](#).

Pengintaian

Nilai ini menunjukkan bahwa GuardDuty telah mendeteksi aktivitas atau pola aktivitas yang mungkin digunakan musuh saat melakukan pengintaian terhadap lingkungan Anda untuk menentukan bagaimana mereka dapat memperluas akses mereka atau memanfaatkan sumber daya Anda. Misalnya, aktivitas ini dapat mencakup pelingkupan kerentanan di AWS lingkungan Anda dengan memeriksa port, membuat panggilan API, mencantumkan pengguna, dan mencantumkan tabel database.

Siluman

Nilai ini menunjukkan bahwa musuh secara aktif mencoba menyembunyikan tindakan mereka. Misalnya, mereka mungkin menggunakan server proksi anonim, sehingga sangat sulit untuk mengukur sifat sebenarnya dari aktivitas tersebut.

Trojan

Nilai ini menunjukkan bahwa serangan menggunakan program Trojan yang diam-diam melakukan aktivitas berbahaya. Terkadang perangkat lunak ini mengambil tampilan program yang sah. Terkadang pengguna secara tidak sengaja menjalankan perangkat lunak ini. Lain kali perangkat lunak ini mungkin berjalan secara otomatis dengan memanfaatkan kerentanan.

UnauthorizedAccess

Nilai ini menunjukkan bahwa GuardDuty mendeteksi aktivitas mencurigakan atau pola aktivitas yang mencurigakan oleh individu yang tidak berwenang.

GuardDuty mesin pemindai deteksi malware

Amazon GuardDuty memiliki mesin pemindaian yang dibangun dan dikelola secara internal dan [vendor pihak ketiga](#). Keduanya menggunakan indikator kompromi (IoCs) yang bersumber dari berbagai feed internal yang memiliki visibilitas di berbagai jenis malware yang mungkin ditargetkan. AWS GuardDuty juga memiliki definisi deteksi yang didasarkan pada aturan YARA yang ditambahkan oleh teknisi keamanan kami, dan deteksi berdasarkan model heuristik dan pembelajaran mesin (ML). Saat memindai objek Amazon S3, Perlindungan GuardDuty Malware menghasilkan hasil yang konsisten saat memindai objek yang sama beberapa kali dengan definisi dan mesin pemindaian yang sama. Deteksi berbasis tanda tangan tidak hanya mencakup pencocokan byte tetapi juga potongan kode yang berpotensi kompleks, dan pemindai dapat mengurai konten dan membuat keputusan.

Mesin pemindai malware tidak melakukan analisis perilaku langsung, di mana peledakan malware memantau sampel saat dijalankan dalam sistem nyata. GuardDuty Solusinya terutama deteksi berbasis file. Untuk mendeteksi malware tanpa file, GuardDuty berikan solusi berbasis agen, seperti untuk [Pemantauan Runtime](#) Amazon EKS, Amazon, EC2 dan Amazon ECS (termasuk). AWS Fargate

Tanpa batasan pada format file yang GuardDuty memindai malware, mesin pemindai yang digunakannya dapat mendeteksi berbagai jenis malware, seperti cryptominers, ransomware, dan webshell. Mesin GuardDuty pemindaian yang dikelola sepenuhnya terus memperbarui daftar tanda tangan malware setiap 15 menit.

Mesin pemindai adalah bagian dari sistem intelijen GuardDuty ancaman yang menggunakan komponen peledakan malware internal. Ini menghasilkan intelijen ancaman baru dengan mengumpulkan malware dan sampel jinak secara independen dari berbagai sumber. File hash tipe IoC dari sistem intelijen ancaman selanjutnya dimasukkan ke mesin pemindaian malware untuk mendeteksi malware berdasarkan hash file buruk yang diketahui.

Menghasilkan temuan sampel di GuardDuty

Amazon GuardDuty membantu Anda menghasilkan temuan sampel untuk memvisualisasikan dan memahami berbagai jenis temuan yang dapat dihasilkannya. Saat Anda menghasilkan temuan sampel, GuardDuty isi daftar temuan Anda saat ini dengan satu sampel untuk setiap jenis temuan yang didukung, termasuk jenis pencarian urutan serangan.

Sampel yang dibuat adalah perkiraan yang diisi dengan nilai placeholder. Sampel ini mungkin terlihat berbeda dari temuan nyata untuk lingkungan Anda, tetapi Anda dapat menggunakannya untuk

menguji berbagai konfigurasi GuardDuty, seperti EventBridge acara atau filter Anda. Untuk daftar nilai yang tersedia untuk menemukan jenis, lihat [GuardDuty menemukan jenis](#) tabel.

Menghasilkan temuan sampel melalui GuardDuty konsol atau API

Pilih metode akses pilihan Anda untuk menghasilkan temuan sampel.

Note

GuardDuty Konsol membantu Anda menghasilkan salah satu dari setiap jenis temuan. Untuk menghasilkan satu atau lebih jenis temuan spesifik, lakukan langkah API/CLI terkait.

Console

Gunakan prosedur berikut untuk membuat sampel temuan. Proses ini menghasilkan satu sampel temuan untuk setiap jenis GuardDuty temuan.

1. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.
2. Pada panel navigasi, silakan pilih Pengaturan.
3. Di halaman Pengaturan, di bawah Sampel temuan, pilih Buat sampel temuan.
4. Di panel navigasi, pilih Temuan. Sampel temuan ditampilkan di halaman Temuan saat ini dengan prefiks [SAMPLE].

API/CLI

Anda dapat menghasilkan satu sampel temuan yang cocok dengan salah satu jenis GuardDuty temuan melalui [CreateSampleFindings](#) API, nilai yang tersedia untuk menemukan tipe tercantum dalam [GuardDuty menemukan jenis](#) tabel.

Ini berguna untuk pengujian aturan CloudWatch Acara atau otomatisasi berdasarkan temuan. Contoh berikut menunjukkan cara menghasilkan temuan sampel tunggal dari Backdoor:EC2/DenialofService.Tcp jenis menggunakan AWS CLI.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/> konsol, atau jalankan `detectorId` [ListDetectors](#) API.

```
aws guardduty create-sample-findings --detector-id 12abc34d567e8fa901bc2d34e56789f0
--finding-types Backdoor:EC2/DenialOfService.Tcp
```

Judul temuan sampel yang dihasilkan melalui metode ini selalu dimulai dengan [SAMPLE] di konsol. Temuan sampel memiliki nilai "sample": true di bagian AdditionalInfo dari rincian JSON temuan.

Untuk memahami rincian temuan, seperti menemukan tingkat keparahan dan sumber daya yang berpotensi dikompromikan, terkait dengan temuan yang dihasilkan, lihat [Tingkat keparahan GuardDuty temuan](#) dan [Detail temuan](#).

Untuk menghasilkan beberapa temuan umum berdasarkan aktivitas simulasi di tempat yang berdedikasi dan terisolasi di Akun AWS lingkungan Anda, lihat [GuardDuty Temuan uji di akun khusus](#).

GuardDuty Temuan uji di akun khusus

Gunakan dokumen ini untuk menjalankan skrip pengujian yang menghasilkan GuardDuty temuan terhadap sumber daya pengujian yang akan digunakan di file Anda. Akun AWS Anda dapat melakukan langkah-langkah ini ketika Anda ingin memahami dan mempelajari tentang jenis GuardDuty temuan tertentu dan bagaimana rincian temuan mencari sumber daya aktual di akun Anda. Pengalaman ini berbeda dengan menghasilkan [Sampel temuan](#). Untuk informasi lebih lanjut tentang pengalaman pengujian GuardDuty temuan, lihat [Pertimbangan](#).

Daftar Isi

- [Pertimbangan](#)
- [GuardDuty temuan skrip tester dapat menghasilkan](#)
- [Langkah 1 - Prasyarat](#)
- [Langkah 2 - Menyebarkan sumber daya AWS](#)
- [Langkah 3 - Jalankan skrip pengujian](#)
- [Langkah 4 - Bersihkan sumber daya AWS tes](#)
- [Memecahkan masalah umum](#)

Pertimbangan

Sebelum Anda melanjutkan, pertimbangkan pertimbangan berikut:

- GuardDuty merekomendasikan untuk menggunakan tester dalam non-produksi khusus. Akun AWS Pendekatan ini akan memastikan bahwa Anda dapat mengidentifikasi GuardDuty temuan yang dihasilkan oleh penguji dengan benar. Selain itu, GuardDuty penguji menyebarkan berbagai sumber daya yang mungkin memerlukan izin IAM di luar apa yang diizinkan di akun lain. Menggunakan akun khusus memastikan bahwa izin dapat dicakup dengan benar dengan batas akun yang jelas.
- Skrip tester menghasilkan lebih dari 100 GuardDuty temuan dengan kombinasi AWS sumber daya yang berbeda. Saat ini, ini tidak termasuk semua. [GuardDuty menemukan jenis](#) Untuk daftar jenis pencarian yang dapat Anda hasilkan dengan skrip penguji ini, lihat [GuardDuty temuan skrip tester dapat menghasilkan](#).

Catatan

Untuk memvisualisasikan jenis pencarian urutan Attack, skrip tester hanya [AttackSequence:EKS/CompromisedCluster](#) menghasilkan dan. [AttackSequence:S3/CompromisedData](#) Untuk memvisualisasikan dan memahami [AttackSequence:IAM/CompromisedCredentials](#), Anda dapat menghasilkan [Sampel temuan](#) di akun Anda.

- Agar GuardDuty penguji berfungsi seperti yang diharapkan, GuardDuty perlu diaktifkan di akun tempat sumber daya penguji digunakan. Bergantung pada pengujian yang akan dijalankan, penguji mengevaluasi apakah rencana GuardDuty perlindungan yang sesuai diaktifkan atau tidak. Untuk setiap rencana perlindungan yang tidak diaktifkan, GuardDuty akan meminta izin untuk mengaktifkan rencana perlindungan yang diperlukan cukup lama GuardDuty untuk melakukan tes yang akan menghasilkan temuan. Nanti, GuardDuty akan menonaktifkan rencana perlindungan setelah pengujian selesai.

Mengaktifkan GuardDuty untuk pertama kalinya

Ketika GuardDuty diaktifkan di akun khusus Anda untuk pertama kalinya di Wilayah tertentu, akun Anda akan secara otomatis terdaftar dalam uji coba gratis 30 hari.

GuardDuty menawarkan paket perlindungan opsional. Pada saat memungkinkan GuardDuty, paket perlindungan tertentu juga diaktifkan dan termasuk dalam uji coba gratis GuardDuty 30 hari. Untuk informasi selengkapnya, lihat [Menggunakan uji GuardDuty coba gratis 30 hari](#).

GuardDuty sudah diaktifkan di akun Anda sebelum menjalankan skrip pengujian

Ketika sudah GuardDuty diaktifkan, maka berdasarkan parameter, skrip tester akan memeriksa status konfigurasi rencana perlindungan tertentu dan pengaturan tingkat akun lainnya yang diperlukan untuk menghasilkan temuan.

Dengan menjalankan skrip pengujian ini, paket perlindungan tertentu mungkin diaktifkan untuk pertama kalinya di akun khusus Anda di Wilayah. Ini akan memulai uji coba gratis 30 hari untuk rencana perlindungan itu. Untuk informasi tentang uji coba gratis yang terkait dengan setiap paket perlindungan, lihat [Menggunakan uji GuardDuty coba gratis 30 hari](#).

- Selama infrastruktur GuardDuty pengujian diterapkan, Anda kadang-kadang dapat menerima [UnauthorizedAccess:EC2/TorClient](#) temuan dari instans. PenTest

GuardDuty temuan skrip tester dapat menghasilkan

Saat ini, skrip pengujian menghasilkan jenis temuan berikut yang terkait dengan log audit Amazon, EC2 Amazon EKS, Amazon S3, IAM, dan EKS:

- [AttackSequence:EKS/CompromisedCluster](#)
- [AttackSequence:S3/CompromisedData](#)
- [Backdoor:EC2/C&CAActivity.B!DNS](#)
- [Backdoor:EC2/DenialOfService.Dns](#)
- [Backdoor:EC2/DenialOfService.Udp](#)
- [CryptoCurrency:EC2/BitcoinTool.B!DNS](#)
- [Impact:EC2/AbusedDomainRequest.Reputation](#)
- [Impact:EC2/BitcoinDomainRequest.Reputation](#)
- [Impact:EC2/MaliciousDomainRequest.Reputation](#)
- [Impact:EC2/SuspiciousDomainRequest.Reputation](#)
- [Recon:EC2/Portscan](#)
- [Trojan:EC2/BlackholeTraffic!DNS](#)
- [Trojan:EC2/DGADomainRequest.C!DNS](#)
- [Trojan:EC2/DNSDataExfiltration](#)
- [Trojan:EC2/DriveBySourceTraffic!DNS](#)
- [Trojan:EC2/DropPoint!DNS](#)

- [Trojan:EC2/PhishingDomainRequest!DNS](#)
- [UnauthorizedAccess:EC2/MaliciousIPCaller.Custom](#)
- [UnauthorizedAccess:EC2/RDPBruteForce](#)
- [UnauthorizedAccess:EC2/SSHBruteForce](#)
- [PenTest:IAMUser/KaliLinux](#)
- [Recon:IAMUser/MaliciousIPCaller.Custom](#)
- [Recon:IAMUser/TorIPCaller](#)
- [Stealth:IAMUser/CloudTrailLoggingDisabled](#)
- [Stealth:IAMUser/PasswordPolicyChange](#)
- [UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS](#)
- [UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom](#)
- [UnauthorizedAccess:IAMUser/TorIPCaller](#)
- [Discovery:Kubernetes/MaliciousIPCaller.Custom](#)
- [Discovery:Kubernetes/SuccessfulAnonymousAccess](#)
- [Discovery:Kubernetes/TorIPCaller](#)
- [Execution:Kubernetes/ExecInKubeSystemPod](#)
- [Impact:Kubernetes/MaliciousIPCaller.Custom](#)
- [Persistence:Kubernetes/ContainerWithSensitiveMount](#)
- [Policy:Kubernetes/AdminAccessToDefaultServiceAccount](#)
- [Policy:Kubernetes/AnonymousAccessGranted](#)
- [PrivilegeEscalation:Kubernetes/PrivilegedContainer](#)
- [UnauthorizedAccess:Lambda/MaliciousIPCaller.Custom](#)
- [Discovery:S3/MaliciousIPCaller.Custom](#)
- [Discovery:S3/TorIPCaller](#)
- [PenTest:S3/KaliLinux](#)
- [Policy:S3/AccountBlockPublicAccessDisabled](#)
- [Policy:S3/BucketAnonymousAccessGranted](#)
- [Policy:S3/BucketBlockPublicAccessDisabled](#)
- [Policy:S3/BucketPublicAccessGranted](#)
- [Stealth:S3/ServerAccessLoggingDisabled](#)

- [UnauthorizedAccess:S3/MaliciousIPCaller.Custom](#)
- [UnauthorizedAccess:S3/TorIPCaller](#)
- [Backdoor:Runtime/C&CActivity.B!DNS](#)
- [CryptoCurrency:Runtime/BitcoinTool.B!DNS](#)
- [DefenseEvasion:Runtime/ProcessInjection.Ptrace](#)
- [DefenseEvasion:Runtime/ProcessInjection.VirtualMemoryWrite](#)
- [Execution:Runtime/ReverseShell](#)
- [Impact:Runtime/AbusedDomainRequest.Reputation](#)
- [Impact:Runtime/BitcoinDomainRequest.Reputation](#)
- [Impact:Runtime/MaliciousDomainRequest.Reputation](#)
- [Impact:Runtime/SuspiciousDomainRequest.Reputation](#)
- [PrivilegeEscalation:Runtime/ContainerMountsHostDirectory](#)
- [PrivilegeEscalation:Runtime/DockerSocketAccessed](#)
- [Trojan:Runtime/BlackholeTraffic!DNS](#)
- [Trojan:Runtime/DGADomainRequest.C!DNS](#)
- [Trojan:Runtime/DriveBySourceTraffic!DNS](#)
- [Trojan:Runtime/DropPoint!DNS](#)
- [Trojan:Runtime/PhishingDomainRequest!DNS](#)

Langkah 1 - Prasyarat

Untuk mempersiapkan lingkungan pengujian Anda, Anda memerlukan item berikut:

- Git — Instal alat baris perintah git berdasarkan sistem operasi yang Anda gunakan.

Ini diperlukan untuk mengkloning [amazon-guardduty-testerrepository](#).

- AWS Command Line Interface— Alat open source yang memungkinkan Anda berinteraksi Layanan AWS dengan menggunakan perintah di shell baris perintah Anda. Untuk informasi selengkapnya, lihat [Memulai AWS CLI](#) di Panduan AWS Command Line Interface Pengguna.
- AWS Systems Manager— Untuk memulai sesi Session Manager dengan node terkelola Anda dengan menggunakan AWS CLI Anda harus menginstal plugin Session Manager di mesin lokal Anda. Untuk informasi selengkapnya, lihat [Plugin Install Session Manager AWS CLI](#) di Panduan AWS Systems Manager Pengguna.

- Node Package Manager (NPM) - Instal NPM untuk menginstal semua dependensi.
- Docker — Anda harus menginstal Docker. Untuk petunjuk penginstalan, lihat [situs web Docker](#).

Untuk memverifikasi bahwa Docker telah diinstal, jalankan perintah berikut dan konfirmasikan ada output yang mirip dengan output berikut:

```
$ docker --version
Docker version 19.03.1
```

- Berlangganan gambar [Kali Linux](#) di AWS Marketplace.

Langkah 2 - Menyebarakan sumber daya AWS

Bagian ini menyediakan daftar konsep kunci dan langkah-langkah untuk menyebarakan AWS sumber daya tertentu di akun khusus Anda.

Konsep

Daftar berikut menyediakan konsep kunci yang terkait dengan perintah yang membantu Anda menyebarakan sumber daya:

- AWS Cloud Development Kit (AWS CDK) CDK adalah kerangka pengembangan perangkat lunak open-source untuk mendefinisikan infrastruktur cloud dalam kode dan menyediakannya. AWS CloudFormation CDK mendukung beberapa bahasa pemrograman untuk mendefinisikan komponen cloud yang dapat digunakan kembali yang dikenal sebagai konstruksi. Anda dapat menyusun ini bersama-sama ke tumpukan dan aplikasi. Kemudian, Anda dapat menerapkan aplikasi CDK Anda AWS CloudFormation untuk menyediakan atau memperbarui sumber daya Anda. Untuk informasi lebih lanjut, lihat [Apa itu AWS CDK?](#) di Panduan AWS Cloud Development Kit (AWS CDK) Pengembang.
- Bootstrapping — Ini adalah proses mempersiapkan AWS lingkungan Anda untuk digunakan dengan AWS CDK. Sebelum Anda menyebarakan tumpukan CDK ke lingkungan, AWS lingkungan harus di-bootstrap terlebih dahulu. Proses penyediaan AWS sumber daya tertentu di lingkungan Anda yang digunakan oleh AWS CDK adalah bagian dari langkah-langkah yang akan Anda lakukan di bagian berikutnya - [Langkah-langkah untuk menyebarakan sumber daya AWS](#)

Untuk informasi selengkapnya tentang cara kerja bootstrap, lihat [Bootstrapping di Panduan Pengembang](#). AWS Cloud Development Kit (AWS CDK)

Langkah-langkah untuk menyebarkan sumber daya AWS

Lakukan langkah-langkah berikut untuk mulai menerapkan sumber daya:

1. Siapkan akun AWS CLI default dan Wilayah kecuali variabel Wilayah akun khusus diatur secara manual dalam `bin/cdk-gd-tester.ts` file. Untuk informasi selengkapnya, lihat [Lingkungan](#) di Panduan AWS Cloud Development Kit (AWS CDK) Pengembang.
2. Jalankan perintah berikut untuk menyebarkan sumber daya:

```
git clone https://github.com/aws-labs/amazon-guardduty-tester && cd amazon-guardduty-tester
npm install
cdk bootstrap
cdk deploy
```

Perintah terakhir (`cdk deploy`) membuat AWS CloudFormation tumpukan atas nama Anda. Nama tumpukan ini adalah `GuardDutyTesterStack`.

Sebagai bagian dari skrip ini, GuardDuty buat sumber daya baru untuk menghasilkan GuardDuty temuan di akun Anda. Ini juga menambahkan pasangan kunci tag berikut: nilai ke instance Amazon EC2 :

`CreatedBy:GuardDuty Test Script`

EC2 Instans Amazon juga menyertakan EC2 instance yang menampung node EKS dan kluster ECS.

Tipe instans

GuardDuty dirancang untuk menggunakan jenis instans hemat biaya yang memberikan kinerja minimum yang diperlukan untuk berhasil melaksanakan pengujian. Karena persyaratan vCPU, grup node Amazon EKS memerlukan `t3.medium`, dan karena peningkatan kapasitas jaringan yang diperlukan untuk DenialOfService menemukan pengujian, node driver memerlukan `m6i.large` Untuk semua tes lainnya, GuardDuty gunakan tipe `t3.micro` instance. Untuk informasi selengkapnya tentang jenis instans, lihat [Ukuran yang tersedia](#) di Panduan Jenis EC2 Instans Amazon.

Langkah 3 - Jalankan skrip penguji

Ini adalah proses dua langkah di mana Anda pertama-tama perlu memulai sesi dengan driver uji dan kemudian, jalankan skrip untuk menghasilkan GuardDuty temuan dengan kombinasi sumber daya tertentu.

Bagian A - Mulai sesi dengan driver tes

1. Setelah resource Anda di-deploy, simpan kode Region ke variabel di sesi terminal Anda saat ini. Gunakan perintah berikut dan ganti *us-east-1* dengan kode Wilayah tempat Anda menggunakan sumber daya:

```
$ REGION=us-east-1
```

2. Script tester hanya tersedia melalui AWS Systems Manager (SSM). Untuk memulai shell interaktif pada instance host tester, kueri host InstanceId.
3. Gunakan perintah berikut untuk memulai sesi Anda untuk skrip tester:

```
aws ssm start-session
  --region $REGION
  --document-name AWS-StartInteractiveCommand
  --parameters command="cd /home/ssm-user/py_tester && bash -l"
  --target $(aws ec2 describe-instances
    --region $REGION
    --filters "Name=tag:Name,Values=Driver-GuardDutyTester"
    --query "Reservations[].Instances[?State.Name=='running'].InstanceId"
    --output text)
```

Bagian B - Menghasilkan temuan

Skrip tester adalah program berbasis Python yang secara dinamis membangun skrip bash untuk menghasilkan temuan berdasarkan masukan Anda. Anda memiliki fleksibilitas untuk menghasilkan temuan berdasarkan satu atau lebih jenis AWS sumber daya, rencana GuardDuty perlindungan, [Tujuan Ancaman](#) (taktik) [Sumber data dasar](#), atau [the section called “GuardDuty temuan skrip tester dapat menghasilkan”](#).

Gunakan contoh perintah berikut sebagai referensi, dan jalankan satu atau beberapa perintah untuk menghasilkan temuan yang ingin Anda jelajahi:

```
python3 guardduty_tester.py
```

```
python3 guardduty_tester.py --all
python3 guardduty_tester.py --s3
python3 guardduty_tester.py --tactics discovery
python3 guardduty_tester.py --ec2 --eks --tactics backdoor policy execution
python3 guardduty_tester.py --eks --runtime only
python3 guardduty_tester.py --ec2 --runtime only --tactics impact
python3 guardduty_tester.py --log-source dns vpc-flowlogs
python3 guardduty_tester.py --finding 'CryptoCurrency:EC2/BitcoinTool.B!DNS'
```

Untuk informasi lebih lanjut tentang parameter yang valid, Anda dapat menjalankan perintah bantuan berikut:

```
python3 guardduty_tester.py --help
```

Bagian C - Tinjau temuan yang dihasilkan

Pilih metode yang disukai untuk melihat temuan yang dihasilkan di akun Anda.

GuardDuty console

1. Masuk ke AWS Management Console dan buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.
2. Di panel navigasi, pilih Temuan.
3. Dari tabel temuan, pilih temuan yang ingin Anda lihat detailnya. Ini akan membuka panel detail temuan. Untuk informasi, lihat [Memahami dan menghasilkan GuardDuty temuan Amazon](#).
4. Jika Anda ingin memfilter temuan ini, gunakan kunci dan nilai tag sumber daya. Misalnya, untuk memfilter temuan yang dihasilkan untuk EC2 instans Amazon, gunakan CreatedBy: GuardDuty Test Script tag key:value pair untuk kunci tag Instance dan kunci tag Instance.

API

- Jalankan [ListFindings](#) untuk melihat temuan untuk ID detektor tertentu. Anda dapat menentukan parameter untuk memfilter temuan.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan [ListDetectors](#) API. detectorId

AWS CLI

- Jalankan AWS CLI perintah berikut untuk melihat temuan yang dihasilkan dan ganti *us-east-1* dan *12abc34d567e8fa901bc2d34EXAMPLE* dengan nilai yang sesuai:

```
aws guardduty list-findings --region us-east-1 --detector-id 12abc34d567e8fa901bc2d34EXAMPLE
```

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan [ListDetectors](#) API. `detectorId`

Untuk informasi selengkapnya tentang parameter yang dapat Anda gunakan untuk memfilter temuan, lihat [daftar-temuan](#) di Referensi AWS CLI Perintah.

Langkah 4 - Bersihkan sumber daya AWS tes

Pengaturan tingkat akun dan pembaruan status konfigurasi lainnya yang dibuat selama [Langkah 3 - Jalankan skrip pengujian](#) kembali ke keadaan semula saat skrip pengujian selesai.

Setelah Anda menjalankan skrip tester, Anda dapat memilih untuk membersihkan sumber daya AWS pengujian. Anda dapat memilih untuk melakukan ini dengan menggunakan salah satu metode berikut:

- Jalankan perintah berikut:

```
cdk destroy
```

- Hapus AWS CloudFormation tumpukan dengan nama GuardDutyTesterStack. Untuk selengkapnya tentang langkah-langkah, lihat [Menghapus tumpukan di AWS CloudFormation konsol](#).

Memecahkan masalah umum

GuardDuty telah mengidentifikasi masalah umum dan merekomendasikan langkah-langkah pemecahan masalah:

- Cloud assembly schema version mismatch— Perbarui AWS CDK CLI ke versi yang kompatibel dengan versi perakitan cloud yang diperlukan, atau ke versi terbaru yang tersedia. Untuk informasi selengkapnya, lihat [AWS CDK Kompatibilitas CLI](#).

- **Docker permission denied**— Tambahkan pengguna akun khusus ke docker atau docker-users sehingga akun khusus dapat menjalankan perintah. Untuk informasi selengkapnya tentang langkah-langkah, lihat opsi [socket Daemon](#).
- **Your requested instance type is not supported in your requested Availability Zone**— Beberapa zona Availability tidak mendukung jenis instans tertentu. Untuk mengidentifikasi zona ketersediaan mana yang mendukung jenis instans pilihan Anda dan mencoba kembali menerapkan AWS sumber daya, lakukan langkah-langkah berikut:
 1. Pilih metode yang disukai untuk menentukan zona Ketersediaan mana yang mendukung jenis instans Anda:

Console

Untuk mengidentifikasi Availability zone yang mendukung tipe instans pilihan

1. Masuk ke AWS Management Console dan buka EC2 konsol Amazon di <https://console.aws.amazon.com/ec2/>.
2. Dengan menggunakan pemilih AWS Region di sudut kanan atas halaman, pilih Wilayah tempat Anda ingin meluncurkan instance.
3. Di panel navigasi, di bawah Instance, pilih Jenis Instance.
4. Dari tabel tipe Instance, pilih jenis instance yang disukai.
5. Di bawah Jaringan, lihat Wilayah yang tercantum di bawah Availability zone.

Berdasarkan informasi ini, Anda mungkin perlu memilih Wilayah baru tempat Anda dapat menyebarkan sumber daya.

AWS CLI

Jalankan perintah berikut untuk melihat daftar Availability zone. Pastikan untuk menentukan jenis instans pilihan Anda dan Region (*us-east-1*).

```
aws ec2 describe-instance-type-offerings --location-type availability-zone --  
filters Name=instance-type,Values=Preferred instance type --region us-east-1 --  
output table
```

Untuk informasi selengkapnya tentang perintah ini, lihat [describe-instance-type-offerings](#) di Referensi AWS CLI Perintah.

Saat menjalankan perintah ini, jika Anda menerima kesalahan, pastikan Anda menggunakan versi terbaru AWS CLI. Untuk informasi selengkapnya, lihat [Pemecahan Masalah](#) di AWS Command Line Interface Panduan Pengguna.

2. Coba gunakan sumber AWS daya lagi dan tentukan zona Ketersediaan yang mendukung jenis instans pilihan Anda.

Untuk mencoba kembali menyebarkan sumber daya AWS

1. Siapkan Region default dalam `bin/cdk-gd-tester.ts` file.
2. Untuk menentukan zona ketersediaan, buka `amazon-guardduty-tester/lib/common/network/vpc.ts` file.
3. Dalam file ini, ganti `maxAzs: 2`, dengan `availabilityZones: ['us-east-1a', 'us-east-1c']`, tempat Anda harus menentukan zona Ketersediaan untuk jenis instans Anda.
4. Lanjutkan dengan langkah-langkah yang tersisa di bawah [Langkah-langkah untuk menyebarkan sumber daya AWS](#).

Melihat temuan yang dihasilkan di GuardDuty konsol

Saat GuardDuty mendeteksi aktivitas yang cocok dengan pola masalah keamanan, GuardDuty buat temuan. Temuan ini dikaitkan dengan jenis sumber daya yang mungkin telah dikompromikan selama aktivitas ini. Anda dapat melihat detail yang terkait dengan setiap temuan yang GuardDuty dihasilkan.

Jika Anda menggunakan akun GuardDuty administrator, Anda dapat melihat temuan yang dihasilkan atas nama akun anggota. Namun, akun anggota dapat melihat temuan yang dihasilkan di akun mereka sendiri. Akun anggota tidak dapat melihat temuan yang dihasilkan untuk akun anggota lainnya.

Langkah-langkah untuk melihat temuan di GuardDuty konsol

1. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.
2. Di panel navigasi kiri, pilih Temuan.

GuardDuty menampilkan temuan dalam format tabel. Secara default, tabel ini diurutkan dalam urutan menurun berdasarkan nilai kolom Terakhir terlihat, menampilkan temuan terbaru di bagian atas.

Temuan dengan ikon pedang



mewakili temuan urutan serangan.

3. Untuk melihat detail yang terkait dengan temuan, pilih Judul. Ini akan membuka panel samping detail temuan. Untuk menemukan urutan serangan, panel samping ini menyertakan versi ringkasan dari urutan serangan, dan untuk memperluas tampilan ini, pilih Lihat detail.

Untuk informasi tentang bidang yang tercantum di panel samping ini, lihat [Detail temuan](#).

4. (Opsional) untuk mengunduh Finding JSON
 - a. Pilih temuan, lalu pilih menu Tindakan.
 - b. Pada menu Tindakan, pilih Lihat dan ekspor JSON.
 - c. Pada jendela Temuan JSON, pilih Unduh.

Note

Dalam beberapa kasus GuardDuty, menyadari bahwa temuan tertentu adalah positif palsu setelah dihasilkan. GuardDuty menyediakan bidang Keyakinan di JSON temuan, dan menetapkan nilainya ke nol. Dengan cara ini GuardDuty memungkinkan Anda tahu bahwa Anda dapat dengan aman mengabaikan temuan tersebut.

Temuan tanpa bidang Keyakinan tidak dianggap positif palsu.

Menavigasi halaman Temuan

Bagian ini memberikan informasi kunci tentang berbagai elemen di halaman Temuan. Ini akan membantu Anda menganalisis temuan yang dihasilkan untuk analisis dan respons ancaman.

Daftar berikut menjelaskan elemen halaman Temuan yang akan membantu Anda lebih memahami temuan yang dihasilkan:

- Jenis ancaman:

Jenis ancaman mencakup GuardDuty temuan individu dan temuan urutan serangan. Secara default, halaman menampilkan Semua temuan.

Untuk memfilter tampilan tabel temuan, pada menu Jenis ancaman, pilih salah satu opsi — Hanya temuan urutan serangan atau Temuan individu saja.

- Kolom Sumber Daya dan Hitung:

Kolom Sumber daya dalam tabel temuan menunjukkan nama AWS sumber daya yang berpotensi dikompromikan. Untuk temuan urutan serangan, kolom ini menunjukkan jumlah AWS sumber daya yang berpotensi dikompromikan. Untuk melihat nama sumber daya, pilih nomor di bawah kolom Sumber Daya.

Kolom Hitung menunjukkan berapa kali GuardDuty mengamati temuan tertentu. Ketika GuardDuty mendeteksi bahwa aktivitas yang cocok dengan masalah keamanan yang diidentifikasi sebelumnya, itu menambah jumlah untuk temuan spesifik tersebut. Untuk temuan urutan serangan, nilai kolom ini menunjukkan jumlah total sinyal dan temuan yang terlibat dalam pembuatan temuan.

- Menyortir temuan berdasarkan kolom tabel:

Jika ada panah di sebelah header kolom, maka Anda dapat mengurutkan tabel temuan berdasarkan kolom. Pilih header kolom untuk mengurutkan temuan dalam urutan peningkatan atau penurunan nilai di kolom itu.

- Temuan penyaringan:

Berdasarkan atribut properti tertentu, seperti `Account ID` dan `Resource type`, Anda dapat memfilter tabel temuan lebih lanjut. Untuk informasi tentang jenis filter yang dapat Anda gunakan, lihat [Penyaringan temuan GuardDuty](#).

- Status dan Aturan Tersimpan:

Menu Status mencakup dua nilai — Saat Ini dan Diarsipkan. Tampilan default adalah Temuan saat ini dalam tabel.

Ketika Anda tidak lagi GuardDuty ingin menghasilkan temuan yang cocok dengan kriteria tertentu, Anda dapat menekan temuan itu. GuardDuty Arsip yang menemukan Ketika GuardDuty mendeteksi temuan ini lagi, Anda tidak akan diberitahu tentang pengamatan ini. Untuk melihat temuan yang diarsipkan secara khusus, pada menu Status, pilih Diarsipkan.

Aturan tersimpan adalah fitur yang membantu Anda secara otomatis memfilter dan mengambil tindakan pada temuan yang sesuai dengan kriteria tertentu. Tindakan dapat mencakup pengarsipan temuan atau menekannya dari notifikasi di masa mendatang.

Untuk informasi selengkapnya, lihat [Aturan penekanan](#).

Tingkat keparahan GuardDuty temuan

Setiap GuardDuty temuan memiliki tingkat keparahan dan nilai yang ditetapkan yang mencerminkan potensi risiko temuan tersebut terhadap lingkungan Anda, sebagaimana ditentukan oleh teknisi keamanan kami. Nilai keparahan dapat jatuh di mana saja dalam kisaran 1,0 hingga 10,0, dengan nilai yang lebih tinggi menunjukkan risiko keamanan yang lebih besar. Untuk membantu Anda menentukan respons terhadap masalah keamanan potensial yang disorot oleh temuan, GuardDuty uraikan rentang ini menjadi tingkat keparahan Kritis, Tinggi, Sedang, dan Rendah.

Temuan jenis tertentu mungkin memiliki tingkat keparahan yang berbeda tergantung pada konteks khusus untuk temuan tersebut. Untuk melihat daftar konsolidasi tingkat keparahan default untuk semua jenis GuardDuty temuan, lihat [GuardDuty jenis temuan aktif](#).

Bagian berikut menjelaskan tingkat keparahan yang ditentukan untuk GuardDuty temuan.

Topik

- [Tingkat keparahan kritis](#)
- [Tingkat keparahan tinggi](#)
- [Tingkat keparahan sedang](#)
- [Tingkat keparahan rendah](#)

Tingkat keparahan kritis

Kisaran nilai: 9.0 - 10.0

Keterangan: Tingkat keparahan kritis menunjukkan bahwa urutan serangan mungkin sedang berlangsung atau baru-baru ini terjadi. Satu atau lebih AWS sumber daya, seperti kredensial masuk pengguna IAM dan bucket Amazon S3, berpotensi dikompromikan atau mungkin telah disusupi.

Rekomendasi: GuardDuty merekomendasikan agar Anda memprioritaskan triaging dan remediasi semua temuan tingkat keparahan kritis karena masalah ini dapat menjadi bagian dari serangan ransomware dan dapat meningkat kapan saja. Lihat detail tentang sumber daya yang terlibat dan mulailah menangani masalah keamanan. Untuk informasi selengkapnya, lihat [Mengatasi temuan](#).

Tingkat keparahan tinggi

Kisaran nilai: 7.0 - 8.9

Deskripsi: Tingkat keparahan yang tinggi menunjukkan bahwa sumber daya yang dimaksud (EC2 instans Amazon atau sekumpulan kredensi masuk pengguna IAM) dikompromikan dan digunakan secara aktif untuk tujuan yang tidak sah.

Rekomendasi: GuardDuty merekomendasikan agar Anda memperlakukan masalah keamanan dengan tingkat keparahan tinggi sebagai prioritas dan mengambil langkah-langkah perbaikan segera untuk mencegah penggunaan sumber daya Anda yang tidak sah lebih lanjut. Misalnya, bersihkan EC2 instans Amazon Anda atau hentikan, atau putar kredensyal IAM. Ikuti langkah-langkah [Mengatasi temuan](#) untuk memulihkan temuan.

Tingkat keparahan sedang

Kisaran nilai: 4.0 - 6.9

Deskripsi: Tingkat keparahan sedang menunjukkan aktivitas mencurigakan yang menyimpang dari perilaku yang diamati secara normal dan, tergantung pada kasus penggunaan Anda, mungkin merupakan indikasi kompromi sumber daya.

Rekomendasi: GuardDuty merekomendasikan untuk menyelidiki sumber daya yang berpotensi terkena dampak pada kenyamanan Anda paling awal. Langkah-langkah remediasi akan bervariasi menurut sumber daya dan menemukan keluarga. Pendekatan yang ditetapkan adalah bagi Anda untuk mengonfirmasi bahwa aktivitas tersebut diotorisasi dan konsisten dengan kasus penggunaan Anda. Jika Anda tidak dapat mengidentifikasi penyebabnya, atau mengonfirmasi bahwa aktivitas tersebut diotorisasi, Anda harus mempertimbangkan sumber daya yang disusupi. Ikuti langkah-langkah [Mengatasi temuan](#) untuk memulihkan temuan.

Berikut adalah beberapa hal yang perlu dipertimbangkan ketika meninjau temuan tingkat menengah:

- Periksa apakah pengguna yang berwenang telah menginstal perangkat lunak baru yang mengubah perilaku sumber daya (misalnya, mengizinkan lalu lintas yang lebih tinggi dari biasanya, atau mengaktifkan komunikasi pada port baru).
- Periksa apakah pengguna yang berwenang mengubah pengaturan bidang kontrol, misalnya, mengubah pengaturan grup keamanan.
- Jalankan pemindaian anti-virus pada sumber daya yang bersangkutan untuk mendeteksi perangkat lunak yang tidak sah.
- Verifikasi izin yang terlampir pada IAM role, pengguna, grup, atau set kredensial yang bersangkutan. Ini mungkin harus diubah atau dihapus.

Tingkat keparahan rendah

Rentang nilai: 1.0 - 3.9

Deskripsi: Tingkat keparahan yang rendah menunjukkan upaya aktivitas mencurigakan yang tidak membahayakan lingkungan Anda, misalnya, pemindaian port atau upaya intrusi yang gagal.

Rekomendasi: Tidak ada tindakan yang disarankan segera, tetapi ada baiknya mencatat informasi ini karena mungkin mengindikasikan seseorang mencari titik lemah di lingkungan Anda.

Detail temuan

Di GuardDuty konsol Amazon, Anda dapat melihat detail pencarian di bagian ringkasan pencarian. Detail menemukan bervariasi berdasarkan jenis temuan.

Ada dua detail utama yang menentukan jenis informasi apa yang tersedia untuk temuan apa pun. Yang pertama adalah jenis sumber daya, yang dapat berupa InstanceAccessKey, S3Bucket, S3Object, Kubernetes cluster, ECS cluster, Container, RDSDBInstance, RDSLimitlessDB, atau Lambda. Detail kedua yang menentukan informasi temuan adalah Peran Sumber Daya. Peran sumber daya bisa Target, artinya sumber daya adalah target aktivitas yang mencurigakan. Untuk temuan tipe instans, peran sumber daya juga dapat menjadi Actor, yang berarti bahwa sumber daya Anda adalah aktor yang melakukan aktivitas mencurigakan. Topik ini menjelaskan beberapa detail umum yang tersedia untuk temuan. Untuk [the section called “Jenis penemuan Runtime Monitoring”](#) dan [Perlindungan Malware untuk tipe pencarian S3](#), peran sumber daya tidak diisi.

Topik

- [Menemukan ikhtisar](#)
- [Sumber Daya](#)
- [Detail pencarian urutan serangan](#)
- [Rincian pengguna database RDS \(DB\)](#)
- [Detail penemuan Runtime Monitoring](#)
- [Detail pemindaian volume EBS](#)
- [Perlindungan Malware untuk EC2 menemukan detail](#)
- [Perlindungan Malware untuk detail penemuan S3](#)
- [Tindakan](#)

- [Aktor atau Target](#)
- [Detail geolokasi](#)
- [Informasi tambahan](#)
- [Bukti](#)
- [Perilaku anomali](#)

Menemukan ikhtisar

Bagian Ikhtisar temuan berisi fitur pengenalan paling dasar dari temuan, termasuk informasi berikut:

- ID Akun — ID AWS akun tempat aktivitas berlangsung yang mendorong GuardDuty untuk menghasilkan temuan ini.
- Hitung — Berapa kali GuardDuty telah mengumpulkan aktivitas yang cocok dengan pola ini dengan ID temuan ini.
- Dibuat pada — Waktu dan tanggal ketika temuan ini pertama kali dibuat. Jika nilai ini berbeda dari Diperbarui pada, ini menunjukkan bahwa aktivitas tersebut telah terjadi beberapa kali dan merupakan masalah yang sedang berlangsung.

Note

Stempel waktu untuk temuan di GuardDuty konsol muncul di zona waktu lokal Anda, sementara ekspor JSON dan output CLI menampilkan stempel waktu di UTC.

- Finding ID — Pengidentifikasi unik untuk jenis temuan ini dan kumpulan parameter. Kejadian baru dari aktivitas yang cocok dengan pola ini akan digabungkan ke ID yang sama.
- Tipe temuan – String berformat yang mewakili tipe aktivitas yang memicu temuan. Untuk informasi selengkapnya, lihat [GuardDuty menemukan format](#).
- Wilayah — AWS Wilayah di mana temuan itu dihasilkan. Untuk informasi selengkapnya tentang Wilayah yang didukung, lihat [Wilayah dan titik akhir](#)
- ID Sumber Daya — ID AWS sumber daya tempat aktivitas berlangsung yang mendorong GuardDuty untuk menghasilkan temuan ini.
- ID Pindai — Berlaku untuk temuan saat Perlindungan GuardDuty Malware untuk EC2 diaktifkan, ini adalah pengenalan pemindaian malware yang berjalan pada volume EBS yang melekat pada EC2 instans atau beban kerja kontainer yang berpotensi dikompromikan. Untuk informasi selengkapnya, lihat [Perlindungan Malware untuk EC2 menemukan detail](#).

- **Keparahan** — Tingkat keparahan yang ditetapkan temuan baik Kritis, Tinggi, Sedang, atau Rendah. Untuk informasi selengkapnya, lihat [Temuan tingkat keparahan](#).
- **Diperbarui di** — Terakhir kali temuan ini diperbarui dengan aktivitas baru yang cocok dengan pola yang mendorong GuardDuty untuk menghasilkan temuan ini.

Sumber Daya

Sumber daya yang terpengaruh memberikan rincian tentang AWS sumber daya yang ditargetkan oleh aktivitas inisiasi. Informasi yang tersedia bervariasi berdasarkan tipe sumber daya dan tipe tindakan.

Peran sumber daya — Peran AWS sumber daya yang memulai temuan. Nilai ini bisa TARGET atau ACTOR, dan mewakili apakah sumber daya Anda adalah target aktivitas mencurigakan atau aktor yang melakukan aktivitas mencurigakan.

Jenis sumber daya — Jenis sumber daya yang terpengaruh. Jika beberapa sumber daya terlibat, temuan dapat mencakup beberapa jenis sumber daya. Jenis sumber daya adalah Instance,, S3Bucket AccessKey, S3Object,,, Container, KubernetesCluster, ECSClusterDB, dan RDSDBInstanceRDSLimitlessLambda. Tergantung tipe sumber dayanya, detail temuan yang berbeda tersedia. Pilih tab opsi sumber daya untuk mempelajari detail yang tersedia untuk sumber daya tersebut.

Instance

Detail contoh:

Note

Beberapa detail instance mungkin hilang jika instance telah dihentikan atau jika pemanggilan API yang mendasarinya berasal dari EC2 instance di Wilayah lain saat melakukan panggilan API Lintas wilayah.

- **ID Instance** — ID dari EC2 instance yang terlibat dalam aktivitas yang diminta GuardDuty untuk menghasilkan temuan.
- **Jenis Instance** — Jenis EC2 instance yang terlibat dalam temuan.
- **Waktu Peluncuran** - Waktu dan tanggal peluncuran instans.

- Outpost ARN — Nama Sumber Daya Amazon (ARN) dari AWS Outposts Hanya berlaku untuk AWS Outposts instance. Untuk informasi lebih lanjut, lihat [Apa itu AWS Outposts?](#) di Panduan Pengguna untuk rak Outposts.
- Nama Grup Keamanan – Nama Grup Keamanan yang melekat pada instans yang terlibat.
- ID Grup Keamanan – ID grup keamanan yang melekat pada instans yang terlibat.
- Status instans – Status instans yang ditargetkan saat ini.
- Availability Zone – Availability Zone AWS Region tempat instans yang terlibat berada.
- ID Image – ID dari Amazon Machine Image yang digunakan untuk membangun instans yang terlibat dalam aktivitas.
- Deskripsi Image – Deskripsi ID Amazon Machine Image yang digunakan untuk membangun instans yang terlibat dalam aktivitas.
- Tanda – Daftar tanda yang melekat pada sumber daya ini, tercantum dalam format key:value.

AccessKey

Akses Detail Kunci:

- ID kunci akses — ID kunci akses pengguna yang terlibat dalam aktivitas yang diminta GuardDuty untuk menghasilkan temuan.
- Principal ID — ID utama pengguna yang terlibat dalam aktivitas yang diminta GuardDuty untuk menghasilkan temuan.
- Jenis pengguna — Jenis pengguna yang terlibat dalam aktivitas yang diminta GuardDuty untuk menghasilkan temuan. Untuk informasi selengkapnya, lihat elemen [CloudTrail UserIdentity](#).
- Nama pengguna — Nama pengguna yang terlibat dalam aktivitas yang diminta GuardDuty untuk menghasilkan temuan.

S3Bucket

Detail ember Amazon S3:

- Nama – Nama bucket yang terlibat dalam temuan.
- ARN – ARN bucket yang terlibat dalam temuan.
- Pemilik – ID pengguna resmi dari pengguna yang memiliki bucket yang terlibat dalam temuan. Untuk informasi selengkapnya tentang pengguna kanonik, IDs lihat pengenalan [AWS akun](#).
- Tipe – Tipe temuan bucket, dapat berupa Tujuan atau Sumber.

- Enkripsi sisi server default — Detail enkripsi untuk bucket.
- Tag Bucket — Daftar tag yang dilampirkan pada sumber daya ini, tercantum dalam format `key:value`.
- Izin Efektif – Evaluasi dari semua izin dan kebijakan efektif pada bucket yang menunjukkan apakah bucket yang terlibat diekspos secara publik. Nilai dapat bersifat publik atau tidak publik.

S3Object

- Detail objek S3 - Termasuk informasi berikut tentang objek S3 yang dipindai:
 - ARN - Nama Sumber Daya Amazon (ARN) dari objek S3 yang dipindai.
 - Kunci — Nama yang ditetapkan ke file saat dibuat di bucket S3.
 - Id Versi — Bila Anda telah mengaktifkan versi bucket, bidang ini menunjukkan Id versi yang terkait dengan versi terbaru dari objek S3 yang dipindai. Untuk informasi selengkapnya, lihat [Menggunakan pembuatan versi di bucket S3 di Panduan Pengguna](#) Amazon S3.
 - ETag - Merupakan versi spesifik dari objek S3 yang dipindai.
 - Hash — Hash dari ancaman yang terdeteksi dalam temuan ini.
- Detail bucket S3 — Termasuk informasi berikut tentang bucket Amazon S3 yang terkait dengan objek S3 yang dipindai:
 - Nama - Menunjukkan nama bucket S3 yang berisi objek.
 - ARN - Nama Sumber Daya Amazon (ARN) dari ember S3.
 - Pemilik — Id Canonical dari pemilik bucket S3.

EKSCluster

Detail klaster Kubernetes:

- Nama — Nama cluster Kubernetes.
- ARN — ARN yang mengidentifikasi cluster.
- Created At — Waktu dan tanggal ketika cluster ini dibuat.

Note

Stempel waktu untuk temuan di GuardDuty konsol muncul di zona waktu lokal Anda, sementara ekspor JSON dan output CLI menampilkan stempel waktu di UTC.

- ID VPC — ID VPC yang terkait dengan cluster Anda.
- Status — Status cluster saat ini.
- Tag — Metadata yang Anda terapkan ke cluster untuk membantu Anda mengkategorikan dan mengaturnya. Setiap tag terdiri dari kunci dan nilai opsional, yang tercantum dalam format `key:value`. Anda bisa menentukan kunci dan nilai.

Tag cluster tidak menyebar ke sumber daya lain yang terkait dengan cluster.

Detail beban kerja Kubernetes:

- Jenis - Jenis beban kerja Kubernetes, seperti pod, deployment, dan job.
- Nama — Nama beban kerja Kubernetes.
- Uid — ID unik dari beban kerja Kubernetes.
- Dibuat pada - Waktu dan tanggal ketika beban kerja ini dibuat.
- Label — Pasangan nilai kunci yang melekat pada beban kerja Kubernetes.
- Container — Detail kontainer yang berjalan sebagai bagian dari beban kerja Kubernetes.
- Namespace — Beban kerja milik namespace Kubernetes ini.
- Volume — Volume yang digunakan oleh beban kerja Kubernetes.
 - Jalur host - Merupakan file atau direktori yang sudah ada sebelumnya di mesin host tempat volume dipetakan.
 - Nama — Nama volume.
- konteks keamanan pod — Mendefinisikan pengaturan privilege dan akses control untuk semua kontainer dalam sebuah pod.
- Jaringan host — Setel ke `true` jika pod disertakan dalam beban kerja Kubernetes.

Detail pengguna Kubernetes:

- Grup - Kubernetes RBAC (kontrol berbasis akses peran) kelompok pengguna yang terlibat dalam aktivitas yang menghasilkan temuan.
- ID — ID unik dari pengguna Kubernetes.
- Nama pengguna — Nama pengguna Kubernetes yang terlibat dalam aktivitas yang menghasilkan temuan.
- Nama sesi — Entitas yang mengambil peran IAM dengan izin Kubernetes RBAC.

ECSCluster

Rincian cluster ECS:

- ARN — ARN yang mengidentifikasi cluster.
- Nama — Nama cluster.
- Status — Status cluster saat ini.
- Jumlah layanan aktif — Jumlah layanan yang berjalan di cluster dalam suatu ACTIVE keadaan. Anda dapat melihat layanan ini dengan [ListServices](#)
- Jumlah instans kontainer terdaftar — Jumlah instance kontainer yang terdaftar ke dalam klaster. Ini termasuk instance kontainer di keduanya ACTIVE dan DRAINING status.
- Menjalankan tugas menghitung — Jumlah tugas di cluster yang berada dalam RUNNING status.
- Tag — Metadata yang Anda terapkan ke cluster untuk membantu Anda mengkategorikan dan mengaturnya. Setiap tag terdiri dari kunci dan nilai opsional, yang tercantum dalam format `key:value`. Anda bisa menentukan kunci dan nilai.
- Kontainer — Detail tentang wadah yang terkait dengan tugas:
 - Nama kontainer — Nama wadah.
 - Gambar kontainer — Gambar wadah.
- Detail tugas — Detail tugas dalam sebuah cluster.
 - ARN — Nama Sumber Daya Amazon (ARN) dari tugas tersebut.
 - Definisi ARN — Nama Sumber Daya Amazon (ARN) dari definisi tugas yang membuat tugas.
 - Versi - Penghitung versi untuk tugas tersebut.
 - Tugas dibuat di — Stempel waktu Unix saat tugas dibuat.
 - Tugas dimulai pada — Stempel waktu Unix saat tugas dimulai.
 - Tugas dimulai oleh — Tag yang ditentukan saat tugas dimulai.

Container

Detail kontainer:

- Container runtime — Container runtime (seperti `docker` atau `containerd`) yang digunakan untuk menjalankan container.
- ID - ID instance kontainer atau entri ARN lengkap untuk instance kontainer.
- Nama — Nama wadah.

- Gambar - Gambar dari contoh container.
- Volume mount — Daftar kedudukan volume container. Sebuah wadah dapat memasang volume di bawah sistem file-nya.
- Konteks keamanan — Konteks keamanan container mendefinisikan hak istimewa dan pengaturan kontrol akses untuk container.
- Detail proses — Menjelaskan detail proses yang terkait dengan temuan.

RDSDBInstance

RDSDBInstance rincian:

Note

Sumber daya ini tersedia dalam temuan Perlindungan RDS yang terkait dengan instance database.

- Database Instance ID — Pengidentifikasi yang terkait dengan instance database yang terlibat dalam GuardDuty temuan.
- Engine — Nama mesin database dari instance database yang terlibat dalam temuan. Nilai yang mungkin kompatibel dengan Aurora MySQL atau kompatibel dengan Aurora PostgreSQL.
- Versi mesin — Versi mesin database yang terlibat dalam GuardDuty temuan.
- Database cluster ID — Pengidentifikasi cluster database yang berisi ID instance database yang terlibat dalam GuardDuty temuan.
- Database instance ARN — ARN yang mengidentifikasi instance database yang terlibat dalam temuan. GuardDuty

RDSLimitlessDB

RDSLimitlessRincian DB:

Sumber daya ini tersedia dalam temuan Perlindungan RDS yang terkait dengan versi mesin yang didukung dari Limitless Database.

- Pengidentifikasi grup shard DB — Nama yang terkait dengan grup shard DB Limitless.

- ID sumber daya grup shard DB — Pengidentifikasi sumber daya dari grup pecahan DB dalam DB Limitless.
- Grup pecahan DB ARN — Nama Sumber Daya Amazon (ARN) yang mengidentifikasi grup pecahan DB.
- Engine — Pengidentifikasi Limitless DB yang terlibat dalam temuan.
- Versi mesin — Versi mesin Limitless DB.
- DB cluster identifier — Nama cluster database yang merupakan bagian dari Limitless DB.

Untuk informasi tentang pengguna dan detail otentikasi dari database yang berpotensi terkena dampak, lihat. [Rincian pengguna database RDS \(DB\)](#)

Lambda

Detail fungsi Lambda

- Nama fungsi — Nama fungsi Lambda yang terlibat dalam temuan.
- Versi fungsi — Versi fungsi Lambda yang terlibat dalam temuan.
- Deskripsi fungsi — Deskripsi fungsi Lambda yang terlibat dalam temuan.
- Fungsi ARN — Nama Sumber Daya Amazon (ARN) dari fungsi Lambda yang terlibat dalam temuan.
- ID Revisi — ID revisi versi fungsi Lambda.
- Peran — Peran eksekusi fungsi Lambda yang terlibat dalam temuan.
- Konfigurasi VPC - Konfigurasi VPC Amazon, termasuk ID VPC, grup keamanan, dan subnet yang terkait dengan fungsi Lambda Anda. IDs
 - ID VPC — ID VPC Amazon yang terkait dengan fungsi Lambda yang terlibat dalam temuan.
 - Subnet IDs — ID subnet yang terkait dengan fungsi Lambda Anda.
 - Grup Keamanan — Kelompok keamanan yang melekat pada fungsi Lambda yang terlibat. Ini termasuk nama grup keamanan dan ID grup.
- Tag — Daftar tag yang dilampirkan ke sumber daya ini, tercantum dalam formatkey: value pasangan.

Detail pencarian urutan serangan

GuardDuty memberikan detail untuk setiap temuan yang dihasilkannya di akun Anda. Detail ini membantu Anda memahami alasan di balik temuan tersebut. Bagian ini berfokus pada detail yang

terkait dengan [Jenis pencarian urutan serangan](#). Ini termasuk wawasan seperti sumber daya yang berpotensi terkena dampak, garis waktu peristiwa, indikator, sinyal, dan titik akhir yang terlibat dalam temuan.

Untuk melihat detail yang terkait dengan sinyal yang merupakan GuardDuty temuan, lihat bagian terkait di halaman ini.

Di GuardDuty konsol, saat Anda memilih pencarian urutan serangan, panel samping detail dibagi menjadi tab berikut:

- Ikhtisar — Memberikan tampilan ringkas tentang detail urutan serangan, termasuk sinyal, taktik MITRE, dan sumber daya yang berpotensi terkena dampak.
- Sinyal — Menampilkan garis waktu peristiwa yang terlibat dalam urutan serangan.
- Sumber Daya — Memberikan informasi tentang sumber daya yang berpotensi terkena dampak, atau sumber daya yang berpotensi berisiko.

Daftar berikut memberikan deskripsi yang terkait dengan rincian pencarian urutan serangan.

Sinyal

Sinyal bisa berupa aktivitas API atau temuan yang GuardDuty digunakan untuk mendeteksi temuan urutan serangan. GuardDuty menganggap sinyal lemah yang tidak menampilkan diri sebagai ancaman yang jelas, menyatukannya, dan berkorelasi dengan temuan yang dihasilkan secara individual. Untuk konteks lebih lanjut, tab Sinyal menyediakan garis waktu sinyal, seperti yang diamati oleh GuardDuty.

Setiap sinyal, yang merupakan GuardDuty temuan, memiliki tingkat keparahan dan nilai yang ditetapkan untuk itu sendiri. Di GuardDuty konsol, Anda dapat memilih setiap sinyal untuk melihat detail terkait.

Aktor

Memberikan rincian tentang aktor ancaman dalam urutan serangan. Untuk informasi selengkapnya, lihat Referensi [Aktor](#) di Amazon GuardDuty API.

Titik akhir

Memberikan rincian tentang titik akhir jaringan yang digunakan dalam urutan serangan ini. Untuk informasi selengkapnya, lihat [NetworkEndpoint](#) di Referensi Amazon GuardDuty API. Untuk informasi tentang cara GuardDuty menentukan lokasi, lihat [Detail geolokasi](#).

Indikator

Termasuk data yang diamati yang cocok dengan pola masalah keamanan. Data ini menentukan mengapa GuardDuty ada indikasi aktivitas yang berpotensi mencurigakan. Misalnya, ketika nama indikatornya `HIGH_RISK_API`, ini menunjukkan tindakan yang biasa digunakan oleh pelaku ancaman, atau tindakan sensitif yang dapat menyebabkan dampak potensial pada Akun AWS, seperti mengakses kredensial atau memodifikasi sumber daya.

Tabel berikut mencakup daftar indikator potensial dan deskripsinya:

Nama indikator	Deskripsi
ATTACK_TACTIC	Taktik MITRE, seperti Discovery and Impact.
ATTACK_TECHNIQUE	Teknik MITRE yang digunakan oleh aktor ancaman dalam urutan serangan. Contohnya termasuk mendapatkan akses ke sumber daya dan menggunakannya dengan cara yang tidak diinginkan, dan mengeksploitasi kerentanan.
CRYPTOMINING_DOMAIN	Menunjukkan nama domain yang terkait dengan kolam atau infrastruktur penambangan cryptocurrency. Misalnya, kueri atau koneksi DNS ke domain ini dari container atau lingkungan Kubernetes dapat mengindikasikan aktivitas cryptomining yang tidak sah. Menunjukkan bahwa Nomor Sistem Otonom (ASN) diidentifikasi sebagai anomali, berdasarkan garis dasar historis pengguna. Untuk informasi selengkapnya, lihat Perilaku anomali .
CRYPTOMINING_IP	Menunjukkan alamat IP yang terkait dengan kolam atau infrastruktur penambangan cryptocurrency. Misalnya, koneksi ke alamat-alamat ini dari container atau lingkungan Kubernetes dapat mengindikasikan aktivitas cryptomining yang tidak sah. Menunjukkan bahwa Nomor Sistem Otonom (ASN) diidentifikasi sebagai anomali, berdasarkan garis dasar historis pengguna. Untuk informasi selengkapnya, lihat Perilaku anomali .
CRYPTOMINING_PROCESS	Menunjukkan proses yang diidentifikasi sebagai perangkat lunak penambangan cryptocurrency yang berjalan di dalam wadah atau

Nama indikator	Deskripsi
	lingkungan Kubernetes. Misalnya, proses ini dapat mengkonsumsi sumber daya CPU yang berlebihan. Menunjukkan bahwa Nomor Sistem Otonom (ASN) diidentifikasi sebagai anomali, berdasarkan garis dasar historis pengguna. Untuk informasi selengkapnya, lihat Perilaku anomali.
HIGH_RISK_API	AWS API yang menyertakan Layanan AWS nama dan eventName menunjukkan tindakan yang biasa digunakan oleh pelaku ancaman, atau merupakan tindakan sensitif yang dapat menyebabkan dampak potensial pada Akun AWS, seperti akses kredensi atau modifikasi sumber daya.
MALICIOUS_DOMAIN	Menunjukkan nama domain dengan dugaan intelijen ancaman yang menunjukkan niat jahat. Misalnya, ini termasuk server perintah dan kontrol (C&C), situs distribusi malware, atau domain phishing yang dihubungi dari container atau lingkungan Kubernetes. Menunjukkan bahwa Nomor Sistem Otonom (ASN) diidentifikasi sebagai anomali, berdasarkan garis dasar historis pengguna. Untuk informasi selengkapnya, lihat Perilaku anomali.
MALICIOUS_IP	Alamat IP telah mengkonfirmasi intelijen ancaman yang menunjukkan niat jahat.
MALICIOUS_PROCESS	Menunjukkan proses yang diduga berbahaya berdasarkan kecerdasan ancaman atau analisis perilaku. Misalnya, ini termasuk malware, pintu belakang, atau alat tidak sah yang dikenal yang dijalankan di dalam container atau lingkungan Kubernetes dengan niat jahat. Menunjukkan bahwa Nomor Sistem Otonom (ASN) diidentifikasi sebagai anomali, berdasarkan garis dasar historis pengguna. Untuk informasi selengkapnya, lihat Perilaku anomali.
SUSPICIOUS_NETWORK	Jaringan ini dikaitkan dengan skor reputasi rendah yang diketahui, seperti penyedia jaringan pribadi virtual (VPN) berisiko dan layanan proxy.

Nama indikator	Deskripsi
SUSPICIOUS_PROCESS	Menunjukkan bahwa Nomor Sistem Otonom (ASN) diidentifikasi sebagai anomali, berdasarkan garis dasar historis pengguna. Untuk informasi selengkapnya, lihat Perilaku anomali .
SUSPICIOUS_USER_AGENT	Agen pengguna dikaitkan dengan aplikasi mencurigakan atau dieksploitasi yang berpotensi diketahui, seperti klien Amazon S3 dan alat serangan.
TOR_IP	Alamat IP dikaitkan dengan node keluar Tor.
UNUSUAL_API_FOR_ACCOUNT	Menunjukkan bahwa AWS API dipanggil secara anomali, berdasarkan garis dasar historis akun. Untuk informasi selengkapnya, lihat Perilaku anomali .
UNUSUAL_ASN_FOR_ACCOUNT	Menunjukkan bahwa Nomor Sistem Otonom (ASN) diidentifikasi sebagai anomali, berdasarkan dasar historis akun tersebut. Untuk informasi selengkapnya, lihat Perilaku anomali .
UNUSUAL_ASN_FOR_USER	Menunjukkan bahwa Nomor Sistem Otonom (ASN) diidentifikasi sebagai anomali, berdasarkan garis dasar historis pengguna. Untuk informasi selengkapnya, lihat Perilaku anomali .

Taktik MITRE

Bidang ini menentukan taktik MITRE ATT&CK yang dicoba oleh aktor ancaman melalui urutan serangan. GuardDuty menggunakan kerangka kerja [MITRE ATT&ACK](#) yang menambahkan konteks ke seluruh urutan serangan. Warna yang digunakan GuardDuty konsol untuk menentukan tujuan ancaman yang telah digunakan oleh aktor ancaman, sejajar dengan warna yang menunjukkan kritis, tinggi, sedang, dan rendah [Temuan tingkat keparahan](#).

Indikator jaringan

Indikator mencakup kombinasi nilai indikator jaringan yang menjelaskan mengapa jaringan menunjukkan perilaku yang mencurigakan. Bagian ini hanya berlaku jika Indikator menyertakan SUSPICIOUS_NETWORK atau MALICIOUS_IP. Contoh berikut menunjukkan bagaimana indikator jaringan dapat dikaitkan dengan indikator, di mana:

- *AnyCompany* adalah Sistem Otonom (AS).

- TUNNEL_VPN, IS_ANONYMOUS, dan ALLOWS_FREE_ACCESS merupakan indikator jaringan.

```
...{
  "key": "SUSPICIOUS_NETWORK",
  "values": [{
    "AnyCompany": [
      "TUNNEL_VPN",
      "IS_ANONYMOUS",
      "ALLOWS_FREE_ACCESS"
    ]
  }]
}
```

Tabel berikut mencakup nilai indikator jaringan dan deskripsinya. Tag ini ditambahkan berdasarkan data intelijen ancaman yang GuardDuty dikumpulkan dari sumber-sumber seperti Spur.

Nilai indikator jaringan	Deskripsi
TUNNEL_VPN	Jaringan atau alamat IP dikaitkan dengan jenis terowongan VPN. Ini mengacu pada protokol khusus yang membantu membangun koneksi yang aman dan terenkripsi antara dua titik melalui jaringan publik.
TUNNEL_PROXY	Jaringan atau alamat IP dikaitkan dengan jenis terowongan Proxy. Ini mengacu pada protokol khusus yang membantu membangun koneksi melalui server proxy.
TUNNEL_RDP	Jaringan atau alamat IP dikaitkan dengan menggunakan metode enkapsulasi lalu lintas desktop jarak jauh (RDP) dalam protokol lain untuk meningkatkan keamanan, melewati pembatasan jaringan, atau mengaktifkan akses jarak jauh melalui firewall.
IS_ANONYMOUS	Jaringan atau alamat IP dikaitkan dengan layanan anonim atau proxy yang dikenal. Ini mungkin menunjukkan potensi aktivitas mencurigakan yang bersembunyi di balik jaringan anonim.
KNOWN_THREAT_OPERATOR	Jaringan atau alamat IP dikaitkan dengan penyedia terowongan berisiko yang diketahui. Ini menunjukkan bahwa aktivitas mencurigakan

Nilai indikator jaringan	Deskripsi
	kan telah terdeteksi dari alamat IP yang ditautkan ke VPN, proxy, atau layanan tunneling lainnya yang sering digunakan untuk tujuan jahat.
ALLOWS_FROEE_ACCESS	Jaringan atau alamat IP dikaitkan dengan operator terowongan yang memungkinkan akses ke layanannya tanpa memerlukan otentikasi atau pembayaran. Ini mungkin juga termasuk akun percobaan atau pengalaman penggunaan terbatas yang ditawarkan oleh berbagai layanan online.
ALLOWS_CRYPTO	Jaringan atau alamat IP dikaitkan dengan penyedia terowongan (seperti VPN atau layanan proxy) yang secara eksklusif menerima cryptocurrency atau mata uang digital lainnya sebagai metode pembayaran.
ALLOWS_TORRENTS	Jaringan atau alamat IP dikaitkan dengan layanan atau platform yang memungkinkan lalu lintas torrent. Layanan semacam itu sering dikaitkan dengan mendukung dan menggunakan torrent, dan kegiatan pelanggaran hak cipta.
RISK_CALLBACK_PROXY	Jaringan atau alamat IP dikaitkan dengan perangkat yang dikenal untuk mengarahkan lalu lintas untuk proxy perumahan, proxy malware, atau jaringan tipe proxy callback lainnya. Ini tidak berarti semua aktivitas di jaringan terkait dengan proxy, melainkan bahwa jaringan memiliki kemampuan untuk merutekan lalu lintas atas nama jaringan proxy ini.
RISK_GEO_MISMATCH	Indikator ini menunjukkan bahwa pusat data atau lokasi hosting jaringan berbeda dari lokasi yang diharapkan dari pengguna dan perangkat di belakangnya. Jika nilai indikator ini tidak ada, itu tidak berarti bahwa tidak ada ketidakcocokan. Ini mungkin menyiratkan bahwa tidak ada cukup data untuk mengkonfirmasi perbedaan tersebut.
IS_SCANNER	Jaringan atau alamat IP dikaitkan dengan melakukan upaya login persisten terhadap formulir web.

Nilai indikator jaringan	Deskripsi
RISK_WEB_SCRAPING	Jaringan alamat IP dikaitkan dengan klien web otomatis dan aktivitas web terprogram lainnya.
CLIENT_BEHAVIOR_FILE_SHARING	Jaringan atau alamat IP dikaitkan dengan perilaku klien yang menunjukkan aktivitas berbagi file, seperti jaringan peer-to-peer (P2P), atau protokol berbagi file.
CATEGORY_COMMERCIAL_VPN	Jaringan atau alamat IP dikaitkan dengan operator terowongan yang dikategorikan sebagai layanan Commercial Virtual Private Network (VPN) tradisional yang beroperasi dalam ruang pusat data.
CATEGORY_FREE_VPN	Jaringan atau alamat IP dikaitkan dengan operator terowongan yang dikategorikan sebagai layanan VPN gratis.
CATEGORY_RESIDENTIAL_PROXY	Alamat jaringan atau IP dikaitkan dengan operator terowongan yang dikategorikan sebagai SDK, malware, atau layanan proxy get-paid-to bersumber.
OPERATOR_XXX	Nama penyedia layanan yang mengoperasikan terowongan ini.

Rincian pengguna database RDS (DB)

Note

Bagian ini berlaku untuk temuan saat Anda mengaktifkan fitur Perlindungan RDS di GuardDuty. Untuk informasi selengkapnya, lihat [GuardDuty Perlindungan RDS](#).

GuardDuty Temuan ini memberikan rincian pengguna dan otentikasi berikut dari database yang berpotensi dikompromikan:

- Pengguna — Nama pengguna yang digunakan untuk melakukan upaya login anomali.
- Aplikasi — Nama aplikasi yang digunakan untuk melakukan upaya login anomali.
- Database — Nama instance database yang terlibat dalam upaya login anomali.

- SSL — Versi Secure Socket Layer (SSL) yang digunakan untuk jaringan.
- Metode autentikasi — Metode otentikasi yang digunakan oleh pengguna yang terlibat dalam temuan.

Untuk informasi tentang sumber daya yang berpotensi dikompromikan, lihat [Sumber Daya](#).

Detail penemuan Runtime Monitoring

Note

Detail ini mungkin tersedia hanya jika GuardDuty menghasilkan salah satu [GuardDuty Jenis penemuan Runtime Monitoring](#).

Bagian ini berisi rincian runtime seperti detail proses dan konteks yang diperlukan. Detail proses menjelaskan informasi tentang proses yang diamati, dan konteks runtime menjelaskan informasi tambahan apa pun tentang aktivitas yang berpotensi mencurigakan.

Detail proses

- Nama — Nama proses.
- Jalur yang dapat dieksekusi — Jalur absolut dari file yang dapat dieksekusi proses.
- Executable SHA-256 — SHA256 Hash dari proses yang dapat dieksekusi.
- Namespace PID — ID proses dalam namespace PID sekunder selain namespace PID tingkat host. Untuk proses di dalam wadah, itu adalah ID proses yang diamati di dalam wadah.
- Direktori kerja saat ini — Direktori kerja saat ini dari proses.
- ID Proses — ID yang ditetapkan untuk proses oleh sistem operasi.
- StartTime — Waktu ketika proses dimulai. Ini dalam format string tanggal UTC (2023-03-22T19:37:20.168Z).
- UUID — ID unik yang ditetapkan untuk proses oleh GuardDuty
- UUID Induk — ID unik dari proses induk. ID ini ditetapkan ke proses induk oleh GuardDuty.
- Pengguna — Pengguna yang menjalankan proses.
- User ID — ID pengguna yang menjalankan proses.
- ID pengguna yang efektif — ID pengguna yang efektif dari proses pada saat acara berlangsung.

- Silsilah — Informasi tentang nenek moyang proses.
 - ID Proses — ID yang ditetapkan untuk proses oleh sistem operasi.
 - UUID — ID unik yang ditetapkan untuk proses oleh GuardDuty
 - Jalur yang dapat dieksekusi — Jalur absolut dari file yang dapat dieksekusi proses.
 - ID pengguna yang efektif — ID pengguna yang efektif dari proses pada saat acara berlangsung.
 - UUID Induk — ID unik dari proses induk. ID ini ditetapkan ke proses induk oleh GuardDuty.
 - Waktu Mulai — Waktu ketika proses dimulai.
 - Namespace PID — ID proses dalam namespace PID sekunder selain namespace PID tingkat host. Untuk proses di dalam wadah, itu adalah ID proses yang diamati di dalam wadah.
 - User ID — User ID pengguna yang menjalankan proses.
 - Nama — Nama proses.

Konteks runtime

Dari bidang berikut, temuan yang dihasilkan mungkin hanya mencakup bidang-bidang yang relevan dengan jenis temuan.

- Mount Source - Jalur pada host yang dipasang oleh wadah.
- Mount Target - Jalur dalam wadah yang dipetakan ke direktori host.
- Jenis Sistem File - Merupakan jenis sistem file yang dipasang.
- Bendera - Merupakan opsi yang mengontrol perilaku acara yang terlibat dalam temuan ini.
- Memodifikasi Proses — Informasi tentang proses yang membuat atau memodifikasi biner, skrip, atau pustaka, di dalam wadah saat runtime.
- Modified At — Stempel waktu di mana proses membuat atau memodifikasi biner, skrip, atau pustaka di dalam wadah saat runtime. Bidang ini dalam format string tanggal UTC (2023-03-22T19:37:20.168Z).
- Library Path — Jalur ke perpustakaan baru yang dimuat.
- LD Preload Value — Nilai variabel LD_PRELOAD lingkungan.
- Socket Path — Jalur ke soket Docker yang diakses.
- Runc Binary Path — Jalan menuju runc biner.
- Release Agent Path - Jalur ke file agen cgroup rilis.
- Contoh Baris Perintah — Contoh baris perintah yang terlibat dalam aktivitas yang berpotensi mencurigakan.

- Kategori Alat - Kategori yang dimiliki alat tersebut. Beberapa contohnya adalah Backdoor Tool, Pentest Tool, Network Scanner, dan Network Sniffer.
- Nama Alat — Nama alat yang berpotensi mencurigakan.
- Script Path — Jalur ke skrip yang dieksekusi yang menghasilkan temuan.
- Threat File Path — Jalur mencurigakan di mana rincian intelijen ancaman ditemukan.
- Nama Layanan — Nama layanan keamanan yang telah dinonaktifkan.

Detail pemindaian volume EBS

Note

Bagian ini berlaku untuk temuan saat Anda mengaktifkan GuardDuty pemindaian malware yang dimulai. [Perlindungan Malware untuk EC2](#)

Pemindaian volume EBS memberikan detail tentang volume EBS yang melekat pada EC2 instans atau beban kerja kontainer yang berpotensi dikompromikan.

- Scan ID — Pengidentifikasi pemindaian malware.
- Pemindaian dimulai pada — Tanggal dan waktu ketika pemindaian malware dimulai.
- Pemindaian selesai pada — Tanggal dan waktu pemindaian malware selesai.
- Trigger Finding ID — ID temuan dari GuardDuty temuan yang memulai pemindaian malware ini.
- Sumber — Nilai potensial adalah Bitdefender dan Amazon.

Untuk informasi selengkapnya tentang mesin pemindai yang digunakan untuk mendeteksi malware, lihat [GuardDuty mesin pemindai deteksi malware](#).

- Deteksi pemindaian — Tampilan lengkap detail dan hasil untuk setiap pemindaian malware.
 - Jumlah item yang dipindai - Jumlah total file yang dipindai. Ini memberikan rincian seperti `totalGb`, `files`, dan `volumes`.
 - Jumlah item yang terdeteksi ancaman — Jumlah total berbahaya yang `files` terdeteksi selama pemindaian.
 - Detail ancaman tingkat keparahan tertinggi — Rincian ancaman tingkat keparahan tertinggi yang terdeteksi selama pemindaian dan jumlah file berbahaya. Ini memberikan rincian seperti `severity`, `threatName`, dan `count`.

- Ancaman terdeteksi oleh Nama - Elemen kontainer mengelompokkan ancaman dari semua tingkat keparahan. Ini memberikan rincian seperti `itemCount`, `uniqueThreatNameCount`, `shortened`, dan `threatNames`.

Perlindungan Malware untuk EC2 menemukan detail

Note

Bagian ini berlaku untuk temuan saat Anda mengaktifkan GuardDuty pemindaian malware yang dimulai. [Perlindungan Malware untuk EC2](#)

Saat Perlindungan Malware untuk EC2 pemindaian mendeteksi malware, Anda dapat melihat detail pemindaian dengan memilih temuan yang sesuai di halaman Temuan di <https://console.aws.amazon.com/guardduty/konsol>. Tingkat keparahan Perlindungan Malware Anda untuk EC2 menemukan tergantung pada tingkat keparahan GuardDuty temuan.

Informasi berikut tersedia di bawah bagian Ancaman terdeteksi di panel detail.

- Nama — Nama ancaman, diperoleh dengan mengelompokkan file dengan deteksi.
- Keparahan — Tingkat keparahan ancaman yang terdeteksi.
- Hash — SHA-256 dari file.
- Jalur file — Lokasi file berbahaya dalam volume EBS.
- Nama file — Nama file di mana ancaman terdeteksi.
- Volume ARN — ARN dari volume EBS yang dipindai.

Informasi berikut tersedia di bawah bagian Detail pemindaian Malware di panel detail.

- Scan ID — ID pemindaian dari pemindaian malware.
- Pemindaian dimulai pada — Tanggal dan waktu pemindaian dimulai.
- Pemindaian selesai pada — Tanggal dan waktu pemindaian selesai.
- File yang dipindai — Jumlah total file dan direktori yang dipindai.
- Total GB yang dipindai — Jumlah penyimpanan yang dipindai selama proses berlangsung.
- Trigger finding ID — ID temuan dari GuardDuty temuan yang memulai pemindaian malware ini.

- Informasi berikut tersedia di bawah bagian Detail volume di panel detail.
 - Volume ARN — Nama Sumber Daya Amazon (ARN) dari volume.
 - Snapshotarn — ARN dari snapshot volume EBS.
 - Status — Status pemindaian volume, seperti `Running`, `Skipped`, dan `Completed`.
 - Jenis enkripsi — Jenis enkripsi yang digunakan untuk mengenkripsi volume. Misalnya, `CMCMK`.
 - Nama perangkat — Nama perangkat. Misalnya, `/dev/xvda`.

Perlindungan Malware untuk detail penemuan S3

Detail pemindaian malware berikut tersedia saat Anda mengaktifkan keduanya GuardDuty dan Perlindungan Malware untuk S3 di: Akun AWS

- Ancaman — Daftar ancaman yang terdeteksi selama pemindaian malware.

Beberapa potensi ancaman dalam file arsip

Jika Anda memiliki file arsip dengan potensi beberapa ancaman di dalamnya, Perlindungan Malware untuk S3 hanya melaporkan ancaman pertama yang terdeteksi. Setelah ini, status pemindaian ditandai sebagai selesai. GuardDuty menghasilkan jenis temuan terkait dan juga mengirimkan EventBridge peristiwa yang dihasilkannya. Untuk informasi selengkapnya tentang memantau pemindaian objek Amazon S3 menggunakan EventBridge peristiwa, lihat skema pemberitahuan contoh untuk `THREATS_FOUND` di.

[Hasil pemindaian objek S3](#)

- Jalur item - Daftar jalur item bersarang dan detail hash dari objek S3 yang dipindai.
 - Jalur item bersarang - Jalur item dari objek S3 yang dipindai tempat ancaman terdeteksi.

Nilai bidang ini hanya tersedia jika objek tingkat atas adalah arsip dan jika ancaman terdeteksi di dalam arsip.

- Hash — Hash dari ancaman yang terdeteksi dalam temuan ini.
- Sumber — Nilai potensial adalah `Bitdefender` dan `Amazon`.

Untuk informasi selengkapnya tentang mesin pemindai yang digunakan untuk mendeteksi malware, lihat [GuardDuty mesin pemindai deteksi malware](#).

Tindakan

Tindakan temuan memberikan rincian tentang jenis aktivitas yang memicu temuan. Informasi yang tersedia bervariasi berdasarkan tipe tindakan.

Tipe tindakan – Tipe aktivitas temuan. Nilai ini dapat berupa `NETWORK_CONNECTION`, `PORT_PROBE`, `DNS_REQUEST`, `_CALL`, atau `RDS_LOGIN_ATTACK`. AWS API Informasi yang tersedia bervariasi berdasarkan tipe tindakan:

- **NETWORK_CONNECTION** - Menunjukkan bahwa lalu lintas jaringan dipertukarkan antara EC2 instance yang diidentifikasi dan host jarak jauh. Tipe tindakan ini memiliki informasi tambahan berikut:
 - Arah koneksi — Arah koneksi jaringan diamati dalam aktivitas yang mendorong GuardDuty untuk menghasilkan temuan. Nilai bisa jadi salah satu dari nilai berikut:
 - **INBOUND** - Menunjukkan bahwa host jarak jauh memulai koneksi ke port lokal pada EC2 instance yang diidentifikasi di akun Anda.
 - **OUTBOUND** - Menunjukkan bahwa EC2 instance yang diidentifikasi memulai koneksi ke host jarak jauh.
 - **TIDAK DIKETAHUI** — Menunjukkan bahwa tidak GuardDuty dapat menentukan arah koneksi.
 - Protokol — Protokol koneksi jaringan diamati dalam aktivitas yang mendorong GuardDuty untuk menghasilkan temuan.
 - IP lokal — Alamat IP sumber asli dari lalu lintas yang memicu temuan. Info ini dapat digunakan untuk membedakan antara alamat IP dari lapisan perantara yang dilalui arus lalu lintas, dan alamat IP sumber asal dari lalu lintas yang memicu temuan. Misalnya, alamat IP pod EKS berbeda dengan alamat IP instans tempat pod EKS berjalan.
 - Diblokir – Menunjukkan apakah port yang ditargetkan diblokir.
- **PORT_PROBE** - Menunjukkan bahwa host jarak jauh memeriksa EC2 instance yang diidentifikasi pada beberapa port terbuka. Tipe tindakan ini memiliki informasi tambahan berikut:
 - IP lokal — Alamat IP sumber asli dari lalu lintas yang memicu temuan. Info ini dapat digunakan untuk membedakan antara alamat IP dari lapisan perantara yang dilalui arus lalu lintas, dan alamat IP sumber asal dari lalu lintas yang memicu temuan. Misalnya, alamat IP pod EKS berbeda dengan alamat IP instans tempat pod EKS berjalan.
 - Diblokir – Menunjukkan apakah port yang ditargetkan diblokir.
- **DNS_REQUEST** - Menunjukkan bahwa EC2 instance yang diidentifikasi menanyakan nama domain. Tipe tindakan ini memiliki informasi tambahan berikut:

- Protokol — Protokol koneksi jaringan diamati dalam aktivitas yang mendorong GuardDuty untuk menghasilkan temuan.
- Diblokir – Menunjukkan apakah port yang ditargetkan diblokir.
- AWS_API_CALL — Menunjukkan bahwa AWS API telah dipanggil. Tipe tindakan ini memiliki informasi tambahan berikut:
 - API — Nama operasi API yang dipanggil dan dengan demikian diminta GuardDuty untuk menghasilkan temuan ini.

 Note

Operasi ini juga dapat mencakup peristiwa non-API yang ditangkap oleh AWS CloudTrail. Untuk informasi selengkapnya, lihat [peristiwa non-API yang ditangkap oleh CloudTrail](#).

- User Agent — Agen pengguna yang membuat permintaan API. Nilai ini memberi tahu Anda apakah panggilan dilakukan dari, AWS layanan AWS SDKs, atau AWS CLI. AWS Management Console
- KODE KESALAHAN - Jika temuan dipicu oleh panggilan API yang gagal, ini menampilkan kode kesalahan untuk panggilan itu.
- Nama layanan — Nama DNS dari layanan yang mencoba membuat panggilan API yang memicu temuan.
- RDS_LOGIN_ATTACK - Menunjukkan bahwa upaya login dilakukan ke database yang berpotensi dikompromikan dari alamat IP jarak jauh.
 - Alamat IP — Alamat IP jarak jauh yang digunakan untuk melakukan upaya login yang berpotensi mencurigakan.

Aktor atau Target

Temuan memiliki bagian Aktor jika peran Sumber Daya adalah TARGET. Ini menunjukkan bahwa sumber daya Anda ditargetkan oleh aktivitas mencurigakan, dan bagian Aktor berisi detail tentang entitas yang menargetkan sumber daya Anda.

Temuan memiliki bagian Target jika peran Sumber Daya adalah ACTOR. Hal ini menunjukkan bahwa sumber daya Anda terlibat dalam aktivitas yang mencurigakan terhadap host jarak jauh, dan bagian ini berisi informasi tentang IP atau domain yang ditargetkan sumber daya Anda.

Informasi yang tersedia di bagian Aktor atau Target dapat mencakup hal-hal berikut:

- **Afiliasi** — Detail tentang apakah AWS akun pemanggil API jarak jauh terkait dengan lingkungan Anda GuardDuty . Jika nilai `inittrue`, pemanggil API berafiliasi dengan akun Anda dalam beberapa cara; jika `false`, pemanggil API berasal dari luar lingkungan Anda.
- **ID Akun Jarak Jauh** — ID akun yang memiliki alamat IP keluar yang digunakan untuk mengakses sumber daya di jaringan akhir.
- **Alamat IP** — Alamat IP yang terlibat dalam aktivitas yang mendorong GuardDuty untuk menghasilkan temuan.
- **Lokasi** — Informasi lokasi untuk alamat IP yang terlibat dalam aktivitas yang diminta GuardDuty untuk menghasilkan temuan.
- **Organisasi** — informasi organisasi ISP dari alamat IP yang terlibat dalam aktivitas yang mendorong GuardDuty untuk menghasilkan temuan.
- **Port** — Nomor port yang terlibat dalam aktivitas yang mendorong GuardDuty untuk menghasilkan temuan.
- **Domain** — Domain yang terlibat dalam aktivitas yang mendorong GuardDuty untuk menghasilkan temuan.
- **Domain dengan akhiran** — Domain tingkat kedua dan teratas yang terlibat dalam aktivitas yang berpotensi mendorong GuardDuty untuk menghasilkan temuan. [Untuk daftar domain tingkat atas dan tingkat kedua, lihat daftar akhiran publik.](#)

Detail geolokasi

GuardDuty menentukan lokasi dan jaringan permintaan dengan menggunakan database MaxMind GeoIP. MaxMind melaporkan akurasi data mereka yang sangat tinggi di tingkat negara, meskipun akurasi bervariasi sesuai dengan faktor-faktor seperti negara dan jenis alamat IP.

Untuk informasi selengkapnya MaxMind, lihat [Geolokasi MaxMind IP](#). Jika Anda yakin salah satu data GeoIP salah, kirimkan permintaan koreksi ke MaxMind [MaxMindCorrect IP2 Geo](#) Data.

Informasi tambahan

Semua temuan memiliki bagian Informasi tambahan yang dapat mencakup informasi berikut:

- **Nama daftar ancaman** — Nama daftar ancaman yang mencakup alamat IP atau nama domain yang terlibat dalam aktivitas yang diminta GuardDuty untuk menghasilkan temuan.

- Sampel — Nilai benar atau salah yang menunjukkan apakah ini adalah temuan sampel.
- Diarsipkan — Nilai benar atau salah yang menunjukkan apakah temuan ini telah diarsipkan.
- Tidak biasa — Detail aktivitas yang tidak diamati secara historis. Ini dapat mencakup pengguna yang tidak biasa (sebelumnya tidak diamati), lokasi, waktu, bucket, perilaku login, atau ASN Org.
- Protokol yang tidak biasa — Protokol koneksi jaringan yang terlibat dalam aktivitas yang mendorong GuardDuty untuk menghasilkan temuan.
- Detail agen — Detail tentang agen keamanan yang saat ini digunakan di kluster EKS di Akun AWS. Ini hanya berlaku untuk jenis pencarian Pemantauan Runtime EKS.
 - Versi agen — Versi agen GuardDuty keamanan.
 - Agen Id — Identifier unik dari agen GuardDuty keamanan.

Bukti

Temuan berdasarkan intelijen ancaman memiliki bagian Bukti yang mencakup informasi berikut:

- Detail intelijen ancaman — Nama daftar ancaman tempat yang dikenali Threat name muncul.
- Nama ancaman — Nama keluarga malware atau pengenalan lain yang terkait dengan ancaman.
- File ancaman SHA256 — SHA256 dari file yang menghasilkan temuan.

Perilaku anomali

Jenis temuan yang berakhir AnomalousBehavior menunjukkan bahwa temuan tersebut dihasilkan oleh model pembelajaran mesin deteksi GuardDuty anomali (ML). Model ML mengevaluasi semua permintaan API ke akun Anda dan mengidentifikasi peristiwa anomali yang terkait dengan taktik yang digunakan oleh musuh. Model ML melacak berbagai faktor permintaan API, seperti pengguna yang membuat permintaan, lokasi tempat permintaan dibuat, dan API khusus yang diminta.

Detail tentang faktor permintaan API yang tidak biasa untuk identitas CloudTrail pengguna yang memanggil permintaan dapat ditemukan di detail temuan. Identitas didefinisikan oleh Elemen [CloudTrail UserIdentity](#), dan nilai yang mungkin adalah Root::IAMUser,,, AssumedRole FederatedUserAWSAccount, atau. AWSService

Selain detail yang tersedia untuk semua GuardDuty temuan yang terkait dengan aktivitas API, AnomalousBehavior temuan memiliki detail tambahan yang diuraikan di bagian berikut. Detail ini dapat dilihat di konsol dan juga tersedia di JSON temuan.

- **Anomalous APIs** — Daftar permintaan API yang dipanggil oleh identitas pengguna di dekat permintaan API utama yang terkait dengan temuan. Panel ini selanjutnya memecah detail peristiwa API dengan cara berikut.
 - API pertama yang terdaftar adalah API utama, yang merupakan permintaan API yang terkait dengan aktivitas berisiko tertinggi yang diamati. Ini adalah API yang memicu temuan dan berkorelasi dengan tahap serangan dari tipe temuan. Ini juga merupakan API yang diuraikan di bagian Tindakan di konsol, dan di JSON temuan.
 - APIs Daftar lainnya adalah anomali tambahan APIs dari identitas pengguna terdaftar yang diamati di dekat API utama. Jika hanya ada satu API pada daftar, model ML tidak mengidentifikasi permintaan API tambahan dari identitas pengguna sebagai anomali.
 - Daftar APIs dibagi berdasarkan apakah API berhasil dipanggil, atau jika API tidak berhasil dipanggil, artinya respons kesalahan diterima. Jenis respons kesalahan yang diterima tercantum di atas setiap API yang tidak berhasil disebut. Jenis respons kesalahan yang mungkin adalah: `access denied`, `access denied exception`, `auth failure`, `instance limit exceeded`, `invalid permission - duplicate`, `invalid permission - not found`, dan `operation not permitted`.
 - APIs dikategorikan oleh layanan terkait mereka.
 - Untuk konteks lebih lanjut, pilih Historis APIs untuk melihat detail tentang bagian atas APIs, hingga maksimum 20, biasanya terlihat untuk identitas pengguna dan semua pengguna dalam akun. Ditandai Langka (kurang dari sebulan sekali), Jarang (beberapa kali sebulan), atau Sering (harian hingga mingguan), tergantung pada seberapa sering mereka digunakan dalam akun Anda. APIs
- **Perilaku Tidak Biasa (Akun)** — Bagian ini memberikan rincian tambahan tentang perilaku yang diprofilkan untuk akun Anda.

Perilaku yang diprofilkan

GuardDuty terus belajar tentang aktivitas dalam akun Anda berdasarkan peristiwa yang disampaikan. Kegiatan ini dan frekuensi yang diamati dikenal sebagai perilaku yang diprofilkan.

Informasi yang dilacak di panel ini mencakup:

- **ASN Org** — Org Autonomous System Number (ASN) tempat panggilan API anomali dibuat.
- **Nama Pengguna** – Nama pengguna yang membuat panggilan API anomali.

- User Agent — Agen pengguna yang digunakan untuk membuat panggilan API anomali. Agen pengguna adalah metode yang digunakan untuk membuat panggilan seperti `aws-cli` atau `Botocore`.
- Tipe Pengguna – Tipe pengguna yang membuat panggilan API anomali. Kemungkinan nilainya adalah `AWS_SERVICE`, `ASSUMED_ROLE`, `IAM_USER`, atau `ROLE`.
- Bucket — Nama bucket S3 yang sedang diakses.
- Perilaku Tidak Biasa (Identitas Pengguna) - Bagian ini memberikan rincian tambahan tentang perilaku yang diprofilkan untuk Identitas Pengguna yang terlibat dengan temuan tersebut. Ketika perilaku tidak diidentifikasi sebagai historis, ini berarti model GuardDuty ML sebelumnya tidak melihat identitas pengguna ini membuat panggilan API ini dengan cara ini dalam periode pelatihan. Berikut adalah detail tambahan tentang Identitas Pengguna yang tersedia:
 - ASN Org – ASN Org tempat panggilan API anomali dibuat.
 - User Agent — Agen pengguna yang digunakan untuk membuat panggilan API anomali. Agen pengguna adalah metode yang digunakan untuk membuat panggilan seperti `aws-cli` atau `Botocore`.
 - Bucket — Nama bucket S3 yang sedang diakses.
- Perilaku Tidak Biasa (Bucket) — Bagian ini memberikan detail tambahan tentang perilaku yang diprofilkan untuk bucket S3 yang terkait dengan temuan tersebut. Jika perilaku tidak diidentifikasi sebagai historis, ini berarti model GuardDuty ML sebelumnya tidak pernah melihat panggilan API yang dilakukan ke bucket ini dengan cara ini dalam periode pelatihan. Informasi yang dilacak di bagian ini meliputi:
 - ASN Org – ASN Org tempat panggilan API anomali dibuat.
 - Nama Pengguna – Nama pengguna yang membuat panggilan API anomali.
 - User Agent — Agen pengguna yang digunakan untuk membuat panggilan API anomali. Agen pengguna adalah metode yang digunakan untuk membuat panggilan seperti `aws-cli` atau `Botocore`.
 - Tipe Pengguna – Tipe pengguna yang membuat panggilan API anomali. Kemungkinan nilainya adalah `AWS_SERVICE`, `ASSUMED_ROLE`, `IAM_USER`, atau `ROLE`.

 Note

Untuk konteks lebih lanjut tentang perilaku historis, pilih Perilaku historis di bagian Perilaku Tidak Biasa (Akun), ID Pengguna, atau Bucket untuk melihat detail tentang perilaku yang diharapkan di akun Anda untuk masing-masing kategori berikut: Langka (kurang dari

sebulan sekali), Jarang (beberapa kali sebulan), atau Sering (harian hingga mingguan), tergantung seberapa sering mereka digunakan dalam akun Anda.

- **Perilaku Tidak Biasa (Database)** - Bagian ini memberikan rincian tambahan tentang perilaku yang diprofilkan untuk instance database yang terkait dengan temuan. Ketika perilaku tidak diidentifikasi sebagai historis, itu berarti bahwa model GuardDuty ML sebelumnya tidak melihat upaya login yang dilakukan ke instance database ini dengan cara ini dalam periode pelatihan. Informasi yang dilacak untuk bagian ini di panel temuan meliputi:
 - **Nama pengguna** — Nama pengguna yang digunakan untuk melakukan upaya login anomali.
 - **ASN Org** — Org ASN tempat upaya login anomali dilakukan.
 - **Nama aplikasi** — Nama aplikasi yang digunakan untuk melakukan upaya login anomali.
 - **Nama database** — Nama instance database yang terlibat dalam upaya login anomali.

Bagian perilaku historis memberikan lebih banyak konteks tentang nama Pengguna yang diamati sebelumnya, Org ASN, nama Aplikasi, dan nama Database untuk database terkait. Setiap nilai unik memiliki hitungan terkait yang mewakili berapa kali nilai ini diamati dalam peristiwa login yang berhasil.

- **Perilaku yang tidak biasa (klaster Akun Kubernetes, namespace Kubernetes, dan nama pengguna Kubernetes)** — Bagian ini memberikan rincian tambahan tentang perilaku yang diprofilkan untuk klaster Kubernetes dan namespace yang terkait dengan temuan tersebut. Ketika perilaku tidak diidentifikasi sebagai historis, itu berarti bahwa model GuardDuty ML sebelumnya tidak mengamati akun, klaster, namespace, atau nama pengguna ini dengan cara ini. Informasi yang dilacak untuk bagian ini di panel temuan meliputi:
 - **Username** — Pengguna yang memanggil Kubernetes API yang terkait dengan temuan tersebut.
 - **Nama Pengguna yang Ditiru** - Pengguna yang ditiru oleh. `username`
 - **Namespace** — Namespace Kubernetes di dalam klaster Amazon EKS tempat aksi terjadi.
 - **User Agent** — Agen pengguna yang terkait dengan panggilan API Kubernetes. Agen pengguna adalah metode yang digunakan untuk melakukan panggilan seperti `kubectl`.
 - **API** — Kubernetes API yang dipanggil oleh `username` dalam klaster Amazon EKS.
 - **Informasi ASN** — Informasi ASN, seperti Organisasi dan ISP, terkait dengan alamat IP pengguna yang melakukan panggilan ini.
 - **Hari dalam seminggu** — Hari dalam seminggu ketika panggilan API Kubernetes dilakukan.
 - **Izin** — Kata kerja Kubernetes dan sumber daya yang diperiksa untuk mengindikasikan apakah `Kubernetes username` dapat menggunakan API Kubernetes atau tidak.

- Nama Akun Layanan — Akun layanan yang terkait dengan beban kerja Kubernetes yang memberikan identitas pada beban kerja.
- Registry — Registry container yang terkait dengan image container yang di-deploy dalam beban kerja Kubernetes.
- Image - Gambar kontainer, tanpa tag dan intisari terkait, yang digunakan dalam beban kerja Kubernetes.
- Image Prefix Config - Awalan gambar dengan konfigurasi keamanan kontainer dan beban kerja diaktifkan, hostNetwork seperti `privileged` atau, untuk wadah yang menggunakan gambar.
- Nama Subjek — Subjek, seperti `usergroup`, atau `serviceAccountName` yang terikat pada peran referensi dalam `RoleBinding` atau `ClusterRoleBinding`.
- Nama Peran — Nama peran yang terlibat dalam pembuatan atau modifikasi peran atau `roleBinding` API.

Anomali berbasis volume S3

Bagian ini merinci informasi kontekstual untuk anomali berbasis volume S3. Temuan berbasis volume ([Exfiltration:S3/AnomalousBehavior](#)) memantau jumlah panggilan API S3 yang tidak biasa yang dilakukan ke bucket S3 oleh pengguna, menunjukkan potensi eksfiltrasi data. Panggilan API S3 berikut dipantau untuk deteksi anomali berbasis volume.

- `GetObject`
- `CopyObject.Read`
- `SelectObjectContent`

Metrik berikut akan membantu membangun dasar perilaku biasa saat entitas IAM mengakses bucket S3. Untuk mendeteksi eksfiltrasi data, temuan deteksi anomali berbasis volume mengevaluasi semua aktivitas terhadap garis dasar perilaku yang biasa. Pilih Perilaku historis di bagian Perilaku Tidak Biasa (Identitas Pengguna), Volume yang Diamati (Identitas Pengguna), dan Volume Teramati (Bucket) untuk melihat metrik berikut.

- Jumlah panggilan `s3-api-name` API yang dipanggil oleh pengguna IAM atau peran IAM (tergantung pada panggilan mana yang dikeluarkan) terkait dengan bucket S3 yang terpengaruh selama 24 jam terakhir.

- Jumlah panggilan `s3-api-name` API yang dipanggil oleh pengguna IAM atau peran IAM (tergantung pada mana yang dikeluarkan) yang terkait dengan semua bucket S3 selama 24 jam terakhir.
- Jumlah panggilan `s3-api-name` API di semua pengguna IAM atau peran IAM (tergantung pada mana yang dikeluarkan) terkait dengan bucket S3 yang terpengaruh selama 24 jam terakhir.

Anomali berbasis aktivitas login RDS

Bagian ini merinci jumlah upaya login yang dilakukan oleh aktor yang tidak biasa

dan dikelompokkan berdasarkan hasil upaya login. [Jenis temuan Perlindungan](#)

[RDS](#) Mengidentifikasi perilaku anomali dengan memantau peristiwa login untuk pola yang tidak biasa `successfulLoginCount`, `failedLoginCount`, dan `incompleteConnectionCount`

- `successfulLoginCount`— Penghitung ini mewakili jumlah koneksi yang berhasil (kombinasi atribut login yang benar) yang dibuat ke instance database oleh aktor yang tidak biasa. Atribut login termasuk nama pengguna, kata sandi, dan nama database.
- `failedLoginCount`— Penghitung ini mewakili jumlah upaya login gagal (gagal) yang dilakukan untuk membuat koneksi ke instance database. Ini menunjukkan bahwa satu atau lebih atribut dari kombinasi login, seperti nama pengguna, kata sandi, atau nama database tidak benar.
- `incompleteConnectionCount`— Penghitung ini mewakili jumlah upaya koneksi yang tidak dapat diklasifikasikan sebagai berhasil atau gagal. Koneksi ini ditutup sebelum database memberikan respons. Misalnya, pemindaian port di mana port database terhubung tetapi tidak ada informasi yang dikirim ke database, atau koneksi dibatalkan sebelum login selesai dalam upaya yang berhasil atau gagal.

GuardDuty menemukan agregasi

GuardDuty memperbarui temuan yang dihasilkan secara dinamis. Jika GuardDuty mendeteksi aktivitas baru yang terkait dengan masalah keamanan yang sama, maka alih-alih membuat temuan baru, GuardDuty akan memperbarui temuan asli dengan detail terbaru. Perilaku ini memungkinkan Anda untuk mengidentifikasi masalah yang sedang berlangsung, tanpa perlu melihat melalui beberapa laporan serupa, dan mengurangi volume keseluruhan temuan untuk masalah keamanan yang diketahui.

Sebagai contoh, untuk `UnauthorizedAccess:EC2/SSHBruteForce` menemukan, beberapa upaya akses terhadap instance Anda akan digabungkan ke ID temuan yang sama, meningkatkan jumlah

Hitungan dalam detail temuan. Ini karena temuan tersebut mewakili satu masalah keamanan dengan instans yang menunjukkan bahwa port SSH pada instans tidak diamankan dengan benar terhadap tipe aktivitas ini. Namun, jika GuardDuty mendeteksi aktivitas akses SSH yang menargetkan instance baru di lingkungan Anda, itu akan membuat temuan baru dengan ID temuan unik untuk mengingatkan Anda tentang fakta bahwa ada masalah keamanan yang terkait dengan sumber daya baru.

Ketika sebuah temuan dikumpulkan, itu diperbarui dengan informasi dari kejadian terbaru dari aktivitas itu. Ini berarti bahwa dalam contoh di atas, jika instans Anda adalah target upaya brute force dari aktor baru, detail temuan akan diperbarui untuk mencerminkan IP jarak jauh dari sumber terbaru dan informasi lama akan diganti. Informasi lengkap tentang upaya aktivitas individual akan tetap tersedia di CloudTrail log atau Log Aliran VPC Anda.

Kriteria yang mengingatkan GuardDuty untuk menghasilkan temuan baru alih-alih menggabungkan yang sudah ada tergantung pada jenis temuan. Kriteria agregasi untuk setiap jenis temuan ditentukan oleh teknisi keamanan kami untuk memberikan gambaran umum tentang masalah keamanan yang berbeda dalam akun Anda.

Saat GuardDuty menghasilkan jenis pencarian urutan serangan di akun Anda, temuan akan dikumpulkan hanya ketika Anda GuardDuty mengidentifikasi sinyal serupa dalam urutan yang sama di akun Anda. Jika tidak, GuardDuty akan menghasilkan urutan serangan lain.

Mengelola GuardDuty temuan Amazon

GuardDuty menawarkan beberapa fitur penting untuk membantu Anda mengurutkan, menyimpan, dan mengelola temuan Anda. Fitur-fitur ini akan membantu Anda menyesuaikan temuan dengan lingkungan spesifik Anda, mengurangi kebisingan dari temuan bernilai rendah, dan membantu Anda fokus pada ancaman terhadap AWS lingkungan unik Anda. Tinjau topik di halaman ini untuk memahami bagaimana Anda dapat menggunakan fitur ini untuk meningkatkan nilai temuan keamanan di lingkungan Anda.

Topik:

[Dasbor ringkasan di Amazon GuardDuty](#)

Pelajari tentang komponen dasbor ringkasan yang tersedia di GuardDuty konsol.

[Penyaringan temuan di GuardDuty](#)

Pelajari cara memfilter GuardDuty temuan berdasarkan kriteria yang Anda tentukan.

[Aturan penindasan di GuardDuty](#)

Pelajari cara memfilter temuan secara otomatis yang GuardDuty memberi tahu Anda melalui aturan penekanan. Aturan penekanan mengarsipkan temuan secara otomatis berdasarkan filter.

[Bekerja dengan daftar IP tepercaya dan daftar ancaman](#)

Sesuaikan lingkup GuardDuty pemantauan menggunakan Daftar IP dan Daftar Ancaman berdasarkan alamat IP yang dapat dirutekan secara publik. Daftar IP tepercaya mencegah temuan non-DNS dihasilkan dari IP yang Anda anggap tepercaya, sementara Daftar Intel Ancaman akan mengingatkan GuardDuty Anda tentang aktivitas yang ditentukan pengguna. IPs

[Mengekspor temuan yang dihasilkan ke Amazon S3](#)

Ekspor temuan yang dihasilkan ke bucket Amazon S3 sehingga Anda dapat menyimpan catatan melewati periode retensi temuan 90 hari di. GuardDuty Gunakan data historis ini untuk melacak potensi aktivitas mencurigakan di akun Anda dan mengevaluasi apakah langkah-langkah perbaikan yang disarankan berhasil.

Memproses GuardDuty temuan dengan Amazon EventBridge

Siapkan notifikasi otomatis untuk GuardDuty temuan melalui EventBridge acara Amazon. Anda juga dapat mengotomatiskan tugas-tugas lain EventBridge untuk membantu Anda menanggapi temuan.

Memahami CloudWatch Log dan alasan melewati sumber daya selama Perlindungan Malware untuk EC2 pemindaian

Pelajari cara mengaudit CloudWatch Log untuk Perlindungan GuardDuty Malware EC2 dan alasan mengapa EC2 instans Amazon atau volume Amazon EBS Anda yang terkena dampak mungkin telah dilewati selama proses pemindaian.

Melaporkan positif palsu dalam Perlindungan Malware untuk EC2

Pelajari cara melaporkan potensi deteksi ancaman positif palsu di Perlindungan Malware untuk S3.

Melaporkan hasil pemindaian objek S3 sebagai positif palsu dalam Perlindungan Malware untuk S3

Pelajari cara melaporkan potensi deteksi ancaman positif palsu di Perlindungan Malware untuk S3.

Dasbor ringkasan di Amazon GuardDuty

Dasbor GuardDuty Ringkasan memberikan tampilan agregat dari GuardDuty temuan yang dihasilkan Akun AWS di Anda saat ini Wilayah AWS.

Jika Anda menggunakan akun GuardDuty administrator, dasbor menyediakan statistik dan data gabungan untuk akun dan akun anggota di organisasi Anda.

Melihat dasbor Ringkasan

1. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.

GuardDuty menampilkan dasbor Ringkasan secara default saat Anda membuka konsol.

2. Pada halaman Ringkasan, pilih yang diinginkan Wilayah AWS dari pemilih Wilayah di sudut kanan atas konsol.
3. Dari menu pemilih rentang tanggal, pilih rentang tanggal yang ingin Anda lihat ringkasannya. Secara default, dasbor menampilkan data untuk hari ini, Hari ini.

Note

Jika tidak ada temuan yang dihasilkan selama rentang tanggal yang dipilih, dasbor tidak akan memiliki data apa pun untuk ditampilkan. Anda dapat menyegarkan dasbor, atau menyesuaikan rentang tanggal.

Topik

- [Gambaran Umum](#)
- [Temuan](#)
- [Jenis temuan yang paling umum](#)
- [Temuan berdasarkan tingkat keparahan](#)
- [Akun dengan sebagian besar temuan](#)
- [Sumber daya dengan temuan](#)
- [Temuan yang paling tidak terjadi](#)
- [Cakupan rencana perlindungan](#)

Gambaran Umum

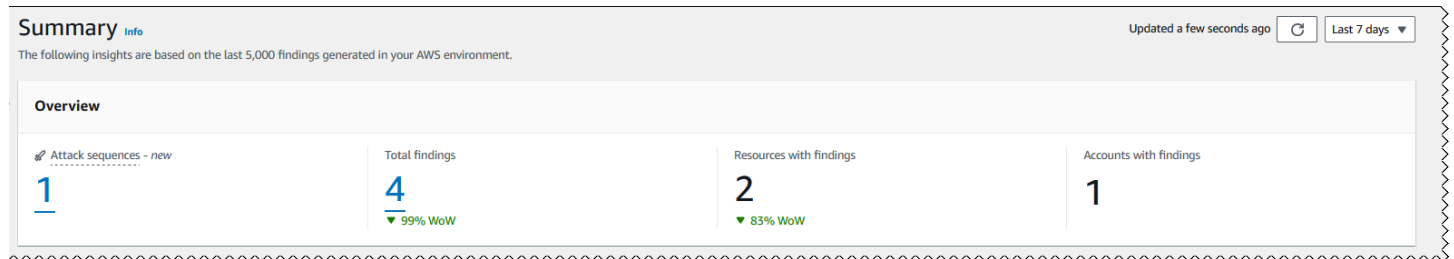
Bagian ini menyediakan data berikut:

- Urutan serangan: Menunjukkan jumlah temuan urutan serangan yang GuardDuty dihasilkan di akun Anda di Wilayah saat ini.

GuardDuty mendeteksi potensi serangan multi-tahap di akun Anda. Anda dapat memilih nomor di bawah Urutan serangan untuk melihat detailnya di halaman Temuan.

- Total temuan: Menunjukkan jumlah total temuan yang dihasilkan di akun Anda di Wilayah saat ini. Ini termasuk temuan individu dan temuan urutan serangan.
- Sumber daya dengan temuan: Menunjukkan jumlah sumber daya yang terkait dengan temuan, dan berpotensi dikompromikan.
- Akun dengan temuan: Menunjukkan jumlah akun di mana setidaknya satu temuan dihasilkan. Jika Anda adalah akun mandiri, nilai di bidang ini adalah 1.

Untuk rentang waktu 7 hari terakhir dan 30 hari terakhir, panel Ikhtisar dapat menunjukkan perbedaan persentase dalam temuan yang dihasilkan minggu ke minggu (WoW) atau bulan ke bulan (MoM), masing-masing. Jika tidak ada temuan yang dihasilkan pada minggu atau bulan sebelumnya, maka tanpa data untuk membandingkan, perbedaan persentase mungkin tidak tersedia.



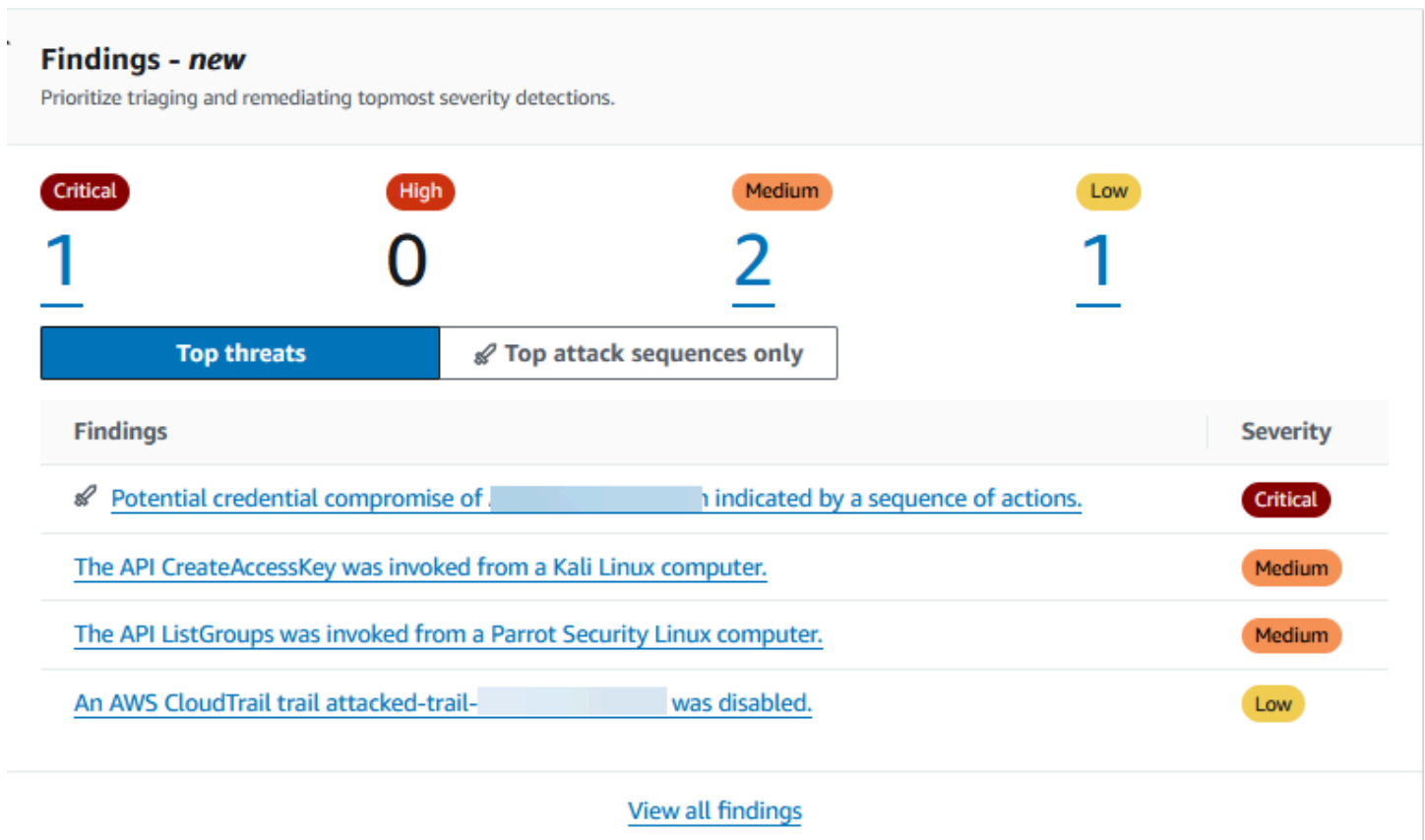
Jika Anda adalah akun GuardDuty administrator, semua bidang ini menyediakan data yang diringkas di semua akun anggota di organisasi Anda.

Temuan

Widget Temuan menampilkan hingga delapan temuan teratas. Temuan ini terdaftar berdasarkan tingkat keparahannya, dengan temuan kritis ditampilkan terlebih dahulu.

Secara default, Anda dapat melihat semua temuan. Untuk hanya melihat data temuan urutan serangan, aktifkan urutan serangan Top saja.

Dalam daftar ini, Anda dapat memilih temuan apa pun untuk melihat detailnya.



Jenis temuan yang paling umum

Bagian ini menyediakan diagram lingkaran yang menggambarkan lima jenis temuan paling umum yang dihasilkan di Wilayah saat ini. Saat mengarahkan kursor ke setiap sektor diagram lingkaran, Anda dapat mengamati hal-hal berikut:

- Jumlah temuan: Menunjukkan berapa kali temuan ini dihasilkan dalam rentang tanggal yang dipilih.
- Keparahan: Menunjukkan tingkat keparahan temuan.
- Persentase: Menunjukkan proporsi jenis temuan ini relatif terhadap total.
- Terakhir dihasilkan: Menunjukkan berapa banyak waktu yang telah berlalu sejak jenis temuan ini terakhir terdeteksi.

Temuan berdasarkan tingkat keparahan

Bagian ini menampilkan diagram batang yang menunjukkan jumlah total temuan selama rentang tanggal yang dipilih. Bagan memecah temuan berdasarkan tingkat keparahan (Kritis, Tinggi, Sedang,

dan Rendah), dan membantu Anda melihat jumlah temuan untuk tanggal tertentu dalam kisaran tersebut.

Untuk melihat hitungan untuk setiap tingkat keparahan pada tanggal tertentu, arahkan kursor ke bilah yang sesuai di bagan.

Akun dengan sebagian besar temuan

Bagian ini menyediakan data berikut:

- **Akun:** Menunjukkan Akun AWS ID tempat temuan dibuat.
- **Hitungan temuan:** Menunjukkan berapa kali temuan dibuat untuk ID akun ini.
- **Terakhir dihasilkan:** Menunjukkan berapa banyak waktu yang telah berlalu sejak jenis temuan terakhir dibuat untuk ID akun ini.
- **Filter keparahan:** Secara default, data ditampilkan untuk jenis temuan tingkat keparahan tinggi. Opsi yang memungkinkan untuk bidang ini adalah Semua tingkat keparahan, Tingkat keparahan kritis, Tingkat keparahan tinggi, dan Tingkat keparahan sedang.

Sumber daya dengan temuan

Bagian ini menyediakan data berikut:

- **Sumber Daya:** Menampilkan jenis sumber daya yang berpotensi terpengaruh dan jika sumber daya ini milik akun Anda, Anda dapat mengakses tautan cepat untuk melihat detail sumber daya. Jika Anda adalah akun GuardDuty administrator, Anda dapat melihat detail sumber daya yang berpotensi terkena dampak dengan mengakses GuardDuty konsol dengan kredensial akun anggota pemilik.
- **Akun:** Menunjukkan Akun AWS ID tempat sumber daya ini berada.
- **Hitungan temuan:** Menunjukkan berapa kali sumber daya ini dikaitkan dengan temuan.
- **Terakhir dihasilkan:** Menunjukkan berapa banyak waktu yang telah berlalu sejak jenis temuan yang terkait dengan sumber daya ini terakhir dihasilkan.
- **Filter tipe sumber daya:** Secara default, data ditampilkan untuk semua jenis sumber daya. Dengan menggunakan filter ini, Anda dapat memilih untuk melihat data untuk jenis sumber daya tertentu, seperti Instance, AccessKey, Lambda, dan lainnya.
- **Filter keparahan:** Secara default, data ditampilkan untuk Semua tingkat keparahan. Dengan menggunakan filter ini, Anda dapat memilih untuk melihat data untuk tingkat keparahan lainnya.

Pilihan yang mungkin adalah Tingkat keparahan kritis, Tingkat keparahan tinggi, tingkat keparahan sedang, dan Semua tingkat keparahan.

Temuan yang paling tidak terjadi

Bagian ini menyoroti menemukan jenis yang jarang terjadi di AWS lingkungan Anda. Widget ini dirancang untuk membantu Anda mengidentifikasi dan menyelidiki potensi pola ancaman yang muncul.

Widget ini menampilkan data berikut:

- Jenis pencarian: Menunjukkan nama tipe temuan.
- Hitungan temuan: Menunjukkan berapa kali jenis temuan ini dihasilkan dalam rentang waktu yang dipilih.
- Terakhir dihasilkan: Menunjukkan berapa banyak waktu yang telah berlalu sejak jenis temuan ini terakhir dihasilkan.
- Filter keparahan: Secara default, data ditampilkan untuk jenis temuan tingkat keparahan tinggi. Opsi yang memungkinkan untuk bidang ini adalah Tingkat keparahan kritis, Tingkat keparahan tinggi, Tingkat keparahan sedang, dan Semua tingkat keparahan.

Cakupan rencana perlindungan

Bagian ini menampilkan statistik untuk akun anggota di organisasi Anda. Ini menunjukkan jumlah akun anggota yang telah diaktifkan GuardDuty (deteksi ancaman dasar) di Wilayah saat ini. Hanya GuardDuty administrator yang didelegasikan yang dapat melihat statistik untuk akun anggota dalam organisasi mereka. Saat Anda membuat AWS organisasi baru, mungkin diperlukan waktu hingga 24 jam untuk menghasilkan statistik untuk seluruh organisasi.

Cara menggunakan widget ini

- Konfigurasi: Jika rencana perlindungan tidak dikonfigurasi, pilih Konfigurasi di bawah kolom Tindakan.
- Melihat akun yang diaktifkan: Arahkan kursor ke bilah di kolom Akun yang diaktifkan untuk melihat berapa banyak akun yang mengaktifkan setiap paket perlindungan. Untuk melihat detail akun lebih lanjut, pilih bilah hijau, dan pilih Lihat akun.

Protection plans coverage		Last updated: 3 hours ago
GuardDuty coverage (foundational) 4/4 accounts		
Protection plan	Enabled accounts	Actions
S3 Protection		Configure
EKS Protection		Configure
Runtime monitoring		Runtime monitoring Enabled accounts 1 Not enabled accounts 3 Configure View accounts
Automated agent management for EKS		
Automated agent configuration for Fargate (ECS only)		
Automated agent management for EC2		Configure
Malware Protection for EC2		Configure
Lambda Protection		Configure
RDS Protection		Configure

Penyaringan temuan di GuardDuty

Filter temuan memungkinkan Anda melihat temuan yang sesuai dengan kriteria yang Anda tentukan dan memfilter temuan yang tidak sesuai. Anda dapat dengan mudah membuat filter pencarian menggunakan GuardDuty konsol Amazon, atau Anda dapat membuatnya dengan [CreateFilterAPI](#) menggunakan JSON. Tinjau bagian berikut untuk memahami cara membuat filter di konsol. Untuk menggunakan filter ini untuk mengarsipkan temuan yang masuk secara otomatis, lihat [Aturan penindasan di GuardDuty](#).

Saat Anda membuat filter, pertimbangkan daftar berikut:

- GuardDuty tidak mendukung kartu liar untuk kriteria filter.
- Anda dapat menentukan minimum satu atribut dan maksimum hingga 50 atribut sebagai kriteria untuk filter tertentu.

- Saat Anda menggunakan operator Sama atau Tidak sama dengan untuk memfilter nilai atribut, seperti ID Akun, Anda dapat menentukan maksimum 50 nilai.
- Setiap atribut kriteria filter dievaluasi sebagai operator AND. Beberapa nilai untuk atribut yang sama dievaluasi sebagai AND/OR.
- Untuk informasi tentang jumlah maksimum filter tersimpan yang dapat Anda buat Akun AWS di masing-masing filter Wilayah AWS, lihat [GuardDuty kuota](#).

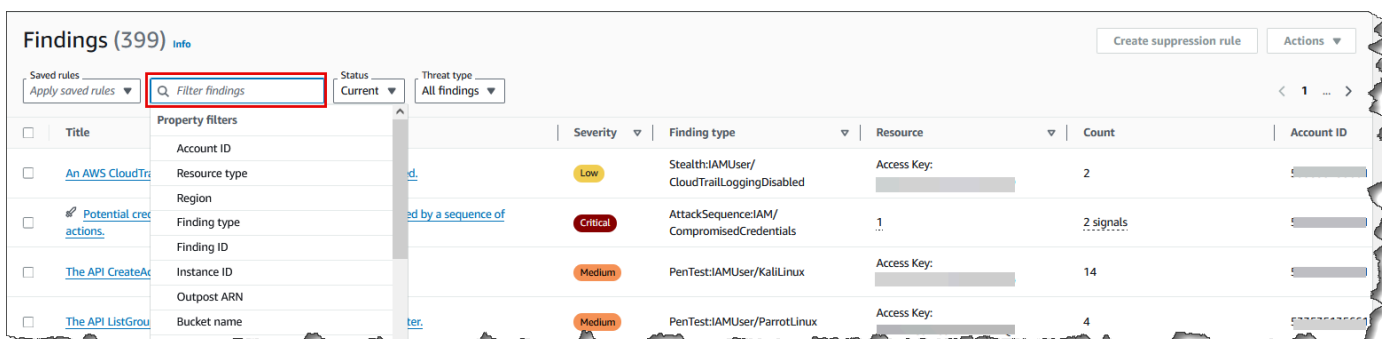
Bagian berikut memberikan petunjuk tentang cara membuat dan menyimpan filter menggunakan GuardDuty konsol, dan perintah API dan CLI. Pilih metode akses pilihan Anda untuk melanjutkan.

Membuat dan menyimpan set filter di GuardDuty konsol

Filter pencarian dapat dibuat dan diuji melalui GuardDuty konsol. Anda dapat menyimpan filter yang dibuat melalui konsol untuk digunakan dalam aturan penekanan atau operasi filter mendatang. Filter terbuat dari setidaknya satu kriteria filter. Terdiri dari satu atribut filter yang dipasangkan dengan setidaknya satu nilai.

Untuk membuat dan menyimpan kriteria filter (konsol)

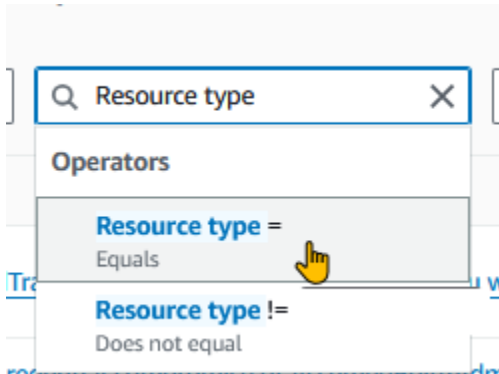
1. Masuk ke AWS Management Console dan buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.
2. Di panel navigasi kiri, pilih Temuan.
3. Pada halaman Temuan, pilih bilah Filter temuan di sebelah menu Aturan tersimpan. Ini akan menampilkan daftar filter Properti yang diperluas.



4. Dari daftar filter yang diperluas, pilih atribut berdasarkan yang ingin Anda filter tabel temuan.

Misalnya, untuk melihat temuan yang sumber daya yang berpotensi terkena dampak adalah S3Bucket, pilih tipe Resource.

- Untuk Operator, pilih salah satu yang akan membantu Anda memfilter temuan untuk mendapatkan hasil yang diinginkan. Untuk melanjutkan contoh dari langkah sebelumnya, pilih Jenis sumber daya =. Ini akan menampilkan daftar jenis sumber daya di GuardDuty.



Jika kasus penggunaan Anda mengharuskan mengecualikan temuan spesifik, Anda dapat memilih Tidak sama atau != operator.

- Tentukan nilai untuk filter properti yang dipilih. Jika perlu, pilih Terapkan. Untuk melanjutkan contoh dari langkah sebelumnya, Anda dapat memilih S3Bucket.

Ini akan menampilkan temuan yang cocok dengan filter yang diterapkan.

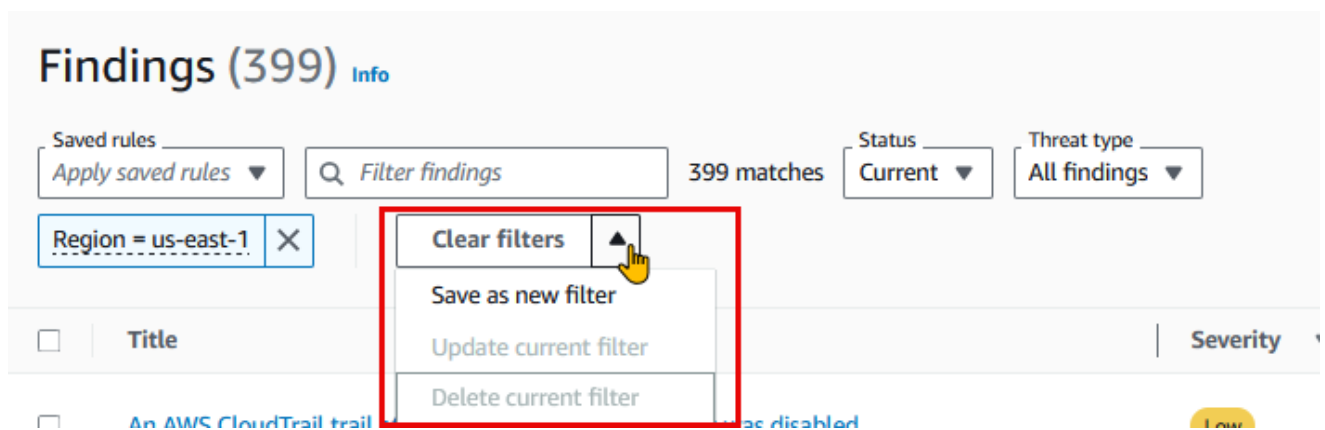
- Untuk menambahkan lebih dari satu kriteria filter, ulangi langkah 3-6.

Untuk daftar lengkap atribut, lihat [Filter properti di GuardDuty](#).

- (Opsional) simpan atribut dan nilai yang ditentukan sebagai filter

Untuk menerapkan kombinasi filter ini lagi di masa mendatang, Anda dapat menyimpan atribut yang ditentukan dan nilainya sebagai set filter.

- Setelah Anda membuat kriteria filter dengan satu atau beberapa filter properti, pilih panah di menu Hapus filter.



- b. Masukkan nama set filter. Nama harus 3-64 karakter. Karakter yang valid adalah a-z, A-Z, 0-9, periode (.), tanda hubung (-), dan garis bawah (_).
- c. Deskripsi adalah opsional. Jika Anda memasukkan deskripsi, itu dapat memiliki hingga 512 karakter.
- d. Pilih Buat.

Membuat dan menyimpan set filter dengan menggunakan GuardDuty API dan CLI

Anda dapat membuat dan menguji filter temuan dengan menggunakan perintah API atau CLI. Filter terbuat dari setidaknya satu kriteria filter. Terdiri dari satu atribut filter yang dipasangkan dengan setidaknya satu nilai. Anda dapat menyimpan filter untuk membuat [Aturan penekanan](#) atau melakukan operasi filter lainnya nanti.

Untuk membuat filter pencarian menggunakan API/CLI

- Jalankan [CreateFilter](#) API dengan menggunakan ID detektor regional Akun AWS tempat Anda ingin membuat filter.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan `detectorId` [ListDetectors](#) API.

- Atau, Anda dapat menggunakan CLI [create-filter](#) untuk membuat dan menyimpan filter. Anda dapat menggunakan satu atau beberapa kriteria filter dari [Filter properti di GuardDuty](#).

Gunakan contoh berikut dengan mengganti nilai placeholder yang ditunjukkan dengan warna merah.

Contoh 1: Buat filter baru untuk melihat semua temuan yang cocok dengan jenis temuan tertentu

Contoh berikut membuat filter yang cocok dengan semua PortScan temuan untuk instance yang dibuat dari gambar tertentu. Nilai placeholder ditampilkan dalam warna merah. Ganti nilai-nilai ini dengan nilai yang sesuai untuk akun Anda. Misalnya, ganti **12abc34d567e8fa901bc2d34EXAMPLE** dengan ID detektor regional Anda.

```
aws guardduty create-filter \  
--detector-id 12abc34d567e8fa901bc2d34EXAMPLE \  
--name FilterExampleName \  

```



```
--finding-criteria '{"Criterion": {"type": {"Equals": ["Recon:EC2/Portscan"]},
"resource.instanceDetails.imageId": {"Equals":["ami-0a7a207083example"]}} }'
```

Contoh 2: Buat filter baru untuk melihat semua temuan yang cocok dengan tingkat keparahan

Contoh berikut membuat filter yang cocok dengan semua temuan yang terkait dengan HIGH tingkat keparahan. Nilai placeholder ditampilkan dalam warna merah. Ganti nilai-nilai ini dengan nilai yang sesuai untuk akun Anda. Misalnya, ganti **12abc34d567e8fa901bc2d34EXAMPLE** dengan ID detektor regional Anda.

```
aws guardduty create-filter \
--detector-id 12abc34d567e8fa901bc2d34EXAMPLE \
--name FilterExampleName \
--finding-criteria '{"Criterion": {"severity": {"Equals": ["7", "8"]}} }'
```

- Untuk API/CLI, [Temuan tingkat keparahan](#) direpresentasikan sebagai angka. Untuk menyaring temuan berdasarkan tingkat keparahan, gunakan nilai berikut:
 - Untuk LOW tingkat keparahan, gunakan { "severity": { "Equals": ["1", "2", "3"] } }
 - Untuk MEDIUM tingkat keparahan, gunakan { "severity": { "Equals": ["4", "5", "6"] } }
 - Untuk HIGH tingkat keparahan, gunakan { "severity": { "Equals": ["7", "8"] } }
 - Untuk CRITICAL tingkat keparahan, gunakan { "severity": { "Equals": ["9", "10"] } }
 - Untuk temuan dengan beberapa tingkat keparahan, gunakan nilai placeholder yang mirip dengan contoh berikut: { "severity": { "Equals": ["7", "8", "9", "10"] } }

Contoh ini akan menunjukkan temuan yang memiliki CRITICAL tingkat keparahan HIGH atau tingkat keparahan.

Note

Jika Anda menentukan contoh dengan hanya satu nilai numerik, bukan semua nilai numerik yang terkait dengan tingkat keparahan, API dan CLI mungkin menampilkan temuan yang difilter. Saat Anda menggunakan set filter tersimpan ini di GuardDuty konsol, itu tidak akan berfungsi seperti yang diharapkan. Ini karena GuardDuty konsol menganggap nilai filter sebagai CRITICAL, HIGHMEDIUM, dan LOW. Misalnya, filter yang dibuat dengan perintah CLI yang menyertakan { "severity": { "Equals":

`["9"] }` } diharapkan menampilkan output yang sesuai di API/CLI. Namun, filter yang disimpan ini mencakup tingkat keparahan sebagian saat digunakan di GuardDuty konsol dan tidak akan menampilkan output yang diharapkan. Hal ini membuat API dan CLI perlu menentukan semua nilai yang terkait dengan setiap tingkat keparahan.

Filter properti di GuardDuty

Apabila Anda membuat filter atau mengurutkan temuan menggunakan operasi API, Anda harus menentukan kriteria filter di JSON. Kriteria filter ini berkorelasi dengan detail JSON temuan. Tabel berikut berisi daftar nama tampilan konsol untuk atribut filter dan nama bidang JSON setaranya.

Nama bidang konsol	Nama bidang JSON
account-id	accountId
ID Temuan	id
Wilayah	region
Kepelikan	kepelikan Anda dapat memfilter jenis temuan berdasarkan tingkat keparahan jenis temuan. Untuk informasi lebih lanjut tentang nilai keparahan, lihat Tingkat keparahan GuardDuty temuan . Jika Anda menggunakan severity dengan API, AWS CLI, atau AWS CloudFormation, itu diberi nilai numerik. Untuk informasi selengkapnya, lihat FindingCriteria di Referensi Amazon GuardDuty API.
Tipe temuan	jenis
Diperbarui pada	updatedAt
Access key ID	sumber daya. accessKeyDetails. accessKeyId
ID utama	sumber daya. accessKeyDetails.Prinsipalid

Nama bidang konsol	Nama bidang JSON
nama pengguna	sumber daya. accessKeyDetails.Nama pengguna
Jenis pengguna	sumber daya. accessKeyDetails.UserType
ID profil instans IAM	Resource.instanceDetails. iamInstanceProfile.id
ID Instans	resource.instanceDetails.instanceId
ID citra instans	resource.instanceDetails.imageId
Kunci tag contoh	resource.instanceDetails.tags.key
Nilai tag instance	resource.instanceDetails.tags.value
IPv6 alamat	resource.instanceDetails.networkInterfaces.ip v6Addresses
IPv4 Alamat pribadi	Resource.instanceDetails.NetworkInterfaces. privateIpAddresses. privateIpAddress
Nama DNS publik	Resource.instanceDetails.NetworkInterfaces. publicDnsName
IP Publik	resource.instanceDetails.networkInterfaces.pu blicIp
ID grup keamanan	resource.instanceDetails.networkInterfaces.se curityGroups.groupId
Nama grup keamanan	resource.instanceDetails.networkInterfaces.se curityGroups.groupName
ID Subnet	resource.instanceDetails.networkInterfaces.su bnetId
ID VPC	resource.instanceDetails.networkInterfaces.vp cId

Nama bidang konsol	Nama bidang JSON
ARN Outpost	resource.instanceDetails.outpostARN
Jenis sumber daya	resource.resourceType
Izin bucket	resource.s3 BucketDetails .publicaccess.effectivePermission
Nama Bucket	sumber BucketDetails daya.s3 .nama
Kunci tanda bucket	BucketDetailsresource.s3 .tags.key
Nilai tanda bucket	BucketDetailsresource.s3 .tags.value
Tipe bucket	sumber BucketDetails daya.s3 .type
Tipe tindakan	service.action.actionType
Panggilan API	service.action. awsApiCallAction.API
Tipe pemanggil API	service.action. awsApiCallAction.callerType
Kode Kesalahan API	service.action. awsApiCallAction.ErrorCode
Kota pemanggil API	service.action. awsApiCallTindakan. remoteIpDetails.city.cityname
Negara pemanggil API	service.action. awsApiCallTindakan. remoteIpDetails.country.countryName
Alamat pemanggil IPv4 API	service.action. awsApiCallTindakan. remoteIpDetails.iPAddressV4
Alamat pemanggil IPv6 API	service.action. awsApiCallTindakan. remoteIpDetails.iPAddressV6
ID ASN pemanggil API	service.action. awsApiCallTindakan. remoteIpDetails.organisasi.asn

Nama bidang konsol	Nama bidang JSON
Nama ASN pemanggil API	service.action. awsApiCallTindakan. remotelpD etails.organisasi.asNorg
Nama layanan pemanggil API	service.action. awsApiCallAction.ServiceName
Domain permintaan DNS	service.action. dnsRequestAction.domain
Akhiran domain permintaan DNS	service.action. dnsRequestAction. domainWit hSuffix
Koneksi jaringan diblokir	service.action. networkConnectionAction.dib lokir
Arah koneksi jaringan	service.action. networkConnectionAction.con nectionDirection
Port lokal koneksi jaringan	service.action. networkConnectionAction. localPortDetails.pelabuhan
Protokol koneksi jaringan	service.action. networkConnectionAction.pro tokol
Kota koneksi jaringan	service.action. networkConnectionAction. remotelpDetails.city.cityname
Negara koneksi jaringan	service.action. networkConnectionAction. remotelpDetails.country.countryName
IPv4 Alamat jarak jauh koneksi jaringan	service.action. networkConnectionAction. remotelpDetails.iPaddressV4
IPv6 Alamat jarak jauh koneksi jaringan	service.action. networkConnectionAction. remotelpDetails.iPaddressV6
ID ASN IP jarak jauh koneksi jaringan	service.action. networkConnectionAction. remotelpDetails.organisasi.asn

Nama bidang konsol	Nama bidang JSON
Nama ASN IP jarak jauh koneksi jaringan	service.action. networkConnectionAction. remotelpDetails.organisasi.asNorg
Port jarak jauh koneksi jaringan	service.action. networkConnectionAction. remotePortDetails.pelabuhan
Akun jarak jauh berafiliasi	service.action. awsApiCallTindakan. remoteAccountDetails.berafiliasi
Alamat penelepon API Kubernetes IPv4	service.action. kubernetesApiCallTindakan. remotelpDetails.iPaddressV4
Alamat penelepon API Kubernetes IPv6	service.action. kubernetesApiCallTindakan. remotelpDetails.iPaddressV6
Namespace Kubernetes	service.action. kubernetesApiCallAction.namespace
ID ASN pemanggil API Kubernetes	service.action. kubernetesApiCallTindakan. remotelpDetails.organisasi.asn
URI permintaan panggilan API Kubernetes	service.action. kubernetesApiCallAction.requesturi
Kode status API Kubernetes	service.action. kubernetesApiCallAction.statusCode
Koneksi jaringan IPv4 alamat lokal	service.action. networkConnectionAction. localIpDetails.iPaddressV4
Koneksi jaringan IPv6 alamat lokal	service.action. networkConnectionAction. localIpDetails.iPaddressV6
Protokol	service.action. networkConnectionAction.protocol
Nama layanan panggilan API	service.action. awsApiCallAction.ServiceName

Nama bidang konsol	Nama bidang JSON
ID akun pemanggil API	service.action. awsApiCallTindakan. remoteAccountDetails.AccountID
Nama daftar ancaman	Service.additionalInfo. threatListName
Peran sumber daya	service.resourceRole
Nama cluster EKS	sumber daya. eksClusterDetails.nama
Nama beban kerja Kubernetes	Resource.kubernetesDetails. kuberneteWorkloadDetails.nama
Namespace beban kerja Kubernetes	Resource.kubernetesDetails. kuberneteWorkloadDetails.namespace
Nama pengguna Kubernetes	Resource.kubernetesDetails. kuberneteUserDetails.nama pengguna
Gambar kontainer Kubernetes	Resource.kubernetesDetails. kuberneteWorkloadDetails.containers.image
Awalan gambar kontainer Kubernetes	Resource.kubernetesDetails. kuberneteWorkloadDetails.containers.imagePrefix
Pindai ID	layanan. ebsVolumeScandetail.scanID
Nama ancaman pemindaian volume EBS	layanan. ebsVolumeScandetail.Skandeteksi.threatDetectedByName.ThreatNames.Name
Nama ancaman pemindaian objek S3	layanan. malwareScanDetails.ancaman. Nama
Tingkat keparahan ancaman	layanan. ebsVolumeScandetail.Skandeteksi.threatDetectedByName.ThreatNames.Keparahan
Berkas SHA	layanan. ebsVolumeScandetail.Skandeteksi.threatDetectedByName.ThreatNames.filepaths.hash

Nama bidang konsol	Nama bidang JSON
Nama cluster ECS	sumber daya. ecsClusterDetails.nama
Gambar kontainer ECS	sumber daya. ecsClusterDetails.taskdetails.containers.image
Definisi tugas ECS ARN	sumber daya. ecsClusterDetails.taskdetails.definitionARN
Gambar wadah mandiri	Resource.containerdetails.image
Id Instans Database	sumber daya. rdsDbInstanceDetail. dbInstanceIdentifier
Id Kluster Basis Data	sumber daya. rdsDbInstanceDetail. dbClusterIdentifier
Mesin basis data	sumber daya. rdsDbInstanceDetail.Engine
Pengguna basis data	sumber daya. rdsDbUserDetail.pengguna
Kunci tag instance database	sumber daya. rdsDbInstancedetails.tags.key
Nilai tag instance database	sumber daya. rdsDbInstancedetails.tags.value
SHA-256 yang dapat dieksekusi	Service.RuntimeDetails.Process.ExecutableSha256
Nama proses	Service.runtimedetails.process.name
Jalur yang dapat dieksekusi	Service.runtimedetails.process.executablePath
Nama fungsi Lambda	Resource.lambdaDetails.FunctionName
Fungsi Lambda ARN	Sumber daya.lambdaDetails.FunctionARN
Tombol tag fungsi Lambda	Sumber daya.lambdadetails.tags.key
Nilai tag fungsi Lambda	Resource.lambdadetails.tags.value

Nama bidang konsol	Nama bidang JSON
Domain permintaan DNS	service.action. dnsRequestAction. domainWithSuffix

Aturan penindasan di GuardDuty

Aturan penekanan adalah satu set kriteria, yang terdiri dari atribut filter yang dipasangkan dengan sebuah nilai, digunakan untuk memfilter temuan dengan secara otomatis mengarsipkan temuan baru yang sesuai dengan kriteria yang ditentukan. Aturan penekanan dapat digunakan untuk memfilter temuan bernilai rendah, temuan positif palsu, atau ancaman yang tidak ingin Anda tindaklanjuti, agar lebih mudah mengenali ancaman keamanan dengan dampak paling besar terhadap lingkungan Anda.

Setelah membuat aturan penekanan, temuan baru yang sesuai dengan kriteria yang ditentukan dalam aturan akan diarsipkan secara otomatis selama aturan penekanan berlaku. Anda dapat menggunakan filter yang ada untuk membuat aturan penekanan atau membuat aturan penekanan dari filter baru yang Anda tentukan. Anda dapat mengonfigurasi aturan penekanan untuk menekan seluruh tipe temuan, atau menentukan kriteria filter yang lebih terperinci guna menekan instans spesifik dari tipe temuan tertentu. Anda dapat mengedit aturan penindasan kapan saja.

Temuan yang ditekan tidak dikirim ke AWS Security Hub, Amazon Simple Storage Service, Amazon Detective, atau EventBridge Amazon, mengurangi tingkat kebisingan jika Anda GuardDuty mengkonsumsi temuan melalui Security Hub, SIEM pihak ketiga, atau aplikasi peringatan dan tiket lainnya. Jika Anda telah mengaktifkan [Perlindungan Malware untuk EC2](#), GuardDuty temuan yang ditekan tidak akan memulai pemindaian malware.

GuardDuty terus menghasilkan temuan bahkan ketika mereka cocok dengan aturan penekanan Anda, namun, temuan tersebut secara otomatis ditandai sebagai diarsipkan. Temuan yang diarsipkan disimpan GuardDuty selama 90 hari dan dapat dilihat kapan saja selama periode tersebut. Anda dapat melihat temuan yang ditekan di GuardDuty konsol dengan memilih Diarsipkan dari tabel temuan, atau melalui GuardDuty API menggunakan [ListFindings](#) API dengan `findingCriteria` kriteria sama dengan `true`. `service.archived`

 Note

Dalam lingkungan multi-akun, hanya GuardDuty administrator yang dapat membuat aturan penindasan.

Menggunakan aturan penekanan dengan Extended Threat Detection

GuardDuty Extended Threat Detection secara otomatis mendeteksi serangan multi-tahap yang menjangkau sumber data, berbagai jenis AWS sumber daya, dan waktu, dalam file. Akun AWS Ini menghubungkan peristiwa di berbagai sumber data untuk mengidentifikasi skenario yang menampilkan diri sebagai ancaman potensial terhadap AWS lingkungan Anda, dan kemudian menghasilkan temuan urutan serangan. Untuk informasi selengkapnya, lihat [Cara kerja Extended Threat Detection](#).

Saat Anda membuat aturan penekanan yang mengarsipkan temuan, Extended Threat Detection tidak dapat menggunakan temuan yang diarsipkan ini saat menghubungkan peristiwa untuk urutan serangan. Aturan penekanan yang luas dapat memengaruhi kemampuan GuardDuty untuk mendeteksi perilaku yang selaras dengan mendeteksi serangan multi-tahap. Temuan yang diarsipkan karena aturan penekanan tidak dianggap sebagai sinyal untuk urutan serangan. Misalnya, jika Anda membuat aturan penindasan yang mengarsipkan semua temuan terkait kluster EKS alih-alih menargetkan aktivitas tertentu yang diketahui, tidak GuardDuty akan dapat menggunakan temuan tersebut untuk mendeteksi urutan serangan di mana aktor ancaman mengeksplotasi wadah, memperoleh token istimewa, dan mengakses sumber daya yang sensitif.

Pertimbangkan rekomendasi berikut dari GuardDuty:

- Lanjutkan menggunakan aturan penindasan untuk mengurangi peringatan dari aktivitas tepercaya yang diketahui.
- Jaga agar aturan penindasan tetap fokus pada perilaku tertentu yang tidak GuardDuty ingin Anda hasilkan temuannya.

Kasus penggunaan umum untuk aturan penekanan dan contoh

Jenis temuan berikut memiliki kasus penggunaan umum untuk menerapkan aturan penekanan. Pilih nama temuan untuk mempelajari lebih lanjut tentang temuan itu. Tinjau deskripsi kasus penggunaan untuk memutuskan apakah Anda ingin membuat aturan penekanan untuk tipe temuan tersebut.

⚠ Important

GuardDuty merekomendasikan agar Anda membangun aturan penekanan secara reaktif dan hanya untuk temuan yang telah berulang kali Anda identifikasi positif palsu di lingkungan Anda.

- [UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS](#)— Gunakan aturan penekanan untuk mengarsipkan temuan yang dihasilkan secara otomatis saat jaringan VPC dikonfigurasi untuk merutekan lalu lintas internet sedemikian rupa sehingga keluar dari gateway lokal daripada dari Gateway Internet VPC.

Temuan ini dibuat saat jaringan dikonfigurasi untuk merutekan lalu lintas internet sedemikian rupa sehingga keluar dari gateway on-premise, bukan dari Gateway Internet VPC (IGW). Konfigurasi umum, seperti penggunaan [AWS Outposts](#), atau koneksi VPN VPC, dapat mengakibatkan lalu lintas dirutekan dengan cara ini. Jika ini adalah perilaku yang diharapkan, Anda disarankan untuk menggunakan aturan penekanan dan membuat aturan yang terdiri dari dua kriteria filter. Kriteria pertama adalah tipe temuan, yaitu `UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS`. Kriteria filter kedua adalah IPv4 alamat pemanggil API dengan alamat IP atau rentang CIDR dari gateway internet lokal Anda. Contoh di bawah ini merupakan filter yang akan Anda gunakan untuk menekan tipe temuan ini berdasarkan alamat IP pemanggil API.

Finding type: `UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS`
API caller IPv4 address: `198.51.100.6`

ℹ Note

Untuk menyertakan beberapa pemanggil API, IPs Anda dapat menambahkan filter IPv4 alamat API Caller baru untuk masing-masing.

- [Recon:EC2/Portscan](#) – Gunakan aturan penekanan untuk mengarsipkan temuan secara otomatis saat menggunakan aplikasi penilaian kerentanan.

Aturan penekanan harus terdiri dari dua kriteria filter. Kriteria pertama harus menggunakan atribut Tipe temuan dengan nilai `Recon:EC2/Portscan`. Kriteria filter kedua harus sesuai dengan instans yang menghosting alat penilaian kerentanan ini. Anda dapat menggunakan atribut ID citra instans atau atribut nilai Tanda, tergantung kriteria yang diidentifikasi dengan instans yang meng-

host alat ini. Contoh di bawah ini merupakan filter yang akan Anda gunakan untuk menekan tipe temuan ini berdasarkan instans dengan AMI tertentu.

Finding type: *Recon:EC2/Portscan* Instance image ID: *ami-999999999*

- [UnauthorizedAccess:EC2/SSHBruteForce](#) – Gunakan aturan penekanan untuk mengarsipkan temuan secara otomatis ketika ditargetkan ke instans bastion.

Jika target upaya brute force adalah host benteng, ini mungkin mewakili perilaku yang diharapkan untuk lingkungan Anda AWS . Jika demikian, kami menyarankan Anda untuk membuat aturan penekanan untuk temuan ini. Aturan penekanan harus terdiri dari dua kriteria filter. Kriteria pertama harus menggunakan atribut Tipe temuan dengan nilai `UnauthorizedAccess:EC2/SSHBruteForce`. Kriteria filter kedua harus sesuai dengan instans yang berfungsi sebagai host bastion. Anda dapat menggunakan atribut ID citra instans atau atribut nilai Tanda, tergantung kriteria yang diidentifikasi dengan instans yang meng-host alat ini. Contoh di bawah ini merupakan filter yang akan Anda gunakan untuk menekan tipe temuan ini berdasarkan instans dengan nilai tanda instans tertentu.

Finding type: *UnauthorizedAccess:EC2/SSHBruteForce* Instance tag value: *devops*

- [Recon:EC2/PortProbeUnprotectedPort](#) – Gunakan aturan penekanan untuk mengarsipkan temuan secara otomatis ketika ditargetkan ke instans yang sengaja diekspos.

Mungkin ada kasus di mana instans sengaja diekspos, misalnya jika instans meng-host server web. Jika ini terjadi di AWS lingkungan Anda, kami sarankan Anda membuat aturan penindasan untuk temuan ini. Aturan penekanan harus terdiri dari dua kriteria filter. Kriteria pertama harus menggunakan atribut Tipe temuan dengan nilai `Recon:EC2/PortProbeUnprotectedPort`. Kriteria filter kedua harus sesuai dengan instans yang berfungsi sebagai host bastion. Anda dapat menggunakan atribut ID citra instans atau atribut nilai Tanda, tergantung kriteria yang dapat diidentifikasi dengan instans yang meng-host alat ini. Contoh di bawah ini merupakan filter yang akan Anda gunakan untuk menekan tipe temuan ini berdasarkan instans dengan kunci tanda instans tertentu di konsol.

Finding type: *Recon:EC2/PortProbeUnprotectedPort* Instance tag key: *prod*

Aturan penekanan yang direkomendasikan untuk temuan Runtime Monitoring

- [PrivilegeEscalation:Runtime/DockerSocketAccessed](#) dihasilkan ketika proses di dalam wadah berkomunikasi dengan soket Docker. Mungkin ada wadah di lingkungan Anda yang mungkin perlu mengakses soket Docker untuk alasan yang sah. Akses dari wadah tersebut akan menghasilkan PrivilegeEscalation:Runtime/DockerSocketAccessed temuan. Jika ini adalah kasus di AWS lingkungan Anda, kami sarankan Anda menyiapkan aturan penekanan untuk jenis temuan ini. Kriteria pertama harus menggunakan bidang Jenis Finding dengan nilai sama dengan PrivilegeEscalation:Runtime/DockerSocketAccessed. Kriteria filter kedua adalah bidang jalur yang dapat dieksekusi dengan nilai yang sama dengan proses executablePath dalam temuan yang dihasilkan. Atau, kriteria filter kedua dapat menggunakan bidang Executable SHA-256 dengan nilai yang sama dengan proses executableSha256 dalam temuan yang dihasilkan.
- Cluster Kubernetes menjalankan server DNS mereka sendiri sebagai pod, seperti. coredns Oleh karena itu, untuk setiap pencarian DNS dari sebuah pod, GuardDuty menangkap dua peristiwa DNS — satu dari pod dan yang lainnya dari pod server. Ini dapat menghasilkan duplikat untuk temuan DNS berikut:
 - [Backdoor:Runtime/C&CAActivity.B!DNS](#)
 - [CryptoCurrency:Runtime/BitcoinTool.B!DNS](#)
 - [Impact:Runtime/AbusedDomainRequest.Reputation](#)
 - [Impact:Runtime/BitcoinDomainRequest.Reputation](#)
 - [Impact:Runtime/MaliciousDomainRequest.Reputation](#)
 - [Impact:Runtime/SuspiciousDomainRequest.Reputation](#)
 - [Trojan:Runtime/BlackholeTraffic!DNS](#)
 - [Trojan:Runtime/DGADomainRequest.C!DNS](#)
 - [Trojan:Runtime/DriveBySourceTraffic!DNS](#)
 - [Trojan:Runtime/DropPoint!DNS](#)
 - [Trojan:Runtime/PhishingDomainRequest!DNS](#)

Temuan duplikat akan mencakup pod, container, dan detail proses yang sesuai dengan pod server DNS Anda. Anda dapat membuat aturan penindasan untuk menekan temuan duplikat ini menggunakan bidang ini. Kriteria filter pertama harus menggunakan bidang jenis Finding dengan nilai sama dengan tipe temuan DNS dari daftar temuan yang disediakan sebelumnya di bagian ini. Kriteria filter kedua dapat berupa jalur Executable dengan nilai yang sama dengan server DNS Anda executablePath atau Executable SHA-256 dengan nilai yang sama dengan server DNS

Anda dalam temuan yang dihasilkan. `executableSHA256` Sebagai kriteria filter ketiga opsional, Anda dapat menggunakan kolom image kontainer Kubernetes dengan nilai yang sama dengan image kontainer pod server DNS Anda dalam temuan yang dihasilkan.

Membuat aturan penindasan di GuardDuty

Aturan penekanan adalah seperangkat kriteria yang mencakup penggunaan atribut filter dan memberikan nilai yang Anda tidak GuardDuty ingin menghasilkan jenis temuan. Jenis temuan yang cocok dengan kriteria ini diarsipkan secara otomatis. Untuk mengurangi kebisingan, temuan yang ditekan tidak dikirim ke salah satu Layanan AWS yang dapat Anda integrasikan. Untuk informasi selengkapnya tentang kasus penggunaan umum untuk membuat aturan penekanan, lihat [Aturan penekanan](#).

Anda dapat memvisualisasikan, membuat, dan mengelola aturan penekanan dengan menggunakan konsol. GuardDuty Aturan penekanan dibuat dengan cara yang sama seperti filter, dan filter tersimpan yang ada dapat digunakan sebagai aturan penekanan. Untuk informasi selengkapnya tentang membuat filter, lihat [Penyaringan temuan di GuardDuty](#).

Pilih metode akses pilihan Anda untuk membuat aturan penindasan untuk GuardDuty menemukan tipe.

Console

Untuk membuat aturan penindasan menggunakan konsol:

1. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.
2. Pada halaman Temuan, fitur Create suppression rule tetap berwarna abu-abu kecuali Anda menambahkan setidaknya satu kriteria filter. Karena aturan penekanan diterapkan pada temuan aktif yang sedang berlangsung, pastikan bahwa menu Status diatur ke Current.
3. Untuk menambahkan satu atau beberapa kriteria filter, ikuti langkah 3 hingga 7 [Adding filters on Findings page](#) inci, lalu lanjutkan dengan langkah-langkah berikut.
4. Setelah Anda menambahkan kriteria filter dan mengonfirmasi bahwa temuan yang difilter memenuhi persyaratan Anda, pilih Buat aturan penekanan.
5. Masukkan Nama untuk aturan penindasan. Nama harus 3-64 karakter. Karakter yang valid adalah a-z, A-Z, 0-9, periode (.), tanda hubung (-), dan garis bawah (_).
6. Deskripsi adalah opsional. Jika Anda memasukkan deskripsi, itu dapat memiliki hingga 512 karakter.

7. Pilih Buat.

Anda juga dapat membuat aturan penekanan dari filter tersimpan yang ada. Untuk informasi selengkapnya tentang membuat filter, lihat [Penyaringan temuan di GuardDuty](#).

Untuk membuat aturan penekanan dari filter tersimpan:

1. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.
2. Pada halaman Temuan, dari menu Aturan tersimpan, pilih aturan set filter tersimpan. Ini akan secara otomatis menampilkan set filter dan temuan yang sesuai dengan kriteria.
3. Anda juga dapat menambahkan lebih banyak kriteria filter ke aturan yang disimpan ini. Jika Anda tidak memerlukan kriteria filter tambahan, lewati langkah ini.

Untuk menambahkan satu atau lebih kriteria filter tambahan, ikuti langkah 2 hingga akhir prosedur sebelumnya -. [To create a suppression rule using the console](#)

4. Jika Anda tidak perlu menambahkan kriteria filter tambahan ke aturan yang disimpan, ikuti langkah 4 hingga akhir prosedur sebelumnya -. [To create a suppression rule using the console](#)

API/CLI

Untuk membuat aturan penekanan menggunakan API:

1. Anda dapat membuat aturan penekanan melalui [CreateFilter](#) API. Untuk melakukannya, tentukan kriteria filter dalam file JSON mengikuti format contoh terperinci di bawah ini. Contoh di bawah ini akan menekan temuan tingkat keparahan rendah yang tidak diarsipkan yang memiliki permintaan DNS ke domain. `test.example.com` Untuk temuan tingkat keparahan sedang, daftar masukan adalah `["4", "5", "7"]`. Untuk temuan tingkat keparahan tinggi, daftar masukan akan `["6", "7", "8"]`. Untuk temuan tingkat keparahan kritis, daftar masukan adalah `["9", "10"]`. Anda juga dapat memfilter berdasarkan satu nilai dalam daftar.

Contoh berikut menambahkan filter untuk temuan tingkat keparahan rendah.

```
{
  "Criterion": {
    "service.archived": {
      "Eq": [
```

```

        "false"
      ]
    },
    "service.action.dnsRequestAction.domain": {
      "Eq": [
        "test.example.com"
      ]
    },
    "severity": {
      "Eq": [
        "1",
        "2",
        "3"
      ]
    }
  }
}

```

Untuk daftar nama bidang JSON dan konsolnya yang setara, lihat [Filter properti di GuardDuty](#).

Untuk menguji kriteria filter Anda, gunakan kriteria JSON yang sama di [ListFindingsAPI](#), dan konfirmasi bahwa temuan yang benar telah dipilih. Untuk menguji kriteria filter Anda menggunakan AWS CLI ikuti contoh menggunakan detectorId dan file.json Anda sendiri.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan [ListDetectorsAPI](#). detectorId

```
aws guardduty list-findings --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
finding-criteria file://criteria.json
```

2. Unggah filter Anda untuk digunakan sebagai aturan penekanan dengan [CreateFilterAPI](#) atau dengan menggunakan AWS CLI mengikuti contoh di bawah ini dengan ID detektor Anda sendiri, nama untuk aturan penekanan, dan file.json.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan [ListDetectorsAPI](#). detectorId

```
aws guardduty create-filter --action ARCHIVE --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --name yourfiltername --finding-criteria
file://criteria.json
```


Anda dapat melihat daftar filter Anda secara terprogram dengan API. [ListFilter](#) Anda dapat melihat detail filter individual dengan memberikan nama filter ke [GetFilter](#) API. Perbarui filter menggunakan [UpdateFilter](#) atau menghapusnya dengan [DeleteFilter](#) API.

Menghapus aturan penindasan di GuardDuty

Bagian ini menyediakan langkah-langkah untuk menghapus aturan penindasan Akun AWS di Anda secara spesifik Wilayah AWS.

Anda mungkin ingin menghapus aturan penekanan yang tidak lagi menggambarkan perilaku yang diharapkan di lingkungan Anda. Anda tidak lagi ingin menekan jenis temuan terkait sehingga GuardDuty dapat menghasilkan tipe temuan.

Jika Anda adalah akun anggota, akun administrator Anda dapat mengambil tindakan ini atas nama Anda. Untuk informasi selengkapnya, lihat [Akun administrator dan hubungan akun anggota](#).

Pilih metode akses pilihan Anda untuk menghapus aturan penekanan untuk GuardDuty menemukan jenis.

Console

1. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.
2. Pada halaman Temuan, pilih Menekan Temuan untuk membuka panel aturan penekanan.
3. Dari tarik-turun Aturan tersimpan, pilih filter yang disimpan.
4. Pilih Hapus aturan.

API/CLI

Jalankan API [DeleteFilter](#). Tentukan nama filter dan ID detektor terkait untuk Wilayah tertentu.

Atau, Anda dapat menggunakan AWS CLI contoh berikut dengan mengganti nilai yang diformat *red*:

```
aws guardduty delete-filter --region us-east-1 --detector-id 12abc34d567e8fa901bc2d34e56789f0 --filter-name filterName
```

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan [ListDetectors](#) API. `detectorId`

Bekerja dengan daftar IP tepercaya dan daftar ancaman

Amazon GuardDuty memantau keamanan AWS lingkungan Anda dengan menganalisis dan memproses Log Aliran VPC, log AWS CloudTrail peristiwa, dan log DNS. Anda dapat menyesuaikan lingkup pemantauan ini dengan mengonfigurasi GuardDuty untuk menghentikan peringatan untuk dipercaya IPs dari daftar IP tepercaya Anda sendiri dan memperingatkan tentang bahaya yang diketahui IPs dari daftar ancaman Anda sendiri.

Daftar IP tepercaya dan daftar ancaman hanya berlaku untuk lalu lintas yang ditujukan untuk alamat IP yang dapat dirutekan secara publik. Efek dari daftar berlaku untuk semua Log Aliran VPC dan CloudTrail temuan, tetapi tidak berlaku untuk temuan DNS.

GuardDuty dapat dikonfigurasi untuk menggunakan jenis daftar berikut.

Daftar IP tepercaya

Daftar IP tepercaya terdiri dari alamat IP yang telah Anda percayai untuk komunikasi yang aman dengan AWS infrastruktur dan aplikasi Anda. GuardDuty tidak menghasilkan log aliran VPC atau CloudTrail temuan untuk alamat IP pada daftar IP tepercaya. Anda dapat menyertakan maksimum 2.000 alamat IP dan rentang CIDR dalam satu daftar IP tepercaya. Pada waktu tertentu, Anda hanya dapat memiliki satu daftar IP tepercaya yang diunggah per akun AWS per Wilayah.

Daftar IP ancaman

Daftar ancaman terdiri dari alamat IP berbahaya yang diketahui. Daftar ini dapat disediakan oleh intelijen ancaman pihak ketiga atau dibuat khusus untuk organisasi Anda. Selain menghasilkan temuan karena aktivitas yang berpotensi mencurigakan, GuardDuty juga menghasilkan temuan berdasarkan daftar ancaman ini. Anda dapat menyertakan maksimum 250.000 alamat IP dan rentang CIDR dalam satu daftar ancaman. GuardDuty hanya menghasilkan temuan berdasarkan aktivitas yang melibatkan alamat IP dan rentang CIDR dalam daftar ancaman Anda; temuan tidak dihasilkan berdasarkan nama domain. Pada titik waktu tertentu, Anda dapat memiliki hingga enam daftar ancaman yang diunggah Akun AWS per setiap Wilayah.

Note

Jika Anda menyertakan IP yang sama pada daftar IP tepercaya dan daftar ancaman, IP tersebut akan diproses oleh daftar IP tepercaya terlebih dahulu, dan tidak akan menghasilkan temuan.

Di lingkungan multi-akun, hanya pengguna dari akun akun GuardDuty administrator yang dapat menambahkan dan mengelola daftar IP tepercaya dan daftar ancaman. Daftar IP tepercaya dan daftar ancaman yang diunggah oleh akun akun administrator dikenakan pada GuardDuty fungsionalitas di akun anggotanya. Dengan kata lain, di akun anggota GuardDuty menghasilkan temuan berdasarkan aktivitas yang melibatkan alamat IP berbahaya yang diketahui dari daftar ancaman akun administrator dan tidak menghasilkan temuan berdasarkan aktivitas yang melibatkan alamat IP dari daftar IP tepercaya akun administrator. Untuk informasi selengkapnya, lihat [Beberapa akun di Amazon GuardDuty](#).

Format daftar

GuardDuty menerima daftar dalam format berikut.

Ukuran maksimum setiap file yang menghosting daftar IP tepercaya atau daftar IP ancaman Anda adalah 35MB. Dalam daftar IP tepercaya dan daftar IP ancaman Anda, alamat IP dan rentang CIDR harus muncul satu per baris. Hanya IPv4 alamat yang diterima. IPv6 alamat tidak didukung.

- Plaintext (TXT)

Format ini mendukung blok CIDR dan alamat IP individual. Daftar contoh berikut menggunakan format Plaintext (TXT).

```
192.0.2.0/24
198.51.100.1
203.0.113.1
```

- Ekspresi Informasi Ancaman Terstruktur (STIX)

Format ini mendukung blok CIDR dan alamat IP individual. Daftar contoh berikut menggunakan format STIX.

```
<?xml version="1.0" encoding="UTF-8"?>
<stix:STIX_Package
```

```

xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:stix="http://stix.mitre.org/stix-1"
xmlns:stixCommon="http://stix.mitre.org/common-1"
xmlns:ttp="http://stix.mitre.org/TTP-1"
xmlns:cybox="http://cybox.mitre.org/cybox-2"
xmlns:AddressObject="http://cybox.mitre.org/objects#AddressObject-2"
xmlns:cyboxVocabs="http://cybox.mitre.org/default_vocabularies-2"
xmlns:stixVocabs="http://stix.mitre.org/default_vocabularies-1"
xmlns:example="http://example.com/"
xsi:schemaLocation="
  http://stix.mitre.org/stix-1 http://stix.mitre.org/XMLSchema/core/1.2/
stix_core.xsd
  http://stix.mitre.org/Campaign-1 http://stix.mitre.org/XMLSchema/campaign/1.2/
campaign.xsd
  http://stix.mitre.org/Indicator-2 http://stix.mitre.org/XMLSchema/indicator/2.2/
indicator.xsd
  http://stix.mitre.org/TTP-2 http://stix.mitre.org/XMLSchema/ttp/1.2/ttp.xsd
  http://stix.mitre.org/default_vocabularies-1 http://stix.mitre.org/XMLSchema/
default_vocabularies/1.2.0/stix_default_vocabularies.xsd
  http://cybox.mitre.org/objects#AddressObject-2 http://cybox.mitre.org/XMLSchema/
objects/Address/2.1/Address_Object.xsd"
id="example:STIXPackage-a78fc4e3-df94-42dd-a074-6de62babfe16"
version="1.2">
<stix:Observables cybox_major_version="1" cybox_minor_version="1">
  <cybox:Observable id="example:observable-80b26f43-
dc41-43ff-861d-19aff31e0236">
    <cybox:Object id="example:object-161a5438-1c26-4275-ba44-a35ba963c245">
      <cybox:Properties xsi:type="AddressObject:AddressObjectType"
category="ipv4-addr">

<AddressObject:Address_Valuecondition="InclusiveBetween">192.0.2.0##comma##192.0.2.255</
AddressObject:Address_Value>
      </cybox:Properties>
    </cybox:Object>
  </cybox:Observable>
  <cybox:Observable id="example:observable-b442b399-aea4-436f-bb34-
b9ef6c5ed8ab">
    <cybox:Object id="example:object-b422417f-bf78-4b34-ba2d-de4b09590a6d">
      <cybox:Properties xsi:type="AddressObject:AddressObjectType"
category="ipv4-addr">
        <AddressObject:Address_Value>198.51.100.1</
AddressObject:Address_Value>
      </cybox:Properties>
    </cybox:Object>
  </cybox:Observable>
</stix:Observables>

```

```

    </cybox:Observable>
    <cybox:Observable
id="example:observable-1742fa06-8b5e-4449-9d89-6f9f32595784">
      <cybox:Object id="example:object-dc73b749-8a31-46be-803f-71df77565391">
        <cybox:Properties xsi:type="AddressObject:AddressObjectType"
category="ipv4-addr">
          <AddressObject:Address_Value>203.0.113.1</
AddressObject:Address_Value>
        </cybox:Properties>
      </cybox:Object>
    </cybox:Observable>
  </stix:Observables>
</stix:STIX_Package>

```

- Buka Pertukaran Ancaman (OTX) TM CSV

Format ini mendukung blok CIDR dan alamat IP individual. Daftar contoh berikut menggunakan format OTX™ CSV.

```
Indicator type, Indicator, Description
CIDR, 192.0.2.0/24, example
IPv4, 198.51.100.1, example
IPv4, 203.0.113.1, example
```

- FireEyeCSV Intelijen Ancaman TM iSight

Format ini mendukung blok CIDR dan alamat IP individual. Daftar contoh berikut menggunakan format FireEye™ CSV.

```
reportId, title, threatScape, audience, intelligenceType, publishDate, reportLink,  
webLink, emailIdentifier, senderAddress, senderName, sourceDomain, sourceIp,  
subject, recipient, emailLanguage, fileName, fileSize, fuzzyHash, fileIdentifier,  
md5, sha1, sha256, description, fileType, packer, userAgent, registry,  
fileCompilationDateTime, filePath, asn, cidr, domain, domainTimeOfLookup,  
networkIdentifier, ip, port, protocol, registrantEmail, registrantName, networkType,  
url, malwareFamily, malwareFamilyId, actor, actorId, observationTime  
  
01-00000001, Example, Test, Operational, threat, 1494944400,  
https://www.example.com/report/01-00000001, https://www.example.com/  
report/01-00000001, , , , , , , , , , , , , , , , , , , 192.0.2.0/24, , ,  
Related, , , , , , network, , Ursnif, 21a14673-0d94-46d3-89ab-8281a0466099, , ,  
1494944400
```

```
01-00000002, Example, Test, Operational, threat, 1494944400,  
https://www.example.com/report/01-00000002, https://www.example.com/  
report/01-00000002, , , , , , , , , , , , , , , , , , , Related,  
198.51.100.1, , , , , network, , Ursnif,  
12ab7bc4-62ed-49fa-99e3-14b92afc41bf, , ,1494944400  
  
01-00000003, Example, Test, Operational, threat, 1494944400,  
https://www.example.com/report/01-00000003, https://www.example.com/  
report/01-00000003, , , , , , , , , , , , , , , , , , Related,  
203.0.113.1, , , , , network, , Ursnif, 8a78c3db-7bcb-40bc-a080-75bd35a2572d, , ,  
1494944400
```

- BuktiTM ET Intelijen Umpan CSV

Format ini hanya mendukung alamat IP individual. Daftar contoh berikut menggunakan format Proofpoint CSV. Parameter ports bersifat opsional. Jika Anda melewati port, pastikan untuk meninggalkan tanda koma (,) di akhir.

```
ip, category, score, first_seen, last_seen, ports (|)
198.51.100.1, 1, 100, 2000-01-01, 2000-01-01,
203.0.113.1, 1, 100, 2000-01-01, 2000-01-01, 80
```

- AlienVaultUmpan Reputasi TM

Format ini hanya mendukung alamat IP individual. Daftar contoh berikut menggunakan AlienVault format.

```
198.51.100.1#4#2#Malicious Host#US##0.0,0.0#3
203.0.113.1#4#2#Malicious Host#US##0.0,0.0#3
```

Izin yang diperlukan untuk mengunggah daftar IP terpercaya dan daftar ancaman

Berbagai identitas IAM memerlukan izin khusus untuk bekerja dengan daftar IP terpercaya dan daftar ancaman. GuardDuty Identitas dengan kebijakan [AmazonGuardDutyFullAccess](#) terkelola terlampir hanya dapat mengganti nama dan menonaktifkan daftar IP terpercaya yang diunggah dan daftar ancaman.

Untuk memberikan berbagai identitas akses penuh untuk bekerja dengan daftar IP tepercaya dan daftar ancaman (selain mengganti nama dan menonaktifkan, ini termasuk menambahkan,

mengaktifkan, menghapus, dan memperbarui lokasi atau nama daftar), pastikan bahwa tindakan berikut ada dalam kebijakan izin yang dilampirkan ke pengguna, grup, atau peran:

```
{
  "Effect": "Allow",
  "Action": [
    "iam:PutRolePolicy",
    "iam>DeleteRolePolicy"
  ],
  "Resource": "arn:aws:iam::555555555555:role/aws-service-role/guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty"
}
```

 Important

Tindakan ini tidak termasuk dalam kebijakan yang AmazonGuardDutyFullAccess dikelola.

Menggunakan enkripsi sisi server untuk daftar IP tepercaya dan daftar ancaman

GuardDuty mendukung jenis enkripsi berikut untuk daftar: SSE- AES256 dan SSE-KMS. SSE-C tidak didukung. Untuk informasi selengkapnya tentang jenis enkripsi untuk S3, lihat [Melindungi data menggunakan enkripsi sisi server](#).

Jika daftar Anda dienkripsi menggunakan enkripsi sisi server SSE-KMS, Anda harus memberikan AWSServiceRoleForAmazonGuardDutyizin peran GuardDuty terkait layanan untuk mendekripsi file agar dapat mengaktifkan daftar. Tambahkan pernyataan berikut ke kebijakan kunci KMS dan ganti ID akun dengan milik Anda sendiri:

```
{
  "Sid": "AllowGuardDutyServiceRole",
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::123456789123:role/aws-service-role/guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty"
  },
  "Action": "kms:Decrypt*",
  "Resource": "*"
}
```

Menambahkan dan mengaktifkan daftar IP terpercaya atau daftar IP ancaman

Pilih salah satu metode akses berikut untuk menambahkan dan mengaktifkan daftar IP terpercaya atau daftar IP ancaman.

Console

(Opsional) langkah 1: Mengambil URL lokasi daftar Anda

1. Buka konsol Amazon S3 di <https://console.aws.amazon.com/s3/>
2. Di panel navigasi, pilih Bucket.
3. Pilih nama bucket Amazon S3 yang berisi daftar spesifik yang ingin Anda tambahkan.
4. Pilih nama objek (daftar) untuk melihat detailnya.
5. Di bawah tab Properties, salin URI S3 untuk objek ini.

Langkah 2: Menambahkan daftar IP terpercaya atau daftar ancaman

Important

Secara default, pada titik waktu tertentu, Anda hanya dapat memiliki satu daftar IP terpercaya. Demikian pula, Anda dapat memiliki hingga enam daftar ancaman.

1. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.
2. Di panel navigasi, pilih Daftar.
3. Pada halaman Manajemen daftar, pilih Tambahkan daftar IP terpercaya atau Tambahkan daftar ancaman.
4. Berdasarkan pilihan Anda, kotak dialog akan muncul. Lakukan langkah-langkah berikut:
 - a. Untuk nama Daftar, masukkan nama untuk daftar Anda.

Kendala penamaan daftar — Nama daftar Anda dapat mencakup huruf kecil, huruf besar, angka, tanda hubung (-), dan garis bawah (_).
 - b. Untuk Lokasi, berikan lokasi tempat Anda mengunggah daftar Anda. Jika Anda belum memilikinya, lihat [Step 1: Fetching location URL of your list](#).

Format URL lokasi

- <https://s3.amazonaws.com/bucket.name/file.txt>
 - <https://s3-aws-region.amazonaws.com/bucket.name/file.txt>
 - <http://bucket.s3.amazonaws.com/file.txt>
 - <http://bucket.s3-aws-region.amazonaws.com/file.txt>
 - <s3://bucket.name/file.txt>
- c. Pilih kotak centang Saya setuju.
- d. Pilih Tambah daftar. Secara default, Status daftar yang ditambahkan adalah Tidak Aktif. Agar daftar menjadi efektif, Anda harus mengaktifkan daftar.

Langkah 3: Mengaktifkan daftar IP tepercaya atau daftar ancaman

1. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.
2. Di panel navigasi, pilih Daftar.
3. Pada halaman Manajemen daftar, pilih daftar yang ingin Anda aktifkan.
4. Pilih Tindakan, lalu pilih Aktifkan. Mungkin diperlukan waktu hingga 15 menit agar daftar menjadi efektif.

API/CLI

Untuk daftar IP tepercaya

- Jalankan [Buat IPSet](#). Pastikan untuk memberikan akun detectorId anggota yang ingin Anda buat daftar IP tepercaya ini.

Kendala penamaan daftar — Nama daftar Anda dapat mencakup huruf kecil, huruf besar, angka, tanda hubung (-), dan garis bawah (_).

- Atau, Anda dapat melakukan ini dengan menjalankan AWS Command Line Interface perintah berikut dan pastikan untuk mengganti detector-id dengan ID detektor dari akun anggota yang akan Anda perbarui daftar IP tepercaya.

```
aws guardduty create-ip-set --detector-id 12abc34d567e8fa901bc2d34e56789f0
--name AnyOrganization List --format TXT --location https://
```

```
s3.amazonaws.com/amzn-s3-demo-bucket2/DOC-EXAMPLE-SOURCE-FILE.format --  
activate
```

Untuk daftar ancaman

- Jalankan [CreateThreatIntelSet](#). Pastikan untuk memberikan akun detectorId anggota yang ingin Anda buat daftar ancaman ini.
 - Atau, Anda dapat melakukan ini dengan menjalankan AWS Command Line Interface perintah berikut. Pastikan untuk memberikan akun anggota yang ingin Anda buat daftar ancaman. detectorId

```
aws guardduty create-threat-intel-set --detector-  
id 12abc34d567e8fa901bc2d34e56789f0 --name AnyOrganization List --format TXT  
--location https://s3.amazonaws.com/amzn-s3-demo-bucket2/DOC-EXAMPLE-  
SOURCE-FILE.format --activate
```

Note

Setelah Anda mengaktifkan atau memperbarui daftar IP apa pun, GuardDuty mungkin memerlukan waktu hingga 15 menit untuk menyinkronkan daftar.

Memperbarui daftar IP tepercaya dan daftar ancaman

Anda dapat memperbarui nama daftar atau alamat IP yang ditambahkan ke daftar yang telah ditambahkan dan diaktifkan. Jika Anda memperbarui daftar, Anda harus mengaktifkannya lagi GuardDuty untuk menggunakan versi terbaru dari daftar.

Pilih salah satu metode akses untuk memperbarui IP tepercaya atau daftar ancaman.

Console

1. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.
2. Di panel navigasi, pilih Daftar.
3. Pada halaman Manajemen daftar, pilih kumpulan IP tepercaya atau daftar ancaman yang ingin Anda perbarui.
4. Pilih Tindakan, dan kemudian pilih Edit.

5. Dalam kotak dialog Perbarui daftar, perbarui informasi sesuai kebutuhan.

Kendala penamaan daftar — Nama daftar Anda dapat mencakup huruf kecil, huruf besar, angka, tanda hubung (-), dan garis bawah (_).

6. Pilih kotak centang Saya setuju, lalu pilih Perbarui daftar. Nilai di kolom Status akan berubah menjadi Tidak Aktif.
7. Mengaktifkan kembali daftar yang diperbarui
 - a. Pada halaman Manajemen daftar, pilih daftar yang ingin Anda aktifkan lagi.
 - b. Pilih Tindakan, lalu pilih Aktifkan.

API/CLI

1. Jalankan [UpdateIPSet](#) untuk memperbarui daftar IP tepercaya.
 - Atau, Anda dapat menjalankan AWS CLI perintah berikut untuk memperbarui daftar IP tepercaya dan pastikan untuk mengganti `detector-id` dengan ID detektor akun anggota yang akan Anda perbarui daftar IP tepercaya.

```
aws guardduty update-ip-set --detector-id 12abc34d567e8fa901bc2d34e56789f0  
--name AnyOrganization List --ip-set-id d4b94fc952d6912b8f3060768example --  
activate
```

2. Jalankan [UpdateThreatIntelSet](#) untuk memperbarui daftar ancaman
 - Atau, Anda dapat menjalankan AWS CLI perintah berikut untuk memperbarui daftar ancaman dan pastikan untuk mengganti `detector-id` dengan ID detektor akun anggota yang akan Anda perbarui daftar ancaman.

```
aws guardduty update-threat-intel-set --detector-  
id 12abc34d567e8fa901bc2d34e56789f0 --name AnyOrganization List --threat-  
intel-set-id d4b94fc952d6912b8f3060768example --activate
```

Menonaktifkan atau menghapus daftar IP tepercaya atau daftar ancaman

Pilih salah satu metode akses untuk menghapus (dengan menggunakan konsol) atau menonaktifkan (dengan menggunakan API/CLI) daftar IP tepercaya, atau daftar ancaman.

Console

1. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.
2. Di panel navigasi, pilih Daftar.
3. Pada halaman Manajemen daftar, pilih daftar yang ingin Anda hapus.
4. Pilih Tindakan, lalu pilih Hapus.
5. Konfirmasikan tindakan dan pilih Hapus. Daftar spesifik tidak akan lagi tersedia di tabel.

API/CLI

1. Untuk daftar IP tepercaya

Jalankan [UpdateIPSet](#) untuk memperbarui daftar IP tepercaya.

- Atau, Anda dapat menjalankan AWS CLI perintah berikut untuk memperbarui daftar IP tepercaya dan pastikan untuk mengganti `detector-id` dengan ID detektor akun anggota yang akan Anda perbarui daftar IP tepercaya.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan `detectorId` [ListDetectors](#) API.

```
aws guardduty update-ip-set --detector-id 12abc34d567e8fa901bc2d34e56789f0
--name AnyOrganization List --ip-set-id d4b94fc952d6912b8f3060768example --
no-activate
```

2. Untuk daftar ancaman

Jalankan [UpdateThreatIntelSet](#) untuk memperbarui daftar ancaman

- Atau, Anda dapat menjalankan AWS CLI perintah berikut untuk memperbarui daftar IP tepercaya dan pastikan untuk mengganti `detector-id` dengan ID detektor akun anggota yang akan Anda perbarui daftar ancaman.

```
aws guardduty update-threat-intel-set --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --name AnyOrganization List --threat-
intel-set-id d4b94fc952d6912b8f3060768example --no-activate
```

Mengekspor GuardDuty temuan yang dihasilkan ke ember Amazon S3

GuardDuty mempertahankan temuan yang dihasilkan untuk jangka waktu 90 hari. GuardDuty mengekspor temuan aktif ke Amazon EventBridge (EventBridge). Anda dapat secara opsional mengekspor temuan yang dihasilkan ke bucket Amazon Simple Storage Service (Amazon S3). Ini akan membantu Anda melacak data historis aktivitas yang berpotensi mencurigakan di akun Anda dan mengevaluasi apakah langkah-langkah perbaikan yang disarankan berhasil.

Setiap temuan aktif baru yang GuardDuty dihasilkan secara otomatis diekspor dalam waktu sekitar 5 menit setelah temuan dihasilkan. Anda dapat mengatur frekuensi seberapa sering pembaruan temuan aktif diekspor ke EventBridge. Frekuensi yang Anda pilih berlaku untuk mengekspor kemunculan baru temuan yang ada ke EventBridge, bucket S3 Anda (saat dikonfigurasi), dan Detektif (saat terintegrasi). Untuk informasi tentang bagaimana GuardDuty menggabungkan beberapa kejadian temuan yang ada, lihat. [GuardDuty menemukan agregasi](#)

Saat mengonfigurasi setelan untuk mengekspor temuan ke bucket Amazon S3, GuardDuty gunakan AWS Key Management Service (AWS KMS) untuk mengenkripsi data temuan di bucket S3. Ini mengharuskan Anda untuk menambahkan izin ke bucket S3 dan AWS KMS kuncinya sehingga GuardDuty dapat menggunakannya untuk mengekspor temuan di akun Anda.

Daftar Isi

- [Pertimbangan](#)
- [Langkah 1 - Izin diperlukan untuk mengekspor temuan](#)
- [Langkah 2 - Melampirkan kebijakan ke kunci KMS Anda](#)
- [Langkah 3 - Melampirkan kebijakan ke bucket Amazon S3](#)
- [Langkah 4 - Mengekspor temuan ke bucket S3 \(Konsol\)](#)
- [Langkah 5 - Mengatur frekuensi untuk mengekspor temuan aktif yang diperbarui](#)

Pertimbangan

Sebelum melanjutkan dengan prasyarat dan langkah-langkah untuk mengekspor temuan, pertimbangkan konsep-konsep kunci berikut:

- Pengaturan ekspor bersifat regional - Anda perlu mengonfigurasi opsi ekspor di setiap Wilayah tempat Anda menggunakan GuardDuty.

- Mengekspor temuan ke bucket Amazon S3 di Wilayah AWS berbagai (Lintas wilayah) GuardDuty — mendukung pengaturan ekspor berikut:
 - Bucket atau objek Amazon S3 Anda, dan AWS KMS kunci harus milik yang sama. Wilayah AWS
 - Untuk temuan yang dihasilkan di Wilayah komersial, Anda dapat memilih untuk mengekspor temuan ini ke ember S3 di Wilayah komersial mana pun. Namun, Anda tidak dapat mengekspor temuan ini ke bucket S3 di Wilayah keikutsertaan.
 - Untuk temuan yang dihasilkan di Wilayah keikutsertaan, Anda dapat memilih untuk mengekspor temuan ini ke Wilayah keikutsertaan yang sama di mana mereka dihasilkan atau Wilayah komersial mana pun. Namun, Anda tidak dapat mengekspor temuan dari satu Wilayah keikutsertaan ke Wilayah keikutsertaan lainnya.
- Izin untuk mengekspor temuan — Untuk mengonfigurasi pengaturan untuk mengekspor temuan aktif, bucket S3 Anda harus memiliki izin yang memungkinkan GuardDuty untuk mengunggah objek. Anda juga harus memiliki AWS KMS kunci yang GuardDuty dapat digunakan untuk mengenkripsi temuan.
- Temuan yang diarsipkan tidak diekspor — Perilaku default adalah bahwa temuan yang diarsipkan, termasuk contoh baru dari temuan yang ditekan, tidak diekspor.

Ketika sebuah GuardDuty temuan dihasilkan sebagai Diarsipkan, Anda harus Membatalkan pengarsipannya. Ini mengubah status pencarian Filter menjadi Aktif. GuardDuty mengekspor pembaruan ke temuan yang tidak diarsipkan yang ada berdasarkan cara Anda mengonfigurasi.

[Langkah 5 - Frekuensi untuk mengekspor temuan](#)

- GuardDuty Akun administrator dapat mengekspor temuan yang dihasilkan di akun anggota terkait — Saat Anda mengonfigurasi temuan ekspor di akun administrator, semua temuan dari akun anggota terkait yang dihasilkan di Wilayah yang sama juga diekspor ke lokasi yang sama dengan yang Anda konfigurasikan untuk akun administrator. Untuk informasi selengkapnya, lihat [Memahami hubungan antara akun GuardDuty administrator dan akun anggota](#).

Langkah 1 - Izin diperlukan untuk mengekspor temuan

Saat mengonfigurasi setelan untuk mengekspor temuan, Anda memilih bucket Amazon S3 tempat Anda dapat menyimpan temuan dan kunci AWS KMS yang akan digunakan untuk enkripsi data. Selain izin untuk GuardDuty tindakan, Anda juga harus memiliki izin untuk tindakan berikut agar berhasil mengonfigurasi pengaturan untuk mengekspor temuan:

- `s3:GetBucketLocation`
- `s3:PutObject`

Jika Anda perlu mengeksport temuan ke awalan tertentu di bucket Amazon S3, Anda juga harus menambahkan izin berikut ke peran IAM:

- `s3:GetObject`
- `s3:ListBucket`

Langkah 2 - Melampirkan kebijakan ke kunci KMS Anda

GuardDuty mengenkripsi data temuan di bucket Anda dengan menggunakan AWS Key Management Service. Agar berhasil mengkonfigurasi pengaturan, Anda harus terlebih dahulu memberikan GuardDuty izin untuk menggunakan kunci KMS. Anda dapat memberikan izin dengan [melampirkan kebijakan ke kunci](#) KMS Anda.

Saat Anda menggunakan kunci KMS dari akun lain, Anda perlu menerapkan kebijakan kunci dengan masuk ke Akun AWS yang memiliki kunci tersebut. Saat Anda mengonfigurasi pengaturan untuk mengeksport temuan, Anda juga memerlukan ARN kunci dari akun yang memiliki kunci tersebut.

Untuk mengubah kebijakan kunci KMS GuardDuty untuk mengenkripsi temuan Anda yang diekspor

1. Buka AWS KMS konsol di <https://console.aws.amazon.com/kms>.
2. Untuk mengubah Wilayah AWS, gunakan pemilih Wilayah di sudut kanan atas halaman.
3. Pilih kunci KMS yang ada atau lakukan langkah-langkah untuk [Membuat kunci baru](#) di Panduan AWS Key Management Service Pengembang, yang akan Anda gunakan untuk mengenkripsi temuan yang diekspor.

Note

Kunci KMS Anda dan bucket Amazon S3 harus sama. Wilayah AWS

Anda dapat menggunakan bucket S3 dan key pair KMS yang sama untuk mengeksport temuan dari Wilayah mana pun yang berlaku. Untuk informasi lebih lanjut, lihat [Pertimbangan](#) untuk mengeksport temuan di seluruh Wilayah.

4. Di bagian Kebijakan kunci, pilih Edit.

Jika Beralih ke tampilan kebijakan ditampilkan, pilih untuk menampilkan Kebijakan kunci, lalu pilih Edit.

5. Salin blok kebijakan berikut ke kebijakan kunci KMS Anda, untuk memberikan GuardDuty izin menggunakan kunci Anda.

```
{
  "Sid": "AllowGuardDutyKey",
  "Effect": "Allow",
  "Principal": {
    "Service": "guardduty.amazonaws.com"
  },
  "Action": "kms:GenerateDataKey",
  "Resource": "KMS key ARN",
  "Condition": {
    "StringEquals": {
      "aws:SourceAccount": "123456789012",
      "aws:SourceArn":
        "arn:aws:guardduty:Region2:123456789012:detector/SourceDetectorID"
    }
  }
}
```

6. Edit kebijakan dengan mengganti nilai berikut yang diformat *red* dalam contoh kebijakan:
 1. Ganti *KMS key ARN* dengan Nama Sumber Daya Amazon (ARN) dari kunci KMS. Untuk menemukan kunci ARN, lihat [Menemukan ID kunci dan ARN](#) di Panduan Pengembang AWS Key Management Service
 2. Ganti *123456789012* dengan Akun AWS ID yang memiliki GuardDuty akun yang mengeksport temuan.
 3. Ganti *Region2* dengan Wilayah AWS tempat GuardDuty temuan dihasilkan.
 4. Ganti *SourceDetectorID* dengan GuardDuty akun di Wilayah tertentu tempat temuan dihasilkan. detectorID

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/> konsol, atau jalankan detectorId [ListDetectors](#) API.

Note

Jika Anda menggunakan GuardDuty di Wilayah keikutsertaan, ganti nilai untuk “Layanan” dengan titik akhir Regional untuk Wilayah tersebut. Misalnya, jika Anda menggunakan GuardDuty di Wilayah Timur Tengah (Bahrain) (me-south-1), ganti dengan.

"Service": "guardduty.amazonaws.com" "Service": "guardduty.me-south-1.amazonaws.com" Untuk informasi tentang titik akhir untuk setiap Wilayah keikutsertaan, lihat [GuardDuty titik akhir](#) dan kuota.

7. Jika Anda menambahkan pernyataan kebijakan sebelum pernyataan akhir, tambahkan koma sebelum menambahkan pernyataan ini. Pastikan bahwa sintaks JSON dari kebijakan kunci KMS Anda valid.

Pilih Simpan.

8. (Opsional) salin kunci ARN ke notepad untuk digunakan pada langkah selanjutnya.

Langkah 3 - Melampirkan kebijakan ke bucket Amazon S3

Tambahkan izin ke bucket Amazon S3 tempat Anda akan mengeksport temuannya GuardDuty sehingga dapat mengunggah objek ke bucket S3 ini. Terlepas dari penggunaan bucket Amazon S3 milik akun Anda atau yang berbeda Akun AWS, Anda harus menambahkan izin ini.

Jika suatu saat, Anda memutuskan untuk mengeksport temuan ke bucket S3 yang berbeda, lalu untuk melanjutkan mengeksport temuan, Anda harus menambahkan izin ke bucket S3 tersebut dan mengonfigurasi pengaturan temuan ekspor lagi.

Jika Anda belum memiliki bucket Amazon S3 tempat Anda ingin mengeksport temuan ini, lihat [Membuat bucket](#) di Panduan Pengguna Amazon S3.

Untuk melampirkan izin ke kebijakan bucket S3 Anda

1. Lakukan langkah-langkah di bawah [Untuk membuat atau mengedit kebijakan bucket](#) di Panduan Pengguna Amazon S3, hingga halaman Edit kebijakan bucket muncul.
2. Kebijakan contoh menunjukkan cara memberikan GuardDuty izin untuk mengeksport temuan ke bucket Amazon S3 Anda. Jika Anda mengubah jalur setelah mengonfigurasi temuan ekspor, Anda harus mengubah kebijakan untuk memberikan izin ke lokasi baru.

Salin contoh kebijakan berikut dan tempelkan ke editor kebijakan Bucket.

Jika Anda menambahkan pernyataan kebijakan sebelum pernyataan akhir, tambahkan koma sebelum menambahkan pernyataan ini. Pastikan bahwa sintaks JSON dari kebijakan kunci KMS Anda valid.

Kebijakan contoh bucket S3

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Allow GetBucketLocation",
      "Effect": "Allow",
      "Principal": {
        "Service": "guardduty.amazonaws.com"
      },
      "Action": "s3:GetBucketLocation",
      "Resource": "Amazon S3 bucket ARN",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "123456789012",
          "aws:SourceArn":
            "arn:aws:guardduty:Region2:123456789012:detector/SourceDetectorID"
        }
      }
    },
    {
      "Sid": "Allow PutObject",
      "Effect": "Allow",
      "Principal": {
        "Service": "guardduty.amazonaws.com"
      },
      "Action": "s3:PutObject",
      "Resource": "Amazon S3 bucket ARN/[optional prefix]/*",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "123456789012",
          "aws:SourceArn":
            "arn:aws:guardduty:Region2:123456789012:detector/SourceDetectorID"
        }
      }
    },
    {
      "Sid": "Deny unencrypted object uploads",
      "Effect": "Deny",
      "Principal": {
        "Service": "guardduty.amazonaws.com"
      },

```

```

    "Action": "s3:PutObject",
    "Resource": "Amazon S3 bucket ARN/[optional prefix]/*",
    "Condition": {
        "StringNotEquals": {
            "s3:x-amz-server-side-encryption": "aws:kms"
        }
    },
    {
        "Sid": "Deny incorrect encryption header",
        "Effect": "Deny",
        "Principal": {
            "Service": "guardduty.amazonaws.com"
        },
        "Action": "s3:PutObject",
        "Resource": "Amazon S3 bucket ARN/[optional prefix]/*",
        "Condition": {
            "StringNotEquals": {
                "s3:x-amz-server-side-encryption-aws-kms-key-id": "KMS key ARN"
            }
        }
    },
    {
        "Sid": "Deny non-HTTPS access",
        "Effect": "Deny",
        "Principal": "*",
        "Action": "s3:*",
        "Resource": "Amazon S3 bucket ARN/[optional prefix]/*",
        "Condition": {
            "Bool": {
                "aws:SecureTransport": "false"
            }
        }
    }
]
}

```

3. Edit kebijakan dengan mengganti nilai berikut yang diformat *red* dalam contoh kebijakan:

1. Ganti *Amazon S3 bucket ARN* dengan Nama Sumber Daya Amazon (ARN) dari bucket Amazon S3. Anda dapat menemukan Bucket ARN di halaman kebijakan Edit bucket di konsol. <https://console.aws.amazon.com/s3/>

2. Ganti **123456789012** dengan Akun AWS ID yang memiliki GuardDuty akun yang mengeksplor temuan.
3. Ganti **Region2** dengan Wilayah AWS tempat GuardDuty temuan dihasilkan.
4. Ganti **SourceDetectorID** dengan GuardDuty akun di Wilayah tertentu tempat temuan dihasilkan. detectorID

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan `detectorId` [ListDetectorsAPI](#).

5. Ganti **[optional prefix]** bagian dari nilai **S3 bucket ARN/[optional prefix]** placeholder dengan lokasi folder opsional yang ingin Anda ekspor temuannya. Untuk informasi selengkapnya tentang penggunaan awalan, lihat [Mengatur objek menggunakan awalan](#) di Panduan Pengguna Amazon S3.

Bila Anda menyediakan lokasi folder opsional yang belum ada, GuardDuty akan membuat lokasi tersebut hanya jika akun yang terkait dengan bucket S3 sama dengan akun yang mengeksplor temuan. Saat Anda mengeksplor temuan ke bucket S3 milik akun lain, lokasi folder harus sudah ada.

6. Ganti **KMS key ARN** dengan Nama Sumber Daya Amazon (ARN) dari kunci KMS yang terkait dengan enkripsi temuan yang diekspor ke bucket S3. Untuk menemukan kunci ARN, lihat [Menemukan ID kunci dan ARN](#) di Panduan Pengembang AWS Key Management Service

Note

Jika Anda menggunakan GuardDuty di Wilayah keikutsertaan, ganti nilai untuk "Layanan" dengan titik akhir Regional untuk Wilayah tersebut. Misalnya, jika Anda menggunakan GuardDuty di Wilayah Timur Tengah (Bahrain) (me-south-1), ganti dengan.

"Service": "guardduty.amazonaws.com" "Service": "guardduty.me-south-1.amazonaws.com" Untuk informasi tentang titik akhir untuk setiap Wilayah keikutsertaan, lihat [GuardDuty titik akhir](#) dan kuota.

4. Pilih Simpan.

Langkah 4 - Mengeksplor temuan ke bucket S3 (Konsol)

GuardDuty memungkinkan Anda untuk mengeksplor temuan ke ember yang ada di ember lain Akun AWS.

Saat membuat bucket S3 baru atau memilih bucket yang ada di akun Anda, Anda dapat menambahkan awalan opsional. Saat mengonfigurasi temuan ekspor, GuardDuty buat folder baru di bucket S3 untuk temuan Anda. Awalan akan ditambahkan ke struktur folder default yang GuardDuty dibuat. Misalnya, format awalan `/AWSLogs/123456789012/GuardDuty/Region` opsional.

Seluruh jalur objek S3 akan menjadi `amzn-s3-demo-bucket/prefix-name/UUID.jsonl.gz`. UUID ini dihasilkan secara acak dan tidak mewakili ID detektor atau ID temuan.

 Important

Kunci KMS dan bucket S3 harus berada di Wilayah yang sama.

Sebelum menyelesaikan langkah-langkah ini, pastikan Anda telah melampirkan kebijakan masing-masing ke kunci KMS dan bucket S3 yang ada.

Untuk mengonfigurasi temuan ekspor

1. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.
2. Pada panel navigasi, silakan pilih Pengaturan.
3. Pada halaman Pengaturan, di bawah opsi ekspor temuan, untuk bucket S3, pilih Konfigurasi sekarang (atau Edit, sesuai kebutuhan).
4. Untuk ember S3 ARN, masukkan. **bucket ARN** Untuk menemukan bucket ARN, lihat [Melihat properti untuk bucket S3](#) di Panduan Pengguna Amazon S3.
5. Untuk ARN kunci KMS, masukkan file. **key ARN** Untuk menemukan kunci ARN, lihat [Menemukan ID kunci dan ARN](#) di Panduan Pengembang AWS Key Management Service
6. Lampirkan kebijakan
 - Lakukan langkah-langkah untuk melampirkan kebijakan bucket S3. Untuk informasi selengkapnya, lihat [Langkah 3 - Melampirkan kebijakan ke bucket Amazon S3](#).
 - Lakukan langkah-langkah untuk melampirkan kebijakan kunci KMS. Untuk informasi selengkapnya, lihat [Langkah 2 - Melampirkan kebijakan ke kunci KMS Anda](#).
7. Pilih Simpan.

Langkah 5 - Mengatur frekuensi untuk mengeksport temuan aktif yang diperbarui

Konfigurasi frekuensi untuk mengeksport temuan aktif yang diperbarui sesuai dengan lingkungan Anda. Secara default, temuan yang diperbarui diekspor setiap 6 jam. Ini berarti bahwa setiap temuan yang diperbarui setelah ekspor terbaru akan disertakan dalam ekspor berikutnya. Jika temuan yang diperbarui diekspor setiap 6 jam dan ekspor dilakukan pada pukul 12:00, setiap temuan yang Anda perbarui setelah pukul 12:00 akan diekspor pada pukul 18:00.

Untuk mengatur frekuensi

1. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.
2. Pilih Pengaturan.
3. Di bagian Opsi ekspor temuan, pilih Frekuensi untuk temuan yang diperbarui. Ini menetapkan frekuensi untuk mengeksport temuan Aktif yang diperbarui ke keduanya EventBridge dan Amazon S3. Anda dapat memilih dari opsi berikut:
 - Perbarui EventBridge dan S3 setiap 15 menit
 - Update EventBridge dan S3 setiap 1 jam
 - Perbarui EventBridge dan S3 setiap 6 jam (default)
4. Pilih Simpan perubahan.

Memproses GuardDuty temuan dengan Amazon EventBridge

GuardDuty secara otomatis menerbitkan (mengirim) temuan sebagai peristiwa ke Amazon EventBridge (sebelumnya CloudWatch Amazon Events), layanan bus acara tanpa server. EventBridge mengirimkan aliran data hampir real-time dari aplikasi dan layanan ke target seperti topik, fungsi, dan aliran Amazon Simple Notification Service (Amazon SNS), fungsi, AWS Lambda dan Amazon Kinesis. Untuk informasi selengkapnya, lihat [Panduan EventBridge Pengguna Amazon](#).

EventBridge memungkinkan pemantauan dan pemrosesan GuardDuty temuan secara otomatis dengan menerima [acara](#). EventBridge menerima peristiwa untuk temuan yang baru dihasilkan dan temuan agregat, di mana kejadian selanjutnya dari temuan yang ada digabungkan dengan aslinya. Setiap GuardDuty temuan diberi ID temuan, dan GuardDuty membuat EventBridge acara untuk setiap temuan dengan ID temuan unik. Untuk informasi tentang cara kerja agregasi GuardDuty, lihat [GuardDuty menemukan agregasi](#).

Selain pemantauan dan pemrosesan otomatis, penggunaan EventBridge memungkinkan retensi jangka panjang dari data temuan Anda. GuardDuty menyimpan temuan selama 90 hari. Dengan EventBridge, Anda dapat mengirim data temuan ke platform penyimpanan pilihan Anda dan menyimpan data selama yang Anda suka. Untuk mempertahankan temuan untuk durasi yang lebih lama, GuardDuty mendukung [Mengekspor temuan yang dihasilkan ke Amazon S3](#).

Topik

- [Memahami frekuensi EventBridge notifikasi di GuardDuty](#)
- [Siapkan topik dan titik akhir Amazon SNS \(Email, Slack, dan Amazon Chime\)](#)
- [Menggunakan Amazon EventBridge untuk GuardDuty temuan](#)
- [Membuat EventBridge aturan untuk GuardDuty temuan](#)
- [EventBridge aturan untuk lingkungan GuardDuty multi-akun](#)

Memahami frekuensi EventBridge notifikasi di GuardDuty

Bagian ini menjelaskan seberapa sering Anda menerima pemberitahuan pencarian melalui EventBridge dan cara memperbarui frekuensi untuk kejadian temuan berikutnya.

Pemberitahuan untuk temuan yang baru dibuat dengan ID temuan unik

GuardDuty mengirimkan notifikasi ini dalam waktu dekat saat menghasilkan temuan dengan ID temuan unik. Pemberitahuan mencakup semua kejadian berikutnya dari kejadian berikutnya dari ID temuan ini selama proses pembuatan notifikasi.

Frekuensi notifikasi untuk temuan yang baru dihasilkan mendekati waktu nyata. Secara default, Anda tidak dapat memodifikasi frekuensi ini.

Pemberitahuan untuk kejadian temuan selanjutnya

GuardDuty menggabungkan semua kejadian berikutnya dari jenis temuan tertentu yang terjadi dalam interval 6 jam menjadi satu peristiwa tunggal. Hanya akun administrator yang dapat memperbarui frekuensi EventBridge notifikasi untuk kejadian penemuan berikutnya. Akun anggota tidak dapat memperbarui frekuensi ini untuk akun mereka sendiri. Misalnya, jika akun GuardDuty administrator yang didelegasikan memperbarui frekuensi menjadi satu jam, semua akun anggota juga akan memiliki frekuensi pemberitahuan satu jam tentang kejadian temuan berikutnya yang dikirim ke EventBridge. Untuk informasi selengkapnya, lihat [Beberapa akun di Amazon GuardDuty](#).

Sebagai akun administrator, Anda dapat menyesuaikan frekuensi default pemberitahuan tentang kejadian temuan berikutnya. Nilai yang mungkin adalah 15 menit, 1 jam, atau default 6 jam. Untuk informasi tentang menyetel frekuensi notifikasi ini, lihat [Langkah 5 - Mengatur frekuensi untuk mengekspor temuan aktif yang diperbarui](#).

Untuk detail selengkapnya tentang akun administrator yang menerima EventBridge pemberitahuan untuk akun anggota, lihat [EventBridge aturan untuk lingkungan multi-akun](#).

Siapkan topik dan titik akhir Amazon SNS (Email, Slack, dan Amazon Chime)

Amazon Simple Notification Service (Amazon SNS) adalah layanan terkelola penuh yang menyediakan pengiriman pesan dari penerbit ke pelanggan. Penerbit berkomunikasi secara asinkron dengan pelanggan dengan mengirim pesan ke suatu topik. Topik adalah jalur akses logis dan saluran komunikasi yang memungkinkan Anda mengelompokkan beberapa titik akhir seperti AWS Lambda, Amazon Simple Queue Service (Amazon SQS), HTTP/S, dan alamat email.

Note

Anda dapat menambahkan topik Amazon SNS ke aturan EventBridge acara pilihan Anda selama atau setelah pembuatan aturan.

Buat topik Amazon SNS

Untuk memulai, Anda harus terlebih dahulu menyiapkan topik di Amazon SNS dan menambahkan titik akhir. Untuk membuat topik, lakukan langkah-langkah di [Langkah 1: Membuat topik](#) di Panduan Pengembang Layanan Pemberitahuan Sederhana Amazon. Setelah topik dibuat, salin topik ARN ke clipboard. Anda akan menggunakan topik ini ARN untuk melanjutkan dengan salah satu pengaturan yang disukai.

Pilih metode yang disukai untuk menentukan di mana Anda ingin mengirim data GuardDuty pencarian.

Email setup

Untuk menyiapkan titik akhir email

Setelah Anda [Create an Amazon SNS topic](#), langkah selanjutnya adalah membuat langganan topik ini. Lakukan langkah-langkah di bawah [Langkah 2: Membuat langganan ke topik Amazon SNS](#) di Panduan Pengembang Layanan Pemberitahuan Sederhana Amazon.

1. Untuk Topik ARN, gunakan topik ARN yang dibuat di langkah. [Create an Amazon SNS topic](#) Topik ARN terlihat mirip dengan yang berikut ini:

```
arn:aws:sns:us-east-2:123456789012:your_topic
```

2. Untuk Protokol, pilih Email.
3. Untuk Endpoint, masukkan alamat email tempat Anda ingin menerima notifikasi dari Amazon SNS.

Setelah langganan dibuat, Anda harus mengonfirmasinya melalui klien email Anda.

Slack setup

Untuk mengkonfigurasi Pengembang Amazon Q di klien aplikasi obrolan - Slack

Setelah Anda [Create an Amazon SNS topic](#), langkah selanjutnya adalah mengkonfigurasi klien untuk Slack.

Lakukan langkah-langkah di bawah [Tutorial: Mulai dengan Slack](#) di Pengembang Amazon Q di aplikasi obrolan Panduan Administrator.

Chime setup

Untuk mengkonfigurasi Pengembang Amazon Q di klien aplikasi obrolan - Chime

Setelah Anda [Create an Amazon SNS topic](#), langkah selanjutnya adalah mengonfigurasi Pengembang Amazon Q untuk Chime.

Lakukan langkah-langkah di bawah [Tutorial: Mulai dengan Amazon Chime](#) di Pengembang Amazon Q dalam aplikasi obrolan Panduan Administrator.

Menggunakan Amazon EventBridge untuk GuardDuty temuan

Dengan EventBridge, Anda membuat aturan untuk menentukan peristiwa yang ingin Anda pantau. Aturan ini juga menentukan layanan target dan aplikasi yang dapat melakukan tindakan otomatis jika peristiwa ini terjadi. [Target](#) adalah tujuan (sumber daya atau titik akhir) yang EventBridge

mengirimkan peristiwa ke saat acara cocok dengan pola acara yang ditentukan dalam aturan. Setiap peristiwa adalah objek JSON yang sesuai dengan EventBridge skema untuk AWS peristiwa dan berisi representasi JSON dari sebuah temuan. Anda dapat menyesuaikan aturan untuk mengirim hanya acara-acara yang memenuhi kriteria tertentu. Untuk informasi selengkapnya, lihat [Topik Skema JSON]. Karena data temuan disusun sebagai suatu [EventBridgeperistiwa](#), Anda dapat memantau, memproses, dan menindaklanjuti temuan dengan menggunakan aplikasi, layanan, dan alat lain.

Untuk menerima pemberitahuan tentang GuardDuty temuan berdasarkan peristiwa, Anda harus membuat EventBridge aturan dan target untuk GuardDuty. Aturan ini memungkinkan EventBridge untuk mengirim pemberitahuan untuk temuan yang GuardDuty menghasilkan target yang ditentukan dalam aturan.

Note

EventBridge dan CloudWatch Acara adalah layanan dan API dasar yang sama. Namun, EventBridge termasuk fitur tambahan yang membantu Anda menerima acara dari aplikasi perangkat lunak sebagai layanan (SaaS) dan aplikasi Anda sendiri. Karena layanan dan API yang mendasarinya sama, skema peristiwa untuk GuardDuty temuan juga sama.

Bagaimana temuan yang diarsipkan dan tidak diarsipkan bekerja dengan GuardDuty EventBridge

Untuk temuan yang Anda arsipkan secara manual, kejadian awal dan semua kejadian selanjutnya dari temuan ini (dihasilkan setelah pengarsipan selesai) dikirim EventBridge berdasarkan frekuensi pemberitahuan tertentu. Untuk informasi selengkapnya, lihat [Memahami frekuensi EventBridge notifikasi di GuardDuty](#).

Untuk temuan yang secara otomatis diarsipkan dengan [Aturan penekanan](#), awal dan semua kejadian selanjutnya dari temuan ini (dihasilkan setelah pengarsipan selesai) tidak dikirim ke EventBridge. Anda dapat melihat temuan yang diarsipkan secara otomatis ini di GuardDuty konsol.

Skema peristiwa

[Pola peristiwa](#) mendefinisikan data yang EventBridge digunakan untuk menentukan apakah akan mengirim acara ke target. EventBridgeAcara untuk GuardDuty memiliki format sebagai berikut:

```
{
  "version": "0",
  "id": "cd2d702e-ab31-411b-9344-793ce56b1bc7",
```

```
"detail-type": "GuardDuty Finding",
"source": "aws.guardduty",
"account": "111122223333",
"time": "1970-01-01T00:00:00Z",
"region": "us-east-1",
"resources": [],
"detail": {GUARDDUTY_FINDING_JSON_OBJECT}
}
```

`detail` Nilai mengembalikan rincian JSON dari temuan tunggal sebagai objek, sebagai lawan mengembalikan seluruh sintaks respons temuan yang mendukung beberapa temuan dalam array.

Untuk daftar lengkap semua parameter yang disertakan `GUARDDUTY_FINDING_JSON_OBJECT`, lihat [GetFindings](#). Parameter `id` yang muncul di `GUARDDUTY_FINDING_JSON_OBJECT` adalah ID temuan yang telah dijelaskan sebelumnya.

Membuat EventBridge aturan untuk GuardDuty temuan

Prosedur berikut menjelaskan cara menggunakan EventBridge konsol Amazon dan [AWS Command Line Interface \(AWS CLI\)](#) untuk membuat EventBridge aturan untuk GuardDuty temuan. Aturan mendeteksi EventBridge peristiwa yang menggunakan skema dan pola peristiwa untuk GuardDuty temuan, dan mengirimkan peristiwa tersebut ke AWS Lambda fungsi untuk diproses.

AWS Lambda adalah layanan komputasi yang dapat Anda gunakan untuk menjalankan kode tanpa menyediakan atau mengelola server. Anda mengemas kode Anda dan mengunggahnya AWS Lambda sebagai fungsi Lambda. AWS Lambda kemudian menjalankan fungsi ketika fungsi dipanggil. Fungsi dapat dipanggil secara manual oleh Anda, secara otomatis dalam respons terhadap peristiwa, atau dalam merespons atas permintaan dari aplikasi atau layanan. Untuk informasi tentang membuat dan memanggil fungsi Lambda, lihat [Panduan Developer AWS Lambda](#).

Pilih metode pilihan Anda untuk membuat EventBridge aturan yang mengirimkan GuardDuty temuan Anda ke target.

Console

Ikuti langkah-langkah berikut untuk menggunakan EventBridge konsol Amazon untuk membuat aturan yang secara otomatis mengirimkan semua peristiwa GuardDuty pencarian ke fungsi Lambda untuk diproses. Aturan menggunakan pengaturan default untuk aturan yang berjalan saat peristiwa tertentu diterima. Untuk detail tentang setelan aturan atau mempelajari cara membuat aturan yang menggunakan setelan khusus, lihat [Membuat aturan yang bereaksi terhadap peristiwa](#) di Panduan EventBridge Pengguna Amazon.

Sebelum Anda membuat aturan ini, buat fungsi Lambda yang Anda inginkan aturan tersebut digunakan sebagai target. Saat Anda membuat aturan tersebut, Anda harus menentukan fungsi ini sebagai target aturan. Target Anda juga bisa menjadi topik SNS yang Anda buat sebelumnya. Untuk informasi selengkapnya, lihat [Siapkan topik dan titik akhir Amazon SNS \(Email, Slack, dan Amazon Chime\)](#).

Untuk membuat aturan acara dengan menggunakan konsol

1. Masuk ke AWS Management Console dan buka EventBridge konsol Amazon di <https://console.aws.amazon.com/events/>.
2. Di panel navigasi, di bawah Bus, pilih Aturan.
3. Di bagian Aturan, pilih Buat aturan.
4. Pada halaman Define rule detail, lakukan hal berikut:
 - a. Untuk Nama, masukkan nama untuk aturan.
 - b. (Opsional) Untuk Deskripsi, masukkan deskripsi singkat tentang aturan.
 - c. Untuk bus Acara, pastikan bahwa default dipilih dan Aktifkan aturan pada bus acara yang dipilih diaktifkan.
 - d. Untuk Tipe aturan, pilih Aturan dengan pola peristiwa.
 - e. Setelah selesai, pilih Selanjutnya.
5. Pada halaman pola acara Build, lakukan hal berikut:
 - a. Untuk sumber Acara, pilih AWS acara atau acara EventBridge mitra.
 - b. (Opsional) Untuk acara Sampel, tinjau peristiwa pencarian sampel GuardDuty untuk mempelajari apa yang mungkin terkandung dalam suatu peristiwa. Untuk melakukan ini, pilih AWS acara. Kemudian, untuk acara Contoh, pilih GuardDutyMenemukan.
 - c. Opsi 1 - Menggunakan formulir pola, template yang EventBridge menyediakan

Di bagian Pola acara, Anda dapat melakukan hal berikut:

1. Untuk metode Creation, pilih Gunakan formulir pola.
2. Untuk Sumber peristiwa, pilih Layanan AWS.
3. Untuk Layanan AWS, pilih GuardDuty.
4. Untuk jenis Event, pilih GuardDuty Finding.

Setelah selesai, pilih Selanjutnya.

d. Opsi 2 - Menggunakan pola acara kustom di JSON

Di bagian Pola acara, Anda dapat melakukan hal berikut:

1. Untuk metode Creation, pilih Custom pattern (JSON editor).
2. Untuk pola Peristiwa, tempel JSON kustom berikut yang akan membuat peringatan untuk temuan sedang, tinggi, dan kritis. Untuk informasi selengkapnya, lihat [Temuan tingkat keparahan](#).

```
{
  "source": [
    "aws.guardduty"
  ],
  "detail-type": [
    "GuardDuty Finding"
  ],
  "detail": {
    "severity": [
      4,
      4.0,
      4.1,
      4.2,
      4.3,
      4.4,
      4.5,
      4.6,
      4.7,
      4.8,
      4.9,
      5,
      5.0,
      5.1,
      5.2,
      5.3,
      5.4,
      5.5,
      5.6,
      5.7,
      5.8,
      5.9,
      6,
      6.0,
```

6.1,
6.2,
6.3,
6.4,
6.5,
6.6,
6.7,
6.8,
6.9,
7,
7.0,
7.1,
7.2,
7.3,
7.4,
7.5,
7.6,
7.7,
7.8,
7.9,
8,
8.0,
8.1,
8.2,
8.3,
8.4,
8.5,
8.6,
8.7,
8.8,
8.9,
9,
9.0,
9.1,
9.2,
9.3,
9.4,
9.5,
9.6,
9.7,
9.8,
9.9,
10,
10.0

```
    ]  
  }  
}
```

Setelah selesai, pilih Selanjutnya.

6. Opsi A - Memilih Layanan AWS - AWS Lambda sebagai target

Pada halaman Pilih target, lakukan hal berikut:

- a. Untuk jenis Target, pilih Layanan AWS.
- b. Untuk Pilih target, pilih Fungsi Lambda. Kemudian, untuk Fungsi, pilih fungsi Lambda yang ingin Anda kirim acara pencarian.
- c. Untuk Konfigurasi versi/alias, masukkan pengaturan versi atau alias untuk fungsi Lambda target.
- d. (Opsional) Untuk Pengaturan tambahan, masukkan pengaturan khusus untuk menentukan data peristiwa mana yang ingin Anda kirim ke fungsi Lambda. Anda juga dapat menentukan cara menangani peristiwa yang tidak berhasil dikirim ke fungsi.
- e. Setelah selesai, pilih Selanjutnya.

7. Opsi B - Memilih topik SNS sebagai target

Pada halaman Pilih target, lakukan hal berikut:

- a. Untuk jenis Target, pilih Layanan AWS.
- b. Untuk Pilih target, pilih Topik SNS. Kemudian, untuk lokasi Target, pilih opsi yang sesuai berdasarkan lokasi target Anda. Untuk Topik, pilih nama topik SNS yang Anda buat.
- c. Perluas Pengaturan tambahan. Untuk Konfigurasi input target, pilih Trafo input.
- d. Pilih Konfigurasikan transformator input.
- e. Salin kode berikut dan tempel di bidang Input Path di bawah bagian Transformator input target.

```
{  
  "severity": "$.detail.severity",  
  "Account_ID": "$.detail.accountId",  
  "Finding_ID": "$.detail.id",  
  "Finding_Type": "$.detail.type",  
  "region": "$.region",  
  "Finding_description": "$.detail.description"
```

```
}
```

- f. Salin kode berikut dan tempel ke bidang Template untuk memformat email.

```
"You have a severity <severity> GuardDuty finding type <Finding_Type> in the  
<region> Region."  
"Finding Description:"  
"<Finding_description>. "  
"For more details open the GuardDuty console at https://  
console.aws.amazon.com/guardduty/home?region=<region>#/findings?search=id  
%3D<Finding_ID>"
```

8. Pada halaman Konfigurasi tag, secara opsional masukkan satu atau beberapa tag untuk ditetapkan ke aturan. Lalu pilih Selanjutnya.
9. Pada halaman Tinjau dan buat, tinjau setelan aturan dan verifikasi apakah sudah benar.

Untuk mengubah pengaturan, pilih Edit di bagian yang berisi pengaturan, lalu masukkan pengaturan yang benar. Anda juga dapat menggunakan tab navigasi untuk membuka halaman yang berisi pengaturan.

10. Setelah Anda selesai memverifikasi pengaturan, pilih Buat aturan.

API

Prosedur berikut menunjukkan cara menggunakan AWS CLI perintah untuk membuat EventBridge aturan dan target untuk GuardDuty. Secara khusus, prosedur ini menunjukkan kepada Anda cara membuat aturan yang memungkinkan EventBridge untuk mengirim peristiwa untuk semua temuan yang GuardDuty dihasilkan ke AWS Lambda fungsi sebagai target aturan.

Note

Dalam contoh ini, kita menggunakan fungsi Lambda sebagai target untuk aturan yang memicu. EventBridge Anda juga dapat mengonfigurasi AWS sumber daya lain sebagai target yang akan dipicu EventBridge. GuardDuty dan EventBridge mendukung jenis target berikut - EC2 instans Amazon, aliran Amazon Kinesis, AWS Step Functions tugas Amazon ECS, mesin status, perintahrun, dan target bawaan. Untuk informasi selengkapnya, lihat [PutTargets](#) di Referensi Amazon EventBridge API.

Untuk membuat aturan dan target

1. Untuk membuat aturan yang memungkinkan EventBridge untuk mengirim peristiwa untuk semua temuan yang GuardDuty dihasilkan, jalankan perintah EventBridge CLI berikut.

```
aws events put-rule --name your-rule-name --event-pattern "{\"source\":  
[\"aws.guarddduty\"]}"
```

Anda dapat menyesuaikan aturan Anda lebih lanjut sehingga menginstruksikan EventBridge untuk mengirim peristiwa hanya untuk subset dari temuan GuardDuty yang dihasilkan. Subset ini didasarkan pada atribut temuan atau atribut yang ditentukan dalam aturan. Misalnya, gunakan perintah CLI berikut untuk membuat aturan yang memungkinkan EventBridge untuk hanya mengirim peristiwa untuk GuardDuty temuan dengan tingkat keparahan 5 atau 8:

```
aws events put-rule --name your-rule-name --event-pattern "{\"source\":  
[\"aws.guarddduty\"],\"detail-type\":[\"GuardDuty Finding\"],\"detail\":  
{\"severity\":[5,8]}}"
```

Untuk tujuan ini, Anda dapat menggunakan salah satu nilai properti yang tersedia di JSON untuk GuardDuty temuan.

2. Untuk melampirkan fungsi Lambda sebagai target untuk aturan yang Anda buat di langkah 1, jalankan perintah CLI berikut CloudWatch .

```
aws events put-targets --rule your-target-name --targets  
Id=1,Arn=arn:aws:lambda:us-east-1:111122223333:function:your_function
```

Pastikan untuk mengganti perintah *your-target-name* di atas dengan fungsi Lambda Anda yang sebenarnya untuk acara tersebut. GuardDuty

3. Untuk menambahkan izin yang diperlukan untuk memanggil target, jalankan perintah CLI Lambda berikut.

```
aws lambda add-permission --function-name your-target-name --statement-id 1 --  
action 'lambda:InvokeFunction' --principal events.amazonaws.com
```

Pastikan untuk mengganti perintah *your_function* di atas dengan fungsi Lambda Anda yang sebenarnya untuk acara tersebut. GuardDuty

EventBridge aturan untuk lingkungan GuardDuty multi-akun

Saat menggunakan akun GuardDuty administrator yang didelegasikan, Anda dapat melihat peristiwa yang dihasilkan di akun anggota dan mengambil tindakan menggunakan aplikasi dan layanan lain. EventBridge aturan di akun administrator Anda akan dipicu berdasarkan temuan yang berlaku dari akun anggota Anda. Jika Anda mengatur pencarian notifikasi melalui EventBridge akun administrator Anda, Anda akan menerima pemberitahuan temuan dari akun dan akun anggota Anda. Misalnya, Anda dapat menggunakan EventBridge untuk mengirim jenis temuan tertentu ke fungsi Lambda yang memproses dan mengirim data ke sistem manajemen insiden dan peristiwa keamanan (SIEM) Anda.

Anda dapat mengidentifikasi akun anggota tempat GuardDuty temuan itu berasal menggunakan `accountId` bidang detail JSON temuan. Untuk membuat aturan acara khusus untuk akun anggota tertentu, buat aturan baru dan gunakan templat berikut dalam pola Acara. Ganti **123456789012** dengan akun anggota yang ingin Anda picu acara. `accountId`

```
{
  "source": [
    "aws.guarddduty"
  ],
  "detail-type": [
    "GuardDuty Finding"
  ],
  "detail": {
    "accountId": [
      "123456789012"
    ]
  }
}
```

Note

Contoh ini membuat aturan yang cocok dengan semua temuan dari ID akun yang ditentukan. Anda dapat menyertakan beberapa akun IDs dengan memisahkannya dengan koma, mengikuti sintaks JSON.

Memahami CloudWatch Log dan alasan melewatkan sumber daya selama Perlindungan Malware untuk EC2 pemindaian

GuardDuty Perlindungan Malware untuk EC2 mempublikasikan peristiwa ke grup CloudWatch log Amazon Anda/`aws/guardduty/malware-scan-events`. Untuk setiap peristiwa yang terkait dengan pemindaian malware, Anda dapat memantau status dan hasil pemindaian sumber daya yang terkena dampak. EC2 Sumber daya Amazon tertentu dan volume Amazon EBS mungkin telah dilewati selama Perlindungan Malware untuk EC2 pemindaian.

Mengaudit CloudWatch Log dalam Perlindungan GuardDuty Malware untuk EC2

Ada tiga jenis peristiwa pemindaian yang didukung dalam grup log/`aws/guardduty/malware-scan-events` CloudWatch .

Perlindungan Malware untuk nama acara EC2 pemindaian	Penjelasan
EC2_SCAN_STARTED	Dibuat saat Perlindungan GuardDuty Malware untuk EC2 memulai proses pemindaian malware, seperti bersiap untuk mengambil snapshot dari volume EBS.
EC2_SCAN_COMPLETED	Dibuat saat Perlindungan GuardDuty Malware untuk EC2 pemindaian selesai untuk setidaknya satu volume EBS dari sumber daya yang terkena dampak. Acara ini juga mencakup <code>snapshotId</code> yang termasuk dalam volume EBS yang dipindai. Setelah pemindaian selesai, hasil pemindaian akan menjadi <code>CLEAN</code> , <code>THREATS_FOUND</code> , atau <code>NOT_SCANNED</code> .
EC2_SCAN_SKIPPED	Dibuat saat Perlindungan GuardDuty Malware untuk EC2 pemindaian melewati semua volume EBS dari sumber daya yang terkena dampak. Untuk mengidentifikasi alasan lewati, pilih

Perlindungan Malware untuk nama acara EC2 pemindaian

Penjelasan

acara yang sesuai, dan lihat detailnya. Untuk informasi lebih lanjut tentang alasan lewati, lihat [Alasan melewati sumber daya selama pemindaian malware](#) di bawah.

Note

Jika Anda menggunakan AWS Organizations, CloudWatch log peristiwa dari akun anggota di Organizations akan dipublikasikan ke akun administrator dan grup log akun anggota.

Pilih metode akses pilihan Anda untuk melihat dan menanyakan CloudWatch acara.

Console

1. Masuk ke AWS Management Console dan buka CloudWatch konsol di <https://console.aws.amazon.com/cloudwatch/>.
2. Di panel navigasi, di bawah Log, pilih Grup log. Pilih grup log/aws/guardduty/malware-scan-events untuk melihat peristiwa pemindaian untuk Perlindungan GuardDuty Malware. EC2

Untuk menjalankan kueri, pilih Wawasan Log.

Untuk informasi tentang menjalankan kueri, lihat [Menganalisis data CloudWatch log dengan Wawasan Log](#) di Panduan CloudWatch Pengguna Amazon.

3. Pilih Pindai ID untuk memantau detail sumber daya yang terkena dampak dan temuan malware. Misalnya, Anda dapat menjalankan kueri berikut untuk memfilter peristiwa CloudWatch log dengan menggunakan scanId. Pastikan untuk menggunakan valid Anda sendiri *scan-id*.

```
fields @timestamp, @message, scanRequestDetails.scanId as scanId
| filter scanId like "77a6f6115da4bd95f4e4ca398492bcc0"
| sort @timestamp asc
```

API/CLI

- Untuk bekerja dengan grup log, lihat [Cari entri log menggunakan AWS CLI di Panduan CloudWatch Pengguna Amazon](#).

Pilih grup log/aws/guardduty/malware-scan-events untuk melihat peristiwa pemindaian untuk Perlindungan GuardDuty Malware. EC2

- Untuk melihat dan memfilter peristiwa log, lihat [GetLogEvents](#) dan [FilterLogEvents](#), masing-masing, di Referensi Amazon CloudWatch API.

GuardDuty Perlindungan Malware untuk retensi EC2 log

Periode penyimpanan log default untuk grup log/aws/guardduty/malware-scan-events adalah 90 hari, setelah itu peristiwa log dihapus secara otomatis. Untuk mengubah kebijakan penyimpanan log untuk grup CloudWatch log Anda, lihat [Mengubah penyimpanan data CloudWatch log di Log](#) di Panduan CloudWatch Pengguna Amazon, atau [PutRetentionPolicy](#) di Referensi CloudWatch API Amazon.

Alasan melewatkan sumber daya selama pemindaian malware

Dalam peristiwa yang terkait dengan pemindaian malware, EC2 sumber daya tertentu dan volume EBS mungkin telah dilewati selama proses pemindaian. Tabel berikut mencantumkan alasan mengapa Perlindungan GuardDuty Malware untuk EC2 tidak memindai sumber daya. Jika berlaku, gunakan langkah-langkah yang diusulkan untuk mengatasi masalah ini, dan pindai sumber daya ini saat berikutnya Perlindungan GuardDuty Malware untuk EC2 memulai pemindaian malware. Masalah lain digunakan untuk memberi tahu Anda tentang jalannya acara dan tidak dapat ditindaklanjuti.

Alasan untuk melewatkan	Penjelasan	Langkah-langkah yang diusulkan	
RESOURCE_NOT_FOUND	Yang resourceArn disediakan untuk memulai pemindaian malware sesuai permintaan tidak ditemukan di lingkungan Anda AWS .	Validasi resourceArn EC2 instans Amazon atau beban kerja container Anda, dan coba lagi.	

Alasan untuk melewati	Penjelasan	Langkah-langkah yang diusulkan	
ACCOUNT_I NELIGIBLE	ID AWS akun tempat Anda mencoba memulai pemindaian malware On-Demand belum diaktifkan. GuardDuty	Verifikasi yang GuardDuty diaktifkan untuk AWS akun ini. Saat Anda mengaktifkan GuardDuty dalam yang baru, Wilayah AWS mungkin diperlukan waktu hingga 20 menit untuk menyinkronkan.	

Alasan untuk melewati	Penjelasan	Langkah-langkah yang diusulkan	
UNSUPPORTED_KEY_ENCRYPTION	GuardDuty Perlindungan Malware untuk EC2 mendukung volume yang tidak terenkripsi dan dienkripsi dengan kunci yang dikelola pelanggan. Itu tidak mendukung pemindaian volume EBS yang dienkripsi menggunakan enkripsi Amazon EBS. Saat ini, ada perbedaan regional di mana alasan lompatan ini tidak berlaku. Untuk informasi lebih lanjut tentang ini Wilayah AWS, lihat Ketersediaan fitur khusus wilayah.	Ganti kunci enkripsi Anda dengan kunci yang dikelola pelanggan. Untuk informasi selengkapanya tentang jenis enkripsi yang GuardDuty mendukung, lihat Volume Amazon EBS yang didukung untuk pemindaian malware.	

Alasan untuk melewati	Penjelasan	Langkah-langkah yang diusulkan	
EXCLUDED_BY_SCAN_SETTINGS	Volume EC2 instans atau EBS dikecualikan selama pemindaian malware. Ada dua kemungkinan - baik tag ditambahkan ke daftar inklusi tetapi sumber daya tidak terkait dengan tag ini, tag ditambahkan ke daftar pengecualian dan sumber daya dikaitkan dengan tag ini, atau GuardDuty Excluded tag diatur true untuk sumber daya ini.	Perbarui opsi pemindaian atau tag yang terkait dengan EC2 sumber daya Amazon Anda. Untuk informasi selengkapnya, lihat Opsional pindai dengan tag yang ditentukan pengguna .	
UNSUPPORTED_VOLUME_SIZE	Volumenya lebih besar dari 2048 GB.	Tidak bisa ditindaklanjuti.	
NO_VOLUME_S_ATTACHED	GuardDuty Perlindungan Malware untuk EC2 menemukan instans di akun Anda tetapi tidak ada volume EBS yang dilampirkan ke instance ini untuk melanjutkan pemindaian.	Tidak bisa ditindaklanjuti.	

Alasan untuk melewati	Penjelasan	Langkah-langkah yang diusulkan	
UNABLE_TO_SCAN	Ini adalah kesalahan layanan internal.	Tidak bisa ditindaklanjuti.	
SNAPSHOT_NOT_FOUND	Snapshot yang dibuat dari volume EBS dan dibagikan dengan akun layanan tidak ditemukan, dan Perlindungan GuardDuty Malware untuk EC2 tidak dapat melanjutkan pemindaian.	Periksa CloudTrail untuk memastikan bahwa snapshot tidak sengaja dihapus.	
SNAPSHOT_QUOTA_REACHED	Anda telah mencapai volume maksimum yang diizinkan untuk snapshot untuk setiap Wilayah. Ini mencegah tidak hanya mempertahankan tetapi juga membuat snapshot baru.	Anda dapat menghapus snapshot lama atau meminta peningkatan kuota. Anda dapat melihat batas default untuk Snapshot per Wilayah dan cara meminta peningkatan kuota di bawah Kuota layanan di Panduan Referensi AWS Umum.	

Alasan untuk melewati	Penjelasan	Langkah-langkah yang diusulkan	
MAX_NUMBER_OF_ATTACHED_VOLUMES_REACHED	Lebih dari 11 volume EBS dilampirkan ke sebuah EC2 instans. GuardDuty Perlindungan Malware untuk EC2 memindai 11 volume EBS pertama, diperoleh dengan menyortir menurut abjad. <code>deviceName</code>	Tidak bisa ditindaklanjuti.	

Alasan untuk melewati	Penjelasan	Langkah-langkah yang diusulkan	
UNSUPPORTED_PRODUCT_CODE_TYPE	GuardDuty dapat memindai sebagian besar contoh dengan <code>productCode asmarketplace</code> . Beberapa instans pasar mungkin tidak memenuhi syarat untuk pemindaian. GuardDuty akan melewati contoh seperti itu dan mencatat alasannya sebagai <code>UNSUPPORTED_PRODUCT_CODE_TYPE</code> . Dukungan ini bervariasi di AWS GovCloud (US) dan Wilayah Tiongkok. Untuk informasi selengkapnya, lihat Ketersediaan fitur khusus wilayah. Untuk informasi selengkapnya, lihat Dibayar AMIs di Panduan EC2 Pengguna Amazon. Untuk informasi tentang <code>productCode</code> , lihat ProductCo	Tidak bisa ditindaklanjuti.	

Alasan untuk melewati	Penjelasan	Langkah-langkah yang diusulkan	
	dedi Referensi Amazon EC2 API.		

Melaporkan positif palsu dalam Perlindungan Malware untuk EC2

GuardDuty Perlindungan Malware untuk EC2 pemindaian dapat mengidentifikasi file yang tidak berbahaya di EC2 instans Amazon atau beban kerja kontainer Anda sebagai berbahaya atau berbahaya. Untuk meningkatkan pengalaman Anda dengan Perlindungan Malware untuk EC2 dan GuardDuty layanan, Anda dapat melaporkan hasil positif palsu jika Anda yakin bahwa file yang diidentifikasi berbahaya atau berbahaya selama pemindaian sebenarnya tidak mengandung malware.

Untuk melaporkan hasil pemindaian EC2 malware Amazon sebagai positif palsu

Untuk memulai proses, hubungi Dukungan. Gunakan langkah-langkah berikut untuk memberikan detail tentang objek S3 yang dipindai:

1. Masuk ke AWS Management Console dan buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.
2. Pilih pemindaian EC2 malware.
3. Pilih pemindaian untuk melihat ID Temuannya.
4. Berikan ID Finding. Anda juga harus memberikan hash SHA-256 dari file tersebut. Ini diperlukan untuk memastikan bahwa Perlindungan GuardDuty Malware for EC2 telah menerima file yang benar.
5. Dukungan Tim akan memberi Anda URL presigned Amazon Simple Storage Service (Amazon S3) yang dapat Anda gunakan untuk mengunggah file yang berpotensi berbahaya dan hash SHA-256. Untuk informasi tentang langkah-langkah untuk mengunggah objek yang dipindai, lihat [Mengunggah objek dengan presigned URLs di Panduan](#) Pengguna Amazon S3.
6. Setelah Anda mengunggah file, beri tahu Dukungan tim.

Dukungan Akan memberikan pengakuan setelah menerima file. Anggota tim GuardDuty layanan akan menganalisis kiriman Anda, dan mengambil langkah-langkah yang tepat untuk meningkatkan pengalaman Anda dengan Perlindungan Malware untuk EC2 dan GuardDuty layanan. Dukungan Tim akan terus memberikan pembaruan status pada kasus Anda. GuardDuty menyimpan objek S3 Anda selama tidak lebih dari 30 hari.

Melaporkan hasil pemindaian objek S3 sebagai positif palsu dalam Perlindungan Malware untuk S3

Perlindungan Malware untuk pemindaian S3 dapat mengidentifikasi objek sebagai berpotensi berbahaya atau berbahaya. Jika Anda yakin bahwa objek S3 yang ditunjukkan tidak mengandung malware, laporkan hasil pemindaian malware ini sebagai positif palsu.

Anda dapat mengirimkan laporan positif palsu bahkan ketika Anda menggunakan Perlindungan Malware untuk S3 secara independen. Dalam hal GuardDuty ini, tidak dirancang untuk menghasilkan temuan. Untuk informasi tentang memeriksa status pemindaian dan status hasil, lihat [Memantau pemindaian objek S3](#).

Untuk melaporkan hasil pemindaian malware objek S3 sebagai positif palsu

Untuk memulai proses, hubungi Dukungan. Gunakan langkah-langkah berikut untuk memberikan detail tentang objek S3 yang dipindai:

1. Masuk ke AWS Management Console dan buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.
2. Tergantung pada kasus penggunaan Anda, pilih langkah-langkah yang sesuai:

Using Malware Protection for S3 with GuardDuty

1. Di panel navigasi, pilih Temuan.
2. Pada halaman Temuan, pilih temuan positif palsu untuk melihat detailnya.
3. Dengan memeriksa detail temuan, berikan Finding ID, Region, Nama bucket S3 yang dilindungi, dan Kunci objek yang dipindai.

Dari detail jalur Item, berikan Hash objek. Ini diperlukan untuk memastikan bahwa GuardDuty telah menerima file yang benar.

Using Malware Protection for S3 independently

Berikan nama bucket S3 yang dilindungi, nama objek yang dipindai, dan Wilayah AWS

3. Dukungan Tim akan memberi Anda URL presigned Amazon Simple Storage Service (Amazon S3) yang dapat Anda gunakan untuk mengunggah file dan hash yang berpotensi berbahaya. Untuk informasi tentang langkah-langkah untuk mengunggah objek yang dipindai, lihat [Mengunggah objek dengan presigned URLs di Panduan Pengguna Amazon S3](#).

4. Setelah mengunggah objek S3, beri tahu tim. Dukungan

Surat Dukungan wasiat memberikan pengakuan menerima objek. Anggota tim GuardDuty layanan akan menganalisis kiriman Anda, dan mengambil langkah-langkah yang tepat untuk meningkatkan pengalaman Anda dengan Perlindungan Malware untuk S3 dan layanan. GuardDuty Dukungan Tim akan terus memberikan pembaruan status pada kasus Anda. GuardDuty menyimpan objek S3 Anda selama tidak lebih dari 30 hari.

Memulihkan temuan GuardDuty keamanan yang terdeteksi

Amazon GuardDuty menghasilkan [temuan](#) yang menunjukkan temuan keamanan potensial yang terkait dengan deteksi ancaman GuardDuty dasar dan rencana perlindungan khusus. Bagian berikut menjelaskan langkah-langkah perbaikan yang disarankan untuk skenario ini. Jika ada skenario remediasi alternatif, skenario tersebut akan dijelaskan dalam deskripsi untuk setiap jenis temuan. Anda dapat mengakses informasi selengkapnya tentang tipe temuan dengan memilihnya dari [tabel Tipe temuan aktif](#).

Daftar Isi

- [Memperbaiki instans Amazon yang berpotensi dikompromikan EC2](#)
- [Memperbaiki bucket S3 yang berpotensi dikompromikan](#)
- [Memperbaiki objek S3 yang berpotensi berbahaya](#)
- [Memulihkan cluster ECS yang berpotensi dikompromikan](#)
- [Memulihkan kredensi yang berpotensi dikompromikan AWS](#)
- [Memulihkan wadah mandiri yang berpotensi dikompromikan](#)
- [Remediasi temuan Perlindungan EKS](#)
- [Remediasi temuan Runtime Monitoring](#)
- [Memulihkan database yang berpotensi dikompromikan](#)
- [Memperbaiki fungsi Lambda yang berpotensi dikompromikan](#)

Memperbaiki instans Amazon yang berpotensi dikompromikan EC2

Saat GuardDuty menghasilkan [jenis pencarian yang menunjukkan EC2 sumber daya Amazon yang berpotensi dikompromikan](#), [Sumber](#) Daya Anda akan menjadi Instance. Jenis temuan potensial bisa [EC2 menemukan jenis](#), [GuardDuty Jenis penemuan Runtime Monitoring](#), atau [Perlindungan Malware untuk EC2 menemukan jenis](#). Jika perilaku yang menyebabkan temuan itu diharapkan di lingkungan Anda, maka pertimbangkan untuk menggunakannya [Aturan penekanan](#).

Lakukan langkah-langkah berikut untuk memulihkan instans Amazon EC2 yang berpotensi dikompromikan:

1. Identifikasi instans Amazon EC2 yang berpotensi dikompromikan

Selidiki instans yang berpotensi disusupi untuk malware dan menghapus malware yang ditemukan. Anda dapat menggunakannya [Pemindaian malware sesuai permintaan di GuardDuty](#) untuk mengidentifikasi malware dalam EC2 contoh yang berpotensi dikompromikan, atau memeriksa [AWS Marketplace](#) untuk melihat apakah ada produk mitra yang bermanfaat untuk mengidentifikasi dan menghapus malware.

2. Isolasi instans Amazon yang berpotensi dikompromikan EC2

Jika memungkinkan, gunakan langkah-langkah berikut untuk mengisolasi instance yang berpotensi dikompromikan:

1. Buat grup keamanan Isolasi khusus. Grup keamanan isolasi seharusnya hanya memiliki akses masuk dan keluar dari alamat IP tertentu. Pastikan bahwa tidak ada aturan masuk atau keluar yang memungkinkan lalu lintas untuk `0.0.0.0/0` (`0-65535`)
2. Kaitkan grup keamanan Isolasi dengan instance ini.
3. Hapus semua asosiasi grup keamanan selain grup keamanan Isolasi yang baru dibuat dari instance yang berpotensi dikompromikan.

Note

Koneksi yang dilacak yang ada tidak akan dihentikan sebagai akibat dari perubahan kelompok keamanan - hanya lalu lintas masa depan yang akan diblokir secara efektif oleh grup keamanan baru.

Untuk informasi tentang memblokir lalu lintas lebih lanjut dari koneksi mencurigakan yang ada, lihat [Menegakkan NACLs berdasarkan jaringan IoCs untuk mencegah lalu lintas lebih lanjut](#) di Playbook Respons Insiden.

3. Identifikasi sumber aktivitas yang mencurigakan

Jika malware terdeteksi, maka berdasarkan jenis temuan di akun Anda, identifikasi dan hentikan aktivitas yang berpotensi tidak sah pada EC2 instans Anda. Ini mungkin memerlukan tindakan seperti menutup port terbuka, mengubah kebijakan akses, dan meningkatkan aplikasi untuk memperbaiki kerentanan.

Jika Anda tidak dapat mengidentifikasi dan menghentikan aktivitas yang tidak sah pada EC2 instans yang berpotensi dikompromikan, sebaiknya Anda menghentikan instans yang disusupi dan menggantinya dengan EC2 instance baru sesuai kebutuhan. Berikut ini adalah sumber daya tambahan untuk mengamankan EC2 instans Anda:

- Bagian Keamanan dan Jaringan dalam [Praktik terbaik untuk Amazon EC2](#)
- [Grup EC2 keamanan Amazon untuk instance Linux](#).
- [Keamanan di Amazon EC2](#)
- [Kiat untuk mengamankan EC2 instans Anda \(Linux\)](#).
- [AWS praktik terbaik keamanan](#)
- [AWS Panduan Teknis Respons Insiden Keamanan](#).

4. Jelajahi AWS re:Post

Jelajahi [AWS re:Post](#) untuk bantuan lebih lanjut.

5. Kirim permintaan dukungan teknis

Jika Anda adalah pelanggan paket dukungan premium, Anda dapat mengirimkan permintaan [dukungan teknis](#).

Memperbaiki bucket S3 yang berpotensi dikompromikan

Saat GuardDuty menghasilkan [GuardDuty Jenis temuan Perlindungan S3](#), ini menunjukkan bahwa ember Amazon S3 Anda telah disusupi. Jika perilaku yang menyebabkan temuan itu diharapkan di lingkungan Anda, maka pertimbangkan untuk membuat [Aturan penekanan](#). Jika perilaku ini tidak diharapkan, ikuti langkah-langkah yang disarankan ini untuk memulihkan bucket Amazon S3 yang berpotensi dikompromikan di lingkungan Anda: AWS

1. Identifikasi sumber daya S3 yang berpotensi dikompromikan.

GuardDuty Temuan untuk S3 akan mencantumkan bucket S3 terkait, Nama Sumber Daya Amazon (ARN), dan pemiliknya dalam detail temuan.

2. Identifikasi sumber aktivitas mencurigakan dan panggilan API yang digunakan.

Panggilan API yang digunakan akan terdaftar sebagai API dalam detail temuan. Sumber akan menjadi prinsipal IAM (baik peran IAM, pengguna, atau akun) dan rincian identifikasi akan tercantum dalam temuan. Bergantung pada jenis sumbernya, alamat IP jarak jauh atau info domain sumber akan tersedia dan dapat membantu Anda mengevaluasi apakah sumber tersebut diotorisasi. Jika temuan melibatkan kredensial dari EC2 instance Amazon, detail untuk sumber daya itu juga akan disertakan.

3. Tentukan apakah sumber panggilan diberi wewenang untuk mengakses sumber daya yang diidentifikasi.

Misalnya, pertimbangkan hal berikut:

- Jika pengguna IAM terlibat, mungkinkah kredensialnya berpotensi dikompromikan? Untuk informasi selengkapnya, lihat [Memulihkan kredensi yang berpotensi dikompromikan AWS](#).
- Jika API dipanggil dari prinsipal yang sebelumnya tidak memiliki riwayat memanggil tipe API ini, apakah sumber ini memerlukan izin akses untuk operasi ini? Dapatkah izin bucket dibatasi secara lebih lanjut?
- Jika akses terlihat dari nama pengguna ANONYMOUS_PRINCIPAL dengan tipe pengguna dari AWSAccount, ini menunjukkan bahwa bucket bersifat publik dan telah diakses. Haruskah bucket ini dibuat publik? Jika tidak, tinjau rekomendasi keamanan di bawah ini untuk solusi alternatif untuk berbagi sumber daya S3.
- Jika akses adalah PreflightRequest panggilan yang berhasil dilihat dari nama pengguna ANONYMOUS_PRINCIPAL dengan tipe pengguna, AWSAccount ini menunjukkan bucket memiliki kumpulan kebijakan berbagi sumber daya lintas asal (CORS). Haruskah ember ini memiliki kebijakan CORS? Jika tidak, pastikan bucket tidak secara tidak sengaja dipublikasikan dan tinjau rekomendasi keamanan di bawah ini untuk solusi alternatif untuk berbagi sumber daya S3. Untuk informasi selengkapnya tentang CORS, lihat [Menggunakan berbagi sumber daya lintas asal \(CORS\) di panduan](#) pengguna S3.

4. Tentukan apakah bucket S3 berisi data sensitif.

Gunakan [Amazon Macie](#) untuk menentukan apakah bucket S3 berisi data sensitif, seperti informasi identitas pribadi (PII), data keuangan, atau kredensial. Jika penemuan data sensitif otomatis diaktifkan untuk akun Macie Anda, tinjau detail bucket S3 untuk mendapatkan pemahaman yang lebih baik tentang konten bucket S3 Anda. Jika fitur ini dinonaktifkan untuk akun Macie Anda, kami sarankan untuk menyalakannya untuk mempercepat penilaian Anda. Atau, Anda dapat membuat dan menjalankan tugas penemuan data sensitif untuk memeriksa objek bucket S3 untuk data sensitif. Untuk informasi selengkapnya, lihat [Menemukan data sensitif dengan Macie](#).

Jika akses diotorisasi, Anda dapat mengabaikan temuan tersebut. <https://console.aws.amazon.com/guardduty/> Konsol memungkinkan Anda untuk mengatur aturan untuk sepenuhnya menekan temuan individu sehingga tidak lagi muncul. Untuk informasi selengkapnya, lihat [Aturan penindasan di GuardDuty](#).

Jika Anda menentukan bahwa data S3 Anda telah diekspos atau diakses oleh pihak yang tidak berwenang, tinjau rekomendasi keamanan S3 berikut untuk memperketat izin dan membatasi akses. Solusi perbaikan yang tepat akan bergantung pada kebutuhan lingkungan spesifik Anda.

Rekomendasi berdasarkan kebutuhan akses bucket S3 tertentu

Daftar berikut memberikan rekomendasi berdasarkan kebutuhan akses bucket Amazon S3 tertentu:

- Untuk cara terpusat untuk membatasi akses publik ke penggunaan data S3 Anda, S3 memblokir akses publik. Blokir pengaturan akses publik dapat diaktifkan untuk titik akses, bucket, dan AWS Akun melalui empat pengaturan berbeda untuk mengontrol perincian akses. Untuk informasi selengkapnya, lihat [Memblokir setelan akses publik](#) di Panduan Pengguna Amazon S3.
- AWS Kebijakan akses dapat digunakan untuk mengontrol bagaimana pengguna IAM dapat mengakses sumber daya Anda atau bagaimana bucket Anda dapat diakses. Untuk informasi selengkapnya, lihat [Menggunakan kebijakan bucket dan kebijakan pengguna](#) di Panduan Pengguna Amazon S3.

Selain itu, Anda dapat menggunakan Titik Akhir Virtual Private Cloud (VPC) dengan kebijakan bucket S3 untuk membatasi akses ke titik akhir VPC tertentu. Untuk informasi selengkapnya, lihat [Mengontrol akses dari titik akhir VPC dengan kebijakan bucket di Panduan](#) Pengguna Amazon S3

- Untuk mengizinkan akses sementara ke objek S3 Anda ke entitas tepercaya di luar akun Anda, Anda dapat membuat URL yang ditandatangani sebelumnya melalui S3. Akses ini dibuat menggunakan kredensial akun Anda dan bergantung pada kredensial yang digunakan dapat bertahan 6 jam hingga 7 hari. Untuk informasi selengkapnya, lihat [Menggunakan presigned URLs untuk mengunduh dan mengunggah objek](#) di Panduan Pengguna Amazon S3.
- Untuk kasus penggunaan yang mengharuskan berbagi objek S3 antara sumber yang berbeda, Anda dapat menggunakan S3 Access Points untuk membuat set izin yang membatasi akses hanya untuk mereka yang berada dalam jaringan pribadi Anda. Untuk informasi selengkapnya, lihat [Mengelola akses ke kumpulan data bersama dengan titik akses](#) di Panduan Pengguna Amazon S3.
- Untuk memberikan akses ke sumber daya S3 ke AWS Akun lain dengan aman, Anda dapat menggunakan daftar kontrol akses (ACL), untuk informasi selengkapnya lihat [Ringkasan daftar kontrol akses \(ACL\) di Panduan Pengguna](#) Amazon S3.

Untuk informasi selengkapnya tentang opsi keamanan S3, lihat [Praktik terbaik keamanan untuk Amazon S3](#) di Panduan Pengguna Amazon S3.

Memperbaiki objek S3 yang berpotensi berbahaya

Saat GuardDuty menghasilkan [Perlindungan Malware untuk tipe pencarian S3](#), ini menunjukkan bahwa objek yang baru diunggah di bucket Amazon S3 Anda berisi malware. Jenis sumber daya adalah S3Object.

Gunakan langkah-langkah yang disarankan berikut untuk berpotensi memulihkan temuan yang dihasilkan:

1. Identifikasi objek S3 yang berpotensi berbahaya dengan memeriksa S3 yang ObjectDetails terkait dengan temuan tersebut.
2. Isolasi objek S3 yang terkena dampak. Jika Anda telah mengaktifkan penandaan pada saat mengaktifkan Perlindungan Malware untuk S3 untuk bucket Amazon S3 terkait, GuardDuty harus menetapkan tag Berbahaya ke objek ini. Gunakan kontrol akses berbasis tag (TBAC) untuk membatasi akses ke objek S3 ini. Untuk informasi selengkapnya, lihat [Menggunakan kontrol akses berbasis tag \(TBAC\)](#).

Atau, jika Anda tidak memerlukan objek ini lagi, Anda juga dapat memilih untuk menghapusnya atau memindahkannya ke ember S3 yang terisolasi. Untuk informasi tentang pertimbangan untuk menghapus objek S3, lihat [Menghapus](#) objek di Panduan Pengguna Amazon S3.

Memulihkan cluster ECS yang berpotensi dikompromikan

Saat GuardDuty menghasilkan [jenis pencarian yang menunjukkan sumber daya Amazon ECS yang berpotensi dikompromikan, maka Sumber](#) Daya Anda akan menjadi. ECSCluster Jenis temuan potensial bisa [GuardDuty Jenis penemuan Runtime Monitoring](#) atau [Perlindungan Malware untuk EC2 menemukan jenis](#). Jika perilaku yang menyebabkan temuan itu diharapkan di lingkungan Anda, maka pertimbangkan untuk menggunakannya [Aturan penekanan](#).

Ikuti langkah-langkah yang disarankan ini untuk memulihkan klaster Amazon ECS yang berpotensi dikompromikan di lingkungan Anda: AWS

1. Identifikasi cluster ECS yang berpotensi dikompromikan.

Perlindungan GuardDuty Malware untuk EC2 menemukan ECS menyediakan detail cluster ECS di panel detail temuan.

2. Evaluasi sumber malware

Evaluasi apakah malware yang terdeteksi ada di gambar wadah. Jika malware ada di gambar, identifikasi semua tugas lain yang berjalan menggunakan gambar ini. Untuk informasi tentang menjalankan tugas, lihat [ListTasks](#).

3. Mengisolasi tugas yang berpotensi terkena dampak

Mengisolasi tugas yang terkena dampak dengan menolak semua lalu lintas masuk dan keluar ke tugas. Menyangkal semua aturan lalu lintas dapat membantu Anda menghentikan serangan yang sudah berlangsung, dengan memutuskan semua koneksi ke tugas.

Jika akses diotorisasi, Anda dapat mengabaikan temuan tersebut. <https://console.aws.amazon.com/guardduty/> Konsol memungkinkan Anda untuk mengatur aturan untuk sepenuhnya menekan temuan individu sehingga tidak lagi muncul. Untuk informasi selengkapnya, lihat [Aturan penindasan di GuardDuty](#).

Memulihkan kredensi yang berpotensi dikompromikan AWS

Saat GuardDuty menghasilkan [Tipe temuan IAM](#), ini menunjukkan bahwa AWS kredensial Anda telah disusupi. Jenis Sumber Daya yang berpotensi dikompromikan adalah AccessKey.

Untuk memulihkan kredensial yang berpotensi dikompromikan di AWS lingkungan Anda, lakukan langkah-langkah berikut:

1. Identifikasi entitas IAM yang berpotensi dikompromikan dan panggilan API yang digunakan.

Panggilan API yang digunakan akan terdaftar sebagai API dalam detail temuan. Entitas IAM (baik peran IAM atau pengguna) dan informasi pengenalanannya akan dicantumkan di bagian Sumber Daya dari rincian temuan. Tipe entitas IAM yang terlibat dapat ditentukan oleh bidang Tipe Pengguna, nama entitas IAM akan berada di bidang Nama pengguna. Tipe entitas IAM yang terlibat dalam temuan juga dapat ditentukan oleh Access key ID yang digunakan.

Untuk kunci yang diawali dengan AKIA:

Jenis kunci ini adalah kredensi jangka panjang yang dikelola pelanggan yang terkait dengan pengguna IAM atau. Pengguna root akun AWS Untuk informasi tentang mengelola kunci akses untuk pengguna IAM, lihat [Mengelola kunci akses untuk pengguna IAM](#).

Untuk kunci yang diawali dengan ASIA:

Tipe kunci ini adalah kredensial sementara jangka pendek yang dihasilkan oleh AWS Security Token Service. Kunci ini hanya ada untuk waktu yang singkat dan tidak dapat dilihat atau dikelola di Konsol AWS Manajemen. Peran IAM akan selalu menggunakan AWS STS kredensial, tetapi juga dapat dibuat untuk Pengguna IAM, untuk informasi lebih lanjut tentang AWS STS lihat [IAM](#): Kredensial keamanan sementara.

Jika peran digunakan, bidang Nama pengguna akan menunjukkan nama dari peran yang digunakan. Anda dapat menentukan bagaimana kunci diminta AWS CloudTrail dengan memeriksa `sessionIssuer` elemen entri CloudTrail log, untuk informasi lebih lanjut lihat [IAM dan AWS STS informasi](#) di CloudTrail

2. Meninjau izin untuk entitas IAM.

Buka konsol IAM. Bergantung pada jenis entitas yang digunakan, pilih tab Pengguna atau Peran, dan temukan entitas yang terpengaruh dengan mengetikkan nama yang diidentifikasi ke dalam bidang pencarian. Gunakan tab Izin dan Penasihat Akses untuk meninjau izin efektif untuk entitas tersebut.

3. Tentukan apakah kredensial entitas IAM digunakan secara sah.

Hubungi pengguna kredensial untuk menentukan apakah aktivitas tersebut disengaja.

Misalnya, cari tahu apakah pengguna melakukan hal berikut:

- Memanggil operasi API yang tercantum dalam temuan GuardDuty
- Memanggil operasi API pada saat yang tercantum dalam temuan GuardDuty
- Memanggil operasi API dari alamat IP yang tercantum dalam temuan GuardDuty

Jika aktivitas ini adalah penggunaan AWS kredensial yang sah, Anda dapat mengabaikan temuan tersebut. GuardDuty <https://console.aws.amazon.com/guardduty/> Konsol memungkinkan Anda untuk mengatur aturan untuk sepenuhnya menekan temuan individu sehingga tidak lagi muncul. Untuk informasi selengkapnya, lihat [Aturan penindasan di GuardDuty](#).

Jika Anda tidak dapat mengonfirmasi apakah aktivitas ini adalah penggunaan yang sah, itu bisa menjadi hasil dari kompromi ke kunci akses tertentu - kredensial masuk pengguna IAM, atau mungkin keseluruhan. Akun AWS Jika Anda mencurigai kredensial Anda telah disusupi, tinjau informasi di [My Akun AWS mungkin disusupi](#) untuk memperbaiki masalah ini.

Memulihkan wadah mandiri yang berpotensi dikompromikan

Saat GuardDuty menghasilkan [tipe pencarian yang menunjukkan kontainer yang berpotensi dikompromikan](#), tipe Resource Anda akan menjadi Container. Jika perilaku yang menyebabkan temuan itu diharapkan di lingkungan Anda, maka pertimbangkan untuk menggunakannya [Aturan penekanan](#).

Untuk memulihkan kredensial yang berpotensi dikompromikan di AWS lingkungan Anda, lakukan langkah-langkah berikut:

1. Isolasi wadah yang berpotensi dikompromikan

Langkah-langkah berikut akan membantu Anda mengidentifikasi beban kerja kontainer yang berpotensi berbahaya:

- Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.
- Pada halaman Temuan, pilih temuan yang sesuai untuk melihat panel temuan.
- Di panel temuan, di bawah bagian Resource affected, Anda dapat melihat ID dan Nama container.

Isolasi wadah ini dari beban kerja kontainer lainnya.

2. Jeda wadah

Tangguhkan semua proses dalam wadah Anda.

Untuk informasi tentang membekukan wadah Anda, lihat [Menjeda wadah](#).

Hentikan wadahnya.

Jika langkah di atas gagal, dan penampung tidak berhenti, hentikan penampung agar tidak berjalan. Jika Anda telah mengaktifkan [Retensi snapshot](#) fitur tersebut, GuardDuty akan mempertahankan snapshot volume EBS Anda yang berisi malware.

Untuk informasi tentang menghentikan wadah, lihat [Menghentikan wadah](#).

3. Evaluasi keberadaan malware

Evaluasi apakah malware ada di gambar kontainer.

Jika akses diotorisasi, Anda dapat mengabaikan temuan tersebut. <https://console.aws.amazon.com/guardduty/>Konsol memungkinkan Anda untuk mengatur aturan untuk sepenuhnya menekan temuan

individu sehingga tidak lagi muncul. GuardDuty Konsol memungkinkan Anda untuk mengatur aturan untuk sepenuhnya menekan temuan individu sehingga tidak lagi muncul. Lihat informasi yang lebih lengkap di [Aturan penindasan di GuardDuty](#).

Remediasi temuan Perlindungan EKS

Amazon GuardDuty menghasilkan [temuan](#) yang menunjukkan potensi masalah keamanan Kubernetes saat Perlindungan EKS diaktifkan untuk akun Anda. Untuk informasi selengkapnya, lihat [Perlindungan EKS](#). Bagian berikut menjelaskan langkah-langkah perbaikan yang disarankan untuk skenario ini. Tindakan remediasi khusus dijelaskan dalam entri untuk jenis temuan spesifik tersebut. Anda dapat mengakses informasi selengkapnya tentang tipe temuan dengan memilihnya dari [tabel Tipe temuan aktif](#).

Jika salah satu jenis temuan Perlindungan EKS dihasilkan secara diharapkan, Anda dapat mempertimbangkan [Aturan penindasan di GuardDuty](#) untuk menambahkan untuk mencegah peringatan di masa mendatang.

Berbagai jenis serangan dan masalah konfigurasi dapat memicu temuan Perlindungan GuardDuty EKS. Panduan ini membantu Anda mengidentifikasi akar penyebab GuardDuty temuan terhadap cluster Anda dan menguraikan panduan remediasi yang tepat. Berikut ini adalah akar penyebab utama yang mengarah pada temuan GuardDuty Kubernetes:

- [Potensi masalah konfigurasi](#)
- [Memulihkan pengguna Kubernetes yang berpotensi dikompromikan](#)
- [Remediasi pod Kubernetes yang berpotensi dikompromikan](#)
- [Remediasi node Kubernetes yang berpotensi dikompromikan](#)
- [Memulihkan gambar kontainer yang berpotensi dikompromikan](#)

Note

Sebelum Kubernetes versi 1.14, `system:unauthenticated` grup ini dikaitkan dengan dan secara default. `system:discovery` `system:basic-user` ClusterRoles Ini memungkinkan akses yang tidak diinginkan dari pengguna anonim. Pembaruan klaster tidak mencabut izin ini, yang berarti bahwa meskipun Anda telah memperbarui klaster Anda ke versi 1.14 atau yang lebih baru, izin ini mungkin masih ada. Kami menyarankan Anda untuk memisahkan izin ini dari grup. `system:unauthenticated`

Untuk informasi selengkapnya tentang menghapus izin ini, lihat [Mengamankan kluster Amazon EKS dengan praktik terbaik](#) di Panduan Pengguna Amazon EKS.

Potensi masalah konfigurasi

Jika temuan menunjukkan masalah konfigurasi, lihat bagian remediasi dari temuan tersebut untuk panduan penyelesaian masalah tertentu. Untuk informasi selengkapnya, lihat jenis temuan berikut yang menunjukkan masalah konfigurasi:

- [Policy:Kubernetes/AnonymousAccessGranted](#)
- [Policy:Kubernetes/ExposedDashboard](#)
- [Policy:Kubernetes/AdminAccessToDefaultServiceAccount](#)
- [Policy:Kubernetes/KubeflowDashboardExposed](#)
- Temuan apa pun yang berakhir di SuccessfulAnonymousAccess

Memulihkan pengguna Kubernetes yang berpotensi dikompromikan

GuardDuty Temuan dapat menunjukkan pengguna Kubernetes yang disusupi ketika pengguna yang diidentifikasi dalam temuan tersebut telah melakukan tindakan API yang tidak terduga. Anda dapat mengidentifikasi pengguna di bagian detail pengguna Kubernetes dari detail temuan di konsol, atau di temuan `resource.kubernetesDetails.kubernetesUserDetails` JSON. Detail pengguna ini mencakup `user name`, `uid`, dan grup Kubernetes yang menjadi milik pengguna.

Jika pengguna mengakses beban kerja menggunakan entitas IAM, Anda dapat menggunakan `Access Key details` bagian tersebut untuk mengidentifikasi detail peran IAM atau pengguna. Lihat jenis pengguna berikut dan panduan remediasinya.

Note

Anda dapat menggunakan Amazon Detective untuk menyelidiki lebih lanjut peran IAM atau pengguna yang diidentifikasi dalam temuan tersebut. Saat melihat detail temuan di GuardDuty konsol, pilih Selidiki di Detektif. Kemudian pilih AWS pengguna atau peran dari item yang terdaftar untuk menyelidikinya di Detektif.

Admin Kubernetes bawaan — Pengguna default yang ditetapkan oleh Amazon EKS ke identitas IAM yang membuat cluster. Jenis pengguna ini diidentifikasi oleh nama `penggunakubernetes-admin`.

Untuk mencabut akses admin Kubernetes bawaan:

- Identifikasi `userType` dari Access Key details bagian.
 - Jika Peran **userType** is dan peran tersebut termasuk dalam peran EC2 instance:
 - Identifikasi contoh itu kemudian ikuti instruksi di [Memperbaiki instans Amazon yang berpotensi dikompromikan EC2](#).
 - Jika `userType` adalah Pengguna, atau Peran yang diasumsikan oleh pengguna:
 1. [Putar tombol akses](#) pengguna tersebut.
 2. Putar rahasia apa pun yang dapat diakses pengguna.
 3. Tinjau informasi di [My Akun AWS dapat dikompromikan](#) untuk rincian lebih lanjut.

Pengguna yang diautentikasi OIDC — Pengguna diberikan akses melalui penyedia OIDC. Biasanya pengguna OIDC memiliki alamat email sebagai nama pengguna. Anda dapat memeriksa apakah cluster Anda menggunakan OIDC dengan perintah berikut: `aws eks list-identity-provider-configs --cluster-name your-cluster-name`

Untuk mencabut akses pengguna yang diautentikasi OIDC:

1. Putar kredensi pengguna tersebut di penyedia OIDC.
2. Putar rahasia apa pun yang dapat diakses pengguna.

AWS-Auth ConfigMap defined user — Pengguna IAM yang diberikan akses melalui `-auth`. AWS ConfigMap Untuk informasi selengkapnya, lihat [Mengelola pengguna atau IAM role untuk klaster Anda](#) di Panduan Pengguna Amazon EKS. Anda dapat meninjau izin mereka menggunakan perintah berikut: `kubectl edit configmaps aws-auth --namespace kube-system`

Untuk mencabut akses pengguna: AWS ConfigMap

1. Gunakan perintah berikut untuk membuka ConfigMap.

```
kubectl edit configmaps aws-auth --namespace kube-system
```

2. Identifikasi peran atau entri pengguna di bagian MapRoles atau MapUsers dengan nama pengguna yang sama seperti yang dilaporkan di bagian detail pengguna Kubernetes pada temuan Anda. GuardDuty Lihat contoh berikut, di mana pengguna admin telah diidentifikasi dalam sebuah temuan.

```

apiVersion: v1
data:
  mapRoles: |
    - rolearn: arn:aws:iam::444455556666:role/eksctl-my-cluster-nodegroup-
      standard-wo-NodeInstanceRole-1WP3NUE306UCF
      user name: system:node:EC2_PrivateDNSName
      groups:
        - system:bootstrappers
        - system:nodes
  mapUsers: |
    - userarn: arn:aws:iam::123456789012:user/admin
      username: admin
      groups:
        - system:masters
    - userarn: arn:aws:iam::111122223333:user/ops-user
      username: ops-user
      groups:
        - system:masters

```

3. Hapus pengguna itu dari ConfigMap. Lihat contoh berikut di mana pengguna admin telah dihapus.

```

apiVersion: v1
data:
  mapRoles: |
    - rolearn: arn:aws:iam::111122223333:role/eksctl-my-cluster-nodegroup-
      standard-wo-NodeInstanceRole-1WP3NUE306UCF
      username: system:node:{{EC2PrivateDNSName}}
      groups:
        - system:bootstrappers
        - system:nodes
  mapUsers: |
    - userarn: arn:aws:iam::111122223333:user/ops-user
      username: ops-user
      groups:
        - system:masters

```

4. Jika userType adalah Pengguna, atau Peran yang diasumsikan oleh pengguna:
- [Putar tombol akses](#) pengguna tersebut.
 - Putar rahasia apa pun yang dapat diakses pengguna.
 - Meninjau informasi di [AWS Akun saya dapat dikompromikan](#) untuk rincian lebih lanjut.

Jika temuan tidak memiliki `resource.accessKeyDetails` bagian, pengguna adalah akun layanan Kubernetes.

Akun layanan — Akun layanan menyediakan identitas untuk pod dan dapat diidentifikasi dengan nama pengguna dengan format

berikut: `system:serviceaccount:namespace:service_account_name`.

Untuk mencabut akses ke akun layanan:

1. Putar kredensial akun layanan.
2. Tinjau panduan untuk kompromi pod di bagian berikut.

Remediasi pod Kubernetes yang berpotensi dikompromikan

Saat GuardDuty menentukan detail pod atau sumber daya beban kerja di dalam `resource.kubernetesDetails.kubernetesWorkloadDetails` bagian tersebut, pod atau sumber daya beban kerja tersebut berpotensi dikompromikan. Sebuah GuardDuty temuan dapat menunjukkan bahwa satu pod telah dikompromikan atau bahwa beberapa pod telah dikompromikan melalui sumber daya tingkat yang lebih tinggi. Lihat skenario kompromi berikut untuk panduan tentang cara mengidentifikasi pod atau pod yang telah disusupi.

Kompromi pod tunggal

Jika type bidang di dalam `resource.kubernetesDetails.kubernetesWorkloadDetails` bagian ini adalah pod, temuan tersebut mengidentifikasi satu pod. Field name adalah name dari pod dan namespace field adalah namespace-nya.

Untuk informasi tentang mengidentifikasi node pekerja yang menjalankan pod, lihat [Mengidentifikasi pod yang menyinggung dan node pekerja](#) di Panduan Praktik Terbaik Amazon EKS.

Pod dikompromikan melalui sumber daya beban kerja

Jika type bidang di dalam `resource.kubernetesDetails.kubernetesWorkloadDetails` bagian mengidentifikasi Sumber Daya Beban Kerja, seperti aDeployment, kemungkinan semua pod dalam sumber daya beban kerja tersebut telah dikompromikan.

Untuk informasi tentang mengidentifikasi semua Pod sumber daya beban kerja dan node yang dijelankannya, lihat [Mengidentifikasi Pod yang menyinggung dan node pekerja menggunakan nama beban kerja](#) di Panduan Praktik Terbaik Amazon EKS.

Pod dikompromikan melalui akun layanan

Jika GuardDuty temuan mengidentifikasi Akun Layanan di `resource.kubernetesDetails.kubernetesUserDetails` bagian tersebut, kemungkinan pod yang menggunakan akun layanan yang diidentifikasi akan disusupi. Nama pengguna yang dilaporkan oleh temuan adalah akun layanan jika memiliki format berikut: `system:serviceaccount:namespace:service_account_name`.

Untuk informasi tentang mengidentifikasi semua pod menggunakan akun layanan dan node tempat mereka berjalan, lihat [Mengidentifikasi Pod yang menyinggung dan node pekerja menggunakan nama akun layanan](#) di Panduan Praktik Terbaik Amazon EKS.

Setelah Anda mengidentifikasi semua pod yang dikompromikan dan node yang dijalankannya, lihat [Mengisolasi pod dengan membuat kebijakan jaringan yang menolak semua lalu lintas masuk dan keluar ke pod di Panduan Praktik Terbaik](#) Amazon EKS.

Untuk memulihkan pod yang berpotensi dikompromikan:

1. Identifikasi kerentanan yang mengganggu pod.
2. Terapkan perbaikan untuk kerentanan itu dan mulai pod pengganti baru.
3. Hapus pod yang rentan.

Untuk informasi selengkapnya, lihat [Menerapkan ulang pod atau sumber daya beban kerja yang dikompromikan di Panduan Praktik](#) Terbaik Amazon EKS.

Jika node pekerja telah diberi peran IAM yang memungkinkan Pod mendapatkan akses ke AWS sumber daya lain, hapus peran tersebut dari instance untuk mencegah kerusakan lebih lanjut dari serangan. Demikian pula, jika Pod telah diberi peran IAM, evaluasi apakah Anda dapat menghapus kebijakan IAM dari peran dengan aman tanpa memengaruhi beban kerja lainnya.

Memulihkan gambar kontainer yang berpotensi dikompromikan

Ketika sebuah GuardDuty temuan menunjukkan kompromi pod, gambar yang digunakan untuk meluncurkan pod berpotensi berbahaya atau dikompromikan. GuardDuty temuan mengidentifikasi gambar kontainer di dalam `resource.kubernetesDetails.kubernetesWorkloadDetails.containers.image` lapangan. Anda dapat menentukan apakah gambar tersebut berbahaya dengan memindai malware.

Untuk memulihkan gambar kontainer yang berpotensi dikompromikan:

1. Berhenti menggunakan gambar segera dan hapus dari repositori gambar Anda.
2. Identifikasi semua pod menggunakan gambar yang berpotensi dikompromikan.

Untuk informasi selengkapnya, lihat [Mengidentifikasi pod dengan gambar dan node pekerja yang rentan atau disusupi](#) di Panduan Praktik Terbaik Amazon EKS.

3. Isolasi pod yang berpotensi dikompromikan, putar kredensialnya, dan kumpulkan data untuk dianalisis. Untuk informasi selengkapnya, lihat [Mengisolasi pod dengan membuat kebijakan jaringan yang menolak semua lalu lintas masuk dan keluar ke pod di Panduan](#) Praktik Terbaik Amazon EKS.
4. Hapus semua pod menggunakan gambar yang berpotensi dikompromikan.

Remediasi node Kubernetes yang berpotensi dikompromikan

GuardDuty Temuan dapat menunjukkan kompromi node jika pengguna yang diidentifikasi dalam temuan mewakili identitas node atau jika temuan menunjukkan penggunaan wadah istimewa.

Identitas pengguna adalah node pekerja jika bidang nama pengguna memiliki format berikut: `system:node:node name`. Misalnya, `system:node:ip-192-168-3-201.ec2.internal`. Hal ini menunjukkan bahwa musuh telah memperoleh akses ke node dan menggunakan kredensial node untuk berbicara dengan titik akhir API Kubernetes.

Temuan menunjukkan penggunaan wadah istimewa jika satu atau beberapa kontainer yang tercantum dalam temuan memiliki bidang `resource.kubernetesDetails.kubernetesWorkloadDetails.containers.securityContext`. temuan yang disetel ke `True`.

Untuk memulihkan node yang berpotensi dikompromikan:

1. Isolasi pod, putar kredensialnya, dan kumpulkan data untuk analisis forensik.

Untuk informasi selengkapnya, lihat [Mengisolasi pod dengan membuat kebijakan jaringan yang menolak semua lalu lintas masuk dan keluar ke pod di Panduan](#) Praktik Terbaik Amazon EKS.

2. Identifikasi akun layanan yang digunakan oleh semua pod yang berjalan pada node yang berpotensi dikompromikan. Tinjau izin mereka dan putar akun layanan jika diperlukan.
3. Hentikan node yang berpotensi dikompromikan.

Remediasi temuan Runtime Monitoring

Saat Anda mengaktifkan Runtime Monitoring untuk akun Anda, Amazon GuardDuty dapat menghasilkan [GuardDuty Jenis penemuan Runtime Monitoring](#) yang menunjukkan potensi masalah keamanan di AWS lingkungan Anda. Masalah keamanan potensial menunjukkan EC2 instans Amazon yang dikompromikan, beban kerja kontainer, kluster Amazon EKS, atau sekumpulan kredensi yang disusupi di lingkungan Anda. AWS Agen keamanan memantau peristiwa runtime dari berbagai jenis sumber daya. Untuk mengidentifikasi sumber daya yang berpotensi dikompromikan, lihat Jenis sumber daya dalam detail temuan yang dihasilkan di GuardDuty konsol. Bagian berikut menjelaskan langkah-langkah remediasi yang direkomendasikan untuk setiap jenis sumber daya.

Instance

Jika tipe Resource dalam rincian temuan adalah Instance, ini menunjukkan bahwa baik EC2 instance atau node EKS berpotensi dikompromikan.

- Untuk memulihkan simpul EKS yang dikompromikan, lihat. [Remediasi node Kubernetes yang berpotensi dikompromikan](#)
- Untuk memulihkan EC2 contoh yang dikompromikan, lihat. [Memperbaiki instans Amazon yang berpotensi dikompromikan EC2](#)

EKSCluster

Jika tipe Resource dalam rincian temuan adalah EKSCluster, ini menunjukkan bahwa baik pod atau wadah di dalam cluster EKS berpotensi dikompromikan.

- Untuk memulihkan pod yang dikompromikan, lihat. [Remediasi pod Kubernetes yang berpotensi dikompromikan](#)
- Untuk memulihkan gambar kontainer yang dikompromikan, lihat. [Memulihkan gambar kontainer yang berpotensi dikompromikan](#)

ECSCluster

Jika jenis Sumber Daya dalam rincian temuan adalah ECSCluster, ini menunjukkan bahwa tugas ECS atau wadah di dalam tugas ECS berpotensi dikompromikan.

1. Identifikasi cluster ECS yang terpengaruh

Temuan GuardDuty Runtime Monitoring memberikan detail cluster ECS di panel detail temuan atau di `resource.ecsClusterDetails` bagian di JSON temuan.

2. Identifikasi tugas ECS yang terpengaruh

Temuan GuardDuty Runtime Monitoring memberikan detail tugas ECS di panel detail temuan atau di `resource.ecsClusterDetails.taskDetails` bagian di JSON temuan.

3. Mengisolasi tugas yang terpengaruh

Mengisolasi tugas yang terkena dampak dengan menolak semua lalu lintas masuk dan keluar ke tugas. Menyangkal semua aturan lalu lintas dapat membantu menghentikan serangan yang sudah berlangsung, dengan memutuskan semua koneksi ke tugas.

4. Memulihkan tugas yang dikompromikan

- a. Identifikasi kerentanan yang mengganggu tugas.
- b. Terapkan perbaikan untuk kerentanan itu dan mulai tugas pengganti baru.
- c. Hentikan tugas yang rentan.

Container

Jika tipe Resource dalam rincian temuan adalah Container, ini menunjukkan bahwa kontainer mandiri berpotensi dikompromikan.

- Untuk memulihkan, lihat [Memulihkan wadah mandiri yang berpotensi dikompromikan](#).
- Jika temuan dihasilkan di beberapa kontainer menggunakan gambar kontainer yang sama, lihat [Memulihkan gambar kontainer yang berpotensi dikompromikan](#).
- Jika kontainer telah mengakses EC2 host yang mendasarinya, kredensi instance terkaitnya mungkin telah disusupi. Untuk informasi selengkapnya, lihat [Memulihkan kredensi yang berpotensi dikompromikan AWS](#).
- Jika aktor yang berpotensi berbahaya telah mengakses node EKS atau EC2 instance yang mendasarinya, lihat remediasi yang disarankan di bawah tab EKSCluster and Instance.

Memulihkan gambar kontainer yang dikompromikan

Ketika sebuah GuardDuty temuan menunjukkan kompromi tugas, gambar yang digunakan untuk meluncurkan tugas bisa berbahaya atau dikompromikan. GuardDuty temuan mengidentifikasi gambar kontainer di dalam `resource.ecsClusterDetails.taskDetails.containers.image`

lapangan. Anda dapat menentukan apakah gambar itu berbahaya atau tidak dengan memindainya untuk malware.

Untuk memulihkan gambar kontainer yang dikompromikan

1. Berhenti menggunakan gambar segera dan hapus dari repositori gambar Anda.
2. Identifikasi semua tugas yang menggunakan gambar ini.
3. Hentikan semua tugas yang menggunakan gambar yang disusupi. Perbarui definisi tugas mereka sehingga mereka berhenti menggunakan gambar yang disusupi.

Memulihkan database yang berpotensi dikompromikan

GuardDuty menghasilkan [Jenis temuan Perlindungan RDS](#) yang menunjukkan perilaku login yang berpotensi mencurigakan dan anomali di Anda [Database yang didukung](#) setelah Anda mengaktifkan [Perlindungan RDS](#). Menggunakan aktivitas login RDS, GuardDuty analisis dan profil ancaman dengan mengidentifikasi pola yang tidak biasa dalam upaya login.

Note

Anda dapat mengakses informasi lengkap tentang jenis temuan dengan memilihnya dari file [GuardDuty jenis temuan aktif](#).

Ikuti langkah-langkah yang disarankan ini untuk memulihkan database Amazon Aurora yang berpotensi dikompromikan di lingkungan Anda. AWS

Topik

- [Memulihkan database yang berpotensi dikompromikan dengan peristiwa login yang berhasil](#)
- [Memulihkan database yang berpotensi dikompromikan dengan peristiwa login yang gagal](#)
- [Memulihkan kredensi yang berpotensi dikompromikan](#)
- [Batasi akses jaringan](#)

Memulihkan database yang berpotensi dikompromikan dengan peristiwa login yang berhasil

Langkah-langkah yang disarankan berikut dapat membantu Anda memulihkan database Aurora yang berpotensi dikompromikan yang menunjukkan perilaku tidak biasa terkait dengan peristiwa login yang berhasil.

1. Identifikasi database dan pengguna yang terpengaruh.

GuardDuty Temuan yang dihasilkan memberikan nama database yang terpengaruh dan detail pengguna yang sesuai. Untuk informasi selengkapnya, lihat [Detail temuan](#).

2. Konfirmasikan apakah perilaku ini diharapkan atau tidak terduga.

Daftar berikut menentukan skenario potensial yang mungkin menyebabkan GuardDuty untuk menghasilkan temuan:

- Seorang pengguna yang masuk ke database mereka setelah waktu yang lama berlalu.
- Seorang pengguna yang masuk ke database mereka sesekali, misalnya, seorang analis keuangan yang log in di setiap kuartal.
- Aktor yang berpotensi mencurigakan yang terlibat dalam upaya login yang berhasil berpotensi membahayakan database.

3. Mulailah langkah ini jika perilakunya tidak terduga.

1. Batasi akses basis data

Batasi akses database untuk akun yang dicurigai dan sumber aktivitas login ini. Untuk informasi selengkapnya, silakan lihat [Memulihkan kredensi yang berpotensi dikompromikan](#) dan [Batasi akses jaringan](#).

2. Menilai dampak dan menentukan informasi apa yang diakses.

- Jika tersedia, tinjau log audit untuk mengidentifikasi potongan-potongan informasi yang mungkin telah diakses. Untuk informasi selengkapnya, lihat [Memantau peristiwa, log, dan aliran di kluster DB Amazon Aurora](#) di Panduan Pengguna Amazon Aurora.
- Tentukan apakah ada informasi sensitif atau dilindungi yang diakses atau dimodifikasi.

Memulihkan database yang berpotensi dikompromikan dengan peristiwa login yang gagal

Langkah-langkah yang disarankan berikut dapat membantu Anda memulihkan database Aurora yang berpotensi dikompromikan yang menunjukkan perilaku yang tidak biasa terkait dengan peristiwa login yang gagal.

1. Identifikasi database dan pengguna yang terpengaruh.

GuardDuty Temuan yang dihasilkan memberikan nama database yang terpengaruh dan detail pengguna yang sesuai. Untuk informasi selengkapnya, lihat [Detail temuan](#).

2. Identifikasi sumber upaya login yang gagal.

GuardDuty Temuan yang dihasilkan menyediakan alamat IP dan organisasi ASN (jika itu adalah koneksi publik) di bawah bagian Aktor dari panel pencarian.

Autonomous System (AS) adalah sekelompok satu atau lebih awalan IP (daftar alamat IP yang dapat diakses pada jaringan) yang dijalankan oleh satu atau lebih operator jaringan yang mempertahankan kebijakan routing tunggal yang didefinisikan dengan jelas. Operator jaringan memerlukan Autonomous System Numbers (ASNs) untuk mengontrol routing dalam jaringan mereka dan untuk bertukar informasi routing dengan penyedia layanan internet lainnya (ISPs).

3. Konfirmasikan bahwa perilaku ini tidak terduga.

Periksa apakah aktivitas ini merupakan upaya untuk mendapatkan akses tidak sah tambahan ke database sebagai berikut:

- Jika sumbernya internal, periksa apakah aplikasi salah konfigurasi dan coba koneksi berulang kali.
- Jika ini adalah aktor eksternal, periksa apakah database yang sesuai menghadap publik atau salah konfigurasi dan dengan demikian memungkinkan pelaku jahat potensial untuk secara kasar memaksa nama pengguna umum.

4. Mulailah langkah ini jika perilakunya tidak terduga.

1. Batasi akses basis data

Batasi akses database untuk akun yang dicurigai dan sumber aktivitas login ini. Untuk informasi selengkapnya, silakan lihat [Memulihkan kredensi yang berpotensi dikompromikan](#) dan [Batasi akses jaringan](#).

2. Lakukan analisis akar penyebab dan tentukan langkah-langkah yang berpotensi menyebabkan aktivitas ini.

Siapkan peringatan untuk mendapatkan pemberitahuan saat aktivitas mengubah kebijakan jaringan dan membuat status tidak aman. Untuk informasi selengkapnya, lihat [Kebijakan Firewall AWS Network Firewall](#) di Panduan AWS Network Firewall Pengembang.

Memulihkan kredensi yang berpotensi dikompromikan

GuardDuty Temuan mungkin menunjukkan bahwa kredensi pengguna untuk database yang terpengaruh telah dikompromikan ketika pengguna yang diidentifikasi dalam temuan telah melakukan operasi database yang tidak terduga. Anda dapat mengidentifikasi pengguna di bagian detail pengguna RDS DB dalam panel pencarian di konsol, atau di `resource.rdsDbUserDetails` dalam temuan JSON. Detail pengguna ini termasuk nama pengguna, aplikasi yang digunakan, database diakses, versi SSL, dan metode otentikasi.

- Untuk mencabut akses atau memutar kata sandi untuk pengguna tertentu yang terlibat dalam temuan, lihat [Keamanan dengan Amazon Aurora MySQL, atau Keamanan dengan Amazon Aurora PostgreSQL](#) di Panduan Pengguna Amazon Aurora.
- Gunakan AWS Secrets Manager untuk menyimpan dengan aman dan secara otomatis memutar rahasia untuk database Amazon Relational Database Service (RDS). Untuk informasi selengkapnya, lihat [AWS Secrets Manager tutorial](#) di Panduan AWS Secrets Manager Pengguna.
- Gunakan autentikasi basis data IAM untuk mengelola akses pengguna database tanpa perlu kata sandi. Untuk informasi selengkapnya, lihat [autentikasi database IAM](#) di Panduan Pengguna Amazon Aurora.

Untuk informasi selengkapnya, lihat [Praktik terbaik keamanan untuk Amazon Relational Database Service](#) di Panduan Pengguna Amazon RDS.

Batasi akses jaringan

GuardDuty Temuan mungkin menunjukkan bahwa database dapat diakses di luar aplikasi Anda, atau Virtual Private Cloud (VPC). Jika alamat IP jarak jauh dalam temuan adalah sumber koneksi yang tidak terduga, audit grup keamanan. Daftar grup keamanan yang dilampirkan ke database tersedia di bawah Grup keamanan di <https://console.aws.amazon.com/rds/konsol>, atau di `resource.rdsDbInstanceDetails.dbSecurityGroups` temuan JSON. Untuk informasi

selengkapnya tentang mengonfigurasi grup keamanan, lihat [Mengontrol akses dengan grup keamanan](#) di Panduan Pengguna Amazon RDS.

Jika Anda menggunakan firewall, batasi akses jaringan ke database dengan mengkonfigurasi ulang Network Access Control Lists (). NACLs Untuk informasi selengkapnya, lihat [Firewall AWS Network Firewall](#) di Panduan AWS Network Firewall Pengembang.

Memperbaiki fungsi Lambda yang berpotensi dikompromikan

Saat GuardDuty menghasilkan [Jenis temuan Perlindungan Lambda](#), fungsi Lambda Anda dapat dikompromikan. Jika aktivitas yang GuardDuty menyebabkan menghasilkan temuan ini diharapkan, Anda dapat mempertimbangkan untuk menggunakannya [Aturan penekanan](#). Kami merekomendasikan untuk menyelesaikan langkah-langkah berikut untuk memulihkan fungsi Lambda yang dikompromikan:

Untuk memulihkan temuan Perlindungan Lambda

1. Identifikasi versi fungsi Lambda yang berpotensi dikompromikan.

GuardDuty Temuan untuk Perlindungan Lambda menyediakan nama, Nama Sumber Daya Amazon (ARN), versi fungsi, dan ID revisi yang terkait dengan fungsi Lambda yang tercantum dalam detail temuan.

2. Identifikasi sumber aktivitas yang berpotensi mencurigakan.
 - a. Tinjau kode yang terkait dengan versi fungsi Lambda yang terlibat dalam temuan.
 - b. Tinjau pustaka dan lapisan yang diimpor dari versi fungsi Lambda yang terlibat dalam temuan.
 - c. Jika Anda telah mengaktifkan [AWS Lambda fungsi Pemindaian dengan Amazon Inspector](#), tinjau temuan [Amazon Inspector](#) yang terkait dengan fungsi Lambda yang terlibat dalam temuan tersebut.
 - d. Tinjau AWS CloudTrail log untuk mengidentifikasi prinsipal yang menyebabkan pembaruan fungsi dan memastikan bahwa aktivitas tersebut diotorisasi atau diharapkan.
3. Memperbaiki fungsi Lambda yang berpotensi terganggu.
 - a. Nonaktifkan pemicu eksekusi fungsi Lambda yang terlibat dalam temuan. Untuk informasi selengkapnya, lihat [DeleteFunctionEventInvokeConfig](#).
 - b. Tinjau kode Lambda dan perbarui impor pustaka dan lapisan [fungsi Lambda](#) untuk menghapus pustaka dan lapisan yang berpotensi mencurigakan.

- c. Mengurangi temuan Amazon Inspector terkait dengan fungsi Lambda yang terlibat dalam temuan tersebut.

Memperkirakan biaya GuardDuty penggunaan

Selama uji coba gratis 30 hari, Anda dapat menggunakan operasi GuardDuty konsol atau API untuk memperkirakan biaya penggunaan rata-rata harian. GuardDuty Estimasi biaya memproyeksikan berapa perkiraan biaya Anda setelah masa percobaan. Namun, untuk meninjau perkiraan biaya yang akurat selama uji coba gratis, GuardDuty merekomendasikan untuk menggunakan AWS Billing at <https://console.aws.amazon.com/costmanagement/>.

Saat Anda beroperasi di lingkungan beberapa akun, akun GuardDuty administrator dapat memantau metrik biaya untuk semua akun anggota.

Catatan tentang Perlindungan Malware untuk biaya penggunaan S3

Biaya penggunaan untuk Perlindungan Malware untuk S3 tidak termasuk dalam Penggunaan di GuardDuty konsol. Untuk informasi selengkapnya, lihat [Meninjau biaya penggunaan untuk Perlindungan Malware untuk S3](#).

Anda dapat melihat estimasi biaya berdasarkan metrik berikut:

- ID Akun — Daftar perkiraan biaya untuk akun Anda, atau untuk akun anggota Anda jika Anda beroperasi sebagai akun GuardDuty administrator.
- Sumber data — Daftar perkiraan biaya untuk semua [Sumber data dasar](#) — peristiwa AWS CloudTrail manajemen, log aliran VPC, dan log kueri DNS Route53 Resolver.
- Fitur - Daftar perkiraan biaya untuk [GuardDuty fitur](#) - peristiwa CloudTrail data untuk S3, Pemantauan Log Audit EKS, data volume EBS, aktivitas login RDS, Pemantauan Runtime EKS, Pemantauan Runtime Fargate, Pemantauan Runtime, atau EC2 Pemantauan Aktivitas Jaringan Lambda.
- Bucket S3 — Daftar perkiraan biaya untuk kejadian data S3 pada bucket tertentu atau bucket termahal untuk akun di lingkungan Anda. Statistik ini hanya tersedia jika Anda mengaktifkan [Perlindungan S3](#) untuk file Akun AWS.

Memahami cara GuardDuty menghitung biaya penggunaan

Perkiraan yang ditampilkan di GuardDuty konsol mungkin sedikit berbeda dari yang ada di AWS Manajemen Penagihan dan Biaya konsol Anda. Daftar berikut menjelaskan bagaimana GuardDuty perkiraan biaya penggunaan:

- Perkiraan GuardDuty penggunaan hanya untuk Wilayah saat ini.
- Biaya GuardDuty penggunaan didasarkan pada 30 hari terakhir penggunaan.
- Perkiraan biaya penggunaan uji coba mencakup perkiraan untuk sumber data dasar dan fitur yang saat ini dalam masa uji coba. Setiap fitur dan sumber data di dalamnya GuardDuty memiliki masa uji coba sendiri tetapi mungkin tumpang tindih dengan periode uji coba GuardDuty atau fitur lain yang diaktifkan pada saat yang sama.
- Perkiraan GuardDuty penggunaan mencakup diskon harga GuardDuty volume per Wilayah, seperti yang dijelaskan di halaman [GuardDutyHarga Amazon](#), tetapi hanya untuk akun individu yang memenuhi tingkatan harga volume. Diskon harga volume tidak termasuk dalam perkiraan untuk penggunaan total gabungan antar akun dalam suatu organisasi. Untuk informasi tentang harga diskon volume penggunaan gabungan, lihat [Penagihan AWS : Diskon Volume](#).
- Jumlah biaya penggunaan untuk masing-masing Akun AWS di organisasi Anda mungkin tidak selalu sama dengan perkiraan biaya 30 hari terakhir untuk sumber data yang dipilih. Tingkat harga dapat berubah saat GuardDuty memproses lebih banyak peristiwa atau data. Untuk informasi selengkapnya, lihat [Tingkat Harga](#) di Panduan AWS Billing Pengguna.

Skenario ini menjelaskan bahwa untuk menghentikan biaya penggunaan untuk Runtime Monitoring, Anda harus menonaktifkan fitur Runtime Monitoring dan EKS Runtime Monitoring.

GuardDuty telah mengkonsolidasikan pengalaman konsol untuk EKS Runtime Monitoring ke Runtime Monitoring. GuardDuty merekomendasikan [Memeriksa status konfigurasi EKS Runtime Monitoring](#) dan [Migrasi dari EKS Runtime Monitoring ke Runtime Monitoring](#).

Sebagai bagian dari migrasi ke Runtime Monitoring, pastikan untuk. [Nonaktifkan Pemantauan Runtime EKS](#) Ini penting karena jika nanti Anda memilih untuk menonaktifkan Runtime Monitoring dan Anda tidak menonaktifkan EKS Runtime Monitoring, Anda akan terus mengeluarkan biaya penggunaan untuk EKS Runtime Monitoring.

Runtime Monitoring - Bagaimana log aliran VPC EC2 dari instans memengaruhi biaya penggunaan

Saat Anda mengelola agen keamanan (baik secara manual atau melalui GuardDuty) di EKS Runtime Monitoring atau Runtime Monitoring untuk EC2 instance, dan saat GuardDuty ini digunakan di instans EC2 Amazon dan menerima [Jenis acara runtime yang dikumpulkan](#) dari instance ini GuardDuty , tidak akan membebankan biaya Akun AWS untuk analisis log aliran VPC dari instans Amazon ini. EC2 Ini membantu GuardDuty menghindari biaya penggunaan ganda di akun.

Bagaimana GuardDuty memperkirakan biaya penggunaan untuk CloudTrail acara

Ketika Anda mengaktifkan GuardDuty, secara otomatis mulai menggunakan log AWS CloudTrail peristiwa yang direkam untuk akun Anda di yang dipilih Wilayah AWS. GuardDuty mereplikasi log [peristiwa layanan Global](#) dan kemudian memproses peristiwa ini secara independen di setiap Wilayah yang telah Anda GuardDuty aktifkan. Ini membantu GuardDuty menjaga profil pengguna dan peran di setiap Wilayah untuk mengidentifikasi anomali.

CloudTrail Konfigurasi Anda tidak memengaruhi biaya GuardDuty penggunaan atau cara GuardDuty memproses log peristiwa Anda. Biaya GuardDuty penggunaan Anda dipengaruhi oleh penggunaan AWS APIs log to Anda CloudTrail. Untuk informasi selengkapnya, lihat [AWS CloudTrail acara manajemen](#).

Meninjau GuardDuty perkiraan biaya penggunaan

GuardDuty Penggunaan ini memberikan perkiraan biaya berdasarkan penggunaan Anda selama 30 hari terakhir per Wilayah AWS. Estimasi penggunaan berbeda dari penggunaan tagihan Anda. Untuk informasi tentang cara GuardDuty memperkirakan biaya penggunaan, lihat [Memahami cara GuardDuty menghitung biaya penggunaan](#). Jika Anda adalah akun GuardDuty administrator, Anda dapat melihat perkiraan biaya untuk setiap akun anggota, yang dipecah berdasarkan sumber data dan akun.

Pilih metode akses pilihan Anda untuk meninjau biaya penggunaan GuardDuty akun Anda.

Untuk meninjau perkiraan biaya GuardDuty penggunaan

Console

1. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.

Pastikan untuk menggunakan akun GuardDuty administrator.

2. Pada panel navigasi, pilih Penggunaan.
3. Pada halaman Penggunaan, akun GuardDuty administrator dengan akun anggota dapat melihat Perkiraan biaya organisasi selama 30 hari terakhir. Ini adalah perkiraan total biaya penggunaan untuk organisasi Anda.
4. GuardDuty akun administrator dapat melihat rincian biaya penggunaan berdasarkan sumber data, atau berdasarkan akun. Akun individu atau mandiri dapat melihat rincian berdasarkan sumber data.

Jika Anda memiliki akun anggota — Pilih tab Berdasarkan akun untuk melihat statistik untuk setiap akun anggota.

Di bawah tab Berdasarkan sumber data, saat Anda memilih sumber data yang memiliki biaya penggunaan yang terkait dengannya, jumlah rincian biaya yang sesuai di tingkat akun mungkin tidak selalu sama.

API/CLI

Jalankan [GetUsageStatistics](#) Operasi API menggunakan kredensial akun GuardDuty administrator. Berikan informasi berikut untuk menjalankan perintah:

- (Wajib) berikan ID GuardDuty detektor Regional dari akun yang ingin Anda ambil statistiknya.
- (Wajib) berikan salah satu jenis statistik untuk diambil: `SUM_BY_ACCOUNT` | `SUM_BY_DATA_SOURCE` | `SUM_BY_RESOURCE` | `SUM_BY_FEATURE` | `TOP_ACCOUNTS_BY_FEATURE`.

Saat ini, `TOP_ACCOUNTS_BY_FEATURE` tidak mendukung pengambilan statistik penggunaan untuk `RDS_LOGIN_EVENTS`.

- (Wajib) menyediakan satu atau beberapa sumber data atau fitur untuk menanyakan statistik penggunaan Anda.
- (Opsional) berikan daftar akun IDs yang ingin Anda ambil statistik penggunaannya.

Anda juga dapat menggunakan AWS Command Line Interface. Perintah berikut adalah contoh tentang mengambil statistik penggunaan untuk semua sumber data dan fitur, dihitung oleh akun. Pastikan untuk mengganti `detector-id` dengan ID detektor valid Anda sendiri. Untuk akun mandiri, perintah ini mengembalikan biaya penggunaan selama 30 hari terakhir hanya untuk akun

Anda. Jika Anda adalah akun GuardDuty administrator dengan akun anggota, Anda melihat biaya yang tercantum berdasarkan akun untuk semua anggota.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan detectorId [ListDetectors](#) API.

Ganti SUM_BY_ACCOUNT dengan jenis yang Anda inginkan untuk menghitung statistik penggunaan.

Untuk memantau biaya hanya untuk sumber data

```
aws guardduty get-usage-statistics --detector-id 12abc34d567e8fa901bc2d34e56789f0
--usage-statistic-type SUM_BY_ACCOUNT --usage-criteria '{"DataSources":
["FLOW_LOGS", "CLOUD_TRAIL", "DNS_LOGS", "S3_LOGS", "KUBERNETES_AUDIT_LOGS",
"EC2_MALWARE_SCAN"]}'
```

Untuk memantau biaya untuk fitur

```
aws guardduty get-usage-statistics --detector-id 12abc34d567e8fa901bc2d34e56789f0
--usage-statistic-type SUM_BY_ACCOUNT --usage-criteria '{"Features":
["FLOW_LOGS", "CLOUD_TRAIL", "DNS_LOGS", "S3_DATA_EVENTS", "EKS_AUDIT_LOGS",
"EBS_MALWARE_PROTECTION", "RDS_LOGIN_EVENTS", "LAMBDA_NETWORK_LOGS",
"EKS_RUNTIME_MONITORING", "FARGATE_RUNTIME_MONITORING", "EC2_RUNTIME_MONITORING"]}'
```

Nama fitur untuk paket perlindungan di GuardDuty API

Saat Anda mengaktifkan Amazon GuardDuty untuk pertama kalinya, Amazon mulai diproses [Sumber data dasar](#) di AWS lingkungan Anda. GuardDuty menggunakan sumber data ini untuk memproses aliran peristiwa independen seperti log aliran VPC, log DNS, dan AWS CloudTrail peristiwa manajemen. Kemudian menganalisis peristiwa ini untuk mengidentifikasi potensi ancaman keamanan dan menghasilkan temuan di akun Anda.

Ketika satu atau lebih rencana perlindungan diaktifkan, maka GuardDuty gunakan data tambahan dari AWS layanan lain di AWS lingkungan Anda untuk memantau dan menganalisis potensi ancaman keamanan. Sumber data tambahan ini disebut fitur.

Ubah dari sumber data ke fitur

Saat Anda menambahkan GuardDuty perlindungan tambahan, seperti Perlindungan S3, Pemantauan Runtime, Perlindungan Lambda, dan lainnya, Anda dapat mengonfigurasi GuardDuty fitur yang sesuai dengan paket perlindungan. Secara historis, GuardDuty perlindungan disebut `dataSources` dalam APIs. Namun, setelah Maret 2023, rencana GuardDuty perlindungan baru sekarang dikonfigurasi sebagai `features` dan tidak `dataSources`. GuardDuty masih mendukung konfigurasi rencana perlindungan yang diluncurkan sebelum Maret 2023, seperti `dataSources` melalui API, tetapi rencana perlindungan baru hanya tersedia sebagai `features`. Untuk informasi tentang rencana perlindungan yang terkena dampak, lihat [GuardDuty Perubahan API](#).

Jika Anda mengelola paket GuardDuty konfigurasi dan perlindungan melalui konsol, Anda tidak terpengaruh secara langsung oleh perubahan ini dan tidak perlu mengambil tindakan apa pun. Perubahan ini mempengaruhi perilaku APIs yang dipanggil untuk mengaktifkan GuardDuty atau melindungi rencana di dalamnya GuardDuty. Jika Anda menggunakan APIs atau AWS CLI untuk mengaktifkan atau mengedit konfigurasi paket perlindungan, Anda harus menggunakan nama fitur terkait. Untuk informasi selengkapnya, lihat [Pemetaan ke `dataSources` `features`](#).

GuardDuty Perubahan API pada Maret 2023

Fitur perlindungan GuardDuty APIs konfigurasi yang tidak termasuk dalam daftar [GuardDuty sumber data dasar](#). Objek fitur berisi detail fitur, seperti nama fitur dan status, dan mungkin berisi konfigurasi tambahan untuk beberapa paket perlindungan. Migrasi ini memengaruhi hal-hal berikut APIs di Referensi Amazon GuardDuty API:

- [CreateDetector](#)
- [GetDetector](#)
- [UpdateDetector](#)
- [GetMemberDetectors](#)
- [UpdateMemberDetectors](#)
- [DescribeOrganizationConfiguration](#)
- [UpdateOrganizationConfiguration](#)
- [GetRemainingFreeTrialDays](#)
- [GetUsageStatistics](#)

Fitur dibandingkan dengan sumber data

Secara historis, semua GuardDuty fitur dilewatkan melalui dataSources objek di API. Mulai Maret 2023, GuardDuty lebih memilih features objek daripada dataSources objek di API. Semua sumber data sebelumnya memiliki fitur yang sesuai, tetapi fitur yang lebih baru mungkin tidak memiliki sumber data yang sesuai.

Daftar berikut menunjukkan perbandingan antara dataSources dan features objek saat melewati API:

- dataSourcesObjek berisi objek untuk setiap jenis perlindungan dan statusnya. featuresObjek adalah daftar fitur yang tersedia yang sesuai dengan setiap jenis perlindungan di dalamnya GuardDuty.

Mulai Maret 2023, aktivasi fitur akan menjadi satu-satunya cara untuk mengonfigurasi GuardDuty fitur baru di AWS lingkungan Anda.

- dataSourcesSkema dalam permintaan atau respons API sama di setiap Wilayah AWS tempat yang GuardDuty tersedia. Namun, setiap fitur mungkin tidak tersedia di setiap Wilayah. Oleh karena itu, nama fitur yang tersedia mungkin berbeda berdasarkan Wilayah.

Memahami cara APIs kerja fitur

GuardDuty APIs Akan terus mengembalikan dataSources objek sebagaimana berlaku, dan mereka juga akan mengembalikan features objek yang berisi informasi yang sama dalam format

yang berbeda. GuardDuty Fitur yang diluncurkan sebelum Maret 2023 akan tersedia melalui `dataSources` objek dan `features` objek. GuardDuty fitur yang diluncurkan sejak Maret 2023 hanya akan tersedia melalui `features` objek. Anda tidak dapat membuat atau memperbarui detektor, atau menjelaskan AWS Organizations penggunaan keduanya `dataSources` dan notasi `features` objek dalam permintaan API yang sama. Untuk mengaktifkan jenis GuardDuty perlindungan, Anda harus memigrasikan sumber data yang ada ke `features` objek dengan menggunakan yang sama APIs yang sekarang menyertakan `features` objek juga.

Note

GuardDuty tidak akan menambahkan sumber data baru setelah modifikasi ini.

GuardDuty telah menghentikan penggunaan sumber data yang terkait dengan rencana perlindungan. Namun, masih mendukung [GuardDuty sumber data dasar](#). Praktik GuardDuty terbaik merekomendasikan penggunaan fitur untuk mengaktifkan atau mengedit konfigurasi untuk paket perlindungan apa pun di akun Anda.

Menggabungkan perubahan fitur di APIs

- Jika Anda mengelola GuardDuty konfigurasi melalui APIs, SDKs, atau AWS CloudFormation template, dan ingin mengaktifkan GuardDuty fitur baru yang potensial, Anda harus memodifikasi kode dan template Anda, masing-masing. Untuk informasi selengkapnya, lihat yang diperbarui APIs di [Referensi Amazon GuardDuty API](#).
- Untuk GuardDuty fitur yang dikonfigurasi sebelum pemutakhiran ini, Anda dapat terus menggunakan APIs, SDKs, atau AWS CloudFormation templat. Namun, kami menyarankan Anda beralih menggunakan `feature` objek.

Semua sumber data memiliki objek fitur yang setara. Untuk informasi selengkapnya, lihat [Pemetaan ke `dataSources` `features`](#).

- Saat ini, `additionalConfiguration` dalam `features` objek hanya tersedia untuk jenis perlindungan tertentu.
 - Untuk jenis perlindungan seperti itu, jika fitur Anda `AdditionalConfiguration` status disetel ke `ENABLED` tetapi konfigurasi fitur Anda tidak status disetel ke `ENABLED`, tidak GuardDuty akan mengambil tindakan apa pun dalam kasus ini.
 - Berikut ini APIs akan terpengaruh oleh ini:
 - [UpdateDetector](#)

- [UpdateMemberDetectors](#)
- [UpdateOrganizationConfiguration](#)

Pemetaan ke **dataSources** dan **features**

Tabel berikut menunjukkan pemetaan jenis perlindungan, **dataSources**, dan **features**.

GuardDuty jenis perlindungan	Nama sumber ^{data*}	Nama fitur
Log Alur VPC	flowLogs(baca saja; tidak dapat dimodifikasi)	FLOW_LOGS (baca saja; tidak dapat dimodifikasi)
Log kueri DNS Route53 Resolver	dnsLogs(baca saja; tidak dapat dimodifikasi)	DNS_LOGS(baca saja; tidak dapat dimodifikasi)
CloudTrail acara	cloudTrail (baca saja; tidak dapat dimodifikasi)	CLOUD_TRAIL (baca saja; tidak dapat dimodifikasi)
S3	s3Logs	S3_DATA_EVENTS
Perlindungan EKS	kubernetes.auditlogs	EKS_AUDIT_LOGS
Perlindungan Malware untuk EC2	malwareProtection.scanEc2InstanceWithFindings.ebsVolumes	EBS_MALWARE_PROTECTION
Acara Login RDS		RDS_LOGIN_EVENTS
Pemantauan Runtime EKS	GuardDuty hanya menyediakan dukungan aktivasi fitur untuk jenis perlindungan ini.	EKS_RUNTIME_MONITORING
Pemantauan Runtime		RUNTIME_MONITORING

GuardDuty jenis perlindungan	Nama sumber ^{data*}	Nama fitur
GuardDuty agen keamanan untuk kluster Amazon EKS		EKS_RUNTIME_MONITORING.additionalConfiguration.EKS_ADDON_MANAGEMENT RUNTIME_MONITORING.additionalConfiguration.EKS_ADDON_MANAGEMENT
GuardDuty agen keamanan untuk cluster Amazon ECS-Fargate		RUNTIME_MONITORING.additionalConfiguration.ECS_FARGATE_AGENT_MANAGEMENT
GuardDuty agen keamanan untuk EC2 instans Amazon		RUNTIME_MONITORING.additionalConfiguration.EC2_AGENT_MANAGEMENT

GuardDuty jenis perlindungan	Nama sumber data*	Nama fitur
Perlindungan Lambda		LAMBDA_NETWORK_LOGS

*GetUsageStatistics menggunakan dataSource namanya sendiri. Untuk informasi lebih lanjut, lihat [Memperkirakan biaya GuardDuty penggunaan](#) atau [GetUsageStatistics](#).

Keamanan di Amazon GuardDuty

Keamanan cloud di AWS adalah prioritas tertinggi. Sebagai AWS pelanggan, Anda mendapat manfaat dari pusat data dan arsitektur jaringan yang dibangun untuk memenuhi persyaratan organisasi yang paling sensitif terhadap keamanan.

Keamanan adalah tanggung jawab bersama antara Anda AWS dan Anda. [Model Tanggung Jawab Bersama](#) menjelaskan hal ini sebagai keamanan cloud dan keamanan di cloud:

- Keamanan cloud — AWS bertanggung jawab untuk melindungi infrastruktur yang menjalankan AWS layanan di AWS Cloud. AWS juga memberi Anda layanan yang dapat Anda gunakan dengan aman. Auditor pihak ketiga secara teratur menguji dan memverifikasi efektivitas keamanan kami sebagai bagian dari [program AWS kepatuhan program AWS](#) . Untuk mempelajari tentang program kepatuhan yang berlaku GuardDuty, lihat [AWS layanan dalam cakupan berdasarkan AWS layanan program kepatuhan](#) .
- Keamanan di cloud — Tanggung jawab Anda ditentukan oleh AWS layanan yang Anda gunakan. Anda juga bertanggung jawab atas faktor lain, termasuk sensitivitas data Anda, persyaratan perusahaan Anda, serta undang-undang dan peraturan yang berlaku.

Dokumentasi ini membantu Anda memahami cara menerapkan model tanggung jawab bersama saat menggunakan GuardDuty. Ini menunjukkan kepada Anda cara mengonfigurasi GuardDuty untuk memenuhi tujuan keamanan dan kepatuhan Anda. Anda juga belajar cara menggunakan AWS layanan lain yang membantu Anda memantau dan mengamankan GuardDuty sumber daya Anda.

Konten

- [Perlindungan data di Amazon GuardDuty](#)
- [Mencatat panggilan GuardDuty API Amazon dengan AWS CloudTrail](#)
- [Identity and Access Management untuk Amazon GuardDuty](#)
- [Validasi kepatuhan untuk Amazon GuardDuty](#)
- [Ketahanan di Amazon GuardDuty](#)
- [Keamanan infrastruktur di Amazon GuardDuty](#)
- [Amazon GuardDuty dan titik akhir VPC antarmuka \(\)AWS PrivateLink](#)

Perlindungan data di Amazon GuardDuty

[Model tanggung jawab AWS bersama model](#) berlaku untuk perlindungan data di Amazon GuardDuty. Seperti yang dijelaskan dalam model AWS ini, bertanggung jawab untuk melindungi infrastruktur global yang menjalankan semua AWS Cloud. Anda bertanggung jawab untuk mempertahankan kendali atas konten yang di-host pada infrastruktur ini. Anda juga bertanggung jawab atas tugas-tugas konfigurasi dan manajemen keamanan untuk Layanan AWS yang Anda gunakan. Lihat informasi yang lebih lengkap tentang privasi data dalam [Pertanyaan Umum Privasi Data](#). Lihat informasi tentang perlindungan data di Eropa di pos blog [Model Tanggung Jawab Bersama dan GDPR AWS](#) di Blog Keamanan AWS .

Untuk tujuan perlindungan data, kami menyarankan Anda melindungi Akun AWS kredensial dan mengatur pengguna individu dengan AWS IAM Identity Center atau AWS Identity and Access Management (IAM). Dengan cara itu, setiap pengguna hanya diberi izin yang diperlukan untuk memenuhi tanggung jawab tugasnya. Kami juga menyarankan supaya Anda mengamankan data dengan cara-cara berikut:

- Gunakan autentikasi multi-faktor (MFA) pada setiap akun.
- Gunakan SSL/TLS untuk berkomunikasi dengan AWS sumber daya. Kami mensyaratkan TLS 1.2 dan menganjurkan TLS 1.3.
- Siapkan API dan pencatatan aktivitas pengguna dengan AWS CloudTrail. Untuk informasi tentang penggunaan CloudTrail jejak untuk menangkap AWS aktivitas, lihat [Bekerja dengan CloudTrail jejak](#) di AWS CloudTrail Panduan Pengguna.
- Gunakan solusi AWS enkripsi, bersama dengan semua kontrol keamanan default di dalamnya Layanan AWS.
- Gunakan layanan keamanan terkelola tingkat lanjut seperti Amazon Macie, yang membantu menemukan dan mengamankan data sensitif yang disimpan di Amazon S3.
- Jika Anda memerlukan modul kriptografi tervalidasi FIPS 140-3 saat mengakses AWS melalui antarmuka baris perintah atau API, gunakan titik akhir FIPS. Lihat informasi selengkapnya tentang titik akhir FIPS yang tersedia di [Standar Pemrosesan Informasi Federal \(FIPS\) 140-3](#).

Kami sangat merekomendasikan agar Anda tidak pernah memasukkan informasi identifikasi yang sensitif, seperti nomor rekening pelanggan Anda, ke dalam tanda atau bidang isian bebas seperti bidang Nama. Ini termasuk saat Anda bekerja dengan GuardDuty atau lainnya Layanan AWS menggunakan konsol, API AWS CLI, atau AWS SDKs. Data apa pun yang Anda masukkan ke dalam tanda atau bidang isian bebas yang digunakan untuk nama dapat digunakan untuk log penagihan

atau log diagnostik. Saat Anda memberikan URL ke server eksternal, kami sangat menganjurkan supaya Anda tidak menyertakan informasi kredensial di dalam URL untuk memvalidasi permintaan Anda ke server itu.

Enkripsi diam

Semua data GuardDuty pelanggan dienkrpsi saat istirahat menggunakan solusi AWS enkripsi.

GuardDuty data, seperti temuan, dienkrpsi saat istirahat menggunakan AWS Key Management Service (AWS KMS) menggunakan kunci yang dikelola pelanggan yang AWS dimiliki.

Enkripsi bergerak

GuardDuty menganalisis data log dari layanan lain. Ini mengenkripsi semua data dalam perjalanan dari layanan ini dengan HTTPS dan KMS. Setelah GuardDuty mengekstrak informasi yang dibutuhkan dari log, mereka dibuang. Untuk informasi selengkapnya tentang cara GuardDuty menggunakan informasi dari layanan lain, lihat [sumber GuardDuty data](#).

GuardDuty data dienkrpsi dalam perjalanan antar layanan.

Memilih untuk tidak menggunakan data Anda untuk perbaikan layanan

Anda dapat memilih untuk tidak menggunakan data Anda untuk mengembangkan dan meningkatkan GuardDuty dan layanan AWS keamanan lainnya dengan menggunakan kebijakan AWS Organizations opt-out. Anda dapat memilih untuk memilih keluar meskipun saat ini GuardDuty tidak mengumpulkan data tersebut. Untuk informasi selengkapnya tentang cara memilih keluar, lihat [kebijakan opt-out layanan AI](#) di AWS Organizations Panduan Pengguna.

Note

Agar Anda dapat menggunakan kebijakan opt-out, AWS akun Anda harus dikelola secara terpusat oleh AWS Organizations. Jika Anda belum membuat organisasi untuk AWS akun Anda, lihat [Membuat dan mengelola organisasi](#) di Panduan AWS Organizations Pengguna.

Memilih keluar memiliki efek sebagai berikut:

- GuardDuty akan menghapus data yang dikumpulkan dan disimpan untuk tujuan peningkatan layanan sebelum Anda memilih keluar (jika ada).

- Setelah Anda memilih keluar, tidak GuardDuty akan lagi mengumpulkan atau menyimpan data ini untuk tujuan peningkatan layanan.

Topik berikut menjelaskan bagaimana setiap fitur dalam GuardDuty berpotensi menangani data Anda untuk peningkatan layanan.

Daftar Isi

- [GuardDuty Pemantauan Runtime](#)
- [GuardDuty Perlindungan Malware](#)

GuardDuty Pemantauan Runtime

GuardDuty Runtime Monitoring menyediakan deteksi ancaman runtime untuk AWS Fargate cluster Amazon Elastic Kubernetes Service (Amazon EKS), hanya Amazon Elastic Container Service (Amazon ECS), dan instans Amazon Elastic Compute Cloud (Amazon) di lingkungan Anda. EC2 AWS Setelah Anda mengaktifkan Runtime Monitoring dan menyebarkan agen GuardDuty keamanan untuk sumber daya Anda, GuardDuty mulai memantau dan menganalisis peristiwa runtime yang terkait dengan sumber daya Anda. Jenis peristiwa runtime ini mencakup peristiwa proses, peristiwa kontainer, peristiwa DNS, dan banyak lagi. Untuk informasi selengkapnya, lihat [Mengumpulkan jenis peristiwa runtime yang menggunakan GuardDuty](#).

GuardDuty mengumpulkan kedua perintah (seperti `curl`, `systemctl`, `cron`) dan argumen terkait (seperti `start`, `stop`, `disable`) dari beban kerja Anda. Misalnya, ketika seseorang menjalankan `systemctl stop service-name`, GuardDuty menangkap perintah `systemctl` dan `stop service-name` argumennya. Informasi terperinci ini GuardDuty membantu mendeteksi ancaman canggih dengan menganalisis pola perintah dan menghubungkan beberapa peristiwa. Misalnya, GuardDuty dapat mengidentifikasi kapan penyerang mencoba menonaktifkan layanan keamanan atau mengeksekusi file berbahaya yang diketahui. Meskipun GuardDuty secara aktif menggunakan data ini untuk deteksi ancaman, saat ini tidak menggunakan perintah dan argumen ini untuk tujuan peningkatan layanan (mungkin melakukannya di masa mendatang). Kepercayaan, privasi, dan keamanan konten Anda adalah prioritas utama kami, dan memastikan bahwa penggunaan kami sesuai dengan komitmen kami kepada Anda. Untuk informasi selengkapnya, lihat [FAQ Privasi Data](#).

GuardDuty Perlindungan Malware

GuardDuty Perlindungan Malware memindai dan mendeteksi malware yang terdapat dalam volume EBS yang dilampirkan ke EC2 instans Amazon dan beban kerja kontainer yang berpotensi dikompromikan, serta file yang baru diunggah di bucket Amazon S3 pilihan Anda. Saat ini, GuardDuty tidak mengumpulkan atau menggunakan malware yang terdeteksi untuk peningkatan layanan. Namun, di masa depan, ketika Perlindungan GuardDuty Malware mengidentifikasi file volume EBS atau file S3 sebagai berbahaya atau berbahaya, Perlindungan GuardDuty Malware akan mengumpulkan dan menyimpan file ini untuk mengembangkan dan meningkatkan deteksi malware, dan layanan. GuardDuty File ini juga dapat digunakan untuk mengembangkan dan meningkatkan layanan AWS keamanan lainnya. Kepercayaan, privasi, dan keamanan konten Anda adalah prioritas utama kami, dan memastikan bahwa penggunaan kami sesuai dengan komitmen kami kepada Anda. Untuk informasi selengkapnya, lihat [FAQ Privasi Data](#).

Mencatat panggilan GuardDuty API Amazon dengan AWS CloudTrail

Amazon GuardDuty terintegrasi dengan AWS CloudTrail, layanan yang menyediakan catatan tindakan yang diambil oleh pengguna, peran, atau AWS layanan di GuardDuty. CloudTrail menangkap semua panggilan API untuk GuardDuty sebagai peristiwa, termasuk panggilan dari GuardDuty konsol dan dari panggilan kode ke GuardDuty APIs. Jika Anda membuat jejak, Anda dapat mengaktifkan pengiriman CloudTrail acara secara terus menerus ke bucket Amazon Simple Storage Service (Amazon S3), termasuk acara untuk GuardDuty. 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 GuardDuty, alamat IP tempat permintaan dibuat, siapa yang membuat permintaan, kapan dibuat, dan detail tambahan.

Untuk informasi selengkapnya CloudTrail, termasuk cara mengonfigurasi dan mengaktifkannya, lihat [Panduan AWS CloudTrail Pengguna](#).

GuardDuty informasi di CloudTrail

CloudTrail diaktifkan di AWS akun Anda saat Anda membuat akun. Ketika aktivitas acara yang didukung terjadi di GuardDuty, aktivitas tersebut direkam dalam suatu CloudTrail peristiwa bersama dengan peristiwa AWS layanan lainnya dalam riwayat Acara. Anda dapat melihat, mencari, dan mengunduh acara terbaru di AWS akun Anda. Untuk informasi selengkapnya, lihat [Melihat peristiwa dengan riwayat CloudTrail acara](#).

Untuk catatan peristiwa yang sedang berlangsung di AWS akun Anda, termasuk acara untuk GuardDuty, buat jejak. Jejak memungkinkan CloudTrail untuk mengirimkan file log ke bucket Amazon S3. Secara default, ketika Anda membuat jejak di konsol, jejak diterapkan ke semua Region. Jejak mencatat peristiwa dari semua Wilayah di AWS partisi dan mengirimkan file log ke bucket Amazon S3 yang Anda tentukan. Selain itu, Anda dapat mengonfigurasi AWS layanan lain untuk menganalisis lebih lanjut dan menindaklanjuti data peristiwa yang dikumpulkan dalam CloudTrail log. Untuk informasi selengkapnya, lihat:

- [Ikhtisar untuk membuat jejak](#)
- [CloudTrail layanan dan integrasi yang didukung](#)
- [Mengonfigurasi notifikasi Amazon SNS untuk CloudTrail](#)
- [Menerima file CloudTrail log dari beberapa wilayah](#) dan [Menerima file CloudTrail log dari beberapa akun](#)

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

- Apakah permintaan dibuat dengan pengguna root atau kredensial masuk pengguna IAM
- Baik permintaan tersebut dibuat dengan kredensial keamanan sementara untuk peran atau pengguna gabungan
- Apakah permintaan itu dibuat oleh AWS layanan lain

Untuk informasi selengkapnya, lihat elemen [CloudTrail UserIdentity](#).

GuardDuty peristiwa pesawat kontrol di CloudTrail

Secara default, CloudTrail mencatat semua operasi GuardDuty API yang disediakan di [Referensi Amazon GuardDuty API](#) sebagai peristiwa dalam CloudTrail file.

GuardDuty peristiwa data di CloudTrail

[GuardDuty Pemantauan Runtime](#) menggunakan agen GuardDuty keamanan yang diterapkan ke cluster Amazon Elastic Kubernetes Service (Amazon EKS), instans Amazon Elastic Compute Cloud (Amazon) AWS Fargate, dan (EC2 Amazon Elastic Container Service (Amazon ECS) saja) tugas untuk `aws-guardduty-agent` mengumpulkan add-on ([Jenis acara runtime yang dikumpulkan](#)) yang AWS mengumpulkan beban kerja Anda dan kemudian mengirimkannya ke untuk deteksi dan analisis ancaman. GuardDuty

Pencatatan dan pemantauan peristiwa data

Anda dapat mengonfigurasi AWS CloudTrail log secara opsional untuk melihat peristiwa data untuk agen GuardDuty keamanan Anda.

Untuk membuat dan mengonfigurasi CloudTrail, lihat [Peristiwa data](#) di Panduan AWS CloudTrail Pengguna dan ikuti petunjuk untuk Mencatat peristiwa data dengan pemilih peristiwa lanjutan di AWS Management Console. Saat mencatat jejak, pastikan untuk membuat perubahan berikut:

- Untuk tipe peristiwa Data, pilih GuardDutydetektor.
- Untuk template pemilih Log, pilih Log semua peristiwa.
- Perluas tampilan JSON untuk konfigurasi. Ini harus mirip dengan JSON berikut:

```
[
  {
    "name": "",
    "fieldSelectors": [
      {
        "field": "eventCategory",
        "equals": [
          "Data"
        ]
      },
      {
        "field": "resources.type",
        "equals": [
          "AWS::GuardDuty::Detector"
        ]
      }
    ]
  }
]
```

Setelah Anda mengaktifkan pemilih untuk jejak, navigasikan ke konsol Amazon S3 di <https://console.aws.amazon.com/s3/> Anda dapat mengunduh peristiwa data dari bucket S3 yang dipilih pada saat mengonfigurasi log. CloudTrail

Contoh: entri file GuardDuty log

Trail adalah konfigurasi yang memungkinkan pengiriman peristiwa sebagai file log ke bucket Amazon S3 yang Anda tentukan. CloudTrail file log berisi satu atau lebih entri log. Peristiwa mewakili permintaan tunggal dari sumber manapun dan mencakup informasi tentang tindakan yang diminta, tanggal dan waktu tindakan, parameter permintaan, dan sebagainya. CloudTrail file log bukanlah jejak tumpukan yang diurutkan dari panggilan API publik, jadi file tersebut tidak muncul dalam urutan tertentu.

Contoh berikut menunjukkan entri CloudTrail log yang menunjukkan peristiwa bidang data.

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "111122223333:aws:ec2-instance:i-123412341234example",
    "arn": "arn:aws:sts::111122223333:assumed-role/aws:ec2-  
instance/i-123412341234example",
    "accountId": "111122223333",
    "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "111122223333:aws:ec2-instance",
        "arn": "arn:aws:iam::111122223333:role/aws:ec2-instance",
        "accountId": "111122223333",
        "userName": "aws:ec2-instance"
      },
      "attributes": {
        "creationDate": "2023-03-05T04:00:21Z",
        "mfaAuthenticated": "false"
      }
    },
    "ec2RoleDelivery": "2.0"
  },
  "eventTime": "2023-03-05T06:03:49Z",
  "eventSource": "guardduty.amazonaws.com",
  "eventName": "SendSecurityTelemetry",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "54.240.230.177",
  "userAgent": "aws-sdk-rust/0.54.1 os/linux lang/rust/1.66.0",
  "requestParameters": null,
```

```

    "responseElements": null,
    "requestID": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "eventID": "a1b2c3d4-5678-90ab-cdef-EXAMPLEebbbb",
    "readOnly": false,
    "resources": [{
      "accountId": "111122223333",
      "type": "AWS::GuardDuty::Detector",
      "ARN": "arn:aws:guardduty:us-
west-2:111122223333:detector/12abc34d567e8fa901bc2d34e56789f0"
    }],
    "eventType": "AwsApiCall",
    "managementEvent": false,
    "recipientAccountId": "111122223333",
    "eventCategory": "Data",
    "tlsDetails": {
      "tlsVersion": "TLSv1.2",
      "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
      "clientProvidedHostHeader": "guardduty-data.us-east-1.amazonaws.com"
    }
  }
}

```

Contoh berikut menunjukkan entri CloudTrail log yang menunjukkan CreateIPThreatIntelSet tindakan (peristiwa bidang kontrol).

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
    "arn": "arn:aws:iam::444455556666:user/Alice",
    "accountId": "444455556666",
    "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2018-06-14T22:54:20Z"
      }
    },
    "sessionIssuer": {
      "type": "Role",
      "principalId": "AIDACKCEVSQ6C2EXAMPLE",
      "arn": "arn:aws:iam::444455556666:user/Alice",
      "accountId": "444455556666",
      "userName": "Alice"
    }
  }
}

```

```
    }  
  },  
  "eventTime": "2018-06-14T22:57:56Z",  
  "eventSource": "guardduty.amazonaws.com",  
  "eventName": "CreateThreatIntelSet",  
  "awsRegion": "us-west-2",  
  "sourceIPAddress": "54.240.230.177",  
  "userAgent": "console.amazonaws.com",  
  "requestParameters": {  
    "detectorId": "12abc34d567e8fa901bc2d34e56789f0",  
    "name": "Example",  
    "format": "TXT",  
    "activate": false,  
    "location": "https://s3.amazonaws.com/bucket.name/file.txt"  
  },  
  "responseElements": {  
    "threatIntelSetId": "1ab200428351c99d859bf61992460d24"  
  },  
  "requestID": "5f6bf981-7026-11e8-a9fc-5b37d2684c5c",  
  "eventID": "81337b11-e5c8-4f91-b141-deb405625bc9",  
  "readOnly": false,  
  "eventType": "AwsApiCall",  
  "recipientAccountId": "444455556666"  
}
```

Dari informasi acara ini, Anda dapat menentukan bahwa permintaan dibuat untuk membuat daftar ancaman Example di GuardDuty. Anda juga dapat melihat bahwa permintaan tersebut dibuat oleh pengguna bernama Alice pada 14 Juni 2018.

Identity and Access Management untuk Amazon GuardDuty

AWS Identity and Access Management (IAM) adalah Layanan AWS yang membantu administrator mengontrol akses ke AWS sumber daya dengan aman. Administrator IAM mengontrol siapa yang dapat diautentikasi (masuk) dan diberi wewenang (memiliki izin) untuk menggunakan sumber daya. GuardDuty IAM adalah Layanan AWS yang dapat Anda gunakan tanpa biaya tambahan.

Topik

- [Audiens](#)
- [Mengautentikasi dengan identitas](#)

- [Mengelola akses menggunakan kebijakan](#)
- [Bagaimana Amazon GuardDuty bekerja dengan IAM](#)
- [Contoh kebijakan berbasis identitas untuk Amazon GuardDuty](#)
- [Menggunakan peran tertaut layanan untuk Amazon GuardDuty](#)
- [AWS kebijakan terkelola untuk Amazon GuardDuty](#)
- [Memecahkan masalah GuardDuty identitas dan akses Amazon](#)

Audiens

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

Pengguna layanan — Jika Anda menggunakan GuardDuty layanan untuk melakukan pekerjaan Anda, administrator Anda memberi Anda kredensi dan izin yang Anda butuhkan. Saat Anda menggunakan lebih banyak GuardDuty fitur untuk melakukan pekerjaan Anda, Anda mungkin memerlukan izin tambahan. Memahami cara mengelola akses dapat membantu Anda meminta izin yang tepat dari administrator Anda. Jika Anda tidak dapat mengakses fitur di GuardDuty, lihat [Memecahkan masalah GuardDuty identitas dan akses Amazon](#).

Administrator layanan — Jika Anda bertanggung jawab atas GuardDuty sumber daya di perusahaan Anda, Anda mungkin memiliki akses penuh ke GuardDuty. Tugas Anda adalah menentukan GuardDuty fitur dan sumber daya mana yang harus diakses pengguna layanan Anda. Kemudian, Anda harus mengirimkan permintaan kepada administrator IAM untuk mengubah izin pengguna layanan Anda. Tinjau informasi di halaman ini untuk memahami konsep dasar IAM. Untuk mempelajari lebih lanjut tentang bagaimana perusahaan Anda dapat menggunakan IAM GuardDuty, lihat [Bagaimana Amazon GuardDuty bekerja dengan IAM](#).

Administrator IAM – Jika Anda adalah administrator IAM, Anda mungkin ingin belajar dengan lebih detail tentang cara Anda menulis kebijakan untuk mengelola akses ke GuardDuty. Untuk melihat contoh kebijakan GuardDuty berbasis identitas yang dapat Anda gunakan di IAM, lihat. [Contoh kebijakan berbasis identitas untuk Amazon GuardDuty](#)

Mengautentikasi dengan identitas

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

Anda dapat masuk AWS sebagai identitas federasi dengan menggunakan kredensi yang disediakan melalui sumber identitas. AWS IAM Identity Center Pengguna (IAM Identity Center), autentikasi masuk tunggal perusahaan Anda, dan kredensi Google atau Facebook Anda adalah contoh identitas federasi. Saat Anda masuk sebagai identitas terfederasi, administrator Anda sebelumnya menyiapkan federasi identitas menggunakan peran IAM. Ketika Anda mengakses AWS dengan menggunakan federasi, Anda secara tidak langsung mengambil peran.

Bergantung pada jenis pengguna Anda, Anda dapat masuk ke AWS Management Console atau portal AWS akses. Untuk informasi selengkapnya tentang masuk AWS, lihat [Cara masuk ke Panduan AWS Sign-In Pengguna Anda Akun AWS](#).

Jika Anda mengakses AWS secara terprogram, AWS sediakan kit pengembangan perangkat lunak (SDK) dan antarmuka baris perintah (CLI) untuk menandatangani permintaan Anda secara kriptografis dengan menggunakan kredensial Anda. Jika Anda tidak menggunakan AWS alat, Anda harus menandatangani permintaan sendiri. Guna mengetahui informasi selengkapnya tentang penggunaan metode yang disarankan untuk menandatangani permintaan sendiri, lihat [AWS Signature Version 4 untuk permintaan API](#) dalam Panduan Pengguna IAM.

Apa pun metode autentikasi yang digunakan, Anda mungkin diminta untuk menyediakan informasi keamanan tambahan. Misalnya, AWS merekomendasikan agar Anda menggunakan otentikasi multi-faktor (MFA) untuk meningkatkan keamanan akun Anda. Untuk mempelajari selengkapnya, lihat [Autentikasi multi-faktor](#) dalam Panduan Pengguna AWS IAM Identity Center dan [Autentikasi multi-faktor AWS di IAM](#) dalam Panduan Pengguna IAM.

Akun AWS pengguna root

Saat Anda membuat Akun AWS, Anda mulai dengan satu identitas masuk yang memiliki akses lengkap ke semua Layanan AWS dan sumber daya di akun. Identitas ini disebut pengguna Akun AWS root dan diakses dengan masuk dengan alamat email dan kata sandi yang Anda gunakan untuk membuat akun. Kami sangat menyarankan agar Anda tidak menggunakan pengguna root untuk tugas sehari-hari. Lindungi kredensial pengguna root Anda dan gunakan kredensial tersebut untuk melakukan tugas yang hanya dapat dilakukan pengguna root. Untuk daftar lengkap tugas yang mengharuskan Anda masuk sebagai pengguna root, lihat [Tugas yang memerlukan kredensial pengguna root](#) dalam Panduan Pengguna IAM.

Identitas gabungan

Sebagai praktik terbaik, mewajibkan pengguna manusia, termasuk pengguna yang memerlukan akses administrator, untuk menggunakan federasi dengan penyedia identitas untuk mengakses Layanan AWS dengan menggunakan kredensi sementara.

Identitas federasi adalah pengguna dari direktori pengguna perusahaan Anda, penyedia identitas web, direktori Pusat Identitas AWS Directory Service, atau pengguna mana pun yang mengakses Layanan AWS dengan menggunakan kredensial yang disediakan melalui sumber identitas. Ketika identitas federasi mengakses Akun AWS, mereka mengambil peran, dan peran memberikan kredensi sementara.

Untuk manajemen akses terpusat, kami sarankan Anda menggunakan AWS IAM Identity Center. Anda dapat membuat pengguna dan grup di Pusat Identitas IAM, atau Anda dapat menghubungkan dan menyinkronkan ke sekumpulan pengguna dan grup di sumber identitas Anda sendiri untuk digunakan di semua aplikasi Akun AWS dan aplikasi Anda. Untuk informasi tentang Pusat Identitas IAM, lihat [Apakah itu Pusat Identitas IAM?](#) dalam Panduan Pengguna AWS IAM Identity Center .

Pengguna dan grup IAM

[Pengguna IAM](#) adalah identitas dalam diri Anda Akun AWS yang memiliki izin khusus untuk satu orang atau aplikasi. Jika memungkinkan, kami merekomendasikan untuk mengandalkan kredensial sementara, bukan membuat pengguna IAM yang memiliki kredensial jangka panjang seperti kata sandi dan kunci akses. Namun, jika Anda memiliki kasus penggunaan tertentu yang memerlukan kredensial jangka panjang dengan pengguna IAM, kami merekomendasikan Anda merotasi kunci akses. Untuk informasi selengkapnya, lihat [Merotasi kunci akses secara teratur untuk kasus penggunaan yang memerlukan kredensial jangka panjang](#) dalam Panduan Pengguna IAM.

[Grup IAM](#) adalah identitas yang menentukan sekumpulan pengguna IAM. Anda tidak dapat masuk sebagai grup. Anda dapat menggunakan grup untuk menentukan izin bagi beberapa pengguna sekaligus. Grup mempermudah manajemen izin untuk sejumlah besar pengguna sekaligus. Misalnya, Anda dapat meminta kelompok untuk menyebutkan IAMAdmins dan memberikan izin kepada grup tersebut untuk mengelola sumber daya IAM.

Pengguna berbeda dari peran. Pengguna secara unik terkait dengan satu orang atau aplikasi, tetapi peran dimaksudkan untuk dapat digunakan oleh siapa pun yang membutuhkannya. Pengguna memiliki kredensial jangka panjang permanen, tetapi peran memberikan kredensial sementara. Untuk mempelajari selengkapnya, lihat [Kasus penggunaan untuk pengguna IAM](#) dalam Panduan Pengguna IAM.

Peran IAM

[Peran IAM](#) adalah identitas dalam diri Anda Akun AWS yang memiliki izin khusus. Peran ini mirip dengan pengguna IAM, tetapi tidak terkait dengan orang tertentu. Untuk mengambil peran IAM sementara AWS Management Console, Anda dapat [beralih dari pengguna ke peran IAM \(konsol\)](#). Anda dapat mengambil peran dengan memanggil operasi AWS CLI atau AWS API atau dengan menggunakan URL kustom. Untuk informasi selengkapnya tentang cara menggunakan peran, lihat [Metode untuk mengambil peran](#) dalam Panduan Pengguna IAM.

Peran IAM dengan kredensial sementara berguna dalam situasi berikut:

- Akses pengguna terfederasi – Untuk menetapkan izin ke identitas terfederasi, Anda membuat peran dan menentukan izin untuk peran tersebut. Ketika identitas terfederasi mengautentikasi, identitas tersebut terhubung dengan peran dan diberi izin yang ditentukan oleh peran. Untuk informasi tentang peran untuk federasi, lihat [Buat peran untuk penyedia identitas pihak ketiga](#) dalam Panduan Pengguna IAM. Jika menggunakan Pusat Identitas IAM, Anda harus mengonfigurasi set izin. Untuk mengontrol apa yang dapat diakses identitas Anda setelah identitas tersebut diautentikasi, Pusat Identitas IAM akan mengorelasikan set izin ke peran dalam IAM. Untuk informasi tentang set izin, lihat [Set izin](#) dalam Panduan Pengguna AWS IAM Identity Center .
- Izin pengguna IAM sementara – Pengguna atau peran IAM dapat mengambil peran IAM guna mendapatkan berbagai izin secara sementara untuk tugas tertentu.
- Akses lintas akun – Anda dapat menggunakan peran IAM untuk mengizinkan seseorang (prinsipal tepercaya) di akun lain untuk mengakses sumber daya di akun Anda. Peran adalah cara utama untuk memberikan akses lintas akun. Namun, dengan beberapa Layanan AWS, Anda dapat melampirkan kebijakan secara langsung ke sumber daya (alih-alih menggunakan peran sebagai proxy). Untuk mempelajari perbedaan antara peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat [Akses sumber daya lintas akun di IAM](#) dalam Panduan Pengguna IAM.
- Akses lintas layanan — Beberapa Layanan AWS menggunakan fitur lain Layanan AWS. Misalnya, saat Anda melakukan panggilan dalam suatu layanan, biasanya layanan tersebut menjalankan aplikasi di Amazon EC2 atau menyimpan objek di Amazon S3. Sebuah layanan mungkin melakukannya menggunakan izin prinsipal yang memanggil, menggunakan peran layanan, atau peran terkait layanan.
- Sesi akses teruskan (FAS) — Saat Anda menggunakan pengguna atau peran IAM untuk melakukan tindakan AWS, Anda dianggap sebagai prinsipal. Ketika Anda menggunakan beberapa layanan, Anda mungkin melakukan sebuah tindakan yang kemudian menginisiasi tindakan lain di layanan yang berbeda. FAS menggunakan izin dari pemanggilan utama Layanan AWS, dikombinasikan dengan permintaan Layanan AWS untuk membuat permintaan ke layanan

hilir. Permintaan FAS hanya dibuat ketika layanan menerima permintaan yang memerlukan interaksi dengan orang lain Layanan AWS atau sumber daya untuk menyelesaikannya. Dalam hal ini, Anda harus memiliki izin untuk melakukan kedua tindakan tersebut. Untuk detail kebijakan ketika mengajukan permintaan FAS, lihat [Sesi akses maju](#).

- Peran layanan – Peran layanan adalah [peran IAM](#) yang dijalankan oleh layanan untuk melakukan tindakan atas nama Anda. Administrator IAM dapat membuat, mengubah, dan menghapus peran layanan dari dalam IAM. Untuk informasi selengkapnya, lihat [Buat sebuah peran untuk mendelegasikan izin ke Layanan AWS](#) dalam Panduan pengguna IAM.
- Peran terkait layanan — Peran terkait layanan adalah jenis peran layanan yang ditautkan ke peran layanan. Layanan AWS Layanan tersebut dapat menjalankan peran untuk melakukan tindakan atas nama Anda. Peran terkait layanan muncul di Anda Akun AWS dan dimiliki oleh layanan. Administrator IAM dapat melihat, tetapi tidak dapat mengedit izin untuk peran terkait layanan.
- Aplikasi yang berjalan di Amazon EC2 — Anda dapat menggunakan peran IAM untuk mengelola kredensi sementara untuk aplikasi yang berjalan pada EC2 instance dan membuat AWS CLI atau AWS permintaan API. Ini lebih baik untuk menyimpan kunci akses dalam EC2 instance. Untuk menetapkan AWS peran ke EC2 instance dan membuatnya tersedia untuk semua aplikasinya, Anda membuat profil instance yang dilampirkan ke instance. Profil instance berisi peran dan memungkinkan program yang berjalan pada EC2 instance untuk mendapatkan kredensi sementara. Untuk informasi selengkapnya, lihat [Menggunakan peran IAM untuk memberikan izin ke aplikasi yang berjalan di EC2 instans Amazon di Panduan Pengguna](#) IAM.

Mengelola akses menggunakan kebijakan

Anda mengontrol akses AWS dengan membuat kebijakan dan melampirkannya ke AWS identitas atau sumber daya. Kebijakan adalah objek AWS yang, ketika dikaitkan dengan identitas atau sumber daya, menentukan izinnya. AWS mengevaluasi kebijakan ini ketika prinsipal (pengguna, pengguna root, atau sesi peran) membuat permintaan. Izin dalam kebijakan menentukan apakah permintaan diizinkan atau ditolak. Sebagian besar kebijakan disimpan AWS sebagai dokumen JSON. Untuk informasi selengkapnya tentang struktur dan isi dokumen kebijakan JSON, lihat [Gambaran umum kebijakan JSON](#) dalam Panduan Pengguna IAM.

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Artinya, prinsipal manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan kondisi apa.

Secara default, pengguna dan peran tidak memiliki izin. Untuk memberikan izin kepada pengguna untuk melakukan tindakan di sumber daya yang mereka perlukan, administrator IAM dapat membuat kebijakan IAM. Administrator kemudian dapat menambahkan kebijakan IAM ke peran, dan pengguna dapat mengambil peran.

Kebijakan IAM mendefinisikan izin untuk suatu tindakan terlepas dari metode yang Anda gunakan untuk melakukan operasinya. Misalnya, anggaplah Anda memiliki kebijakan yang mengizinkan tindakan `iam:GetRole`. Pengguna dengan kebijakan tersebut bisa mendapatkan informasi peran dari AWS Management Console, API AWS CLI, atau AWS API.

Kebijakan berbasis identitas

Kebijakan berbasis identitas adalah dokumen kebijakan izin JSON yang dapat Anda lampirkan ke sebuah identitas, seperti pengguna IAM, grup pengguna IAM, atau peran IAM. Kebijakan ini mengontrol jenis tindakan yang dapat dilakukan oleh pengguna dan peran, di sumber daya mana, dan berdasarkan kondisi seperti apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, lihat [Tentukan izin IAM kustom dengan kebijakan terkelola pelanggan](#) dalam Panduan Pengguna IAM.

Kebijakan berbasis identitas dapat dikategorikan lebih lanjut sebagai kebijakan inline atau kebijakan yang dikelola. Kebijakan inline disematkan langsung ke satu pengguna, grup, atau peran. Kebijakan terkelola adalah kebijakan mandiri yang dapat Anda lampirkan ke beberapa pengguna, grup, dan peran dalam Akun AWS. Kebijakan AWS terkelola mencakup kebijakan terkelola dan kebijakan yang dikelola pelanggan. Untuk mempelajari cara memilih antara kebijakan yang dikelola atau kebijakan inline, lihat [Pilih antara kebijakan yang dikelola dan kebijakan inline](#) dalam Panduan Pengguna IAM.

Kebijakan berbasis sumber daya

Kebijakan berbasis sumber daya adalah dokumen kebijakan JSON yang Anda lampirkan ke sumber daya. Contoh kebijakan berbasis sumber daya adalah kebijakan kepercayaan peran IAM dan kebijakan bucket Amazon S3. Dalam layanan yang mendukung kebijakan berbasis sumber daya, administrator layanan dapat menggunakannya untuk mengontrol akses ke sumber daya tertentu. Untuk sumber daya tempat kebijakan dilampirkan, kebijakan menentukan tindakan apa yang dapat dilakukan oleh prinsipal tertentu pada sumber daya tersebut dan dalam kondisi apa. Anda harus [menentukan prinsipal](#) dalam kebijakan berbasis sumber daya. Prinsipal dapat mencakup akun, pengguna, peran, pengguna federasi, atau Layanan AWS.

Kebijakan berbasis sumber daya merupakan kebijakan inline yang terletak di layanan tersebut. Anda tidak dapat menggunakan kebijakan AWS terkelola dari IAM dalam kebijakan berbasis sumber daya.

Daftar kontrol akses (ACLs)

Access control lists (ACLs) mengontrol prinsipal mana (anggota akun, pengguna, atau peran) yang memiliki izin untuk mengakses sumber daya. ACLs mirip dengan kebijakan berbasis sumber daya, meskipun mereka tidak menggunakan format dokumen kebijakan JSON.

Amazon S3, AWS WAF, dan Amazon VPC adalah contoh layanan yang mendukung ACLs.

Untuk mempelajari selengkapnya ACLs, lihat [Ringkasan daftar kontrol akses \(ACL\)](#) di Panduan Pengembang Layanan Penyimpanan Sederhana Amazon.

Jenis-jenis kebijakan lain

AWS mendukung jenis kebijakan tambahan yang kurang umum. Jenis-jenis kebijakan ini dapat mengatur izin maksimum yang diberikan kepada Anda oleh jenis kebijakan yang lebih umum.

- **Batasan izin** – Batasan izin adalah fitur lanjutan tempat Anda mengatur izin maksimum yang dapat diberikan oleh kebijakan berbasis identitas ke entitas IAM (pengguna IAM atau peran IAM). Anda dapat menetapkan batasan izin untuk suatu entitas. Izin yang dihasilkan adalah perpotongan antara kebijakan berbasis identitas milik entitas dan batasan izinnya. Kebijakan berbasis sumber daya yang menentukan pengguna atau peran dalam bidang `Principal` tidak dibatasi oleh batasan izin. Penolakan eksplisit dalam salah satu kebijakan ini akan menggantikan pemberian izin. Untuk informasi selengkapnya tentang batasan izin, lihat [Batasan izin untuk entitas IAM](#) dalam Panduan Pengguna IAM.
- **Kebijakan kontrol layanan (SCPs)** — SCPs adalah kebijakan JSON yang menentukan izin maksimum untuk organisasi atau unit organisasi (OU) di AWS Organizations. AWS Organizations adalah layanan untuk mengelompokkan dan mengelola secara terpusat beberapa Akun AWS yang dimiliki bisnis Anda. Jika Anda mengaktifkan semua fitur dalam organisasi, Anda dapat menerapkan kebijakan kontrol layanan (SCPs) ke salah satu atau semua akun Anda. SCP membatasi izin untuk entitas di akun anggota, termasuk masing-masing. Pengguna root akun AWS. Untuk informasi selengkapnya tentang Organizations dan SCPs, lihat [Kebijakan kontrol layanan](#) di Panduan AWS Organizations Pengguna.
- **Kebijakan kontrol sumber daya (RCPs)** — RCPs adalah kebijakan JSON yang dapat Anda gunakan untuk menetapkan izin maksimum yang tersedia untuk sumber daya di akun Anda tanpa memperbarui kebijakan IAM yang dilampirkan ke setiap sumber daya yang Anda miliki. RCP membatasi izin untuk sumber daya di akun anggota dan dapat memengaruhi izin efektif untuk identitas, termasuk Pengguna root akun AWS, terlepas dari apakah itu milik organisasi Anda. Untuk informasi selengkapnya tentang Organizations dan RCPs, termasuk daftar dukungan

Layanan AWS tersebut RCPs, lihat [Kebijakan kontrol sumber daya \(RCPs\)](#) di Panduan AWS Organizations Pengguna.

- Kebijakan sesi – Kebijakan sesi adalah kebijakan lanjutan yang Anda berikan sebagai parameter ketika Anda membuat sesi sementara secara programatis untuk peran atau pengguna terfederasi. Izin sesi yang dihasilkan adalah perpotongan antara kebijakan berbasis identitas pengguna atau peran dan kebijakan sesi. Izin juga bisa datang dari kebijakan berbasis sumber daya. Penolakan eksplisit dalam salah satu kebijakan ini akan menggantikan pemberian izin. Untuk informasi selengkapnya, lihat [Kebijakan sesi](#) dalam Panduan Pengguna IAM.

Berbagai jenis kebijakan

Ketika beberapa jenis kebijakan berlaku pada suatu permintaan, izin yang dihasilkan lebih rumit untuk dipahami. Untuk mempelajari cara AWS menentukan apakah akan mengizinkan permintaan saat beberapa jenis kebijakan terlibat, lihat [Logika evaluasi kebijakan](#) di Panduan Pengguna IAM.

Bagaimana Amazon GuardDuty bekerja dengan IAM

Sebelum Anda menggunakan IAM untuk mengelola akses GuardDuty, pelajari fitur IAM yang tersedia untuk digunakan. GuardDuty

Fitur IAM yang dapat Anda gunakan dengan Amazon GuardDuty

Fitur IAM	GuardDuty dukungan
Kebijakan berbasis identitas	Ya
Kebijakan berbasis sumber daya	Tidak
Tindakan kebijakan	Ya
Sumber daya kebijakan	Ya
Kunci kondisi kebijakan	Ya
ACLs	Tidak
ABAC (tanda dalam kebijakan)	Parsial
Kredensial sementara	Ya

Fitur IAM	GuardDuty dukungan
Izin principal	Ya
Peran layanan	Ya
Peran terkait layanan	Ya

Untuk mendapatkan tampilan tingkat tinggi tentang cara GuardDuty dan AWS layanan lain bekerja dengan sebagian besar fitur IAM, lihat [AWS layanan yang bekerja dengan IAM di Panduan Pengguna IAM](#).

Kebijakan berbasis identitas untuk GuardDuty

Mendukung kebijakan berbasis identitas: Ya

Kebijakan berbasis identitas adalah dokumen kebijakan izin JSON yang dapat Anda lampirkan ke sebuah identitas, seperti pengguna IAM, grup pengguna IAM, atau peran IAM. Kebijakan ini mengontrol jenis tindakan yang dapat dilakukan oleh pengguna dan peran, di sumber daya mana, dan berdasarkan kondisi seperti apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, lihat [Tentukan izin IAM kustom dengan kebijakan terkelola pelanggan](#) dalam Panduan Pengguna IAM.

Dengan kebijakan berbasis identitas IAM, Anda dapat menentukan secara spesifik apakah tindakan dan sumber daya diizinkan atau ditolak, serta kondisi yang menjadi dasar dikabulkan atau ditolaknya tindakan tersebut. Anda tidak dapat menentukan secara spesifik prinsipal dalam sebuah kebijakan berbasis identitas karena prinsipal berlaku bagi pengguna atau peran yang melekat kepadanya. Untuk mempelajari semua elemen yang dapat Anda gunakan dalam kebijakan JSON, lihat [Referensi elemen kebijakan JSON IAM](#) dalam Panduan Pengguna IAM.

Contoh kebijakan berbasis identitas untuk GuardDuty

Untuk melihat contoh kebijakan GuardDuty berbasis identitas, lihat. [Contoh kebijakan berbasis identitas untuk Amazon GuardDuty](#)

Kebijakan berbasis sumber daya dalam GuardDuty

Mendukung kebijakan berbasis sumber daya: Tidak

Kebijakan berbasis sumber daya adalah dokumen kebijakan JSON yang Anda lampirkan ke sumber daya. Contoh kebijakan berbasis sumber daya adalah kebijakan kepercayaan peran IAM dan kebijakan bucket Amazon S3. Dalam layanan yang mendukung kebijakan berbasis sumber daya, administrator layanan dapat menggunakannya untuk mengontrol akses ke sumber daya tertentu. Untuk sumber daya tempat kebijakan dilampirkan, kebijakan menentukan tindakan apa yang dapat dilakukan oleh prinsipal tertentu pada sumber daya tersebut dan dalam kondisi apa. Anda harus [menentukan prinsipal](#) dalam kebijakan berbasis sumber daya. Prinsipal dapat mencakup akun, pengguna, peran, pengguna federasi, atau. Layanan AWS

Untuk mengaktifkan akses lintas akun, Anda dapat menentukan secara spesifik seluruh akun atau entitas IAM di akun lain sebagai prinsipal dalam kebijakan berbasis sumber daya. Menambahkan prinsipal akun silang ke kebijakan berbasis sumber daya hanya setengah dari membangun hubungan kepercayaan. Ketika prinsipal dan sumber daya berbeda Akun AWS, administrator IAM di akun tepercaya juga harus memberikan izin entitas utama (pengguna atau peran) untuk mengakses sumber daya. Mereka memberikan izin dengan melampirkan kebijakan berbasis identitas kepada entitas. Namun, jika kebijakan berbasis sumber daya memberikan akses ke principal dalam akun yang sama, tidak diperlukan kebijakan berbasis identitas tambahan. Untuk informasi selengkapnya, lihat [Akses sumber daya lintas akun di IAM](#) dalam Panduan Pengguna IAM.

Tindakan kebijakan untuk GuardDuty

Mendukung tindakan kebijakan: Ya

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Artinya, prinsipal manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan kondisi apa.

Elemen `Action` dari kebijakan JSON menjelaskan tindakan yang dapat Anda gunakan untuk mengizinkan atau menolak akses dalam sebuah kebijakan. Tindakan kebijakan biasanya memiliki nama yang sama dengan operasi AWS API terkait. Ada beberapa pengecualian, misalnya tindakan hanya izin yang tidak memiliki operasi API yang cocok. Ada juga beberapa operasi yang memerlukan beberapa tindakan dalam suatu kebijakan. Tindakan tambahan ini disebut tindakan dependen.

Sertakan tindakan dalam kebijakan untuk memberikan izin untuk melakukan operasi terkait.

Untuk melihat daftar GuardDuty tindakan, lihat [Tindakan yang ditentukan oleh Amazon GuardDuty](#) di Referensi Otorisasi Layanan.

Tindakan kebijakan GuardDuty menggunakan awalan berikut sebelum tindakan:

```
guardduty
```

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

```
"Action": [  
    "guardduty:action1",  
    "guardduty:action2"  
]
```

Untuk melihat contoh kebijakan GuardDuty berbasis identitas, lihat. [Contoh kebijakan berbasis identitas untuk Amazon GuardDuty](#)

Sumber daya kebijakan untuk GuardDuty

Mendukung sumber daya kebijakan: Ya

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Artinya, prinsipal manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan kondisi apa.

Elemen kebijakan JSON `Resource` menentukan objek yang menjadi target penerapan tindakan. Pernyataan harus menyertakan elemen `Resource` atau `NotResource`. Praktik terbaiknya, tentukan sumber daya menggunakan [Amazon Resource Name \(ARN\)](#). Anda dapat melakukan ini untuk tindakan yang mendukung jenis sumber daya tertentu, yang dikenal sebagai izin tingkat sumber daya.

Untuk tindakan yang tidak mendukung izin di tingkat sumber daya, misalnya operasi pencantuman, gunakan wildcard (*) untuk menunjukkan bahwa pernyataan tersebut berlaku untuk semua sumber daya.

```
"Resource": "*"
```

Untuk melihat daftar jenis sumber daya dan jenis GuardDuty sumber daya ARNs, lihat [Sumber daya yang ditentukan oleh Amazon GuardDuty](#) di Referensi Otorisasi Layanan. Untuk mempelajari tindakan mana yang dapat Anda tentukan ARN dari setiap sumber daya, lihat [Tindakan yang ditentukan oleh Amazon](#). GuardDuty

Untuk melihat contoh kebijakan GuardDuty berbasis identitas, lihat. [Contoh kebijakan berbasis identitas untuk Amazon GuardDuty](#)

Kunci kondisi kebijakan untuk GuardDuty

Mendukung kunci kondisi kebijakan khusus layanan: Yes

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Artinya, prinsipal manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan kondisi apa.

Elemen Condition (atau blok Condition) akan memungkinkan Anda menentukan kondisi yang menjadi dasar suatu pernyataan berlaku. Elemen Condition bersifat opsional. Anda dapat membuat ekspresi bersyarat yang menggunakan [operator kondisi](#), misalnya sama dengan atau kurang dari, untuk mencocokkan kondisi dalam kebijakan dengan nilai-nilai yang diminta.

Jika Anda menentukan beberapa elemen Condition dalam sebuah pernyataan, atau beberapa kunci dalam elemen Condition tunggal, maka AWS akan mengevaluasinya menggunakan operasi AND logis. Jika Anda menentukan beberapa nilai untuk satu kunci kondisi, AWS mengevaluasi kondisi menggunakan OR operasi logis. Semua kondisi harus dipenuhi sebelum izin pernyataan diberikan.

Anda juga dapat menggunakan variabel placeholder saat menentukan kondisi. Sebagai contoh, Anda dapat memberikan izin kepada pengguna IAM untuk mengakses sumber daya hanya jika izin tersebut mempunyai tanda yang sesuai dengan nama pengguna IAM mereka. Untuk informasi selengkapnya, lihat [Elemen kebijakan IAM: variabel dan tanda](#) dalam Panduan Pengguna IAM.

AWS mendukung kunci kondisi global dan kunci kondisi khusus layanan. Untuk melihat semua kunci kondisi AWS global, lihat [kunci konteks kondisi AWS global](#) di Panduan Pengguna IAM.

Untuk melihat daftar kunci GuardDuty kondisi, lihat [Kunci kondisi untuk Amazon GuardDuty](#) di Referensi Otorisasi Layanan. Untuk mempelajari tindakan dan sumber daya yang dapat Anda gunakan kunci kondisi, lihat [Tindakan yang ditentukan oleh Amazon GuardDuty](#).

Untuk melihat contoh kebijakan GuardDuty berbasis identitas, lihat. [Contoh kebijakan berbasis identitas untuk Amazon GuardDuty](#)

Daftar kontrol akses (ACLs) di GuardDuty

Mendukung ACLs: Tidak

Access control lists (ACLs) mengontrol prinsipal mana (anggota akun, pengguna, atau peran) yang memiliki izin untuk mengakses sumber daya. ACLs mirip dengan kebijakan berbasis sumber daya, meskipun mereka tidak menggunakan format dokumen kebijakan JSON.

Kontrol akses berbasis atribut (ABAC) dengan GuardDuty

Mendukung ABAC (tag dalam kebijakan): Sebagian

Kontrol akses berbasis atribut (ABAC) adalah strategi otorisasi yang menentukan izin berdasarkan atribut. Dalam AWS, atribut ini disebut tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke banyak AWS sumber daya. Penandaan ke entitas dan sumber daya adalah langkah pertama dari ABAC. Kemudian rancanglah kebijakan ABAC untuk mengizinkan operasi ketika tanda milik prinsipal cocok dengan tanda yang ada di sumber daya yang ingin diakses.

ABAC sangat berguna di lingkungan yang berkembang dengan cepat dan berguna di situasi saat manajemen kebijakan menjadi rumit.

Untuk mengendalikan akses berdasarkan tanda, berikan informasi tentang tanda di [elemen kondisi](#) dari kebijakan menggunakan kunci kondisi `aws:ResourceTag/key-name`, `aws:RequestTag/key-name`, atau `aws:TagKeys`.

Jika sebuah layanan mendukung ketiga kunci kondisi untuk setiap jenis sumber daya, nilainya adalah Ya untuk layanan tersebut. Jika suatu layanan mendukung ketiga kunci kondisi untuk hanya beberapa jenis sumber daya, nilainya adalah Parsial.

Untuk informasi selengkapnya tentang ABAC, lihat [Tentukan izin dengan otorisasi ABAC](#) dalam Panduan Pengguna IAM. Untuk melihat tutorial yang menguraikan langkah-langkah pengaturan ABAC, lihat [Menggunakan kontrol akses berbasis atribut \(ABAC\)](#) dalam Panduan Pengguna IAM.

Menggunakan kredensi sementara dengan GuardDuty

Mendukung kredensial sementara: Ya

Beberapa Layanan AWS tidak berfungsi saat Anda masuk menggunakan kredensi sementara. Untuk informasi tambahan, termasuk yang Layanan AWS bekerja dengan kredensi sementara, lihat [Layanan AWS yang bekerja dengan IAM di Panduan Pengguna IAM](#).

Anda menggunakan kredensi sementara jika Anda masuk AWS Management Console menggunakan metode apa pun kecuali nama pengguna dan kata sandi. Misalnya, ketika Anda mengakses AWS

menggunakan tautan masuk tunggal (SSO) perusahaan Anda, proses tersebut secara otomatis membuat kredensial sementara. Anda juga akan secara otomatis membuat kredensial sementara ketika Anda masuk ke konsol sebagai seorang pengguna lalu beralih peran. Untuk informasi selengkapnya tentang peralihan peran, lihat [Beralih dari pengguna ke peran IAM \(konsol\)](#) dalam Panduan Pengguna IAM.

Anda dapat membuat kredensial sementara secara manual menggunakan API AWS CLI atau AWS . Anda kemudian dapat menggunakan kredensial sementara tersebut untuk mengakses AWS. 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](#).

Izin utama lintas layanan untuk GuardDuty

Mendukung sesi akses maju (FAS): Ya

Saat Anda menggunakan pengguna atau peran IAM untuk melakukan tindakan AWS, Anda dianggap sebagai prinsipal. Ketika Anda menggunakan beberapa layanan, Anda mungkin melakukan sebuah tindakan yang kemudian menginisiasi tindakan lain di layanan yang berbeda. FAS menggunakan izin dari pemanggilan utama Layanan AWS, dikombinasikan dengan permintaan Layanan AWS untuk membuat permintaan ke layanan hilir. Permintaan FAS hanya dibuat ketika layanan menerima permintaan yang memerlukan interaksi dengan orang lain Layanan AWS atau sumber daya untuk menyelesaikannya. Dalam hal ini, Anda harus memiliki izin untuk melakukan kedua tindakan tersebut. Untuk detail kebijakan ketika mengajukan permintaan FAS, lihat [Sesi akses maju](#).

Peran layanan untuk GuardDuty

Mendukung peran layanan: Ya

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 [Buat sebuah peran untuk mendelegasikan izin ke Layanan AWS](#) dalam Panduan pengguna IAM.

Warning

Mengubah izin untuk peran layanan dapat merusak GuardDuty fungsionalitas. Edit peran layanan hanya jika GuardDuty memberikan panduan untuk melakukannya.

Peran terkait layanan untuk GuardDuty

Mendukung peran terkait layanan: Ya

Peran terkait layanan adalah jenis peran layanan yang ditautkan ke. Layanan AWS Layanan tersebut dapat menjalankan peran untuk melakukan tindakan atas nama Anda. Peran terkait layanan muncul di Anda Akun AWS dan dimiliki oleh layanan. Administrator IAM dapat melihat, tetapi tidak dapat mengedit izin untuk peran terkait layanan.

Untuk detail tentang membuat atau mengelola peran GuardDuty terkait layanan, lihat [Menggunakan peran tertaut layanan untuk Amazon GuardDuty](#)

Untuk detail tentang pembuatan atau manajemen peran terkait layanan, lihat [Layanan AWS yang berfungsi dengan IAM](#). Cari layanan dalam tabel yang memiliki Yes di kolom Peran terkait layanan. Pilih tautan Ya untuk melihat dokumentasi peran terkait layanan untuk layanan tersebut.

Contoh kebijakan berbasis identitas untuk Amazon GuardDuty

Secara default, pengguna dan peran tidak memiliki izin untuk membuat atau mengubah sumber daya GuardDuty. Mereka juga tidak dapat melakukan tugas dengan menggunakan AWS Management Console, AWS Command Line Interface (AWS CLI), atau AWS API. Untuk memberikan izin kepada pengguna untuk melakukan tindakan di sumber daya yang mereka perlukan, administrator IAM dapat membuat kebijakan IAM. Administrator kemudian dapat menambahkan kebijakan IAM ke peran, dan pengguna dapat mengambil peran.

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

Untuk detail tentang tindakan dan jenis sumber daya yang ditentukan oleh GuardDuty, termasuk format ARNs untuk setiap jenis sumber daya, lihat [Kunci tindakan, sumber daya, dan kondisi untuk Amazon GuardDuty](#) di Referensi Otorisasi Layanan.

Topik

- [Praktik terbaik kebijakan](#)
- [Menggunakan konsol GuardDuty](#)
- [Izin diperlukan untuk mengaktifkan GuardDuty](#)
- [Mengizinkan pengguna melihat izin mereka sendiri](#)
- [Kebijakan IAM khusus untuk memberikan akses hanya-baca GuardDuty](#)
- [Tolak Akses ke GuardDuty Temuan](#)

- [Menggunakan kebijakan IAM khusus untuk membatasi akses ke sumber daya GuardDuty](#)

Praktik terbaik kebijakan

Kebijakan berbasis identitas menentukan apakah seseorang dapat membuat, mengakses, atau menghapus GuardDuty sumber daya di akun Anda. Tindakan ini membuat Akun AWS Anda dikenai biaya. Ketika Anda membuat atau mengedit kebijakan berbasis identitas, ikuti panduan dan rekomendasi ini:

- Mulailah dengan kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit — Untuk mulai memberikan izin kepada pengguna dan beban kerja Anda, gunakan kebijakan AWS terkelola yang memberikan izin untuk banyak kasus penggunaan umum. Mereka tersedia di Anda Akun AWS. Kami menyarankan Anda mengurangi izin lebih lanjut dengan menentukan kebijakan yang dikelola AWS pelanggan yang khusus untuk kasus penggunaan Anda. Untuk informasi selengkapnya, lihat [Kebijakan yang dikelola AWS](#) atau [Kebijakan yang dikelola AWS untuk fungsi tugas](#) dalam Panduan Pengguna IAM.
- Menerapkan izin dengan hak akses paling rendah – Ketika Anda menetapkan izin dengan kebijakan IAM, hanya berikan izin yang diperlukan untuk melakukan tugas. Anda melakukannya dengan mendefinisikan tindakan yang dapat diambil pada sumber daya tertentu dalam kondisi tertentu, yang juga dikenal sebagai izin dengan hak akses paling rendah. Untuk informasi selengkapnya tentang cara menggunakan IAM untuk mengajukan izin, lihat [Kebijakan dan izin dalam IAM](#) dalam Panduan Pengguna IAM.
- Gunakan kondisi dalam kebijakan IAM untuk membatasi akses lebih lanjut – Anda dapat menambahkan suatu kondisi ke kebijakan Anda untuk membatasi akses ke tindakan dan sumber daya. Sebagai contoh, Anda dapat menulis kondisi kebijakan untuk menentukan bahwa semua permintaan harus dikirim menggunakan SSL. Anda juga dapat menggunakan ketentuan untuk memberikan akses ke tindakan layanan jika digunakan melalui yang spesifik Layanan AWS, seperti AWS CloudFormation. Untuk informasi selengkapnya, lihat [Elemen kebijakan JSON IAM: Kondisi](#) dalam Panduan Pengguna IAM.
- Gunakan IAM Access Analyzer untuk memvalidasi kebijakan IAM Anda untuk memastikan izin yang aman dan fungsional – IAM Access Analyzer memvalidasi kebijakan baru dan yang sudah ada sehingga kebijakan tersebut mematuhi bahasa kebijakan IAM (JSON) dan praktik terbaik IAM. IAM Access Analyzer menyediakan lebih dari 100 pemeriksaan kebijakan dan rekomendasi yang dapat ditindaklanjuti untuk membantu Anda membuat kebijakan yang aman dan fungsional. Untuk informasi selengkapnya, lihat [Validasi kebijakan dengan IAM Access Analyzer](#) dalam Panduan Pengguna IAM.

- Memerlukan otentikasi multi-faktor (MFA) - Jika Anda memiliki skenario yang mengharuskan pengguna IAM atau pengguna root di Anda, Akun AWS aktifkan MFA untuk keamanan tambahan. Untuk meminta MFA ketika operasi API dipanggil, tambahkan kondisi MFA pada kebijakan Anda. Untuk informasi selengkapnya, lihat [Amankan akses API dengan MFA](#) dalam Panduan Pengguna IAM.

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

Menggunakan konsol GuardDuty

Untuk mengakses GuardDuty konsol Amazon, Anda harus memiliki set izin minimum. Izin ini harus memungkinkan Anda untuk membuat daftar dan melihat detail tentang GuardDuty sumber daya di Anda Akun AWS. Jika Anda membuat kebijakan berbasis identitas yang lebih ketat daripada izin minimum yang diperlukan, konsol tidak akan berfungsi sebagaimana mestinya untuk entitas (pengguna atau peran) dengan kebijakan tersebut.

Anda tidak perlu mengizinkan izin konsol minimum untuk pengguna yang melakukan panggilan hanya ke AWS CLI atau AWS API. Sebagai gantinya, izinkan akses hanya ke tindakan yang sesuai dengan operasi API yang coba mereka lakukan.

Untuk memastikan bahwa pengguna dan peran masih dapat menggunakan GuardDuty konsol, lampirkan juga kebijakan GuardDuty ConsoleAccess atau ReadOnly AWS terkelola ke entitas. Untuk informasi selengkapnya, lihat [Menambah izin untuk pengguna](#) dalam Panduan Pengguna IAM.

Izin diperlukan untuk mengaktifkan GuardDuty

Untuk memberikan izin yang harus dimiliki oleh berbagai identitas IAM (pengguna, grup, dan peran), lampirkan [AWS kebijakan terkelola: AmazonGuardDutyFullAccess_v2 \(disarankan\)](#) kebijakan yang diperlukan untuk mengaktifkan GuardDuty.

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 API atau secara terprogram. AWS CLI AWS

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

```

    "Statement": [
      {
        "Sid": "ViewOwnUserInfo",
        "Effect": "Allow",
        "Action": [
          "iam:GetUserPolicy",
          "iam:ListGroupsForUser",
          "iam:ListAttachedUserPolicies",
          "iam:ListUserPolicies",
          "iam:GetUser"
        ],
        "Resource": ["arn:aws:iam::*:user/${aws:username}"]
      },
      {
        "Sid": "NavigateInConsole",
        "Effect": "Allow",
        "Action": [
          "iam:GetGroupPolicy",
          "iam:GetPolicyVersion",
          "iam:GetPolicy",
          "iam:ListAttachedGroupPolicies",
          "iam:ListGroupPolicies",
          "iam:ListPolicyVersions",
          "iam:ListPolicies",
          "iam:ListUsers"
        ],
        "Resource": "*"
      }
    ]
  }
}

```

Kebijakan IAM khusus untuk memberikan akses hanya-baca GuardDuty

Untuk memberikan akses hanya-baca ke GuardDuty Anda dapat menggunakan kebijakan AmazonGuardDutyReadOnlyAccess terkelola.

Untuk membuat kebijakan kustom yang memberikan akses hanya baca peran IAM, pengguna, atau grup GuardDuty, Anda dapat menggunakan pernyataan berikut:

```

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

```

```

    "Effect": "Allow",
    "Action": [
        "guardduty:ListMembers",
        "guardduty:GetMembers",
        "guardduty:ListInvitations",
        "guardduty:ListDetectors",
        "guardduty:GetDetector",
        "guardduty:ListFindings",
        "guardduty:GetFindings",
        "guardduty:ListIPSets",
        "guardduty:GetIPSet",
        "guardduty:ListThreatIntelSets",
        "guardduty:GetThreatIntelSet",
        "guardduty:GetMasterAccount",
        "guardduty:GetInvitationsCount",
        "guardduty:GetFindingsStatistics",
        "guardduty:DescribeMalwareScans",
        "guardduty:UpdateMalwareScanSettings",
        "guardduty:GetMalwareScanSettings"
    ],
    "Resource": "*"
}
]
}

```

Tolak Akses ke GuardDuty Temuan

Anda dapat menggunakan kebijakan berikut untuk menolak peran IAM, pengguna, atau akses grup ke GuardDuty temuan. Pengguna tidak dapat melihat temuan atau detail tentang temuan, tetapi mereka dapat mengakses semua GuardDuty operasi lainnya:

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "guardduty:CreateDetector",
        "guardduty>DeleteDetector",
        "guardduty:UpdateDetector",
        "guardduty:GetDetector",
        "guardduty:ListDetectors",
        "guardduty:CreateIPSet",

```

```

        "guardduty:DeleteIPSet",
        "guardduty:UpdateIPSet",
        "guardduty:GetIPSet",
        "guardduty:ListIPSets",
        "guardduty:CreateThreatIntelSet",
        "guardduty:DeleteThreatIntelSet",
        "guardduty:UpdateThreatIntelSet",
        "guardduty:GetThreatIntelSet",
        "guardduty:ListThreatIntelSets",
        "guardduty:ArchiveFindings",
        "guardduty:UnarchiveFindings",
        "guardduty:CreateSampleFindings",
        "guardduty:CreateMembers",
        "guardduty:InviteMembers",
        "guardduty:GetMembers",
        "guardduty:DeleteMembers",
        "guardduty:DisassociateMembers",
        "guardduty:StartMonitoringMembers",
        "guardduty:StopMonitoringMembers",
        "guardduty:ListMembers",
        "guardduty:GetMasterAccount",
        "guardduty:DisassociateFromMasterAccount",
        "guardduty:AcceptAdministratorInvitation",
        "guardduty:ListInvitations",
        "guardduty:GetInvitationsCount",
        "guardduty:DeclineInvitations",
        "guardduty:DeleteInvitations"
    ],
    "Resource": "*"
},
{
    "Effect": "Allow",
    "Action": [
        "iam:CreateServiceLinkedRole"
    ],
    "Resource": "arn:aws:iam::123456789012:role/aws-service-role/
guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty",
    "Condition": {
        "StringLike": {
            "iam:AWSServiceName": "guardduty.amazonaws.com"
        }
    }
},
{

```

```
    "Effect": "Allow",
    "Action": [
        "iam:PutRolePolicy",
        "iam:DeleteRolePolicy"
    ],
    "Resource": "arn:aws:iam::123456789012:role/aws-service-role/
guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty"
    }
}
```

Menggunakan kebijakan IAM khusus untuk membatasi akses ke sumber daya GuardDuty

Untuk menentukan akses pengguna GuardDuty berdasarkan ID detektor, Anda dapat menggunakan semua [tindakan GuardDuty API](#) dalam kebijakan IAM kustom, kecuali operasi berikut:

- guardduty:CreateDetector
- guardduty:DeclineInvitations
- guardduty>DeleteInvitations
- guardduty:GetInvitationsCount
- guardduty:ListDetectors
- guardduty:ListInvitations

Gunakan operasi berikut dalam kebijakan IAM untuk menentukan akses pengguna GuardDuty berdasarkan IPSet ID dan ThreatIntelSet ID:

- guardduty>DeleteIPSet
- guardduty>DeleteThreatIntelSet
- guardduty:GetIPSet
- guardduty:GetThreatIntelSet
- guardduty:UpdateIPSet
- guardduty:UpdateThreatIntelSet

Contoh berikut ini menunjukkan cara membuat kebijakan menggunakan beberapa operasi sebelumnya:

- Kebijakan ini memungkinkan pengguna untuk menjalankan operasi `guardduty:UpdateDetector`, menggunakan ID detektor 1234567 di Wilayah `us-east-1`:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "guardduty:UpdateDetector",
      ],
      "Resource": "arn:aws:guardduty:us-east-1:123456789012:detector/1234567"
    }
  ]
}
```

- Kebijakan ini memungkinkan pengguna untuk menjalankan `guardduty:UpdateIPSet` operasi, menggunakan ID detektor 1234567 dan ID 000000 di IPSet Wilayah `us-east-1`:

 Note

Pastikan bahwa pengguna memiliki izin yang diperlukan untuk mengakses daftar IP terpercaya dan daftar ancaman di GuardDuty. Untuk informasi selengkapnya, lihat [Izin yang diperlukan untuk mengunggah daftar IP terpercaya dan daftar ancaman](#).

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "guardduty:UpdateIPSet",
      ],
      "Resource": "arn:aws:guardduty:us-east-1:123456789012:detector/1234567/ipset/000000"
    }
  ]
}
```

- Kebijakan ini memungkinkan pengguna untuk menjalankan `guardduty:UpdateIPSet` operasi, menggunakan ID detektor dan ID 000000 di Wilayah us-east-1: IPSet

 Note

Pastikan bahwa pengguna memiliki izin yang diperlukan untuk mengakses daftar IP terpercaya dan daftar ancaman di GuardDuty. Untuk informasi selengkapnya, lihat [izin yang diperlukan untuk mengunggah daftar IP terpercaya dan daftar ancaman](#).

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "guardduty:UpdateIPSet",
      ],
      "Resource": "arn:aws:guardduty:us-east-1:123456789012:detector/*/
ipset/000000"
    }
  ]
}
```

- Kebijakan ini memungkinkan pengguna untuk menjalankan `guardduty:UpdateIPSet` operasi, menggunakan ID detektor dan IPSet ID apa pun di Wilayah us-east-1:

 Note

Pastikan bahwa pengguna memiliki izin yang diperlukan untuk mengakses daftar IP terpercaya dan daftar ancaman di GuardDuty. Untuk informasi selengkapnya, lihat [izin yang diperlukan untuk mengunggah daftar IP terpercaya dan daftar ancaman](#).

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

```

        "guardduty:UpdateIPSet",
      ],
      "Resource": "arn:aws:guardduty:us-east-1:123456789012:detector/1234567/
ipset/*"
    }
  ]
}

```

Menggunakan peran tertaut layanan untuk Amazon GuardDuty

Amazon GuardDuty menggunakan peran AWS Identity and Access Management [terkait layanan](#) (IAM). Peran terkait layanan (SLR) adalah jenis IAM role unik yang terhubung langsung ke GuardDuty Peran yang terhubung dengan layanan ditentukan sebelumnya oleh GuardDuty dan mencakup semua izin yang GuardDuty diperlukan untuk menghubungi AWS layanan lainnya atas nama Anda.

Dengan peran terkait layanan, Anda dapat mengatur GuardDuty tanpa menambahkan izin yang diperlukan secara manual. GuardDuty menentukan izin peran yang terhubung dengan layanan, dan kecuali izin ditentukan lain, hanya GuardDuty dapat mengambil peran tersebut. Izin yang ditentukan mencakup kebijakan kepercayaan dan kebijakan izin, dan kebijakan izin tersebut tidak dapat dilampirkan ke entitas IAM lainnya.

GuardDuty memberikan dukungan dengan peran yang terhubung dengan layanan di semua Wilayah yang tersedia GuardDuty . Untuk informasi selengkapnya, lihat [Wilayah dan titik akhir](#).

Anda dapat menghapus peran yang GuardDuty terhubung dengan layanan hanya setelah menonaktifkan terlebih dahulu GuardDuty di semua Wilayah yang mengaktifkan. Ini melindungi GuardDuty sumber daya karena Anda tidak dapat secara tidak sengaja menghapus izin untuk mengaksesnya.

Untuk informasi tentang layanan lain yang mendukung peran tertaut layanan, lihat [AWS layanan yang dapat digunakan dengan IAM](#) di Panduan Pengguna IAM dan cari layanan yang memiliki Ya di kolom Peran Tertaut Layanan. Pilih Ya dengan sebuah tautan untuk melihat dokumentasi peran terkait layanan untuk layanan tersebut.

Izin peran terkait layanan untuk GuardDuty

GuardDuty menggunakan peran yang terhubung dengan layanan (SLR) bernama `AWSServiceRoleForAmazonGuardDuty` SLR memungkinkan GuardDuty untuk melakukan tugas-tugas berikut. Ini juga memungkinkan GuardDuty untuk memasukkan metadata yang

diambil milik EC2 instance dalam temuan yang GuardDuty dapat menghasilkan tentang potensi ancaman. Peran terkait layanan `AWSServiceRoleForAmazonGuardDuty` memercayai layanan `guardduty.amazonaws.com` untuk menjalankan peran.

Kebijakan izin membantu GuardDuty melakukan tugas berikut:

- Gunakan EC2 tindakan Amazon untuk mengelola dan mengambil informasi tentang EC2 instans, gambar, dan komponen jaringan Anda seperti VPCs, subnet, dan gateway transit.
- Gunakan AWS Systems Manager tindakan untuk mengelola asosiasi SSM di EC2 instans Amazon saat Anda mengaktifkan Pemantauan GuardDuty Waktu Proses dengan agen otomatis untuk Amazon. EC2 Ketika konfigurasi agen GuardDuty otomatis dinonaktifkan, GuardDuty pertimbangkan hanya EC2 instance yang memiliki tag inklusi (`GuardDutyManaged:true`).
- Gunakan AWS Organizations tindakan untuk menjelaskan akun terkait dan ID organisasi.
- Gunakan tindakan Amazon S3 untuk mengambil informasi tentang bucket dan objek S3.
- Gunakan AWS Lambda tindakan untuk mengambil informasi tentang fungsi dan tag Lambda Anda.
- Gunakan tindakan Amazon EKS untuk mengelola dan mengambil informasi tentang kluster EKS dan mengelola [add-on Amazon EKS di kluster EKS](#). Tindakan EKS juga mengambil informasi tentang tag yang terkait GuardDuty dengan.
- Gunakan IAM untuk membuat Perlindungan Malware [Izin peran terkait layanan untuk Perlindungan Malware untuk EC2](#) EC2 setelah diaktifkan.
- Gunakan tindakan Amazon ECS untuk mengelola dan mengambil informasi tentang kluster Amazon ECS, dan mengelola setelan akun Amazon ECS. `guarddutyActivate` Tindakan yang berkaitan dengan Amazon ECS juga mengambil informasi tentang tag yang terkait dengannya. GuardDuty

Peran dikonfigurasi dengan [kebijakan AWS terkelola](#) berikut, bernama `AmazonGuardDutyServiceRolePolicy`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "GuardDutyGetDescribeListPolicy",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeInstances",
        "ec2:DescribeImages",
```

```

        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeTransitGatewayAttachments",
        "organizations:ListAccounts",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetEncryptionConfiguration",
        "s3:GetBucketTagging",
        "s3:GetAccountPublicAccessBlock",
        "s3:ListAllMyBuckets",
        "s3:GetBucketAcl",
        "s3:GetBucketPolicy",
        "s3:GetBucketPolicyStatus",
        "lambda:GetFunctionConfiguration",
        "lambda:ListTags",
        "eks:ListClusters",
        "eks:DescribeCluster",
        "ec2:DescribeVpcEndpointServices",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcs",
        "ecs:ListClusters",
        "ecs:DescribeClusters"
    ],
    "Resource": "*"
},
{
    "Sid": "GuardDutyCreateSLRPolicy",
    "Effect": "Allow",
    "Action": "iam:CreateServiceLinkedRole",
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "iam:AWSServiceName": "malware-protection.guardduty.amazonaws.com"
        }
    }
},
{
    "Sid": "GuardDutyCreateVpcEndpointPolicy",
    "Effect": "Allow",
    "Action": "ec2:CreateVpcEndpoint",
    "Resource": "arn:aws:ec2:*:*:vpc-endpoint/*",
    "Condition": {

```

```

        "ForAnyValue:StringEquals": {
            "aws:TagKeys": "GuardDutyManaged"
        },
        "StringLike": {
            "ec2:VpceServiceName": [
                "com.amazonaws.*.guardduty-data",
                "com.amazonaws.*.guardduty-data-fips"
            ]
        }
    },
    {
        "Sid": "GuardDutyModifyDeleteVpcEndpointPolicy",
        "Effect": "Allow",
        "Action": [
            "ec2:ModifyVpcEndpoint",
            "ec2:DeleteVpcEndpoints"
        ],
        "Resource": "arn:aws:ec2:*:*:vpc-endpoint/*",
        "Condition": {
            "Null": {
                "aws:ResourceTag/GuardDutyManaged": false
            }
        }
    },
    {
        "Sid": "GuardDutyCreateModifyVpcEndpointNetworkPolicy",
        "Effect": "Allow",
        "Action": [
            "ec2:CreateVpcEndpoint",
            "ec2:ModifyVpcEndpoint"
        ],
        "Resource": [
            "arn:aws:ec2:*:*:vpc/*",
            "arn:aws:ec2:*:*:security-group/*",
            "arn:aws:ec2:*:*:subnet/*"
        ]
    },
    {
        "Sid": "GuardDutyCreateTagsDuringVpcEndpointCreationPolicy",
        "Effect": "Allow",
        "Action": "ec2:CreateTags",
        "Resource": "arn:aws:ec2:*:*:vpc-endpoint/*",
        "Condition": {

```

```

        "StringEquals": {
            "ec2:CreateAction": "CreateVpcEndpoint"
        },
        "ForAnyValue:StringEquals": {
            "aws:TagKeys": "GuardDutyManaged"
        }
    },
    {
        "Sid": "GuardDutySecurityGroupManagementPolicy",
        "Effect": "Allow",
        "Action": [
            "ec2:AuthorizeSecurityGroupIngress",
            "ec2:AuthorizeSecurityGroupEgress",
            "ec2:RevokeSecurityGroupIngress",
            "ec2:RevokeSecurityGroupEgress",
            "ec2>DeleteSecurityGroup"
        ],
        "Resource": "arn:aws:ec2:*:*:security-group/*",
        "Condition": {
            "Null": {
                "aws:ResourceTag/GuardDutyManaged": false
            }
        }
    },
    {
        "Sid": "GuardDutyCreateSecurityGroupPolicy",
        "Effect": "Allow",
        "Action": "ec2:CreateSecurityGroup",
        "Resource": "arn:aws:ec2:*:*:security-group/*",
        "Condition": {
            "StringLike": {
                "aws:RequestTag/GuardDutyManaged": "*"
            }
        }
    },
    {
        "Sid": "GuardDutyCreateSecurityGroupForVpcPolicy",
        "Effect": "Allow",
        "Action": "ec2:CreateSecurityGroup",
        "Resource": "arn:aws:ec2:*:*:vpc/*"
    },
    {
        "Sid": "GuardDutyCreateTagsDuringSecurityGroupCreationPolicy",

```

```

    "Effect": "Allow",
    "Action": "ec2:CreateTags",
    "Resource": "arn:aws:ec2:*:*:security-group/*",
    "Condition": {
      "StringEquals": {
        "ec2:CreateAction": "CreateSecurityGroup"
      },
      "ForAnyValue:StringEquals": {
        "aws:TagKeys": "GuardDutyManaged"
      }
    }
  },
  {
    "Sid": "GuardDutyCreateEksAddonPolicy",
    "Effect": "Allow",
    "Action": "eks:CreateAddon",
    "Resource": "arn:aws:eks:*:*:cluster/*",
    "Condition": {
      "ForAnyValue:StringEquals": {
        "aws:TagKeys": "GuardDutyManaged"
      }
    }
  },
  {
    "Sid": "GuardDutyEksAddonManagementPolicy",
    "Effect": "Allow",
    "Action": [
      "eks:DeleteAddon",
      "eks:UpdateAddon",
      "eks:DescribeAddon"
    ],
    "Resource": "arn:aws:eks:*:*:addon/*/aws-guardduty-agent/*"
  },
  {
    "Sid": "GuardDutyEksClusterTagResourcePolicy",
    "Effect": "Allow",
    "Action": "eks:TagResource",
    "Resource": "arn:aws:eks:*:*:cluster/*",
    "Condition": {
      "ForAnyValue:StringEquals": {
        "aws:TagKeys": "GuardDutyManaged"
      }
    }
  }
},

```



```

{
  "Sid": "GuardDutyEcsPutAccountSettingsDefaultPolicy",
  "Effect": "Allow",
  "Action": "ecs:PutAccountSettingDefault",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "ecs:account-setting": [
        "guardDutyActivate"
      ]
    }
  }
},
{
  "Sid": "SsmCreateDescribeUpdateDeleteStartAssociationPermission",
  "Effect": "Allow",
  "Action": [
    "ssm:DescribeAssociation",
    "ssm:DeleteAssociation",
    "ssm:UpdateAssociation",
    "ssm:CreateAssociation",
    "ssm:StartAssociationsOnce"
  ],
  "Resource": "arn:aws:ssm:*:*:association/*",
  "Condition": {
    "StringEquals": {
      "aws:ResourceTag/GuardDutyManaged": "true"
    }
  }
},
{
  "Sid": "SsmAddTagsToResourcePermission",
  "Effect": "Allow",
  "Action": [
    "ssm:AddTagsToResource"
  ],
  "Resource": "arn:aws:arn:aws:ssm:*:*:association/*",
  "Condition": {
    "ForAllValues:StringEquals": {
      "aws:TagKeys": [
        "GuardDutyManaged"
      ]
    },
    "StringEquals": {

```

```

        "aws:ResourceTag/GuardDutyManaged": "true"
      }
    },
    {
      "Sid": "SsmCreateUpdateAssociationInstanceDocumentPermission",
      "Effect": "Allow",
      "Action": [
        "ssm:CreateAssociation",
        "ssm:UpdateAssociation"
      ],
      "Resource": "arn:aws:ssm:*:*:document/AmazonGuardDuty-
ConfigureRuntimeMonitoringSsmPlugin"
    },
    {
      "Sid": "SsmSendCommandPermission",
      "Effect": "Allow",
      "Action": "ssm:SendCommand",
      "Resource": [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ssm:*:*:document/AmazonGuardDuty-
ConfigureRuntimeMonitoringSsmPlugin"
      ]
    },
    {
      "Sid": "SsmGetCommandStatus",
      "Effect": "Allow",
      "Action": "ssm:GetCommandInvocation",
      "Resource": "*"
    }
  ]
}

```

Berikut ini adalah kebijakan kepercayaan yang dilampirkan ke peran yang terhubung dengan layanan `AWSServiceRoleForAmazonGuardDuty`:

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "guardduty.amazonaws.com"
      }
    }
  ]
}

```

```
    },  
    "Action": "sts:AssumeRole"  
  }  
]  
}
```

Untuk detail tentang pembaruan AmazonGuardDutyServiceRolePolicy kebijakan, lihat [GuardDuty pembaruan kebijakan AWS terkelola](#). Untuk peringatan otomatis tentang perubahan kebijakan ini, berlangganan RSS feed pada halaman. [Riwayat dokumen](#)

Membuat peran yang terhubung dengan layanan untuk GuardDuty

Peran `AWSServiceRoleForAmazonGuardDuty` yang terhubung dengan layanan dibuat secara otomatis saat Anda mengaktifkan GuardDuty untuk pertama kalinya atau mengaktifkan GuardDuty di Wilayah yang didukung tempat sebelumnya Anda tidak mengaktifkannya. Anda juga dapat membuat peran terkait layanan secara manual menggunakan konsol IAM, AWS CLI, atau API IAM.

 Important

Peran yang terhubung dengan layanan yang dibuat untuk akun administrator yang GuardDuty didelegasikan tidak berlaku untuk akun anggota. GuardDuty

Anda harus mengonfigurasi izin untuk mengizinkan kepala IAM (seperti pengguna, grup, atau peran) untuk membuat, mengedit, atau menghapus peran terkait layanan. Agar peran `AWSServiceRoleForAmazonGuardDuty` terkait layanan berhasil dibuat, prinsip IAM yang Anda gunakan GuardDuty dengan harus memiliki izin yang diperlukan. Untuk memberikan izin yang diperlukan, lampirkan kebijakan berikut untuk pengguna, grup, atau peran ini:

 Note

Ganti sampel *account ID* dalam contoh berikut dengan Akun AWS ID Anda yang sebenarnya.

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

```

        "Effect": "Allow",
        "Action": [
            "guardduty:*"
        ],
        "Resource": "*"
    },
    {
        "Effect": "Allow",
        "Action": [
            "iam:CreateServiceLinkedRole"
        ],
        "Resource": "arn:aws:iam::123456789012:role/aws-service-role/
guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty",
        "Condition": {
            "StringLike": {
                "iam:AWSServiceName": "guardduty.amazonaws.com"
            }
        }
    },
    {
        "Effect": "Allow",
        "Action": [
            "iam:PutRolePolicy",
            "iam>DeleteRolePolicy"
        ],
        "Resource": "arn:aws:iam::123456789012:role/aws-service-role/
guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty"
    }
]
}

```

Untuk informasi selengkapnya tentang membuat peran secara manual, lihat [Membuat peran tertaut layanan](#) dalam Panduan Pengguna IAM.

Mengedit peran yang terhubung dengan layanan untuk GuardDuty

GuardDuty tidak mengizinkan Anda untuk mengedit peran yang `AWSServiceRoleForAmazonGuardDuty` terkait dengan layanan. Setelah membuat peran terkait layanan, Anda tidak dapat mengubah nama peran karena berbagai entitas mungkin mereferensikan peran tersebut. Namun, Anda dapat menyunting penjelasan peran menggunakan IAM. Untuk informasi selengkapnya, lihat [Mengedit peran terkait layanan](#) dalam Panduan Pengguna IAM.

Menghapus peran terkait layanan untuk GuardDuty

Jika Anda tidak perlu lagi menggunakan fitur atau layanan yang memerlukan peran terkait layanan, sebaiknya hapus peran tersebut. Dengan begitu, Anda tidak memiliki entitas yang tidak digunakan yang tidak dipantau atau dikelola secara aktif.

Important

Jika Anda telah mengaktifkan Perlindungan Malware untuk EC2, menghapus `AWSServiceRoleForAmazonGuardDuty` tidak secara otomatis menghapus `AWSServiceRoleForAmazonGuardDutyMalwareProtection`. Jika ingin menghapus `AWSServiceRoleForAmazonGuardDutyMalwareProtection`, lihat [Menghapus peran terkait layanan untuk Perlindungan Malware](#). EC2

Anda harus menonaktifkan GuardDuty terlebih dahulu di semua Wilayah yang mengaktifkannya untuk menghapus `AWSServiceRoleForAmazonGuardDuty`. Jika GuardDuty layanan tidak dinonaktifkan saat Anda mencoba untuk menghapus peran yang terhubung dengan layanan, penghapusan gagal. Untuk informasi selengkapnya, lihat [Menangguhkan atau menonaktifkan GuardDuty](#).

Ketika Anda menonaktifkan GuardDuty, `AWSServiceRoleForAmazonGuardDuty` tidak akan dihapus secara otomatis. Jika Anda mengaktifkan GuardDuty lagi, itu akan mulai menggunakan yang sudah ada `AWSServiceRoleForAmazonGuardDuty`.

Untuk menghapus peran terkait layanan secara manual menggunakan IAM

Gunakan konsol IAM, AWS CLI, atau IAM API untuk menghapus peran terkait `AWSServiceRoleForAmazonGuardDuty` layanan. Untuk informasi selengkapnya, lihat [Menghapus peran terkait layanan](#) dalam Panduan Pengguna IAM.

Didukung Wilayah AWS

Amazon GuardDuty mendukung penggunaan peran `AWSServiceRoleForAmazonGuardDuty` terkait layanan di semua Wilayah AWS tempat yang GuardDuty tersedia. Untuk daftar Wilayah yang saat ini GuardDuty tersedia, lihat [GuardDuty titik akhir dan kuota Amazon](#) di Referensi Umum Amazon Web

Izin peran terkait layanan untuk Perlindungan Malware untuk EC2

Perlindungan Malware untuk EC2 menggunakan peran yang terhubung dengan layanan (SLR). `AWSServiceRoleForAmazonGuardDutyMalwareProtection` SLR ini memungkinkan

Perlindungan Malware EC2 untuk melakukan pemindaian tanpa agen untuk mendeteksi malware di akun Anda. GuardDuty Ini memungkinkan GuardDuty untuk membuat snapshot volume EBS di akun Anda, dan berbagi snapshot itu dengan akun layanan. GuardDuty Setelah GuardDuty mengevaluasi snapshot, itu termasuk EC2 instance yang diambil dan metadata beban kerja kontainer dalam Perlindungan Malware untuk temuan. EC2 Peran terkait layanan `AWSServiceRoleForAmazonGuardDutyMalwareProtection` memercayai layanan `malware-protection.guardduty.amazonaws.com` untuk menjalankan peran.

Kebijakan izin untuk peran ini membantu Perlindungan Malware EC2 untuk melakukan tugas-tugas berikut:

- Gunakan tindakan Amazon Elastic Compute Cloud (Amazon EC2) untuk mengambil informasi tentang EC2 instans, volume, dan snapshot Amazon Anda. Perlindungan Malware untuk EC2 juga memberikan izin untuk mengakses metadata cluster Amazon EKS dan Amazon ECS.
- Buat snapshot untuk volume EBS yang `GuardDutyExcluded` tag belum disetel. `true` Secara default, snapshot dibuat dengan `GuardDutyScanId` tag. Jangan hapus tag ini, jika tidak, Perlindungan Malware for tidak EC2 akan memiliki akses ke snapshot.

 Important

Saat Anda mengatur `GuardDutyExcluded` ke `true`, GuardDuty layanan tidak akan dapat mengakses snapshot ini di masa mendatang. Ini karena pernyataan lain dalam peran terkait layanan ini GuardDuty mencegah melakukan tindakan apa pun pada snapshot yang disetel ke `GuardDutyExcluded`. `true`

- Izinkan berbagi dan menghapus snapshot hanya jika `GuardDutyScanId` tag ada dan `GuardDutyExcluded` tag tidak disetel ke. `true`

 Note

Tidak mengizinkan Perlindungan Malware EC2 untuk membuat snapshot publik.

- Akses kunci terkelola pelanggan, kecuali yang memiliki `GuardDutyExcluded` tag yang disetel ke `true`, untuk memanggil `CreateGrant` untuk membuat dan mengakses volume EBS terenkripsi dari snapshot terenkripsi yang akan dibagikan dengan akun layanan. GuardDuty Untuk daftar akun GuardDuty layanan untuk setiap Wilayah, lihat [GuardDuty akun layanan oleh Wilayah AWS](#).

- Akses CloudWatch log pelanggan untuk membuat Perlindungan Malware untuk grup EC2 log serta menempatkan log peristiwa pemindaian malware di bawah grup `/aws/guardduty/malware-scan-events` log.
- Izinkan pelanggan untuk memutuskan apakah mereka ingin menyimpan snapshot di mana malware terdeteksi, di akun mereka. Jika pemindaian mendeteksi malware, peran terkait layanan memungkinkan GuardDuty untuk menambahkan dua tag ke snapshot - dan. `GuardDutyFindingDetected` `GuardDutyExcluded`

 Note

`GuardDutyFindingDetectedTag` menentukan bahwa snapshot berisi malware.

- Tentukan apakah volume dienkripsi dengan kunci terkelola EBS. GuardDuty melakukan `DescribeKey` tindakan untuk menentukan kunci `key Id` yang dikelola EBS di akun Anda.
- Ambil snapshot volume EBS yang dienkripsi menggunakan Kunci yang dikelola AWS, dari Anda Akun AWS dan salin ke file. [GuardDuty akun layanan](#) Untuk tujuan ini, kami menggunakan izin `GetSnapshotBlock` dan `ListSnapshotBlocks`. GuardDuty kemudian akan memindai snapshot di akun layanan. Saat ini, Perlindungan Malware untuk EC2 dukungan pemindaian volume EBS yang dienkripsi Kunci yang dikelola AWS mungkin tidak tersedia di semua. Wilayah AWS Untuk informasi selengkapnya, lihat [Ketersediaan fitur khusus wilayah](#).
- Izinkan Amazon EC2 menelepon AWS KMS atas nama Perlindungan Malware EC2 untuk melakukan beberapa tindakan kriptografi pada kunci yang dikelola pelanggan. Tindakan seperti `kms:ReEncryptTo` dan `kms:ReEncryptFrom` diperlukan untuk berbagi snapshot yang dienkripsi dengan kunci yang dikelola pelanggan. Hanya kunci-kunci yang dapat diakses yang `GuardDutyExcluded` tag tidak disetel `true`.

Peran dikonfigurasi dengan [kebijakan AWS terkelola](#) berikut, bernama `AmazonGuardDutyMalwareProtectionServiceRolePolicy`.

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "DescribeAndListPermissions",
    "Effect": "Allow",
    "Action": [
      "ec2:DescribeInstances",
      "ec2:DescribeVolumes",
      "ec2:DescribeSnapshots",
```

```

        "ecs:ListClusters",
        "ecs:ListContainerInstances",
        "ecs:ListTasks",
        "ecs:DescribeTasks",
        "eks:DescribeCluster"
    ],
    "Resource": "*"
},
{
    "Sid": "CreateSnapshotVolumeConditionalStatement",
    "Effect": "Allow",
    "Action": "ec2:CreateSnapshot",
    "Resource": "arn:aws:ec2:*:*:volume/*",
    "Condition": {
        "Null": {
            "aws:ResourceTag/GuardDutyExcluded": "true"
        }
    }
},
{
    "Sid": "CreateSnapshotConditionalStatement",
    "Effect": "Allow",
    "Action": "ec2:CreateSnapshot",
    "Resource": "arn:aws:ec2:*:*:snapshot/*",
    "Condition": {
        "ForAnyValue:StringEquals": {
            "aws:TagKeys": "GuardDutyScanId"
        }
    }
},
{
    "Sid": "CreateTagsPermission",
    "Effect": "Allow",
    "Action": "ec2:CreateTags",
    "Resource": "arn:aws:ec2:*:*:*/*",
    "Condition": {
        "StringEquals": {
            "ec2:CreateAction": "CreateSnapshot"
        }
    }
},
{
    "Sid": "AddTagsToSnapshotPermission",
    "Effect": "Allow",

```



```

    "Action": "ec2:CreateTags",
    "Resource": "arn:aws:ec2:*:*:snapshot/*",
    "Condition": {
      "StringLike": {
        "ec2:ResourceTag/GuardDutyScanId": "*"
      },
      "ForAllValues:StringEquals": {
        "aws:TagKeys": [
          "GuardDutyExcluded",
          "GuardDutyFindingDetected"
        ]
      }
    }
  },
  {
    "Sid": "DeleteAndShareSnapshotPermission",
    "Effect": "Allow",
    "Action": [
      "ec2:DeleteSnapshot",
      "ec2:ModifySnapshotAttribute"
    ],
    "Resource": "arn:aws:ec2:*:*:snapshot/*",
    "Condition": {
      "StringLike": {
        "ec2:ResourceTag/GuardDutyScanId": "*"
      },
      "Null": {
        "aws:ResourceTag/GuardDutyExcluded": "true"
      }
    }
  },
  {
    "Sid": "PreventPublicAccessToSnapshotPermission",
    "Effect": "Deny",
    "Action": [
      "ec2:ModifySnapshotAttribute"
    ],
    "Resource": "arn:aws:ec2:*:*:snapshot/*",
    "Condition": {
      "StringEquals": {
        "ec2:Add/group": "all"
      }
    }
  }
},

```

```

{
  "Sid": "CreateGrantPermission",
  "Effect": "Allow",
  "Action": "kms:CreateGrant",
  "Resource": "arn:aws:kms:*:*:key/*",
  "Condition": {
    "Null": {
      "aws:ResourceTag/GuardDutyExcluded": "true"
    },
    "StringLike": {
      "kms:EncryptionContext:aws:ebs:id": "snap-*"
    },
    "ForAllValues:StringEquals": {
      "kms:GrantOperations": [
        "Decrypt",
        "CreateGrant",
        "GenerateDataKeyWithoutPlaintext",
        "ReEncryptFrom",
        "ReEncryptTo",
        "RetireGrant",
        "DescribeKey"
      ]
    },
    "Bool": {
      "kms:GrantIsForAWSResource": "true"
    }
  }
},
{
  "Sid": "ShareSnapshotKMSPermission",
  "Effect": "Allow",
  "Action": [
    "kms:ReEncryptTo",
    "kms:ReEncryptFrom"
  ],
  "Resource": "arn:aws:kms:*:*:key/*",
  "Condition": {
    "StringLike": {
      "kms:ViaService": "ec2.*.amazonaws.com"
    },
    "Null": {
      "aws:ResourceTag/GuardDutyExcluded": "true"
    }
  }
}

```

```

    },
    {
      "Sid": "DescribeKeyPermission",
      "Effect": "Allow",
      "Action": "kms:DescribeKey",
      "Resource": "arn:aws:kms:*:*:key/*"
    },
    {
      "Sid": "GuardDutyLogGroupPermission",
      "Effect": "Allow",
      "Action": [
        "logs:DescribeLogGroups",
        "logs:CreateLogGroup",
        "logs:PutRetentionPolicy"
      ],
      "Resource": "arn:aws:logs:*:*:log-group:/aws/guardduty/*"
    },
    {
      "Sid": "GuardDutyLogStreamPermission",
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams"
      ],
      "Resource": "arn:aws:logs:*:*:log-group:/aws/guardduty/*:log-stream:*"
    },
    {
      "Sid": "EBSDirectAPIPermissions",
      "Effect": "Allow",
      "Action": [
        "ebs:GetSnapshotBlock",
        "ebs:ListSnapshotBlocks"
      ],
      "Resource": "arn:aws:ec2:*:*:snapshot/*",
      "Condition": {
        "StringLike": {
          "aws:ResourceTag/GuardDutyScanId": "*"
        },
        "Null": {
          "aws:ResourceTag/GuardDutyExcluded": "true"
        }
      }
    }
  }
}

```

```
]
}
```

Kebijakan kepercayaan berikut dilampirkan ke peran yang `AWSServiceRoleForAmazonGuardDutyMalwareProtection` terhubung dengan layanan:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "malware-protection.guardduty.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Membuat peran terkait layanan untuk Perlindungan Malware untuk EC2

Peran `AWSServiceRoleForAmazonGuardDutyMalwareProtection` yang terhubung dengan layanan dibuat secara otomatis saat Anda mengaktifkan Perlindungan Malware EC2 untuk pertama kalinya atau mengaktifkan Perlindungan Malware untuk EC2 Wilayah yang didukung tempat sebelumnya Anda tidak mengaktifkannya. Anda juga dapat membuat peran terkait layanan `AWSServiceRoleForAmazonGuardDutyMalwareProtection` secara manual menggunakan konsol IAM, CLI IAM, atau API IAM.

 Note

Secara default, jika Anda baru mengenal Amazon GuardDuty, Perlindungan Malware untuk EC2 diaktifkan secara otomatis.

 Important

Peran yang terhubung dengan layanan yang dibuat untuk akun GuardDuty administrator yang didelegasikan tidak berlaku untuk akun anggota. GuardDuty

Anda harus mengonfigurasi izin untuk mengizinkan kepala IAM (seperti pengguna, grup, atau peran) untuk membuat, mengedit, atau menghapus peran terkait layanan. Agar peran `AWSServiceRoleForAmazonGuardDutyMalwareProtection` terkait layanan berhasil dibuat, identitas IAM yang Anda gunakan GuardDuty dengan harus memiliki izin yang diperlukan. Untuk memberikan izin yang diperlukan, lampirkan kebijakan berikut untuk pengguna, grup, atau peran ini:

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": "guardduty:*",
    "Resource": "*"
  },
  {
    "Effect": "Allow",
    "Action": "iam:CreateServiceLinkedRole",
    "Resource": "*",
    "Condition": {
      "StringLike": {
        "iam:AWSServiceName": [
          "malware-protection.guardduty.amazonaws.com"
        ]
      }
    }
  },
  {
    "Effect": "Allow",
    "Action": [
      "organizations:EnableAWSServiceAccess",
      "organizations:RegisterDelegatedAdministrator",
      "organizations:ListDelegatedAdministrators",
      "organizations:ListAWSServiceAccessForOrganization",
      "organizations:DescribeOrganizationalUnit",
      "organizations:DescribeAccount",
      "organizations:DescribeOrganization"
    ],
    "Resource": "*"
  },
  {
    "Effect": "Allow",
    "Action": "iam:GetRole",
    "Resource": "arn:aws:iam::*:role/*AWSServiceRoleForAmazonGuardDutyMalwareProtection"
```

```
}  
]  
}
```

Untuk informasi selengkapnya tentang membuat peran secara manual, lihat [Membuat peran tertaut layanan](#) dalam Panduan Pengguna IAM.

Mengedit peran terkait layanan untuk Perlindungan Malware untuk EC2

Perlindungan Malware untuk EC2 tidak mengizinkan Anda untuk mengedit peran yang `AWSServiceRoleForAmazonGuardDutyMalwareProtection` terkait dengan layanan. Setelah membuat peran terkait layanan, Anda tidak dapat mengubah nama peran karena berbagai entitas mungkin mereferensikan peran tersebut. Namun, Anda dapat menyunting penjelasan peran menggunakan IAM. Untuk informasi selengkapnya, lihat [Mengedit peran terkait layanan](#) dalam Panduan Pengguna IAM.

Menghapus peran terkait layanan untuk Perlindungan Malware untuk EC2

Jika Anda tidak perlu lagi menggunakan fitur atau layanan yang memerlukan peran terkait layanan, sebaiknya hapus peran tersebut. Dengan begitu, Anda tidak memiliki entitas yang tidak digunakan yang tidak dipantau atau dikelola secara aktif.

Important

Untuk menghapus `AWSServiceRoleForAmazonGuardDutyMalwareProtection`, Anda harus menonaktifkan Perlindungan Malware terlebih dahulu untuk EC2 semua Wilayah yang mengaktifkannya.

Jika Perlindungan Malware untuk EC2 tidak dinonaktifkan saat Anda mencoba untuk menghapus peran yang terhubung dengan layanan, penghapusan akan gagal. Pastikan Anda menonaktifkan Perlindungan Malware terlebih dahulu EC2 di akun Anda.

Ketika Anda memilih Nonaktifkan untuk menghentikan Perlindungan Malware untuk EC2 layanan, `AWSServiceRoleForAmazonGuardDutyMalwareProtection` tidak dihapus secara otomatis. Jika Anda kemudian memilih Aktifkan untuk memulai Perlindungan Malware untuk EC2 layanan lagi, GuardDuty akan mulai menggunakan yang ada `AWSServiceRoleForAmazonGuardDutyMalwareProtection`.

Untuk menghapus peran tertaut layanan secara manual menggunakan IAM

Gunakan konsol IAM, AWS CLI, atau IAM API untuk menghapus `AWSServiceRoleForAmazonGuardDutyMalwareProtection` peran terkait layanan. Untuk informasi selengkapnya, lihat [Menghapus peran terkait layanan](#) dalam Panduan Pengguna IAM.

Wilayah AWS yang Didukung

Amazon GuardDuty mendukung penggunaan peran `AWSServiceRoleForAmazonGuardDutyMalwareProtection` terkait layanan di semua Wilayah AWS tempat Perlindungan Malware EC2 tersedia.

Untuk daftar Wilayah yang saat ini GuardDuty tersedia, lihat [GuardDuty titik akhir dan kuota Amazon](#) di. Referensi Umum Amazon Web

Note

Perlindungan Malware untuk saat EC2 ini tidak tersedia di AWS GovCloud (AS-Timur) dan AWS GovCloud (AS-Barat).

AWS kebijakan terkelola untuk Amazon GuardDuty

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 Akun AWS Anda. Untuk informasi selengkapnya tentang kebijakan AWS [AWS terkelola, lihat kebijakan terkelola](#) di Panduan Pengguna IAM.

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

Elemen kebijakan Version menetapkan aturan sintaksis bahasa yang akan digunakan untuk memproses kebijakan. Kebijakan berikut mencakup versi saat ini yang didukung IAM. Untuk informasi selengkapnya, lihat [elemen kebijakan IAM JSON: Versi](#).

AWS kebijakan terkelola: AmazonGuardDutyFullAccess_v2 (disarankan)

Anda dapat melampirkan kebijakan AmazonGuardDutyFullAccess_v2 ke identitas IAM Anda. Antara AmazonGuardDutyFullAccess_v2 dan [AmazonGuardDutyFullAccess](#), GuardDuty merekomendasikan melampirkan AmazonGuardDutyFullAccess_v2 karena menawarkan keamanan yang ditingkatkan dan membatasi tindakan administratif untuk prinsipal GuardDuty layanan. Kebijakan ini masih akan memungkinkan pengguna akses penuh untuk melakukan semua GuardDuty tindakan dan mengakses sumber daya yang diperlukan.

Detail izin

AmazonGuardDutyFullAccess_v2 Kebijakan ini mencakup izin berikut:

- GuardDuty— Memungkinkan pengguna akses penuh ke semua GuardDuty tindakan.
- IAM:
 - Memungkinkan pengguna untuk membuat GuardDuty peran terkait layanan.
 - Memungkinkan melihat dan mengelola peran IAM dan kebijakan mereka untuk GuardDuty.
 - Memungkinkan pengguna untuk meneruskan peran GuardDuty yang menggunakan peran ini untuk mengaktifkan fitur Perlindungan GuardDuty Malware untuk S3. Ini terlepas dari bagaimana Anda mengaktifkan Perlindungan Malware untuk S3 - dalam GuardDuty layanan atau secara independen.
 - Izin untuk melakukan `iam:GetRole` tindakan
AWSServiceRoleForAmazonGuardDutyMalwareProtection menetapkan apakah peran terkait layanan (SLR) untuk Perlindungan Malware untuk EC2 ada di akun.
- Organizations:
 - Memungkinkan pengguna untuk membaca (melihat) struktur GuardDuty organisasi dan akun.
 - Memungkinkan pengguna untuk menunjuk administrator yang didelegasikan dan mengelola anggota untuk organisasi. GuardDuty


```

{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "GuardDutyFullAccess",
    "Effect": "Allow",
    "Action": "guarddduty:*",
    "Resource": "*"
  },
  {
    "Sid": "CreateGuardDutyServiceLinkedRole",
    "Effect": "Allow",
    "Action": "iam:CreateServiceLinkedRole",
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "iam:AWSServiceName": [
          "guarddduty.amazonaws.com",
          "malware-protection.guarddduty.amazonaws.com"
        ]
      }
    }
  },
  {
    "Sid": "GuardDutyOrganizationsReadOnly",
    "Effect": "Allow",
    "Action": [
      "organizations:ListAWSServiceAccessForOrganization",
      "organizations:DescribeOrganizationalUnit",
      "organizations:DescribeAccount",
      "organizations:DescribeOrganization",
      "organizations:ListAccounts"
    ],
    "Resource": "*"
  },
  {
    "Sid": "GuardDutyOrganizationsAdminAccess",
    "Effect": "Allow",
    "Action": [
      "organizations:EnableAWSServiceAccess",
      "organizations:DisableAWSServiceAccess",
      "organizations:RegisterDelegatedAdministrator",
      "organizations:DeregisterDelegatedAdministrator",
      "organizations:ListDelegatedAdministrators"
    ]
  }
]
}

```

```

    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "organizations:ServicePrincipal": [
                "guardduty.amazonaws.com",
                "malware-protection.guardduty.amazonaws.com"
            ]
        }
    }
},
{
    "Sid": "GuardDutyIamRoleAccess",
    "Effect": "Allow",
    "Action": "iam:GetRole",
    "Resource": "arn:aws:iam::*:role/*AWSServiceRoleForAmazonGuardDutyMalwareProtection"
},
{
    "Sid": "PassRoleToMalwareProtectionPlan",
    "Effect": "Allow",
    "Action": "iam:PassRole",
    "Resource": "arn:aws:iam::*:role/*",
    "Condition": {
        "StringEquals": {
            "iam:PassedToService": "malware-protection-plan.guardduty.amazonaws.com"
        }
    }
}
]
}

```

AWS kebijakan terkelola: AmazonGuardDutyFullAccess

Anda dapat melampirkan kebijakan AmazonGuardDutyFullAccess ke identitas IAM Anda.

Important

Untuk keamanan yang ditingkatkan dan izin terbatas pada prinsipal GuardDuty layanan, kami sarankan Anda untuk menggunakannya. [AWS kebijakan terkelola: AmazonGuardDutyFullAccess_v2 \(disarankan\)](#)

Kebijakan ini memberikan izin administratif yang memungkinkan pengguna mengakses penuh untuk melakukan semua GuardDuty tindakan dan sumber daya.

Detail izin

Kebijakan ini mencakup izin berikut.

- **GuardDuty**— Memungkinkan pengguna akses penuh ke semua GuardDuty tindakan.
- **IAM:**
 - Memungkinkan pengguna untuk membuat peran GuardDuty terkait layanan.
 - Memungkinkan akun administrator GuardDuty untuk mengaktifkan akun anggota.
 - Memungkinkan pengguna untuk meneruskan peran GuardDuty yang menggunakan peran ini untuk mengaktifkan fitur Perlindungan GuardDuty Malware untuk S3. Ini terlepas dari bagaimana Anda mengaktifkan Perlindungan Malware untuk S3 - dalam GuardDuty layanan atau secara independen.
- **Organizations**— Memungkinkan pengguna untuk menunjuk administrator yang didelegasikan dan mengelola anggota untuk organisasi. GuardDuty

Izin untuk melakukan `iam:GetRole` tindakan

`AWSServiceRoleForAmazonGuardDutyMalwareProtection` menetapkan apakah peran terkait layanan (SLR) untuk Perlindungan Malware untuk EC2 ada di akun.

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "AmazonGuardDutyFullAccessSid1",
    "Effect": "Allow",
    "Action": "guardduty:*",
    "Resource": "*"
  },
  {
    "Sid": "CreateServiceLinkedRoleSid1",
    "Effect": "Allow",
    "Action": "iam:CreateServiceLinkedRole",
    "Resource": "*",
    "Condition": {
      "StringLike": {
        "iam:AWSServiceName": [
```

```

        "guardduty.amazonaws.com",
        "malware-protection.guardduty.amazonaws.com"
    ]
}
},
{
    "Sid": "ActionsForOrganizationsSid1",
    "Effect": "Allow",
    "Action": [
        "organizations:EnableAWSServiceAccess",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts"
    ],
    "Resource": "*"
},
{
    "Sid": "IamGetRoleSid1",
    "Effect": "Allow",
    "Action": "iam:GetRole",
    "Resource": "arn:aws:iam::*:role/
*AWSServiceRoleForAmazonGuardDutyMalwareProtection"
},
{
    "Sid": "AllowPassRoleToMalwareProtectionPlan",
    "Effect": "Allow",
    "Action": [
        "iam:PassRole"
    ],
    "Resource": "arn:aws:iam::*:role/*",
    "Condition": {
        "StringEquals": {
            "iam:PassedToService": "malware-protection-
plan.guardduty.amazonaws.com"
        }
    }
}
]

```

```
}
```

AWS kebijakan terkelola: AmazonGuardDutyReadOnlyAccess

Anda dapat melampirkan kebijakan AmazonGuardDutyReadOnlyAccess ke identitas IAM Anda.

Kebijakan ini memberikan izin hanya-baca yang memungkinkan pengguna melihat GuardDuty temuan dan detail organisasi Anda. GuardDuty

Detail izin

Kebijakan ini mencakup izin berikut.

- **GuardDuty**— Memungkinkan pengguna untuk melihat GuardDuty temuan dan melakukan operasi API yang dimulai dengan `Get`, `List`, atau `Describe`.
- **Organizations**— Memungkinkan pengguna untuk mengambil informasi tentang konfigurasi GuardDuty organisasi Anda, termasuk rincian akun administrator yang didelegasikan.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "guarddduty:Describe*",
        "guarddduty:Get*",
        "guarddduty:List*"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts"
      ],
    },
  ],
}
```

```
        "Resource": "*"
    }
  ]
}
```

AWS kebijakan terkelola: AmazonGuardDutyServiceRolePolicy

Anda tidak dapat melampirkan AmazonGuardDutyServiceRolePolicy ke entitas IAM Anda. Kebijakan AWS terkelola ini dilampirkan pada peran terkait layanan yang memungkinkan Anda GuardDuty melakukan tindakan atas nama Anda. Untuk informasi selengkapnya, lihat [Izin peran terkait layanan untuk GuardDuty](#).

GuardDuty pembaruan kebijakan AWS terkelola

Lihat detail tentang pembaruan kebijakan AWS terkelola GuardDuty sejak layanan ini mulai melacak perubahan ini. Untuk peringatan otomatis tentang perubahan pada halaman ini, berlangganan umpan RSS di halaman Riwayat GuardDuty dokumen.

Perubahan	Deskripsi	Tanggal
AmazonGuardDutyFullAccess_v2 — Menambahkan kebijakan baru	Menambahkan AmazonGuardDutyFullAccess_v2 kebijakan baru. Ini direkomendasikan karena izinnya meningkatkan keamanan dengan membatasi tindakan administratif pada prinsipal GuardDuty layanan berdasarkan peran dan kebijakan IAM, dan integrasi. AWS Organizations	Juni 04, 2025
AmazonGuardDutyServiceRolePolicy – Pembaruan ke kebijakan yang ada	Menambahkan ec2:DescribeVpcs izin. Ini memungkinkan GuardDuty untuk melacak pembaruan VPC, seperti mengambil CIDR VPC.	Agustus 22, 2024

Perubahan	Deskripsi	Tanggal
AmazonGuardDutyServiceRolePolicy – Pembaruan ke kebijakan yang ada	Menambahkan izin yang memungkinkan Anda meneruskan peran IAM GuardDuty saat Anda mengaktifkan Perlindungan Malware untuk S3. <pre>{ "Sid": "AllowPassRoleToMalwareProtectionPlan", "Effect": "Allow", "Action": ["iam:PassRole"], "Resource": "arn:aws:iam::*:role/*", "Condition": { "StringEquals": { "iam:PassedToService": "guardduty.amazonaws.com" } } }</pre>	Juni 10, 2024

Perubahan	Deskripsi	Tanggal
AmazonGuardDutyServiceRolePolicy — Perbarui ke kebijakan yang ada.	Gunakan AWS Systems Manager tindakan untuk mengelola asosiasi SSM di EC2 instans Amazon saat Anda mengaktifkan Pemantauan GuardDuty Waktu Proses dengan agen otomatis untuk Amazon. EC2 Ketika konfigurasi agen GuardDuty otomatis dinonaktifkan, GuardDuty pertimbangkan hanya EC2 instance yang memiliki tag inklusi (GuardDuty Managed :true).	26 Maret 2024
AmazonGuardDutyServiceRolePolicy — Perbarui ke kebijakan yang ada.	GuardDuty telah menambahkan izin baru - <code>organization:DescribeOrganization</code> untuk mengambil ID organisasi akun VPC Amazon bersama dan menetapkan kebijakan titik akhir VPC Amazon dengan ID organisasi.	Februari 9, 2024

Perubahan	Deskripsi	Tanggal
AmazonGuardDutyMalwareProtectionServiceRolePolicy — Perbarui ke kebijakan yang ada.	Perlindungan Malware for EC2 telah menambahkan dua izin - GetSnapshotBlock dan ListSnapshotBlocks untuk mengambil snapshot volume EBS (dienkripsi menggunakan Kunci yang dikelola AWS) dari Anda Akun AWS dan menyalinnya ke akun GuardDuty layanan sebelum memulai pemindaian malware.	25 Jan 2024
AmazonGuardDutyServiceRolePolicy – Pembaruan ke kebijakan yang ada	Menambahkan izin baru GuardDuty untuk memungkinkan menambahkan guarddutyActivate setelah akun Amazon ECS, serta melakukan daftar dan menjelaskan operasi di kluster Amazon ECS.	November 26, 2023
AmazonGuardDutyReadOnlyAccess – Pembaruan ke kebijakan yang ada	GuardDuty menambahkan kebijakan baru organizations untukListAccounts .	16 November 2023
AmazonGuardDutyFullAccess – Pembaruan ke kebijakan yang ada	GuardDuty menambahkan kebijakan baru organizations untukListAccounts .	16 November 2023

Perubahan	Deskripsi	Tanggal
AmazonGuardDutyServiceRolePolicy – Pembaruan ke kebijakan yang ada	GuardDuty menambahkan izin baru untuk mendukung fitur GuardDuty EKS Runtime Monitoring yang akan datang.	8 Maret 2023
AmazonGuardDutyServiceRolePolicy – Pembaruan ke kebijakan yang ada	GuardDuty telah menambahkan izin baru untuk memungkinkan membuat peran terkait Layanan GuardDuty untuk Perlindungan Malware untuk EC2 Ini akan membantu GuardDuty merampingkan proses mengaktifkan Perlindungan Malware untuk EC2 GuardDuty sekarang dapat melakukan tindakan IAM berikut:	21 Februari 2023

```
{
  "Effect": "Allow",
  "Action": "iam:CreateServiceLinkedRole",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "iam:AWSServiceName": "malware-protection.guardduty.amazonaws.com"
    }
  }
}
```

Perubahan	Deskripsi	Tanggal
AmazonGuardDutyFullAccess – Pembaruan ke kebijakan yang ada	GuardDuty ARN yang diperbarui untuk <code>iam:GetRole . *AWSServiceRoleForAmazonGuardDutyMalwareProtection</code>	26 Jul 2022
AmazonGuardDutyFullAccess – Pembaruan ke kebijakan yang ada	GuardDuty menambahkan yang baru <code>AWSServiceName</code> untuk memungkinkan pembuatan peran terkait layanan menggunakan Perlindungan GuardDuty Malware <code>iam:CreateServiceLinkedRole</code> untuk layanan. EC2 GuardDuty sekarang dapat melakukan <code>iam:GetRole</code> tindakan untuk mendapatkan informasi untuk <code>AWSServiceRole</code> .	26 Jul 2022

Perubahan	Deskripsi	Tanggal
AmazonGuardDutyServiceRolePolicy – Pembaruan ke kebijakan yang ada	GuardDuty menambahkan izin baru GuardDuty untuk memungkinkan pengguna tindakan EC2 jaringan Amazon untuk meningkatkan temuan. GuardDuty sekarang dapat melakukan EC2 tindakan berikut untuk mendapatkan informasi tentang bagaimana EC2 instans Anda berkomunikasi. Informasi ini digunakan untuk meningkatkan akurasi penemuan. • <code>ec2:DescribeVpcEndpoints</code> • <code>ec2:DescribeSubnets</code> • <code>ec2:DescribeVpcPeeringConnections</code> • <code>ec2:DescribeTransitGatewayAttachments</code>	Agustus 3, 2021
GuardDuty mulai melacak perubahan	GuardDuty mulai melacak perubahan untuk kebijakan yang AWS dikelola.	Agustus 3, 2021

Memecahkan masalah GuardDuty identitas dan akses Amazon

Gunakan informasi berikut untuk membantu Anda mendiagnosis dan memperbaiki masalah umum yang mungkin Anda temui saat bekerja dengan GuardDuty dan IAM.

Topik

- [Saya tidak berwenang untuk melakukan tindakan di GuardDuty](#)
- [Saya tidak berwenang untuk melakukan iam:PassRole.](#)
- [Saya ingin mengizinkan orang-orang di luar saya Akun AWS untuk mengakses GuardDuty sumber daya saya.](#)

Saya tidak berwenang untuk melakukan tindakan di GuardDuty

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 suatu sumber daya `my-example-widget` rekaan, tetapi tidak memiliki izin `guardduty:GetWidget` rekaan.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
guardduty:GetWidget on resource: my-example-widget
```

Dalam hal ini, kebijakan untuk pengguna `mateojackson` harus diperbarui untuk mengizinkan akses ke sumber daya `my-example-widget` dengan menggunakan tindakan `guardduty: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 yang tidak diizinkan untuk melakukan `iam:PassRole` tindakan, kebijakan Anda harus diperbarui agar Anda dapat meneruskan peran GuardDuty.

Beberapa Layanan AWS memungkinkan Anda untuk meneruskan peran yang ada ke layanan tersebut alih-alih membuat peran layanan baru atau peran terkait layanan. Untuk melakukannya, Anda harus memiliki izin untuk meneruskan peran ke layanan.

Contoh kesalahan berikut terjadi ketika pengguna IAM bernama `marymajor` mencoba menggunakan konsol tersebut untuk melakukan tindakan di GuardDuty. Namun, tindakan tersebut memerlukan layanan untuk mendapatkan izin yang diberikan oleh peran layanan. Mary tidak memiliki izin untuk meneruskan peran tersebut pada layanan.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
iam:PassRole
```

Dalam kasus ini, kebijakan Mary harus diperbarui agar dia mendapatkan izin untuk melakukan tindakan `iam:PassRole` tersebut.

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

Saya ingin mengizinkan orang-orang di luar saya Akun AWS untuk mengakses GuardDuty 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 layanan yang mendukung kebijakan berbasis sumber daya atau daftar kontrol akses (ACLs), Anda dapat menggunakan kebijakan tersebut untuk memberi orang akses ke sumber daya Anda.

Untuk mempelajari selengkapnya, periksa referensi berikut:

- Untuk mempelajari apakah GuardDuty mendukung fitur-fitur ini, lihat [Bagaimana Amazon GuardDuty bekerja dengan IAM](#).
- Untuk mempelajari cara menyediakan akses ke sumber daya Anda di seluruh sumber daya Akun AWS yang Anda miliki, lihat [Menyediakan akses ke pengguna IAM di pengguna lain Akun AWS yang Anda miliki](#) di Panduan Pengguna IAM.
- Untuk mempelajari cara menyediakan akses ke sumber daya Anda kepada pihak ketiga Akun AWS, lihat [Menyediakan akses yang Akun AWS dimiliki oleh pihak ketiga](#) dalam Panduan Pengguna IAM.
- Untuk mempelajari cara memberikan akses melalui federasi identitas, lihat [Menyediakan akses ke pengguna terautentikasi eksternal \(federasi identitas\)](#) dalam Panduan Pengguna IAM.
- Untuk mempelajari perbedaan antara menggunakan peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat [Akses sumber daya lintas akun di IAM di Panduan Pengguna IAM](#).

Validasi kepatuhan untuk Amazon GuardDuty

Untuk mempelajari apakah an Layanan AWS berada dalam lingkup program kepatuhan tertentu, lihat [Layanan AWS di Lingkup oleh Program Kepatuhan Layanan AWS](#) dan pilih program kepatuhan yang Anda minati. Untuk informasi umum, lihat [Program AWS Kepatuhan Program AWS](#) .

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

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

- [Kepatuhan dan Tata Kelola Keamanan](#) – Panduan implementasi solusi ini membahas pertimbangan arsitektur serta memberikan langkah-langkah untuk menerapkan fitur keamanan dan kepatuhan.
- [Referensi Layanan yang Memenuhi Syarat HIPAA](#) — Daftar layanan yang memenuhi syarat HIPAA. Tidak semua memenuhi Layanan AWS syarat HIPAA.
- [AWS Sumber Daya AWS](#) — Kumpulan buku kerja dan panduan ini mungkin berlaku untuk industri dan lokasi Anda.
- [AWS Panduan Kepatuhan Pelanggan](#) - Memahami model tanggung jawab bersama melalui lensa kepatuhan. Panduan ini merangkum praktik terbaik untuk mengamankan Layanan AWS dan memetakan panduan untuk kontrol keamanan di berbagai kerangka kerja (termasuk Institut Standar dan Teknologi Nasional (NIST), Dewan Standar Keamanan Industri Kartu Pembayaran (PCI), dan Organisasi Internasional untuk Standardisasi (ISO)).
- [Mengevaluasi Sumber Daya dengan Aturan](#) dalam Panduan AWS Config Pengembang — AWS Config Layanan menilai seberapa baik konfigurasi sumber daya Anda mematuhi praktik internal, pedoman industri, dan peraturan.
- [AWS Security Hub](#)— Ini Layanan AWS memberikan pandangan komprehensif tentang keadaan keamanan Anda di dalamnya AWS. Security Hub menggunakan kontrol keamanan untuk sumber daya AWS Anda serta untuk memeriksa kepatuhan Anda terhadap standar industri keamanan dan praktik terbaik. Untuk daftar layanan dan kontrol yang didukung, lihat [Referensi kontrol Security Hub](#).
- [Amazon GuardDuty](#) — Ini Layanan AWS mendeteksi potensi ancaman terhadap beban kerja Akun AWS, kontainer, dan data Anda dengan memantau lingkungan Anda untuk aktivitas mencurigakan dan berbahaya. GuardDuty dapat membantu Anda mengatasi berbagai persyaratan kepatuhan, seperti PCI DSS, dengan memenuhi persyaratan deteksi intrusi yang diamanatkan oleh kerangka kerja kepatuhan tertentu.
- [AWS Audit Manager](#)Ini Layanan AWS membantu Anda terus mengaudit AWS penggunaan Anda untuk menyederhanakan cara Anda mengelola risiko dan kepatuhan terhadap peraturan dan standar industri.

Ketahanan di Amazon GuardDuty

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 di Amazon GuardDuty

Sebagai layanan terkelola, Amazon GuardDuty 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 GuardDuty melalui jaringan. Klien harus mendukung hal-hal berikut:

- Keamanan Lapisan Pengangkutan (TLS). Kami mensyaratkan TLS 1.2 dan menganjurkan TLS 1.3.
- Sandi cocok dengan sistem kerahasiaan maju sempurna (perfect forward secrecy, PFS) seperti DHE (Ephemeral Diffie-Hellman) atau ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Sebagian besar sistem modern seperti Java 7 dan versi lebih baru mendukung mode-mode ini.

Selain itu, permintaan harus ditandatangani menggunakan ID kunci akses dan kunci akses rahasia yang terkait dengan prinsipal IAM. Atau Anda bisa menggunakan [AWS Security Token Service](#) (AWS STS) untuk membuat kredensial keamanan sementara guna menandatangani permintaan.

Amazon GuardDuty dan titik akhir VPC antarmuka ()AWS PrivateLink

Anda dapat membuat koneksi pribadi antara VPC dan Amazon GuardDuty dengan membuat antarmuka VPC endpoint. Endpoint antarmuka didukung oleh [AWS PrivateLink](#), teknologi yang memungkinkan Anda mengakses secara pribadi GuardDuty APIs tanpa gateway internet, perangkat NAT, koneksi VPN, atau koneksi Direct AWS Connect. Instans di VPC Anda tidak memerlukan alamat IP publik untuk berkomunikasi. GuardDuty APIs Lalu lintas antara VPC Anda dan GuardDuty tidak meninggalkan jaringan Amazon.

Setiap titik akhir antarmuka diwakili oleh satu atau beberapa [Antarmuka Jaringan Elastis](#) di subnet Anda.

Untuk informasi selengkapnya, lihat [Titik akhir VPC Antarmuka \(AWS PrivateLink\) di Panduan.AWS PrivateLink](#)

Pertimbangan untuk titik akhir GuardDuty VPC

Sebelum menyiapkan titik akhir VPC antarmuka GuardDuty, pastikan Anda meninjau [properti dan batasan titik akhir Antarmuka](#) dalam Panduan.AWS PrivateLink

GuardDuty mendukung panggilan ke semua tindakan API-nya dari VPC Anda.

Buat VPC endpoint antarmuka untuk GuardDuty

Anda dapat membuat titik akhir VPC untuk GuardDuty layanan menggunakan konsol VPC Amazon atau (). AWS Command Line Interface AWS CLI Untuk informasi selengkapnya, lihat [Membuat titik akhir antarmuka](#) di AWS PrivateLink Panduan.

Buat titik akhir VPC untuk GuardDuty menggunakan nama layanan berikut:

- `com.amazonaws. region.guardduty`
- `com.amazonaws. region.guardduty-fips` (titik akhir FIPS)

Jika Anda mengaktifkan DNS pribadi untuk titik akhir, Anda dapat membuat permintaan API untuk GuardDuty menggunakan nama DNS default untuk Wilayah, misalnya, `guardduty.us-east-1.amazonaws.com`

Untuk informasi selengkapnya, lihat [Mengakses layanan melalui titik akhir antarmuka](#) di AWS PrivateLink Panduan.

Membuat kebijakan titik akhir VPC untuk GuardDuty

Anda dapat melampirkan kebijakan titik akhir ke VPC endpoint yang mengendalikan akses ke GuardDuty. Kebijakan titik akhir menentukan informasi berikut:

- Prinsipal yang dapat melakukan tindakan.
- Tindakan yang dapat dilakukan.
- Sumber daya yang menjadi target tindakan.

Untuk informasi selengkapnya, lihat [Mengontrol akses ke layanan dengan titik akhir VPC di Panduan](#).AWS PrivateLink

Contoh: Kebijakan titik akhir VPC untuk tindakan GuardDuty

Berikut ini adalah contoh kebijakan endpoint untuk GuardDuty. Saat dilampirkan ke titik akhir, kebijakan ini memberikan akses ke GuardDuty tindakan yang tercantum untuk semua prinsipal di semua sumber daya.

```
{
  "Statement": [
    {
      "Principal": "*",
      "Effect": "Allow",
      "Action": [
        "guardduty:listDetectors",
        "guardduty:getDetector",
        "guardduty:getFindings"
      ],
      "Resource": "*"
    }
  ]
}
```

Subnet bersama

Anda tidak dapat membuat, mendeskripsikan, memodifikasi, atau menghapus titik akhir VPC di subnet yang dibagikan dengan Anda. Namun, Anda dapat menggunakan titik akhir VPC di subnet

yang dibagikan dengan Anda. Untuk informasi tentang berbagi VPC, lihat [Membagikan VPC Anda dengan akun lain di Panduan Pengguna](#) Amazon VPC.

GuardDuty Berintegrasi dengan layanan AWS keamanan

GuardDuty dapat diintegrasikan dengan layanan AWS keamanan lainnya. Layanan ini dapat menyerap data dari GuardDuty untuk memungkinkan Anda melihat temuan dengan cara baru. Tinjau opsi integrasi berikut untuk mempelajari lebih lanjut tentang cara layanan tersebut disiapkan untuk bekerja dengannya GuardDuty.

Integrasi dengan GuardDuty AWS Security Hub

AWS Security Hub mengumpulkan data keamanan dari seluruh AWS akun, layanan, dan produk mitra pihak ketiga yang didukung untuk menilai keadaan keamanan lingkungan Anda sesuai dengan standar industri dan praktik terbaik. Selain mengevaluasi postur keamanan Anda, Security Hub menciptakan lokasi terpusat untuk temuan di semua AWS layanan terintegrasi Anda, dan produk AWS Mitra. Mengaktifkan Security Hub dengan GuardDuty akan secara otomatis memungkinkan data GuardDuty temuan dicerna oleh Security Hub.

Untuk informasi selengkapnya tentang menggunakan Security Hub dengan GuardDuty lihat [Integrasi dengan AWS Security Hub](#).

Integrasi GuardDuty dengan Amazon Detective

Amazon Detective menggunakan data log dari seluruh AWS akun Anda untuk membuat visualisasi data untuk sumber daya dan alamat IP yang berinteraksi dengan lingkungan Anda. Visualisasi Detective membantu Anda menyelidiki masalah keamanan dengan cepat dan mudah. Anda dapat beralih dari GuardDuty menemukan detail ke informasi di konsol Detektif setelah kedua layanan diaktifkan.

Untuk informasi lebih lanjut tentang menggunakan Detektif dengan GuardDuty lihat. [Integrasi dengan Amazon Detective](#)

Integrasi dengan AWS Security Hub

[AWS Security Hub](#) memberi Anda gambaran menyeluruh tentang status keamanan Anda dalam AWS dan membantu Anda memeriksa lingkungan Anda terhadap standar industri keamanan dan praktik terbaik. Security Hub mengumpulkan data keamanan dari berbagai AWS akun, layanan, dan produk mitra pihak ketiga yang didukung serta membantu Anda menganalisis tren keamanan dan mengidentifikasi masalah keamanan prioritas tertinggi.

GuardDuty Integrasi Amazon dengan Security Hub memungkinkan Anda mengirim temuan dari Security Hub GuardDuty ke Security Hub. Security Hub kemudian dapat menyertakan temuan tersebut dalam analisis postur keamanan Anda.

Daftar Isi

- [Bagaimana Amazon GuardDuty mengirimkan temuan ke AWS Security Hub](#)
 - [Jenis temuan yang GuardDuty dikirim ke Security Hub](#)
 - [Latensi untuk mengirimkan temuan baru](#)
 - [Mencoba kembali saat Security Hub tidak tersedia](#)
 - [Memperbarui temuan yang ada di Security Hub](#)
 - [Melihat GuardDuty temuan di AWS Security Hub](#)
 - [Menafsirkan GuardDuty menemukan nama di AWS Security Hub](#)
 - [Temuan standar dari GuardDuty](#)
 - [Mengaktifkan dan mengonfigurasi integrasi](#)
 - [Menggunakan GuardDuty kontrol di Security Hub](#)
 - [Menghentikan publikasi temuan ke Security Hub](#)

Bagaimana Amazon GuardDuty mengirimkan temuan ke AWS Security Hub

Pada tahun AWS Security Hub, masalah keamanan dilacak sebagai temuan. Beberapa temuan berasal dari masalah yang terdeteksi oleh AWS layanan lain atau oleh mitra pihak ketiga. Security Hub juga memiliki seperangkat aturan yang digunakan untuk mendeteksi masalah keamanan dan menghasilkan temuan.

Security Hub menyediakan alat untuk mengelola temuan dari seluruh sumber tersebut. Anda dapat melihat dan mem-filter daftar temuan dan melihat detail suatu temuan. Untuk informasi lebih lanjut, lihat [Melihat temuan](#) dalam Panduan Pengguna AWS Security Hub . Anda juga dapat melacak status penyelidikan temuan. Untuk informasi lebih lanjut, lihat [Mengambil tindakan pada temuan](#) dalam Panduan Pengguna AWS Security Hub .

Semua temuan di Security Hub menggunakan format JSON standar yang disebut AWS Security Finding Format (ASFF). ASFF mencakup detail tentang sumber masalah, sumber daya yang terdampak, dan status temuan saat ini. Lihat [AWS Security Finding Format \(ASFF\)](#) di Panduan Pengguna AWS Security Hub .

Amazon GuardDuty adalah salah satu AWS layanan yang mengirimkan temuan ke Security Hub.

Jenis temuan yang GuardDuty dikirim ke Security Hub

Setelah Anda mengaktifkan GuardDuty dan Security Hub di akun yang sama dalam akun yang sama Wilayah AWS, GuardDuty mulai kirim semua temuan yang dihasilkan ke Security Hub. Temuan ini dikirim ke Security Hub menggunakan [AWS Security Finding Format \(ASFF\)](#). Dalam ASFF, bidang Types menyediakan jenis temuan.

Latensi untuk mengirimkan temuan baru

Saat GuardDuty membuat temuan baru, biasanya dikirim ke Security Hub dalam waktu lima menit.

Mencoba kembali saat Security Hub tidak tersedia

Jika Security Hub tidak GuardDuty tersedia, coba lagi mengirimkan temuan sampai diterima.

Memperbarui temuan yang ada di Security Hub

Setelah mengirimkan temuan ke Security Hub, GuardDuty mengirimkan pembaruan untuk mencerminkan pengamatan tambahan dari aktivitas temuan ke Security Hub. Pengamatan baru dari temuan ini dikirim ke Security Hub berdasarkan [Langkah 5 - Frekuensi untuk mengeksport temuan](#) pengaturan di Anda Akun AWS.

Saat Anda mengarsipkan atau membatalkan arsip temuan, GuardDuty tidak akan mengirim temuan itu ke Security Hub. Temuan yang tidak diarsipkan secara manual yang nantinya menjadi aktif tidak GuardDuty dikirim ke Security Hub.

Melihat GuardDuty temuan di AWS Security Hub

Masuk ke AWS Management Console dan buka AWS Security Hub konsol di <https://console.aws.amazon.com/securityhub/>.

Anda sekarang dapat menggunakan salah satu cara berikut untuk melihat GuardDuty temuan di konsol Security Hub:

Opsi 1: Menggunakan Integrasi di Security Hub

1. Di panel navigasi kiri, pilih Integrasi.
2. Pada halaman Integrasi, periksa Status untuk Amazon: GuardDuty.
 - Jika Status Menerima temuan, maka pilih Lihat temuan di sebelah Menerima temuan.
 - Jika tidak, maka untuk informasi selengkapnya tentang cara kerja Integrasi, lihat [Integrasi Security Hub](#) di AWS Security Hub Panduan Pengguna.

Opsi 2: Menggunakan Temuan di Security Hub

1. Di panel navigasi kiri, pilih Temuan.
2. Pada halaman Temuan, tambahkan filter Nama produk dan masukkan **GuardDuty** untuk melihat hanya GuardDuty temuan.

Menafsirkan GuardDuty menemukan nama di AWS Security Hub

GuardDuty mengirimkan temuan ke Security Hub menggunakan [AWS Security Finding Format \(ASFF\)](#). Dalam ASFF, bidang Types menyediakan jenis temuan. Jenis ASFF menggunakan skema penamaan yang berbeda dari GuardDuty tipe. Tabel di bawah ini merinci semua jenis GuardDuty temuan dengan rekan ASFF mereka saat muncul di Security Hub.

Note

Untuk beberapa jenis GuardDuty temuan Security Hub memberikan nama temuan ASFF yang berbeda tergantung pada apakah Peran Sumber Daya detail temuan adalah ACTOR atau TARGET. Untuk informasi selengkapnya, lihat [Detail temuan](#).

GuardDuty menemukan jenis	Tipe temuan ASFF
AttackSequence:IAM/CompromisedCredentials	TTPs/AttackSequence:IAM/CompromisedC redentials
AttackSequence:S3/CompromisedData	TTPs/AttackSequence:S3/CompromisedData
Backdoor:EC2/C&CActivity.B	TTPs/Command and Control/Backdoor:EC2- C&CActivity.B
Backdoor:EC2/C&CActivity.B!DNS	TTPs/Command and Control/Backdoor:EC2- C&CActivity.B!DNS
Backdoor:EC2/DenialOfService.Dns	TTPs/Command and Control/Backdoor:EC2- DenialOfService.Dns
Backdoor:EC2/DenialOfService.Tcp	TTPs/Command and Control/Backdoor:EC2- DenialOfService.Tcp

GuardDuty menemukan jenis	Tipe temuan ASFF
Backdoor:EC2/DenialOfService.Udp	TTPs/Command and Control/Backdoor:EC2-DenialOfService.Udp
Backdoor:EC2/DenialOfService.UdpOnTcpPorts	TTPs/Command and Control/Backdoor:EC2-DenialOfService.UdpOnTcpPorts
Backdoor:EC2/DenialOfService.UnusualProtocol	TTPs/Command and Control/Backdoor:EC2-DenialOfService.UnusualProtocol
Backdoor:EC2/Spambot	TTPs/Command and Control/Backdoor:EC2-Spambot
Behavior:EC2/NetworkPortUnusual	Unusual Behaviors/VM/Behavior:EC2-NetworkPortUnusual
Behavior:EC2/TrafficVolumeUnusual	Unusual Behaviors/VM/Behavior:EC2-TrafficVolumeUnusual
Backdoor:Lambda/C&CActivity.B	TTPs/Command and Control/Backdoor:Lambda-C&CActivity.B
Backdoor:Runtime/C&CActivity.B	TTPs/Command and Control/Backdoor:Runtime-C&CActivity.B
Backdoor:Runtime/C&CActivity.B!DNS	TTPs/Command and Control/Backdoor:Runtime-C&CActivity.B!DNS
CredentialAccess:IAMUser/AnomalousBehavior	TTPs/Credential Access/IAMUser-AnomalousBehavior
CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed	TTPs/AnomalousBehavior/CredentialAccess:Kubernetes-SecretsAccessed
CredentialAccess:Kubernetes/MaliciousIPCaller	TTPs/CredentialAccess/CredentialAccess:Kubernetes-MaliciousIPCaller
CredentialAccess:Kubernetes/MaliciousIPCaller.Custom	TTPs/CredentialAccess/CredentialAccess:Kubernetes-MaliciousIPCaller.Custom

GuardDuty menemukan jenis	Tipe temuan ASFF
CredentialAccess:Kubernetes/SuccessfulAnonymousAccess	TTPs/CredentialAccess/CredentialAccess:Kubernetes-SuccessfulAnonymousAccess
CredentialAccess:Kubernetes/TorIPCaller	TTPs/CredentialAccess/CredentialAccess:Kubernetes-TorIPCaller
CredentialAccess:RDS/AnomalousBehavior.FailedLogin	TTPs/Credential Access/CredentialAccess:RDS-AnomalousBehavior.FailedLogin
CredentialAccess:RDS/AnomalousBehavior.SuccessfulBruteForce	TTPs/Credential Access/RDS-AnomalousBehavior.SuccessfulBruteForce
CredentialAccess:RDS/AnomalousBehavior.SuccessfulLogin	TTPs/Credential Access/RDS-AnomalousBehavior.SuccessfulLogin
CredentialAccess:RDS/MaliciousIPCaller.FailedLogin	TTPs/Credential Access/RDS-MaliciousIPCaller.FailedLogin
CredentialAccess:RDS/MaliciousIPCaller.SuccessfulLogin	TTPs/Credential Access/RDS-MaliciousIPCaller.SuccessfulLogin
CredentialAccess:RDS/TorIPCaller.FailedLogin	TTPs/Credential Access/RDS-TorIPCaller.FailedLogin
CredentialAccess:RDS/TorIPCaller.SuccessfulLogin	TTPs/Credential Access/RDS-TorIPCaller.SuccessfulLogin
CryptoCurrency:EC2/BitcoinTool.B	TTPs/Command and Control/CryptoCurrency:EC2-BitcoinTool.B
CryptoCurrency:EC2/BitcoinTool.B!DNS	TTPs/Command and Control/CryptoCurrency:EC2-BitcoinTool.B!DNS
CryptoCurrency:Lambda/BitcoinTool.B	TTPs/Command and Control/CryptoCurrency:Lambda-BitcoinTool.B Effects/Resource Consumption/CryptoCurrency:Lambda-BitcoinTool.B

GuardDuty menemukan jenis	Tipe temuan ASFF
CryptoCurrency:Runtime/BitcoinTool.B	TTPs/Command and Control/CryptoCurrency:Runtime-BitcoinTool.B
CryptoCurrency:Runtime/BitcoinTool.B!DNS	TTPs/Command and Control/CryptoCurrency:Runtime-BitcoinTool.B!DNS
DefenseEvasion:EC2/UnusualDNSResolver	TTPs/DefenseEvasion/EC2:Unusual-DNS-Resolver
DefenseEvasion:EC2/UnusualDoHActivity	TTPs/DefenseEvasion/EC2:Unusual-DoH-Activity
DefenseEvasion:EC2/UnusualDoTActivity	TTPs/DefenseEvasion/EC2:Unusual-DoT-Activity
DefenseEvasion:IAMUser/AnomalousBehavior	TTPs/Defense Evasion/IAMUser-AnomalousBehavior
DefenseEvasion:Kubernetes/MaliciousIPCaller	TTPs/DefenseEvasion/DefenseEvasion:Kubernetes-MaliciousIPCaller
DefenseEvasion:Kubernetes/MaliciousIPCaller.Custom	TTPs/DefenseEvasion/DefenseEvasion:Kubernetes-MaliciousIPCaller.Custom
DefenseEvasion:Kubernetes/SuccessfulAnonymousAccess	TTPs/DefenseEvasion/DefenseEvasion:Kubernetes-SuccessfulAnonymousAccess
DefenseEvasion:Kubernetes/TorIPCaller	TTPs/DefenseEvasion/DefenseEvasion:Kubernetes-TorIPCaller
DefenseEvasion:Runtime/FilelessExecution	TTPs/Defense Evasion/DefenseEvasion:Runtime-FilelessExecution
DefenseEvasion:Runtime/ProcessInjection.Proc	TTPs/Defense Evasion/DefenseEvasion:Runtime-ProcessInjection.Proc
DefenseEvasion:Runtime/ProcessInjection.Ptrace	TTPs/Defense Evasion/DefenseEvasion:Runtime-ProcessInjection.Ptrace

GuardDuty menemukan jenis	Tipe temuan ASFF
DefenseEvasion:Runtime/ProcessInjection.VirtualMemoryWrite	TTPs/Defense Evasion/DefenseEvasion:Runtime-ProcessInjection.VirtualMemoryWrite
DefenseEvasion:Runtime/PtraceAntiDebugging	TTPs/DefenseEvasion/DefenseEvasion:Runtime-PtraceAntiDebugging
DefenseEvasion:Runtime/SuspiciousCommand	TTPs/DefenseEvasion/DefenseEvasion:Runtime-SuspiciousCommand
Penemuan:IAMUser/AnomalousBehavior	TTPs/Discovery/IAMUser-AnomalousBehavior
Discovery:Kubernetes/AnomalousBehavior.PermissionChecked	TTPs/AnomalousBehavior/Discovery:Kubernetes-PermissionChecked
Discovery:Kubernetes/MaliciousIPCaller	TTPs/Discovery/Discovery:Kubernetes-MaliciousIPCaller
Discovery:Kubernetes/MaliciousIPCaller.Custom	TTPs/Discovery/Discovery:Kubernetes-MaliciousIPCaller.Custom
Discovery:Kubernetes/SuccessfulAnonymousAccess	TTPs/Discovery/Discovery:Kubernetes-SuccessfulAnonymousAccess
Discovery:Kubernetes/TorIPCaller	TTPs/Discovery/Discovery:Kubernetes-TorIPCaller
Discovery:RDS/MaliciousIPCaller	TTPs/Discovery/RDS-MaliciousIPCaller
Discovery:RDS/TorIPCaller	TTPs/Discovery/RDS-TorIPCaller
Discovery:Runtime/SuspiciousCommand	TTPs/Discovery/Discovery:Runtime-SuspiciousCommand
Discovery:S3/AnomalousBehavior	TTPs/Discovery:S3-AnomalousBehavior
Discovery:S3/BucketEnumeration.Unusual	TTPs/Discovery:S3-BucketEnumeration.Unusual

GuardDuty menemukan jenis	Tipe temuan ASFF
Discovery:S3/MaliciousIPCaller.Custom	TTPs/Discovery:S3-MaliciousIPCaller.Custom
Discovery:S3/TorIPCaller	TTPs/Discovery:S3-TorIPCaller
Discovery:S3/MaliciousIPCaller	TTPs/Discovery:S3-MaliciousIPCaller
Exfiltration:IAMUser/AnomalousBehavior	TTPs/Exfiltration/IAMUser-AnomalousBehavior
Execution:Kubernetes/ExecInKubeSystemPod	TTPs/Execution/Execution:Kubernetes-ExecInKubeSystemPod
Execution:Kubernetes/AnomalousBehavior.ExecInPod	TTPs/AnomalousBehavior/Execution:Kubernetes-ExecInPod
Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed	TTPs/AnomalousBehavior/Execution:Kubernetes-WorkloadDeployed
Impact:Kubernetes/MaliciousIPCaller	TTPs/Impact/Impact:Kubernetes-MaliciousIPCaller
Impact:Kubernetes/MaliciousIPCaller.Custom	TTPs/Impact/Impact:Kubernetes-MaliciousIPCaller.Custom
Impact:Kubernetes/SuccessfulAnonymousAccess	TTPs/Impact/Impact:Kubernetes-SuccessfulAnonymousAccess
Impact:Kubernetes/TorIPCaller	TTPs/Impact/Impact:Kubernetes-TorIPCaller
Persistence:Kubernetes/ContainerWithSensitiveMount	TTPs/Persistence/Persistence:Kubernetes-ContainerWithSensitiveMount
Persistence:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount	TTPs/AnomalousBehavior/Persistence:Kubernetes-WorkloadDeployed!ContainerWithSensitiveMount
PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer	TTPs/AnomalousBehavior/PrivilegeEscalation:Kubernetes-WorkloadDeployed!PrivilegedContainer

GuardDuty menemukan jenis	Tipe temuan ASFF
Persistence:Kubernetes/MaliciousIPCaller	TTPs/Persistence/Persistence:Kubernetes-MaliciousIPCaller
Persistence:Kubernetes/MaliciousIPCaller.Custom	TTPs/Persistence/Persistence:Kubernetes-MaliciousIPCaller.Custom
Persistence:Kubernetes/SuccessfulAnonymousAccess	TTPs/Persistence/Persistence:Kubernetes-SuccessfulAnonymousAccess
Persistence:Kubernetes/TorIPCaller	TTPs/Persistence/Persistence:Kubernetes-TorIPCaller
Execution:EC2/MaliciousFile	TTPs/Execution/Execution:EC2-MaliciousFile
Execution:ECS/MaliciousFile	TTPs/Execution/Execution:ECS-MaliciousFile
Execution:Kubernetes/MaliciousFile	TTPs/Execution/Execution:Kubernetes-MaliciousFile
Execution:Container/MaliciousFile	TTPs/Execution/Execution:Container-MaliciousFile
Execution:EC2/SuspiciousFile	TTPs/Execution/Execution:EC2-SuspiciousFile
Execution:ECS/SuspiciousFile	TTPs/Execution/Execution:ECS-SuspiciousFile
Execution:Kubernetes/SuspiciousFile	TTPs/Execution/Execution:Kubernetes-SuspiciousFile
Execution:Container/SuspiciousFile	TTPs/Execution/Execution:Container-SuspiciousFile
Execution:Runtime/MaliciousFileExecuted	TTPs/Execution/Execution:Runtime-MaliciousFileExecuted
Execution:Runtime/NewBinaryExecuted	TTPs/Execution/Execution:Runtime-NewBinaryExecuted

GuardDuty menemukan jenis	Tipe temuan ASFF
Execution:Runtime/NewLibraryLoaded	TTPs/Execution/Execution:Runtime-New LibraryLoaded
Execution:Runtime/ReverseShell	TTPs/Execution/Execution:Runtime-ReverseShell
Execution:Runtime/SuspiciousCommand	TTPs/Execution/Execution:Runtime-SuspiciousCommand
Execution:Runtime/SuspiciousShellCreated	TTPs/Execution/Execution:Runtime-SuspiciousShellCreated
Execution:Runtime/SuspiciousTool	TTPs/Execution/Execution:Runtime-SuspiciousTool
Exfiltration:S3/AnomalousBehavior	TTPs/Exfiltration:S3-AnomalousBehavior
Exfiltration:S3/ObjectRead.Unusual	TTPs/Exfiltration:S3-ObjectRead.Unusual
Exfiltration:S3/MaliciousIPCaller	TTPs/Exfiltration:S3-MaliciousIPCaller
Impact:EC2/AbusedDomainRequest.Reputation	TTPs/Impact:EC2-AbusedDomainRequest.Reputation
Impact:EC2/BitcoinDomainRequest.Reputation	TTPs/Impact:EC2-BitcoinDomainRequest.Reputation
Impact:EC2/MaliciousDomainRequest.Reputation	TTPs/Impact:EC2-MaliciousDomainRequest.Reputation
Impact:EC2/PortSweep	TTPs/Impact/Impact:EC2-PortSweep
Impact:EC2/SuspiciousDomainRequest.Reputation	TTPs/Impact:EC2-SuspiciousDomainRequest.Reputation
Impact:EC2/WinRMBruteForce	TTPs/Impact/Impact:EC2-WinRMBruteForce
Dampak:IAMUser/AnomalousBehavior	TTPs/Impact/IAMUser-AnomalousBehavior

GuardDuty menemukan jenis	Tipe temuan ASFF
Impact:Runtime/AbusedDomainRequest.Reputation	TTPs/Impact/Impact:Runtime-AbusedDomainRequest.Reputation
Impact:Runtime/BitcoinDomainRequest.Reputation	TTPs/Impact/Impact:Runtime-BitcoinDomainRequest.Reputation
Impact:Runtime/CryptoMinerExecuted	TTPs/Impact/Impact:Runtime-CryptoMinerExecuted
Impact:Runtime/MaliciousDomainRequest.Reputation	TTPs/Impact/Impact:Runtime-MaliciousDomainRequest.Reputation
Impact:Runtime/SuspiciousDomainRequest.Reputation	TTPs/Impact/Impact:Runtime-SuspiciousDomainRequest.Reputation
Impact:S3/AnomalousBehavior.Delete	TTPs/Impact:S3-AnomalousBehavior.Delete
Impact:S3/AnomalousBehavior.Permission	TTPs/Impact:S3-AnomalousBehavior.Permission
Impact:S3/AnomalousBehavior.Write	TTPs/Impact:S3-AnomalousBehavior.Write
Impact:S3/ObjectDelete.Unusual	TTPs/Impact:S3-ObjectDelete.Unusual
Impact:S3/PermissionsModification.Unusual	TTPs/Impact:S3-PermissionsModification.Unusual
Impact:S3/MaliciousIPCaller	TTPs/Impact:S3-MaliciousIPCaller
InitialAccess:IAMUser/AnomalousBehavior	TTPs/Initial Access/IAMUser-AnomalousBehavior
Object:S3/MaliciousFile	TTPs/Object/Object:S3-MaliciousFile
PenTest:IAMUser/KaliLinux	TTPs/PenTest:IAMUser/KaliLinux
PenTest:IAMUser/ParrotLinux	TTPs/PenTest:IAMUser/ParrotLinux
PenTest:IAMUser/PentooLinux	TTPs/PenTest:IAMUser/PentooLinux

GuardDuty menemukan jenis	Tipe temuan ASFF
PenTest:S3/KaliLinux	TTPs/PenTest:S3-KaliLinux
PenTest:S3/ParrotLinux	TTPs/PenTest:S3-ParrotLinux
PenTest:S3/PentooLinux	TTPs/PenTest:S3-PentooLinux
Kegigihan:/IAMUserAnomalousBehavior	TTPs/Persistence/IAMUser-AnomalousBehavior
Persistence:IAMUser/NetworkPermissions	TTPs/Persistence/Persistence:IAMUser-NetworkPermissions
Persistence:IAMUser/ResourcePermissions	TTPs/Persistence/Persistence:IAMUser-ResourcePermissions
Persistence:IAMUser/UserPermissions	TTPs/Persistence/Persistence:IAMUser-UserPermissions
Persistence:Runtime/SuspiciousCommand	TTPs/Persistence/Persistence:Runtime-SuspiciousCommand
Policy:IAMUser/RootCredentialUsage	TTPs/Policy:IAMUser-RootCredentialUsage
Policy:IAMUser/ShortTermRootCredentialUsage	TTPs/Policy:IAMUser-ShortTermRootCredentialUsage
Policy:Kubernetes/AdminAccessToDefaultServiceAccount	Software and Configuration Checks/AWS Security Best Practices/Policy:Kubernetes-AdminAccessToDefaultServiceAccount
Policy:Kubernetes/AnonymousAccessGranted	Software and Configuration Checks/AWS Security Best Practices/Policy:Kubernetes-AnonymousAccessGranted
Policy:Kubernetes/ExposedDashboard	Software and Configuration Checks/AWS Security Best Practices/Policy:Kubernetes-ExposedDashboard

GuardDuty menemukan jenis	Tipe temuan ASFF
Policy:Kubernetes/KubeflowDashboardExposed	Software and Configuration Checks/AWS Security Best Practices/Policy:Kubernetes-KubeflowDashboardExposed
Policy:S3/AccountBlockPublicAccessDisabled	TTPs/Policy:S3-AccountBlockPublicAccessDisabled
Policy:S3/BucketAnonymousAccessGranted	TTPs/Policy:S3-BucketAnonymousAccessGranted
Policy:S3/BucketBlockPublicAccessDisabled	Effects/Data Exposure/Policy:S3-BucketBlockPublicAccessDisabled
Policy:S3/BucketPublicAccessGranted	TTPs/Policy:S3-BucketPublicAccessGranted
PrivilegeEscalation:IAMUser/AnomalousBehavior	TTPs/Privilege Escalation/IAMUser-AnomalousBehavior
PrivilegeEscalation:IAMUser/AdministrativePermissions	TTPs/Privilege Escalation/PrivilegeEscalation:IAMUser-AdministrativePermissions
PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated	TTPs/AnomalousBehavior/PrivilegeEscalation:Kubernetes-RoleBindingCreated
PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated	TTPs/AnomalousBehavior/PrivilegeEscalation:Kubernetes-RoleCreated
PrivilegeEscalation:Kubernetes/PrivilegedContainer	TTPs/PrivilegeEscalation/PrivilegeEscalation:Kubernetes-PrivilegedContainer
PrivilegeEscalation:Runtime/ContainerMountsHostDirectory	TTPs/Privilege Escalation/PrivilegeEscalation:Runtime-ContainerMountsHostDirectory
PrivilegeEscalation:Runtime/CGroupsReleaseAgentModified	TTPs/Privilege Escalation/PrivilegeEscalation:Runtime-CGroupsReleaseAgentModified
PrivilegeEscalation:Runtime/DockerSocketAccessed	TTPs/Privilege Escalation/PrivilegeEscalation:Runtime-DockerSocketAccessed

GuardDuty menemukan jenis	Tipe temuan ASFF
PrivilegeEscalation:Runtime/ElevationToRoot	TTPs/Privilege Escalation/PrivilegeEscalation:Runtime-ElevationToRoot
PrivilegeEscalation:Runtime/RuncContainerEscape	TTPs/Privilege Escalation/PrivilegeEscalation:Runtime-RuncContainerEscape
PrivilegeEscalation:Runtime/SuspiciousCommand	Software and Configuration Checks/PrivilegeEscalation:Runtime-SuspiciousCommand
PrivilegeEscalation:Runtime/UserfaultfdUsage	TTPs/Privilege Escalation/PrivilegeEscalation:Runtime-UserfaultfdUsage
Recon:EC2/PortProbeEMRUnprotectedPort	TTPs/Discovery/Recon:EC2-PortProbeEMRUnprotectedPort
Recon:EC2/PortProbeUnprotectedPort	TTPs/Discovery/Recon:EC2-PortProbeUnprotectedPort
Recon:EC2/Portscan	TTPs/Discovery/Recon:EC2-Portscan
Recon:IAMUser/MaliciousIPCaller	TTPs/Discovery/Recon:IAMUser-MaliciousIPCaller
Recon:IAMUser/MaliciousIPCaller.Custom	TTPs/Discovery/Recon:IAMUser-MaliciousIPCaller.Custom
Recon:IAMUser/NetworkPermissions	TTPs/Discovery/Recon:IAMUser-NetworkPermissions
Recon:IAMUser/ResourcePermissions	TTPs/Discovery/Recon:IAMUser-ResourcePermissions
Recon:IAMUser/TorIPCaller	TTPs/Discovery/Recon:IAMUser-TorIPCaller
Recon:IAMUser/UserPermissions	TTPs/Discovery/Recon:IAMUser-UserPermissions

GuardDuty menemukan jenis	Tipe temuan ASFF
ResourceConsumption:IAMUser/ComputeResources	Unusual Behaviors/User/ResourceConsumption:IAMUser-ComputeResources
Stealth:IAMUser/CloudTrailLoggingDisabled	TTPs/Defense Evasion/Stealth:IAMUser-CloudTrailLoggingDisabled
Stealth:IAMUser/LoggingConfigurationModified	TTPs/Defense Evasion/Stealth:IAMUser-LoggingConfigurationModified
Stealth:IAMUser/PasswordPolicyChange	TTPs/Defense Evasion/Stealth:IAMUser-PasswordPolicyChange
Stealth:S3/ServerAccessLoggingDisabled	TTPs/Defense Evasion/Stealth:S3-ServerAccessLoggingDisabled
Trojan:EC2/BlackholeTraffic	TTPs/Command and Control/Trojan:EC2-BlackholeTraffic
Trojan:EC2/BlackholeTraffic!DNS	TTPs/Command and Control/Trojan:EC2-BlackholeTraffic!DNS
Trojan:EC2/DGADomainRequest.B	TTPs/Command and Control/Trojan:EC2-DGADomainRequest.B
Trojan:EC2/DGADomainRequest.C!DNS	TTPs/Command and Control/Trojan:EC2-DGADomainRequest.C!DNS
Trojan:EC2/DNSDataExfiltration	TTPs/Command and Control/Trojan:EC2-DNSDataExfiltration
Trojan:EC2/DriveBySourceTraffic!DNS	TTPs/Initial Access/Trojan:EC2-DriveBySourceTraffic!DNS
Trojan:EC2/DropPoint	Effects/Data Exfiltration/Trojan:EC2-DropPoint
Trojan:EC2/DropPoint!DNS	Effects/Data Exfiltration/Trojan:EC2-DropPoint!DNS

GuardDuty menemukan jenis	Tipe temuan ASFF
Trojan:EC2/PhishingDomainRequest!DNS	TTPs/Command and Control/Trojan:EC2-PhishingDomainRequest!DNS
Trojan:Lambda/BlackholeTraffic	TTPs/Command and Control/Trojan:Lambda-BlackholeTraffic
Trojan:Lambda/DropPoint	Effects/Data Exfiltration/Trojan:Lambda-DropPoint
Trojan:Runtime/BlackholeTraffic	TTPs/Command and Control/Trojan:Runtime-BlackholeTraffic
Trojan:Runtime/BlackholeTraffic!DNS	TTPs/Command and Control/Trojan:Runtime-BlackholeTraffic!DNS
Trojan:Runtime/DGADomainRequest.C!DNS	TTPs/Command and Control/Trojan:Runtime-DGADomainRequest.C!DNS
Trojan:Runtime/DriveBySourceTraffic!DNS	TTPs/Initial Access/Trojan:Runtime-DriveBySourceTraffic!DNS
Trojan:Runtime/DropPoint	Effects/Data Exfiltration/Trojan:Runtime-DropPoint
Trojan:Runtime/DropPoint!DNS	Effects/Data Exfiltration/Trojan:Runtime-DropPoint!DNS
Trojan:Runtime/PhishingDomainRequest!DNS	TTPs/Command and Control/Trojan:Runtime-PhishingDomainRequest!DNS
UnauthorizedAccess:EC2/MaliciousIPCaller.Custom	TTPs/Command and Control/UnauthorizedAccess:EC2-MaliciousIPCaller.Custom
UnauthorizedAccess:EC2/MetadataDNSRebind	TTPs/UnauthorizedAccess:EC2-MetadataDNSRebind
UnauthorizedAccess:EC2/RDPBruteForce	TTPs/Initial Access/UnauthorizedAccess:EC2-RDPBruteForce

GuardDuty menemukan jenis	Tipe temuan ASFF
UnauthorizedAccess:EC2/SSHBruteForce	TTPs/Initial Access/UnauthorizedAccess:EC2-SSHBruteForce
UnauthorizedAccess:EC2/TorClient	Effects/Resource Consumption/UnauthorizedAccess:EC2-TorClient
UnauthorizedAccess:EC2/TorRelay	Effects/Resource Consumption/UnauthorizedAccess:EC2-TorRelay
UnauthorizedAccess:IAMUser/ConsoleLogin	Unusual Behaviors/User/Unauthorized Access:IAMUser-ConsoleLogin
UnauthorizedAccess:IAMUser/ConsoleLoginSuccess.B	TTPs/UnauthorizedAccess:IAMUser-ConsoleLoginSuccess.B
UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS	Effects/Data Exfiltration/UnauthorizedAccess:IAMUser-InstanceCredentialExfiltration.InsideAWS
UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS	Effects/Data Exfiltration/UnauthorizedAccess:IAMUser-InstanceCredentialExfiltration.OutsideAWS
UnauthorizedAccess:IAMUser/MaliciousIPCaller	TTPs/UnauthorizedAccess:IAMUser-MaliciousIPCaller
UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom	TTPs/UnauthorizedAccess:IAMUser-MaliciousIPCaller.Custom
UnauthorizedAccess:IAMUser/TorIPCaller	TTPs/Command and Control/UnauthorizedAccess:IAMUser-TorIPCaller
UnauthorizedAccess:Lambda/MaliciousIPCaller.Custom	TTPs/Command and Control/UnauthorizedAccess:Lambda-MaliciousIPCaller.Custom
UnauthorizedAccess:Lambda/TorClient	Effects/Resource Consumption/UnauthorizedAccess:Lambda-TorClient

GuardDuty menemukan jenis	Tipe temuan ASFF
UnauthorizedAccess:Lambda/TorRelay	Effects/Resource Consumption/UnauthorizedAccess:Lambda-TorRelay
UnauthorizedAccess:Runtime/MetadataDNSRebind	TTPs/UnauthorizedAccess:Runtime-MetadataDNSRebind
UnauthorizedAccess:Runtime/TorRelay	Effects/Resource Consumption/UnauthorizedAccess:Runtime-TorRelay
UnauthorizedAccess:Runtime/TorClient	Effects/Resource Consumption/UnauthorizedAccess:Runtime-TorClient
UnauthorizedAccess:S3/MaliciousIPCaller.Custom	TTPs/UnauthorizedAccess:S3-MaliciousIPCaller.Custom
UnauthorizedAccess:S3/TorIPCaller	TTPs/UnauthorizedAccess:S3-TorIPCaller

Temuan standar dari GuardDuty

GuardDuty mengirimkan temuan ke Security Hub menggunakan [AWS Security Finding Format \(ASFF\)](#).

Berikut adalah contoh temuan khas dari GuardDuty.

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:guardduty:us-east-1:193043430472:detector/
d4b040365221be2b54a6264dc9a4bc64/finding/46ba0ac2845071e23ccdeb2ae03bfdea",
  "ProductArn": "arn:aws:securityhub:us-east-1:product/aws/guardduty",
  "GeneratorId": "arn:aws:guardduty:us-east-1:193043430472:detector/
d4b040365221be2b54a6264dc9a4bc64",
  "AwsAccountId": "193043430472",
  "Types": [
    "TTPs/Initial Access/UnauthorizedAccess:EC2-SSHBruteForce"
  ],
  "FirstObservedAt": "2020-08-22T09:15:57Z",
  "LastObservedAt": "2020-09-30T11:56:49Z",
  "CreatedAt": "2020-08-22T09:34:34.146Z",
```

```

"UpdatedAt": "2020-09-30T12:14:00.206Z",
"Severity": {
  "Product": 2,
  "Label": "MEDIUM",
  "Normalized": 40
},
"Title": "199.241.229.197 is performing SSH brute force attacks against
i-0c10c2c7863d1a356.",
"Description": "199.241.229.197 is performing SSH brute force attacks against
i-0c10c2c7863d1a356. Brute force attacks are used to gain unauthorized access to your
instance by guessing the SSH password.",
"SourceUrl": "https://us-east-1.console.aws.amazon.com/guardduty/home?region=us-
east-1#/findings?macros=current&fId=46ba0ac2845071e23ccdeb2ae03bfdea",
"ProductFields": {
  "aws/guardduty/service/action/networkConnectionAction/remotePortDetails/portName":
"Unknown",
  "aws/guardduty/service/archived": "false",
  "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/organization/
asnOrg": "CENTURYLINK-US-LEGACY-QWEST",
  "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/geoLocation/
lat": "42.5122",
  "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/ipAddressV4":
"199.241.229.197",
  "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/geoLocation/
lon": "-90.7384",
  "aws/guardduty/service/action/networkConnectionAction/blocked": "false",
  "aws/guardduty/service/action/networkConnectionAction/remotePortDetails/port":
"46717",
  "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/country/
countryName": "United States",
  "aws/guardduty/service/serviceName": "guardduty",
  "aws/guardduty/service/evidence": "",
  "aws/guardduty/service/action/networkConnectionAction/localIpDetails/ipAddressV4":
"172.31.43.6",
  "aws/guardduty/service/detectorId": "d4b040365221be2b54a6264dc9a4bc64",
  "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/organization/
org": "CenturyLink",
  "aws/guardduty/service/action/networkConnectionAction/connectionDirection":
"INBOUND",
  "aws/guardduty/service/eventFirstSeen": "2020-08-22T09:15:57Z",
  "aws/guardduty/service/eventLastSeen": "2020-09-30T11:56:49Z",
  "aws/guardduty/service/action/networkConnectionAction/localPortDetails/portName":
"SSH",
  "aws/guardduty/service/action/actionType": "NETWORK_CONNECTION",

```

```

    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/city/
cityName": "Dubuque",
    "aws/guardduty/service/additionalInfo": "",
    "aws/guardduty/service/resourceRole": "TARGET",
    "aws/guardduty/service/action/networkConnectionAction/localPortDetails/port": "22",
    "aws/guardduty/service/action/networkConnectionAction/protocol": "TCP",
    "aws/guardduty/service/count": "74",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/organization/
asn": "209",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/organization/
isp": "CenturyLink",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/guardduty/
arn:aws:guardduty:us-east-1:193043430472:detector/d4b040365221be2b54a6264dc9a4bc64/
finding/46ba0ac2845071e23ccdeb2ae03bfdea",
    "aws/securityhub/ProductName": "GuardDuty",
    "aws/securityhub/CompanyName": "Amazon"
  },
  "Resources": [
    {
      "Type": "AwsEc2Instance",
      "Id": "arn:aws:ec2:us-east-1:193043430472:instance/i-0c10c2c7863d1a356",
      "Partition": "aws",
      "Region": "us-east-1",
      "Tags": {
        "Name": "kubect1"
      },
      "Details": {
        "AwsEc2Instance": {
          "Type": "t2.micro",
          "ImageId": "ami-02354e95b39ca8dec",
          "IPv4Addresses": [
            "18.234.130.16",
            "172.31.43.6"
          ],
          "VpcId": "vpc-a0c2d7c7",
          "SubnetId": "subnet-4975b475",
          "LaunchedAt": "2020-08-03T23:21:57Z"
        }
      }
    }
  ],
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  }
}

```



```
},  
  "RecordState": "ACTIVE"  
}
```

Mengaktifkan dan mengonfigurasi integrasi

Untuk menggunakan integrasi dengan AWS Security Hub, Anda harus mengaktifkan Security Hub. Untuk informasi tentang cara mengaktifkan Security Hub, lihat [Menyiapkan Security Hub](#) di Panduan Pengguna AWS Security Hub .

Saat Anda mengaktifkan keduanya GuardDuty dan Security Hub, integrasi diaktifkan secara otomatis. GuardDutysegera mulai mengirim temuan ke Security Hub.

Menggunakan GuardDuty kontrol di Security Hub

AWS Security Hub menggunakan kontrol keamanan untuk mengevaluasi AWS sumber daya Anda, dan memeriksa kepatuhan Anda terhadap standar industri keamanan dan praktik terbaik. Anda dapat menggunakan kontrol yang terkait dengan GuardDuty sumber daya dan rencana perlindungan yang dipilih. Untuk informasi selengkapnya, lihat [GuardDutykontrol Amazon](#) di Panduan AWS Security Hub Pengguna.

Untuk daftar semua kontrol di seluruh AWS layanan dan sumber daya, lihat [referensi kontrol Security Hub](#) di Panduan AWS Security Hub Pengguna.

Menghentikan publikasi temuan ke Security Hub

Untuk berhenti mengirim temuan ke Security Hub, Anda dapat menggunakan konsol Security Hub atau API.

Lihat [Menonaktifkan dan mengaktifkan alur temuan dari integrasi \(konsol\)](#) atau [Menonaktifkan alur temuan dari integrasi \(Security Hub API, AWS CLI\)](#) di Panduan Pengguna.AWS Security Hub

Integrasi dengan Amazon Detective

[Amazon Detective](#) membantu Anda menganalisis dan menyelidiki peristiwa keamanan dengan cepat di satu atau beberapa AWS akun dengan menghasilkan visualisasi data yang mewakili cara sumber daya Anda berperilaku dan berinteraksi dari waktu ke waktu. Detective menciptakan visualisasi temuan. GuardDuty

Detective menyerap rincian pencarian untuk semua jenis temuan, dan menyediakan akses ke profil entitas untuk menyelidiki entitas berbeda yang terlibat dengan temuan tersebut. Entitas dapat berupa Akun AWS, AWS sumber daya dalam akun, atau Alamat IP eksternal yang telah berinteraksi dengan sumber daya Anda. GuardDuty Konsol mendukung pivoting ke Amazon Detective dari entitas berikut, tergantung pada jenis pencarian: peran IAM Akun AWS, pengguna, atau sesi peran, agen pengguna, pengguna federasi, instans Amazon EC2, atau alamat IP.

Daftar Isi

- [Mengaktifkan integrasi](#)
- [Berputar ke Detektif Amazon dari sebuah temuan GuardDuty](#)
- [Menggunakan integrasi dengan lingkungan GuardDuty multi-akun](#)

Mengaktifkan integrasi

Untuk menggunakan Amazon Detective dengan GuardDuty Anda harus terlebih dahulu mengaktifkan Amazon Detective. Untuk informasi tentang cara mengaktifkan Detektif, lihat [Memulai Detektif Amazon di Panduan Pengguna Detektif Amazon](#).

Saat Anda mengaktifkan keduanya GuardDuty dan Detektif, integrasi diaktifkan secara otomatis. Setelah diaktifkan, Detektif akan segera menelan data temuan Anda GuardDuty.

Note

GuardDuty mengirimkan temuan ke Detective berdasarkan frekuensi ekspor GuardDuty temuan. Secara default, frekuensi ekspor untuk pembaruan temuan yang ada adalah 6 jam. Untuk memastikan Detektif menerima pembaruan terbaru untuk temuan Anda, disarankan agar Anda mengubah frekuensi ekspor menjadi 15 menit di setiap wilayah tempat Anda menggunakan Detektif. GuardDuty Untuk informasi selengkapnya, lihat [Langkah 5 - Mengatur frekuensi untuk mengekspor temuan aktif yang diperbarui](#).

Berputar ke Detektif Amazon dari sebuah temuan GuardDuty

1. Masuk ke <https://console.aws.amazon.com/guardduty/konsol>.
2. Pilih satu temuan dari tabel temuan Anda.
3. Pilih Selidiki dengan Detektif dari panel rincian temuan.

4. Pilih aspek temuan untuk diselidiki dengan Amazon Detective. Konsol Detective akan terbuka untuk temuan atau entitas tersebut.

Jika pivot tidak berperilaku seperti yang diharapkan, lihat [Memecahkan masalah pivot di Panduan Pengguna Detektif Amazon](#).

 Note

Jika Anda mengarsipkan GuardDuty temuan di konsol Detektif, temuan itu akan diarsipkan di GuardDuty konsol juga.

Menggunakan integrasi dengan lingkungan GuardDuty multi-akun

Jika Anda mengelola lingkungan multi-akun di GuardDuty, Anda harus menambahkan akun anggota Anda ke Amazon Detective untuk melihat visualisasi data Detektif untuk temuan dan entitas di akun tersebut.

Disarankan agar Anda menggunakan akun GuardDuty Administrator yang sama dengan akun administrator untuk Detektif. Untuk informasi selengkapnya tentang menambahkan akun anggota di Detektif, lihat [Mengelola akun](#) di Panduan Pengguna Detektif Amazon.

 Note

Detective adalah layanan regional. Artinya, Anda harus mengaktifkan Detective dan menambahkan akun anggota Anda di setiap wilayah tempat Anda ingin menggunakan integrasi.

Menangguhkan atau menonaktifkan GuardDuty

Anda dapat menggunakan GuardDuty konsol untuk menangguhkan atau menonaktifkan GuardDuty layanan. Anda tidak dikenakan biaya untuk menggunakan GuardDuty ketika layanan ditangguhkan.

- Semua akun anggota harus dipisahkan atau dihapus sebelum Anda dapat menangguhkan atau menonaktifkan GuardDuty.
- Jika Anda menangguhkan GuardDuty, itu tidak lagi memantau keamanan AWS lingkungan Anda atau menghasilkan temuan baru. Temuan Anda yang ada tetap utuh dan tidak terpengaruh oleh GuardDuty penangguhan. Anda dapat memilih untuk mengaktifkan kembali GuardDuty nanti.
- Ketika Anda menonaktifkan GuardDuty di akun, itu akan dinonaktifkan hanya untuk yang saat ini dipilih Wilayah AWS. Jika Anda ingin menonaktifkan sepenuhnya GuardDuty, Anda harus menonaktifkannya di setiap Wilayah tempat diaktifkan.
- Jika Anda menonaktifkan GuardDuty, temuan Anda yang ada dan GuardDuty konfigurasi hilang dan tidak dapat dipulihkan. Jika Anda ingin menyimpan temuan yang ada, Anda harus mengekspornya sebelum mengonfirmasi untuk menonaktifkan GuardDuty. Untuk informasi tentang cara mengekspor temuan, lihat [Mengekspor temuan yang dihasilkan ke Amazon S3](#).
- Jika Anda telah mengaktifkan Perlindungan Malware untuk S3 untuk satu atau beberapa bucket yang dilindungi di akun Anda, maka menangguhkan atau menonaktifkan GuardDuty tidak memengaruhi status bucket yang dilindungi di bawah Perlindungan Malware untuk S3. Bahkan setelah menangguhkan atau menonaktifkan GuardDuty, akun Anda akan terus mengeluarkan biaya penggunaan yang terkait dengan fitur Perlindungan Malware untuk S3. Untuk informasi tentang menonaktifkan Perlindungan Malware untuk S3, lihat [Menonaktifkan Perlindungan Malware untuk S3 untuk bucket yang dilindungi](#).

Untuk menangguhkan atau menonaktifkan GuardDuty

1. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.
2. Pada panel navigasi, silakan pilih Pengaturan.
3. Di GuardDuty bagian Tangguhkan, pilih Tangguhkan GuardDuty atau Nonaktifkan GuardDuty, lalu Konfirmasikan tindakan Anda.

Untuk mengaktifkan kembali GuardDuty setelah menangguhkan

1. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.

2. Pada panel navigasi, silakan pilih Pengaturan.
3. Pilih Aktifkan kembali GuardDuty.

Berlangganan pengumuman Amazon GuardDuty SNS

Bagian ini menyediakan informasi tentang berlangganan Amazon SNS (Simple Notification Service) GuardDuty untuk pengumuman untuk menerima notifikasi tipe temuan yang baru dirilis, pembaruan untuk tipe temuan yang ada, dan perubahan fungsionalitas lainnya. Notifikasi tersedia dalam semua format yang didukung Amazon SNS.

GuardDuty SNS mengirimkan pengumuman tentang pembaruan ke GuardDuty layanan di seluruh AWS akun berlangganan apa pun. Untuk menerima notifikasi tentang temuan dalam akun Anda, lihat [Memproses GuardDuty temuan dengan Amazon EventBridge](#).

Note

Pengguna IAM Anda harus memiliki `sns::subscribe` izin untuk berlangganan SNS.

Anda dapat berlangganan antrean Amazon SQS untuk topik notifikasi ini, tetapi Anda harus menggunakan ARN topik yang berada di Wilayah yang sama. Untuk informasi selengkapnya, lihat [Tutorial: Berlangganan antrean Amazon SQS ke topik Amazon SNS dalam panduan pengembang Amazon Simple Queue Service](#).

Anda juga dapat menggunakan AWS Lambda fungsi untuk memicu peristiwa ketika notifikasi diterima. Untuk informasi selengkapnya, lihat [Memanggil fungsi Lambda menggunakan notifikasi Amazon SNS](#) dalam panduan developer Amazon Simple Queue Service.

Topik Amazon SNS ARNs untuk setiap Wilayah ditunjukkan di bawah ini.

Wilayah AWS	ARN topik Amazon SNS
US East (N. Virginia) - us-east-1	arn:aws:sns:us-east-1:242987662583:GuardDutyAnnouncements
AS Timur (Ohio) - us-east-2	arn:aws:sns:us-east-2:118283430703:GuardDutyAnnouncements

Wilayah AWS	ARN topik Amazon SNS
AS Barat (California U.) - us-west-1	arn:aws:sns:us-west-1:144182107116:GuardDutyAnnouncements
US West (Oregon) - us-west-2	arn:aws:sns:us-west-2:934957504740:GuardDutyAnnouncements
Kanada (Tengah) - ca-central-1	arn:aws:sns:ca-central-1:107430051933:GuardDutyAnnouncements
Kanada Barat (Calgary) - ca-west-1	arn:aws:sns:ca-west-1:440427180217:GuardDutyAnnouncements
Eropa (Stockholm) - eu-north-1	arn:aws:sns:eu-north-1:973841112453:GuardDutyAnnouncements
Eropa (Irlandia) - eu-west-1	arn:aws:sns:eu-west-1:965013871422:GuardDutyAnnouncements
Eropa (London) - eu-west-2	arn:aws:sns:eu-west-2:506403581195:GuardDutyAnnouncements

Wilayah AWS	ARN topik Amazon SNS
Eropa (Paris) - eu-west-3	arn:aws:sns:eu-west-3:436163563069:GuardDutyAnnouncements
Eropa (Frankfurt am Main) - eu-central-1	arn:aws:sns:eu-central-1:378365507264:GuardDutyAnnouncements
Eropa (Zurich) - eu-central-2	arn:aws:sns:eu-central-2:383009515534:GuardDutyAnnouncements
Asia Pasifik (Hong Kong) - ap-east-1	arn:aws:sns:ap-east-1:646602203151:GuardDutyAnnouncements
Asia Pacific (Tokyo) - ap-northeast-1	arn:aws:sns:ap-northeast-1:741172661024:GuardDutyAnnouncements
Asia Pasifik (Seoul) - ap-northeast-2	arn:aws:sns:ap-northeast-2:464168911255:GuardDutyAnnouncements
Asia Pacific (Singapura) — ap-southeast-1	arn:aws:sns:ap-southeast-1:476419727788:GuardDutyAnnouncements

Wilayah AWS	ARN topik Amazon SNS
Asia Pasifik (Sydney) - ap-southeast-2	arn:aws:sns:ap-southeast-2:457615622431:GuardDutyAnnouncements
Asia Pasifik (Mumbai) - ap-south-1	arn:aws:sns:ap-south-1:926826061926:GuardDutyAnnouncements
Amerika Selatan (Sao Paulo) - sa-east-1	arn:aws:sns:sa-east-1:955633302743:GuardDutyAnnouncements
AWS GovCloud (AS-Barat) - us-gov-west-1	arn:aws-us-gov:sns:us-gov-west-1:430639793359:GuardDutyAnnouncements
Tiongkok (Beijing) - cn-north-1	arn:aws-cn:sns:cn-north-1:002991280229:GuardDutyAnnouncements
Tiongkok (Ningxia) - cn-northwest-1	arn:aws-cn:sns:cn-northwest-1:003033775354:GuardDutyAnnouncements
Middle East (Bahrain) — me-south-1	arn:aws:sns:me-south-1:552740612889:GuardDutyAnnouncements

Wilayah AWS	ARN topik Amazon SNS
Middle East (UAE) - me-central-1	arn:aws:sns:me-central-1:030935290150:GuardDutyAnnouncements
Eropa (Milan) - eu-south-1	arn:aws:sns:eu-south-1:188461706213:GuardDutyAnnouncements
Eropa (Spanyol) - eu-south-2	arn:aws:sns:eu-south-2:445632894446:GuardDutyAnnouncements
AWS GovCloud (AS-Timur) - us-gov-east-1	arn:aws:sns:us-gov-east-1:143972945659:GuardDutyAnnouncements
Asia Pasifik (Osaka) - ap-northeast-3	arn:aws:sns:ap-northeast-3:129086577509:GuardDutyAnnouncements
Asia Pasifik (Jakarta) - ap-southeast-3	arn:aws:sns:ap-southeast-3:225965583551:GuardDutyAnnouncements
Asia Pasifik (Hyderabad) - ap-south-2	arn:aws:sns:ap-south-2:595653072700:GuardDutyAnnouncements

Wilayah AWS	ARN topik Amazon SNS
Asia Pasifik (Melbourne) - ap-southeast-4	arn:aws:sns:ap-southeast-4:529900636122:GuardDutyAnnouncements
Asia Pasifik (Malaysia) - ap-southeast-5	arn:aws:sns:ap-southeast-5:343218181797:GuardDutyAnnouncements
Israel (Tel Aviv) - il-central-1	arn:aws:sns:il-central-1:847886274986:GuardDutyAnnouncements
Asia Pasifik (Thailand) - ap-southeast-7	arn:aws:sns:ap-southeast-7:863518448376:GuardDutyAnnouncements
Meksiko (Tengah) - mx-central-1	arn:aws:sns:mx-central-1:060795916546:GuardDutyAnnouncements

Untuk berlangganan email notifikasi GuardDuty pembaruan di AWS Management Console

1. [Buka konsol Amazon SNS di https://console.aws.amazon.com/sns/v3/home](https://console.aws.amazon.com/sns/v3/home).
2. Dalam daftar Wilayah, pilih Wilayah yang sama dengan ARN topik yang akan dijadikan langganan. Contoh ini menggunakan Wilayah us-west-2.
3. Di sebelah kiri panel navigasi, pilih Berlangganan, Buat berlangganan.
4. Pada kotak dialog Buat Langganan, untuk ARN Topik, tempel ARN topik: `arn:aws:sns:us-west-2:934957504740:GuardDutyAnnouncements`.

5. Untuk Protokol, pilih Email. Untuk Titik Akhir, ketik alamat email yang bisa Anda gunakan untuk menerima notifikasi.
6. Pilih Buat langganan.
7. Di aplikasi email Anda, buka pesan dari AWS Notifikasi dan buka tautan untuk mengonfirmasi berlangganan Anda.

Browser web Anda menampilkan respons konfirmasi dari Amazon SNS.

Untuk berlangganan email notifikasi GuardDuty pembaruan dengan AWS CLI

1. Jalankan perintah berikut dengan AWS CLI:

```
aws sns --region us-west-2 subscribe --topic-arn arn:aws:sns:us-west-2:934957504740:GuardDutyAnnouncements --protocol email --notification-endpoint your_email@your_domain.com
```

2. Di aplikasi email Anda, buka pesan dari AWS Notifikasi dan buka tautan untuk mengonfirmasi berlangganan Anda.

Browser web Anda menampilkan respons konfirmasi dari Amazon SNS.

Format pesan Amazon SNS

Contoh pesan pemberitahuan GuardDuty umum:

```
{
  "Type" : "Notification",
  "MessageId" : "9101dc6b-726f-4df0-8646-ec2f94e674bc",
  "TopicArn" : "arn:aws:sns:us-west-2:934957504740:GuardDutyAnnouncements",
  "Message" : "{\"version\":\"1\",\"type\":\"GENERAL\",\"message\":{\"title\":\"Updated AmazonGuardDutyFullAccess policy\",\"body\":\"Added permission that allows you to pass an IAM role to GuardDuty when you enable Malware Protection for S3.\",\"links\":[\"https://docs.aws.amazon.com//guardduty/latest/ug/security-iam-awsmanpol.html#security-iam-awsmanpol-AmaonGuardDutyFullAccess\"]}}",
  "Timestamp" : "2018-03-09T00:25:43.483Z",
  "SignatureVersion" : "1",
  "Signature" : "XWox8GDGLRiCgD0Xlo/fG9Lu/88P8S0FL6M6oQY0mUFzkucuhoblsdea3BjqdChcWR7qdhMPQnLpN7y9iBrWVUqdAGJrukAI8athvAS+4AQD/V/QjrhsEnlj+GaiW+ozAu006X6Gop0zFGnCtPMR0jCMrMonjz7HpV/8KRuMZR3pyQYm5d4wWB7xBPYhUMuLoZ1V8YFs55FMtgQV/
```

```
YLhSYuEu0BP1GMtLQauxDksc0tPP/vjhGQLFx1Q9LTadcQiRHtNIBxWL87PSI
+BVvkin6AL7PhksvdQ7FAGhFxsit+6p8Gy0vKCqaeBG7HZhR1AbpyVka7JSNR0/6ssyrlj1g==",
  "SigningCertURL" : "https://sns.us-west-2.amazonaws.com/
SimpleNotificationService-433026a4050d206028891664da859041.pem",
  "UnsubscribeURL" : "https://sns.us-west-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-
west-2:934957504740:GuardDutyAnnouncements:9225ed2b-7228-4665-8a01-c8a5db6859f4"
}
```

Nilai Pesan yang diuraikan (dengan tanda kutip yang lolos dihapus) ditunjukkan di bawah ini:

```
{
  "version": "1",
  "type": "GENERAL",
  "message": [
    {
      "title": "Updated AmazonGuardDutyFullAccess policy",
      "body": "Added permission that allows you to pass an IAM role to
GuardDuty when you enable Malware Protection for S3.",
      "links": [
        "https://docs.aws.amazon.com//guardduty/latest/ug/security-iam-
awsmanpol.html#security-iam-awsmanpol-AmazonGuardDutyFullAccess"
      ]
    }
  ]
}
```

Contoh pesan notifikasi GuardDuty pembaruan tentang temuan baru ditunjukkan di bawah ini:

```
{
  "Type" : "Notification",
  "MessageId" : "9101dc6b-726f-4df0-8646-ec2f94e674bc",
  "TopicArn" : "arn:aws:sns:us-west-2:934957504740:GuardDutyAnnouncements",
  "Message" : "{\"version\":\"1\", \"type\":\"NEW_FINDINGS\", \"findingDetails
\": [{ \"link\":\"https://docs.aws.amazon.com//guardduty/latest/ug/
guardduty_unauthorized.html\", \"findingType\":\"UnauthorizedAccess:EC2/TorClient\",
\"findingDescription\":\"This finding informs you that an EC2 instance in your AWS
environment is making connections to a Tor Guard or an Authority node. Tor is software
for enabling anonymous communication. Tor Guards and Authority nodes act as initial
gateways into a Tor network. This traffic can indicate that this EC2 instance is
acting as a client on a Tor network. A common use for a Tor client is to circumvent
network monitoring and filter for access to unauthorized or illicit content. Tor
```

```
clients can also generate nefarious Internet traffic, including attacking SSH servers.
This activity can indicate that your EC2 instance is compromised.\\}\\}\\",
  "Timestamp" : "2018-03-09T00:25:43.483Z",
  "SignatureVersion" : "1",
  "Signature" : "XWox8GDGLRiCgD0Xlo/
fG9Lu/88P8S0FL6M6oQY0mUFzkucuhoblsdea3BjqdCHcWR7qdhMPQnLpN7y9iBrWVUqdAGJrukAI8athvAS
+4AQD/V/QjrhsEnlj+GaiW
+ozAu006X6Gop0zFGnCtPMR0jCMrMonjz7Hpv/8KRuMZR3pyQYm5d4wWB7xBPYhUMuLoZ1V8YFs55FMtgQV/
YLhSYuEu0BP1GMtLQauxDksc0tPP/vjhGQLFx1Q9LTadcQiRHtNIBxWL87PSI
+BVvkin6AL7PhksvdQ7FAGhFxsit+6p8Gy0vKCqaeBG7HZhR1AbpyVka7JSNR0/6ssyrlj1g==",
  "SigningCertURL" : "https://sns.us-west-2.amazonaws.com/
SimpleNotificationService-433026a4050d206028891664da859041.pem",
  "UnsubscribeURL" : "https://sns.us-west-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-
west-2:934957504740:GuardDutyAnnouncements:9225ed2b-7228-4665-8a01-c8a5db6859f4"
}
```

Nilai Pesan yang diuraikan (dengan tanda kutip yang lolos dihapus) ditunjukkan di bawah ini:

```
{
  "version": "1",
  "type": "NEW_FINDINGS",
  "findingDetails": [{
    "link": "https://docs.aws.amazon.com//guardduty/latest/ug/
guardduty_unauthorized.html",
    "findingType": "UnauthorizedAccess:EC2/TorClient",
    "findingDescription": "This finding informs you that an EC2 instance in your
AWS environment is making connections to a Tor Guard or an Authority node. Tor is
software for enabling anonymous communication. Tor Guards and Authority nodes act as
initial gateways into a Tor network. This traffic can indicate that this EC2 instance
is acting as a client on a Tor network. A common use for a Tor client is to circumvent
network monitoring and filter for access to unauthorized or illicit content. Tor
clients can also generate nefarious Internet traffic, including attacking SSH servers.
This activity can indicate that your EC2 instance is compromised."
  ]
}
```

Contoh pesan notifikasi GuardDuty pembaruan tentang pembaruan GuardDuty fungsionalitas ditunjukkan di bawah ini:

```
{
  "Type" : "Notification",
  "MessageId" : "9101dc6b-726f-4df0-8646-ec2f94e674bc",
```

```

    "TopicArn" : "arn:aws:sns:us-west-2:934957504740:GuardDutyAnnouncements",
    "Message" : "{\"version\":\"1\",\"type\":\"NEW_FEATURES\",\"featureDetails\
\": [{\"featureDescription\":\"Customers with high-volumes of global CloudTrail
events should see a net positive impact on their GuardDuty costs.\"}, {\"featureLink
\": \"https://docs.aws.amazon.com//guardduty/latest/ug/guardduty_data-
sources.html#guardduty_controlplane\"}]}\",
    "Timestamp" : "2018-03-09T00:25:43.483Z",
    "SignatureVersion" : "1",
    "Signature" : "XWox8GDGLRiCgD0Xlo/
fG9Lu/88P8S0FL6M6oQY0mUFzkucuhoblsdea3BjqdCHcWR7qdhMPQnLpN7y9iBrWVUqdAGJrukAI8athvAS
+4AQD/V/QjrhsEnlj+GaiW
+ozAu006X6Gop0zFGnCtPMR0jCMrMonjz7Hpv/8KRuMZR3pyQYm5d4wWB7xBPYhUMuLoZ1V8YFs55FMtgQV/
YLhSYuEu0BP1GMtLQauxDksc0tPP/vjhGQLFx1Q9LTadcQiRHtNIBxWL87PSI
+BVvkin6AL7PhksvdQ7FAGhfXsit+6p8Gy0vKCqaeBG7HZhR1AbpyVka7JSNR0/6ssyrlj1g==",
    "SigningCertURL" : "https://sns.us-west-2.amazonaws.com/
SimpleNotificationService-433026a4050d206028891664da859041.pem",
    "UnsubscribeURL" : "https://sns.us-west-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-
west-2:934957504740:GuardDutyAnnouncements:9225ed2b-7228-4665-8a01-c8a5db6859f4"
}

```

Nilai Pesan yang diuraikan (dengan tanda kutip yang lolos dihapus) ditunjukkan di bawah ini:

```

{
  "version": "1",
  "type": "NEW_FEATURES",
  "featureDetails": [{
    "featureDescription": "Customers with high-volumes of global CloudTrail events
should see a net positive impact on their GuardDuty costs.",
    "featureLink": "https://docs.aws.amazon.com//guardduty/latest/ug/
guardduty_data-sources.html#guardduty_controlplane"
  }]
}

```

Contoh pesan notifikasi GuardDuty pembaruan tentang temuan terbaru ditunjukkan di bawah ini:

```

{
  "Type": "Notification",
  "MessageId": "9101dc6b-726f-4df0-8646-ec2f94e674bc",
  "TopicArn": "arn:aws:sns:us-west-2:934957504740:GuardDutyAnnouncements",
  "Message": "{\"version\":\"1\",\"type\":\"UPDATED_FINDINGS\",
\"findingDetails\": [{\"link\":\"https://docs.aws.amazon.com//guardduty/latest/ug/

```

```
guardduty_unauthorized.html\", \"findingType\": \"UnauthorizedAccess:EC2/TorClient\",
\"description\": \"Increased severity value from 5 to 8.\\\"}}\",
  \"Timestamp\": \"2018-03-09T00:25:43.483Z\",
  \"SignatureVersion\": \"1\",
  \"Signature\": \"XWox8GDGLRiCgD0Xlo/
fG9Lu/88P8S0FL6M6oQY0mUFzkucuhoblsdea3BjqdCHcWR7qdhMPQnLpN7y9iBrWVUqdAGJrukAI8athvAS
+4AQD/V/QjrhsEnlj+GaiW
+ozAu006X6Gop0zFGnCtPMR0jCMrMonjz7Hpv/8KRuMZR3pyQYm5d4wWB7xBPYhUMuLoZ1V8YFs55FMtgQV/
YLhSYuEu0BP1GMtLQauxDksc0tPP/vjhGQLFx1Q9LTadcQiRHtNIBxWL87PSI
+BVvkin6AL7PhksvdQ7FagHfXsit+6p8Gy0vKCqaeBG7HZhR1AbpyVka7JSNR0/6ssyrlj1g==\",
  \"SigningCertURL\": \"https://sns.us-west-2.amazonaws.com/
SimpleNotificationService-433026a4050d206028891664da859041.pem\",
  \"UnsubscribeURL\": \"https://sns.us-west-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-
west-2:934957504740:GuardDutyAnnouncements:9225ed2b-7228-4665-8a01-c8a5db6859f4\"
}
```

Nilai Pesan yang diuraikan (dengan tanda kutip yang lolos dihapus) ditunjukkan di bawah ini:

```
{
  \"version\": \"1\",
  \"type\": \"UPDATED_FINDINGS\",
  \"findingDetails\": [{
    \"link\": \"https://docs.aws.amazon.com//guardduty/latest/ug/
guardduty_unauthorized.html\",
    \"findingType\": \"UnauthorizedAccess:EC2/TorClient\",
    \"description\": \"Increased severity value from 5 to 8.\"
  }]
}
```


GuardDuty Kuota Amazon

Anda Akun AWS memiliki kuota default, sebelumnya disebut sebagai batas, untuk masing-masing. Layanan AWS Kecuali dinyatakan lain, setiap kuota bersifat khusus per Wilayah. Anda dapat meminta kenaikan untuk beberapa kuota, dan kuota lainnya tidak dapat ditingkatkan.

Untuk melihat kuota GuardDuty, buka konsol [Service Quotas](#). Di panel navigasi, pilih Layanan AWS dan pilih Amazon GuardDuty.

Untuk meminta penambahan kuota, lihat [Meminta penambahan kuota](#) di Panduan Pengguna Service Quotas.

Anda Akun AWS memiliki kuota berikut untuk Amazon GuardDuty per Wilayah.

Note

- Untuk kuota khusus untuk Perlindungan GuardDuty Malware EC2, lihat [Kuota dalam Perlindungan Malware untuk EC2](#).
- Untuk kuota khusus untuk Perlindungan Malware untuk S3, lihat. [Kuota dalam Perlindungan Malware untuk S3](#)

GuardDuty kuota per Wilayah

Sumber Daya	Default	Komentar
Detektor	1	Jumlah maksimum sumber daya detektor yang dapat Anda buat per akun AWS per Wilayah. Anda tidak dapat meminta kenaikan kuota.
Filter	100	Jumlah maksimum filter yang disimpan

Sumber Daya	Default	Komentar
		per AWS akun per Wilayah. Anda tidak dapat meminta kenaikan kuota.
Menemukan periode retensi	90 hari	Jumlah maksimum hari temuan dipertahankan. Anda tidak dapat meminta kenaikan kuota.
Alamat IP dan rentang CIDR per Daftar IP Tepercaya	2.000	Jumlah maksimum alamat IP dan rentang CIDR yang dapat Anda sertakan dalam satu Daftar IP Tepercaya. Anda tidak dapat meminta kenaikan kuota.
Alamat IP dan rentang CIDR per Daftar Ancaman	250.000	Jumlah maksimum alamat IP dan rentang CIDR yang dapat Anda sertakan dalam Daftar Ancaman. Anda tidak dapat meminta kenaikan kuota.

Sumber Daya	Default	Komentar
Ukuran file maksimum	35 MB	Ukuran file maksimum untuk file yang digunakan untuk mengunggah daftar alamat IP atau rentang CIDR yang disertakan dalam Daftar IP Tepercaya atau Daftar Ancaman. Anda tidak dapat meminta kenaikan kuota.
Akun anggota (dengan undangan)	5000	Jumlah maksimum akun anggota yang terkait dengan akun administrator. Anda tidak dapat meminta kenaikan kuota.

Sumber Daya	Default	Komentar
Akun anggota	50.000	Jumlah maksimum akun anggota yang terkait dengan akun administrator melalui AWS Organizations. Ini termasuk akun anggota yang ditambahkan ke organisasi melalui undangan. Nilai default ini tergantung pada kuota Anda saat ini untuk akun anggota di AWS Organizations. Jumlah akun anggota GuardDuty yang ditambahkan tidak AWS Organizations dapat melebihi jumlah akun anggota di organisasi Anda. Untuk informasi tentang jumlah Akun AWS dalam organisasi, lihat Nilai maksimum dan minimum dalam Panduan AWS Organizations Pengguna.

Sumber Daya	Default	Komentar
Ancaman intel set	6	Jumlah maksimum set intel Ancaman yang dapat Anda tambahkan per akun AWS per Wilayah. Anda tidak dapat meminta kenaikan kuota.
Set IP tepercaya	1	Jumlah maksimum set IP tepercaya yang dapat diunggah dan diaktifkan Akun AWS per Wilayah. Anda tidak dapat meminta kenaikan kuota.

Memecahkan Masalah Amazon GuardDuty

Saat Anda menerima masalah yang terkait dengan melakukan tindakan khusus GuardDuty, lihat topik di bagian ini.

Topik

- [Mengekspor temuan ke Amazon S3 - kesalahan akses](#)
- [Perlindungan Malware untuk EC2 masalah](#)
- [Masalah Runtime Monitoring](#)
- [Masalah pemecahan masalah lainnya](#)

Mengekspor temuan ke Amazon S3 - kesalahan akses

Saat Anda mengekspor GuardDuty temuan ke bucket Amazon S3 (tujuan penerbitan), jika GuardDuty tidak dapat mengakses tujuan penerbitan ini, Anda mungkin mendapatkan kesalahan akses.

Setelah Anda mengonfigurasi pengaturan untuk mengekspor temuan, jika GuardDuty tidak dapat mengekspor temuan, akan menampilkan pesan kesalahan pada halaman Pengaturan di GuardDuty konsol. Hal ini berpotensi terjadi ketika tidak GuardDuty dapat lagi mengakses sumber daya target. Misalnya, jika bucket Amazon S3 Anda telah dihapus atau izin untuk mengakses bucket diubah. Ini juga berpotensi terjadi ketika tidak GuardDuty dapat lagi mengakses AWS KMS kunci yang digunakan untuk mengenkripsi data di bucket Amazon S3 Anda. Ketika GuardDuty tidak dapat mengekspor, ia mengirimkan pemberitahuan ke email yang terkait dengan akun untuk memberikan informasi tentang masalah ini.

Bagaimana cara mengatasi kesalahan akses?

Untuk mengatasi masalah ini, pastikan sumber daya yang sesuai ada dan GuardDuty memiliki izin untuk mengakses sumber daya yang diperlukan.

Untuk informasi selengkapnya, lihat [Mengekspor temuan yang dihasilkan ke Amazon S3](#).

Apa yang terjadi jika Anda tidak menyelesaikan kesalahan ini?

Jika Anda tidak menyelesaikan masalah sebelum periode retensi temuan 90 hari selesai GuardDuty, temuan Anda tidak akan diekspor. GuardDuty akan menonaktifkan pencarian pengaturan ekspor untuk akun ini di Wilayah tertentu.

Untuk mulai mengeksplor temuan lagi, perbarui pengaturan konfigurasi di Wilayah tertentu.

Perlindungan Malware untuk EC2 masalah

Bagian ini mencantumkan kesalahan yang mungkin Anda alami saat menyiapkan atau menggunakan Perlindungan Malware untuk EC2.

Tidak ada izin AWS Organizations manajemen yang diperlukan saat mengaktifkan pemindaian GuardDuty malware yang dimulai

Ketika Anda ingin mengelola beberapa akun dengan menggunakan AWS Organizations dan Anda mendapatkan kesalahan ini — `The request failed because you do not have required AWS Organization master permission.` maka Anda kehilangan izin untuk mengaktifkan GuardDuty pemindaian malware yang dimulai untuk beberapa akun di organisasi Anda.

Untuk informasi tentang memberikan izin ke akun manajemen, lihat [Membangun akses tepercaya untuk mengaktifkan GuardDuty pemindaian malware yang dimulai](#).

Saya memulai pemindaian malware On-Demand tetapi menghasilkan kesalahan izin yang diperlukan hilang.

Jika Anda menerima kesalahan yang menunjukkan bahwa Anda tidak memiliki izin yang diperlukan untuk memulai pemindaian malware Sesuai Permintaan di EC2 instans Amazon, verifikasi bahwa Anda telah melampirkan [AWS kebijakan terkelola: AmazonGuardDutyFullAccess_v2 \(disarankan\)](#) kebijakan tersebut ke peran IAM Anda.

Jika Anda anggota AWS organisasi dan masih menerima kesalahan yang sama, sambungkan dengan akun manajemen Anda. Untuk informasi selengkapnya, lihat [AWS Organizations SCP — Akses ditolak](#).

Saya menerima **iam:GetRole** kesalahan saat bekerja dengan Perlindungan Malware untuk EC2.

Jika Anda menerima kesalahan ini —`Unable to get role: AWSServiceRoleForAmazonGuardDutyMalwareProtection`, itu berarti Anda kehilangan izin untuk mengaktifkan pemindaian malware yang GuardDuty dimulai atau menggunakan pemindaian malware sesuai permintaan. Verifikasi bahwa Anda telah melampirkan [AWS kebijakan terkelola: AmazonGuardDutyFullAccess_v2 \(disarankan\)](#) kebijakan ke peran IAM Anda.

Saya adalah akun GuardDuty administrator yang perlu mengaktifkan GuardDuty pemindaian malware yang dimulai tetapi tidak menggunakan kebijakan AWS terkelola: AmazonGuardDutyFullAccess untuk mengelola GuardDuty

- Konfigurasi peran IAM yang Anda gunakan GuardDuty untuk memiliki izin yang diperlukan untuk mengaktifkan pemindaian malware GuardDuty yang dimulai. Untuk informasi selengkapnya tentang izin yang diperlukan, lihat [Membuat peran terkait layanan untuk Perlindungan Malware EC2](#).
- Lampirkan [AWS kebijakan terkelola: AmazonGuardDutyFullAccess_v2 \(disarankan\)](#) ke peran IAM Anda. Ini akan membantu Anda mengaktifkan GuardDuty pemindaian malware yang dimulai untuk akun anggota.

Masalah Runtime Monitoring

Bagian ini mencantumkan kesalahan yang mungkin Anda alami saat menyiapkan atau menggunakan Runtime Monitoring.

Masalah cakupan runtime

Ketika cakupan runtime dari sumber daya yang dilindungi Anda menjadi Tidak Sehat, GuardDuty konsol menyediakan jenis masalah yang tepat. Setelah Anda memiliki jenis masalah, gunakan dokumen berikut untuk melihat langkah pemecahan masalah untuk setiap jenis sumber daya yang didukung:

- [Memecahkan masalah cakupan EC2 runtime Amazon](#)
- [Memecahkan masalah cakupan runtime Amazon ECS-Fargate](#)
- [Memecahkan masalah cakupan runtime Amazon EKS](#)

Memecahkan masalah kesalahan memori di Runtime Monitoring (hanya dukungan Amazon EC2)

Bagian ini menyediakan langkah-langkah pemecahan masalah ketika Anda mengalami kesalahan kehabisan memori berdasarkan [CPU dan batas memori](#) untuk menyebarkan agen GuardDuty keamanan secara manual.

Jika systemd menghentikan GuardDuty agen karena out-of-memory masalah dan Anda mengevaluasi bahwa memberikan lebih banyak memori kepada GuardDuty agen masuk akal, Anda dapat memperbarui batasnya.

1. Dengan izin root, buka `/lib/systemd/system/amazon-guardduty-agent.service`.
2. Temukan `MemoryLimit` dan `MemoryMax`, dan perbarui kedua nilainya.

```
MemoryLimit=256MB
MemoryMax=256MB
```

3. Setelah memperbarui nilai, restart GuardDuty agen dengan menggunakan perintah berikut:

```
sudo systemctl daemon-reload
sudo systemctl restart amazon-guardduty-agent
```

4. Jalankan perintah berikut untuk melihat status:

```
sudo systemctl status amazon-guardduty-agent
```

Output yang diharapkan akan menunjukkan batas memori baru:

```
Main PID: 2540 (amazon-guardduty)
Tasks: 16
Memory: 21.9M (limit: 256.0M)
```

AWS Step Functions Alur kerja saya gagal secara tak terduga

Jika GuardDuty kontainer berkontribusi pada kegagalan alur kerja, lihat [Memecahkan masalah cakupan runtime Amazon ECS-Fargate](#). Jika masalah berlanjut, maka untuk mencegah kegagalan alur kerja karena GuardDuty penampungan, lakukan salah satu langkah berikut:

- Tambahkan `false` tagGuardDutyManaged: ke cluster Amazon ECS terkait.
- Nonaktifkan konfigurasi agen otomatis untuk AWS Fargate (khusus ECS) di tingkat akun.
Tambahkan tag inklusiGuardDutyManaged: `true` ke cluster Amazon ECS terkait yang ingin Anda lanjutkan pemantauan dengan agen GuardDuty otomatis.

Masalah pemecahan masalah lainnya

Jika Anda tidak menemukan skenario yang sesuai dengan masalah Anda, lihat opsi pemecahan masalah berikut:

- Untuk masalah IAM umum saat Anda mengakses <https://console.aws.amazon.com/guardduty/>, lihat [Memecahkan masalah GuardDuty identitas dan akses Amazon](#).
- Untuk masalah autentikasi dan otorisasi saat Anda mengakses AWS AWS Console Home, lihat [Memecahkan Masalah IAM](#).

GuardDuty Wilayah Amazon dan titik akhir

Untuk melihat di Wilayah AWS mana Amazon GuardDuty tersedia, lihat [GuardDuty titik akhir Amazon](#) di. Referensi Umum Amazon Web Services

Kami menyarankan Anda mengaktifkan semua GuardDuty yang didukung Wilayah AWS. Hal ini memungkinkan GuardDuty untuk menghasilkan temuan tentang aktivitas yang tidak sah atau tidak biasa bahkan di Wilayah yang tidak Anda gunakan secara aktif. Ini juga memungkinkan GuardDuty untuk memantau AWS CloudTrail peristiwa yang didukung Wilayah AWS, kemampuannya untuk mendeteksi aktivitas yang melibatkan layanan global berkurang.

Ketersediaan fitur khusus wilayah

Daftar perbedaan regional untuk menentukan ketersediaan GuardDuty fitur.

ListFindings dan GetFindingsStatistics APIs

Itu [GetFindingsStatistics](#) dan [ListFindings](#) APIs memiliki consoleOnly bendera sementara. Bila Anda menggunakan salah satu atau keduanya APIs, consoleOnly tanda berarti bahwa API dapat mengambil hasil hingga batas maksimum 1000.

Perlindungan Malware untuk EC2

GuardDuty mendukung [Perlindungan Malware untuk EC2](#) fitur di [AWS Dedicated Local Zones](#).

Dukungan API umum

Berikut ini APIs dalam Referensi Amazon GuardDuty API mungkin memiliki perbedaan regional karena tidak tersedianya beberapa sumber data atau fitur yang ditentukan Wilayah AWS sebelumnya:

- [CreateDetector](#)
- [UpdateDetector](#)
- [UpdateMemberDetectors](#)
- [UpdateOrganizationConfiguration](#)
- [GetDetector](#)
- [GetMemberDetectors](#)
- [DescribeOrganizationConfiguration](#)

Jenis EC2 pencarian Amazon — [DefenseEvasion:EC2/UnusualDoHActivity](#) dan [DefenseEvasion:EC2/UnusualDoTActivity](#)

Tabel berikut menunjukkan di Wilayah AWS mana GuardDuty tersedia tetapi kedua jenis EC2 temuan Amazon ini belum didukung.

Wilayah AWS	Kode Wilayah
Asia Pasifik (Seoul)	ap-northeast-2
Asia Pacific (Osaka)	ap-northeast-3
Asia Pasifik (Jakarta)	ap-southeast-3

AWS GovCloud (US) Daerah

Untuk informasi terbaru, lihat [Amazon GuardDuty](#) di Panduan AWS GovCloud (US) Pengguna.

Wilayah Tiongkok

Untuk informasi terbaru, lihat [Ketersediaan fitur dan perbedaan implementasi](#).

GuardDuty tindakan dan parameter warisan

Amazon GuardDuty telah menghentikan beberapa tindakan dan parameter API tetapi masih mendukungnya. Praktik terbaik adalah menggunakan tindakan dan parameter API baru yang menggantikan opsi lama. Tabel berikut membandingkan tindakan dan parameter lama dan baru.

Tindakan/ parameter lama	Tindakan/parameter baru	Perbandingan
DisassociateFromMasterAccount	DisassociateFromAdministratorAccount	Dengan implementasi yang sama di kedua tindakan, GuardDuty gunakan istilah Administrator dalam <code>DisassociateFromAdministratorAccount</code> .
autoEnable parameter dalam DescribeOrganizationConfiguration dan UpdateOrganizationConfiguration	autoEnableOrganizationMembers	Dengan <code>autoEnableOrganizationMembers</code> , akun GuardDuty administrator dapat mengaudit dan menegakkan GuardDuty semua akun anggota ke salah satu nilai. Dengan menggunakan APIs, mungkin diperlukan waktu hingga 24 jam untuk memperbarui konfigurasi untuk semua akun anggota. Untuk informasi selengkapnya tentang kemungkinan nilai <code>autoEnableOrganizationMembers</code> bidang, lihat autoEnableOrganizationAnggota .
dataSources parameter dalam yang APIs tercantum dalam GuardDuty Perubahan API	features	Mulai Maret 2023, Anda dapat mengonfigurasi GuardDuty Perlindungan Malware untuk EC2 dan menggunakan features paket GuardDuty perlindungan baru. Rencana perlindungan diluncurkan sebelum Maret 2023, termasuk

Tindakan/ parameter lama	Tindakan/parameter baru	Perbandingan
pada Maret 2023.		Perlindungan Malware untuk penggunaan dataSources konfigurasi yang EC2 masih mendukung. Jika Anda menggunakan APIs untuk mengonfigurasi paket perlindungan, setiap permintaan API dapat menyertakan dataSources atau features, tidak keduanya.

Riwayat dokumen untuk Amazon GuardDuty

Tabel berikut menjelaskan perubahan penting pada dokumentasi sejak rilis terakhir Panduan GuardDuty Pengguna Amazon. Untuk notifikasi tentang pembaruan dokumentasi ini, Anda dapat berlangganan ke umpan RSS.

Perubahan	Deskripsi	Tanggal
Fungsionalitas yang diperbarui - Deteksi Ancaman Diperpanjang	GuardDuty Extended Threat Detection kini memperluas dukungan untuk kluster Amazon EKS dengan menghubungkan beberapa sinyal keamanan di seluruh log audit EKS, perilaku proses runtime, dan aktivitas API. AWS Aktifkan Perlindungan EKS, Runtime Monitoring (dengan add-on EKS), atau keduanya untuk memaksimalkan deteksi ancaman . Untuk mengidentifikasi potensi ancaman, GuardDuty memperkenalkan tipe temuan baru AttackSequence —:EKS/CompromisedCluster Untuk informasi selengkapnya, lihat Deteksi Ancaman Diperpanjang .	Juni 17, 2025
Fungsionalitas yang diperbarui - Perlindungan Malware untuk S3	Perlindungan Malware untuk S3 tidak mendukung pemindaian arsip dengan rasio kompresi yang sangat tinggi. File-file ini akan dilewati selama pemindaia	Juni 13, 2025

n dan ditandai dengan hasil pemindaian. UNSUPPORTED Untuk informasi selengkapnya, lihat [status pemindaian potensial objek S3 dan status hasil](#).

[Fungsionalitas yang diperbarui - Perlindungan Malware untuk EC2](#)

Perlindungan Malware for EC2 telah menambahkan dukungan untuk memindai sebagian besar instance dengan productCode asmarketplace . Ini berlaku untuk pemindaian malware yang GuardDuty dimulai dan pemindaian malware On-Demand. Untuk informasi selengkapnya, lihat [Alasan melewati sumber daya selama pemindaian malware](#).

Juni 13, 2025

[Kebijakan AmazonGuardDutyFullAccess_v2 baru](#)

Menambahkan AmazonGuardDutyFullAccess_v2 kebijakan baru dengan izin untuk meningkatkan keamanan dengan membatasi tindakan administratif pada prinsipal GuardDuty layanan. Untuk informasi tentang kebijakan yang direkomendasikan ini, lihat [kebijakan AWS terkelola: AmazonGuardDutyFullAccess_v2](#).

4 Juni 2025

[Dukungan Wilayah yang Diperluas untuk Perlindungan RDS](#)

GuardDuty Perlindungan RDS sekarang tersedia di Wilayah Meksiko (Tengah), Asia Pasifik (Thailand), dan Asia Pasifik (Malaysia). Perlindungan RDS membantu Anda mendeteksi perilaku login yang berpotensi mencurigakan di Aurora MySQL yang didukung, Aurora PostgreSQL (termasuk Limitless Database), dan RDS untuk PostgreSQL. Dalam hal deteksi ancaman, GuardDuty menghasilkan temuan Perlindungan RDS. Untuk informasi selengkapnya tentang basis data yang didukung dan mengaktifkan rencana perlindungan ini di Wilayah yang baru didukung, lihat Perlindungan [RDS](#).

4 Juni 2025

[Fungsionalitas yang diperbarui - Runtime Monitoring](#)

GuardDuty Runtime Monitoring merilis agen keamanan baru versi 1.7.1 untuk sumber daya Amazon. EC2 Untuk informasi selengkapnya tentang versi agen baru dan daftar sumber daya tambahan untuk memperbarui agen keamanan Anda, lihat [versi rilis agen GuardDuty keamanan](#).

3 Juni 2025

[Support untuk Extended Threat Detection](#)

GuardDuty Extended Threat Detection sekarang tersedia di Asia Pasifik (Thailand) (ap-tenggara - 7). Tanpa aktivasi yang diperlukan, ia mendeteksi serangan multi-tahap yang menjangkau sumber data, berbagai jenis sumber AWS daya, dan waktu, dalam file. Akun AWS Ketika ancaman potensial terdeteksi, itu menghasilkan temuan urutan serangan. Untuk informasi selengkapnya, lihat [Deteksi Ancaman Diperpanjang](#).

12 Mei 2025

[Support untuk Wilayah Meksiko \(Tengah\)](#)

Amazon sekarang GuardDuty tersedia di Wilayah Meksiko (Tengah) mx-centra 1-1 (). Untuk mengaktifkan GuardDuty di Wilayah ini, lihat [Memulai](#). Anda dapat menerima pemberitahuan tentang pembaruan GuardDuty fitur dan deteksi ancaman dengan [Berlangganan pengumuman Amazon GuardDuty SNS](#) di Wilayah ini.

7 Mei 2025

[Fungsionalitas yang diperbarui](#)
[- Runtime Monitoring](#)

GuardDuty Runtime Monitorin
g merilis agen keamanan
baru versi 1.10.0 untuk
sumber daya Amazon EKS.
Untuk informasi selengkap
nya tentang versi agen baru
dan daftar sumber daya
tambahan untuk memperbar
ui agen keamanan Anda, lihat
[versi rilis agen GuardDuty
keamanan.](#)

April 4, 2025

[Fungsionalitas yang diperbarui](#)
[- Runtime Monitoring](#)

GuardDuty Runtime Monitorin
g merilis agen keamanan
baru versi 1.7.0 untuk sumber
daya Amazon ECS-Fargate.
Untuk informasi selengkap
nya tentang versi agen baru
dan daftar sumber daya
tambahan untuk memperbar
ui agen keamanan Anda, lihat
[versi rilis agen GuardDuty
keamanan.](#)

April 4, 2025

[Fungsionalitas yang diperbarui](#)
[- Runtime Monitoring](#)

GuardDuty Runtime Monitorin
g merilis agen keamanan
baru versi 1.7.0 untuk sumber
daya Amazon. EC2 Untuk
informasi selengkapnya
tentang versi agen baru
dan daftar sumber daya
tambahan untuk memperbar
ui agen keamanan Anda, lihat
[versi rilis agen GuardDuty
keamanan.](#)

April 3, 2025

[Support untuk Wilayah Asia Pasifik \(Thailand\)](#)

Amazon sekarang GuardDuty tersedia di Wilayah Asia Pasifik (Thailand). Untuk informasi tentang fitur yang didukung di Wilayah ini, lihat Ketersediaan [fitur khusus wilayah](#). Untuk mengaktifkan GuardDuty di Wilayah ini, lihat [Memulai](#). Anda dapat menerima pemberitahuan tentang pembaruan GuardDuty fitur dan deteksi ancaman dengan [Berlangganan pengumuman Amazon GuardDuty SNS](#).

April 1, 2025

[Fungsionalitas diperbarui](#)

Dasbor Ringkasan sekarang menunjukkan wawasan berdasarkan semua temuan keamanan yang dihasilkan, menghilangkan batasan 5.000 temuan sebelumnya. Untuk informasi tentang wawasan ini, lihat [Dasbor GuardDuty ringkasan](#).

Maret 17, 2025

[Fungsionalitas yang diperbarui](#)
[- Runtime Monitoring](#)

GuardDuty Runtime Monitorin
g merilis agen keamanan
baru versi 1.9.0 untuk sumber
daya Amazon EKS. Untuk
informasi selengkapnya
tentang versi agen baru
dan daftar sumber daya
tambahan untuk memperbar
ui agen keamanan Anda, lihat
[versi rilis agen GuardDuty
keamanan](#).

Maret 2, 2025

[Fungsionalitas yang diperbarui](#)
[- Runtime Monitoring](#)

GuardDuty Runtime Monitorin
g telah menambahkan jenis
masalah cakupan baru (Agen
Tidak Disediakan) untuk
sumber daya Amazon. EC2
Untuk informasi tentang
pemecahan masalah ini,
lihat [Memecahkan masalah
cakupan waktu proses EC2
Amazon](#).

Februari 21, 2025

[Fungsionalitas yang diperbarui](#)
[- Runtime Monitoring](#)

GuardDuty Runtime Monitorin
g merilis agen keamanan baru
untuk sumber daya Amazon
EC2 dan Amazon ECS-Farga
te. Untuk informasi selengkap
nya tentang versi agen baru
dan daftar sumber daya
tambahan untuk memperbar
ui agen keamanan Anda, lihat
[versi rilis agen GuardDuty
keamanan](#).

Februari 6, 2025

[GuardDuty dukungan di Wilayah Asia Pasifik \(Malaysia\) yang ada](#)

GuardDuty Extended Threat Detection sekarang tersedia di Wilayah Asia Pasifik (Malaysia). Untuk informasi selengkapnya, lihat [Deteksi Ancaman Diperpanjang](#).

Januari 28, 2025

[Support untuk Wilayah Asia Pasifik \(Malaysia\)](#)

Amazon sekarang GuardDuty tersedia di Wilayah Asia Pasifik (Malaysia). Untuk informasi tentang fitur yang didukung di Wilayah ini, lihat Ketersediaan [fitur khusus wilayah](#). Untuk mengaktifkan GuardDuty di Wilayah ini, lihat [Memulai](#). Anda dapat menerima pemberitahuan tentang pembaruan GuardDuty fitur dan deteksi ancaman dengan [Berlangganan pengumuman Amazon GuardDuty SNS](#).

Januari 16, 2025

[Fungsionalitas yang diperbarui](#) [- Runtime Monitoring](#)

GuardDuty Runtime Monitoring telah memperbarui informasi tambahan dan langkah-langkah pemecahan masalah untuk masalah cakupan Amazon ECS-Fargate yang terkait dengan Agen yang tidak disediakan. Untuk informasi selengkapnya tentang Agen bukan jenis masalah yang disediakan, lihat Memecahkan [masalah cakupan waktu proses Amazon ECS-Fargate](#).

Januari 8, 2025

[Jenis temuan baru - Policy:IAMUser/ShortTermRootCredentialUsage](#)

GuardDuty memperkenalkan jenis temuan baru yang memberi tahu Anda saat kredensi pengguna terbatas, yang dibuat untuk yang tercantum Akun AWS di lingkungan Anda, digunakan untuk membuat permintaan. Layanan AWS Untuk informasi selengkapnya, lihat [Kebijakan:IAMUser/ShortTermRootCredentialUsage](#).

Januari 8, 2025

[Fitur baru - Deteksi Ancaman GuardDuty Diperpanjang](#)

Desember 1, 2024

GuardDuty mengumumkan Extended Threat Detection untuk mendeteksi urutan serangan multi-tahap yang menjangkau sumber data GuardDuty dasar dan sumber AWS daya di Anda Akun AWS, selama periode waktu tertentu. Tanpa biaya tambahan, kemampuan ini diaktifkan secara otomatis untuk semua akun yang telah diaktifkan GuardDuty. Fitur ini mengumumkan dua jenis GuardDuty temuan baru, yang disebut [Attack sequence finding types](#). Untuk informasi selengkapnya, lihat [Deteksi Ancaman Diperpanjang](#).

[Fungsionalitas lintas layanan yang ditingkatkan - Pemantauan Runtime dan Perlindungan Malware untuk EC2](#)

Dampak fitur Amazon Elastic Kubernetes Service (Amazon EKS) baru pada fitur Amazon: GuardDuty

Desember 1, 2024

- Amazon EKS Auto Mode
 - Baik Runtime Monitoring untuk Amazon EKS dan Perlindungan Malware untuk EC2 mendukung ini.
- Amazon EKS Hybrid Nodes
 - Baik Runtime Monitoring untuk Amazon EKS dan Perlindungan Malware untuk EC2 tidak mendukung ini.

Untuk informasi selengkapnya, lihat [Cara Runtime Monitoring bekerja dengan kluster Amazon EKS](#) dan [Perlindungan Malware](#) untuk EC2

[Fungsionalitas yang diperbarui dalam Runtime Monitoring - Amazon EKS](#)

Runtime Monitoring merilis agen baru versi 1.8.1 (v1.8.1-eks-build.2) untuk sumber daya Amazon EKS. Dengan versi agen baru ini, GuardDuty memperluas dukungan Runtime Monitoring untuk sumber daya Amazon EKS yang berjalan di, RedHat CentOS, dan Fedora. Untuk informasi selengkapnya, lihat [Memvalidasi persyaratan arsitektur](#). Untuk informasi tentang catatan rilis, lihat [agen GuardDuty keamanan untuk sumber daya Amazon EKS](#).

November 23, 2024

[Fungsionalitas yang diperbarui dalam Runtime Monitoring - Amazon EC2](#)

Runtime Monitoring merilis agen baru versi 1.5.0 untuk sumber daya Amazon EC2 . Dengan versi agen baru ini, GuardDuty memperluas dukungan Runtime Monitoring untuk EC2 sumber daya Amazon yang berjalan di, RedHat CentOS, dan Fedora. Untuk informasi selengkapnya, lihat [Memvalidasi persyaratan arsitektur](#). Untuk informasi tentang catatan rilis, lihat [agen GuardDuty keamanan untuk EC2 sumber daya Amazon](#).

November 20, 2024

[Fungsionalitas yang diperbarui dalam Runtime Monitoring - Amazon ECS-Fargate](#)

Runtime Monitoring merilis agen baru versi 1.5.0 untuk sumber daya Amazon ECS-Fargate. Untuk informasi selengkapnya tentang catatan rilis, lihat [agen GuardDuty keamanan untuk AWS Fargate \(khusus Amazon ECS\)](#).

November 14, 2024

[Fungsionalitas yang diperbarui dalam Perlindungan Malware untuk EC2](#)

GuardDuty Perlindungan Malware for EC2 telah menambahkan tiga jenis pencarian Runtime Monitoring ke daftar [Temuan yang memanggil pemindaian malware GuardDuty yang dimulai pada](#) instans Amazon. EC2 Akun yang telah mengaktifkan Perlindungan Malware untuk EC2 akan mengamati GuardDuty pemindaian malware yang dimulai saat GuardDuty menghasilkan salah satu temuan berikut:

November 7, 2024

- [Execution:Runtime/MaliciousFileExecuted](#)
- [Execution:Runtime/SuspiciousShellCreated](#)
- [PrivilegeEscalation:Runtime/ElevationToRoot](#)

Fungsionalitas yang diperbarui dalam Perlindungan RDS

GuardDuty RDS Protection menambahkan versi mesin [Aurora PostgreSQL](#) Limitless Database yang baru dirilis ke daftar database yang didukung. 16.4-limitless

Untuk Akun AWS itu telah mengaktifkan Perlindungan RDS, secara otomatis GuardDuty akan mulai memantau perilaku login untuk Limitless Database. Akun yang telah menggunakan uji coba gratis 30 hari untuk Perlindungan RDS akan dikenakan biaya penggunaan yang terkait dengan Limitless Database, bersama dengan basis data lain yang didukung yang dipantau. Untuk informasi lebih lanjut, lihat [Perlindungan RDS](#).

6 November 2024

[Perluasan wilayah - GuardDuty dan AWS PrivateLink integrasi](#)

GuardDuty sekarang memperluas dukungan Wilayah untuk [Amazon GuardDuty dan antarmuka VPC AWS PrivateLink endpoint](#) (). Sebelumnya, dukungan Wilayah tersedia untuk AS Timur (Virginia N.), Eropa (Irlandia), dan Israel (Tel Aviv). Dukungan ini sekarang diperluas ke semua Wilayah AWS tempat GuardDuty yang tersedia. Untuk informasi selengkapnya tentang perbedaan regional, lihat [Ketersediaan fitur khusus wilayah](#).

6 November 2024

[Fungsionalitas yang diperbarui dalam Runtime Monitoring - Amazon ECS-Fargate](#)

Runtime Monitoring merilis agen baru versi 1.4.1 untuk sumber daya Amazon ECS-Fargate. Untuk informasi selengkapnya tentang catatan rilis, lihat [agen GuardDuty keamanan untuk AWS Fargate \(khusus Amazon ECS\)](#).

Oktober 24, 2024

[Ditambahkan dukungan untuk operasi GuardDuty CloudFormation tag](#)

GuardDuty sekarang mendukung pembaruan kunci tag dan nilai, dan tag tingkat tumpukan. Untuk melakukan ini, tambahkan guardduty :tagResource izin ke peran IAM. Untuk selengkapnya GuardDuty CloudFormation, lihat [referensi jenis GuardDuty sumber daya Amazon](#) di Panduan AWS CloudFormation Pengguna.

Oktober 24, 2024

[Fungsionalitas yang diperbarui dalam Perlindungan GuardDuty Malware untuk S3](#)

Saat mengaktifkan perlindungan malware untuk S3, Anda dapat memilih peran layanan yang memiliki izin yang diperlukan untuk melakukan tindakan pemindaian malware atas nama Anda. Untuk informasi selengkapnya tentang mengaktifkan Perlindungan Malware untuk S3, lihat [Mengonfigurasi Perlindungan Malware untuk S3 untuk bucket S3](#) Anda.

Oktober 22, 2024

Fungsionalitas diperbarui

Oktober 21, 2024

GuardDuty menyempurnakan jenis [UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS](#) temuan untuk mendeteksi penggunaan AWS kredensial EC2 instans Amazon dari titik akhir VPC (AWS PrivateLink) Akun AWS yang tidak terkait dengan peran instans Amazon. EC2 GuardDuty Kemampuan baru ini mendeteksi potensi penyalahgunaan kredensial EC2 instans Amazon dan menyediakan konteks remote Akun AWS menggunakan kredensial sesi eksfiltrasi. Untuk informasi selengkapnya tentang titik akhir AWS layanan yang didukung oleh deteksi baru ini, lihat [Mencatat peristiwa aktivitas jaringan](#) di Panduan AWS CloudTrail Pengguna.

[Fungsionalitas yang diperbarui - GuardDuty Runtime Monitoring](#)

GuardDuty Runtime Monitoring menambahkan tiga jenis temuan berikut yang memberi tahu Anda saat perintah mencurigakan dijalankan pada EC2 instans Amazon atau beban kerja container dalam lingkungan Anda: AWS

Oktober 10, 2024

- [Discovery:Runtime/SuspiciousCommand](#)
- [Persistence:Runtime/SuspiciousCommand](#)
- [PrivilegeEscalation:Runtime/SuspiciousCommand](#)

[Fitur baru - Menambahkan dukungan untuk titik akhir VPC](#)

GuardDuty sekarang terintegrasi dengan AWS PrivateLink dan mendukung titik akhir VPC. Untuk informasi selengkapnya tentang AWS PrivateLink integrasi, lihat [Amazon GuardDuty dan antarmuka VPC endpoint](#) ().AWS PrivateLink

September 17, 2024

[Fungsionalitas yang diperbarui dalam Runtime Monitoring - Amazon EKS](#)

Runtime Monitoring merilis agen baru versi 1.7.1 untuk sumber daya Amazon EKS. Untuk informasi selengkapnya tentang catatan rilis, lihat [agen GuardDuty keamanan untuk Amazon EKS](#).

September 13, 2024

[Fungsionalitas yang diperbarui dalam Perlindungan Malware untuk S3](#)

Perlindungan Malware untuk S3 menambahkan bidang baru, `s3Throttled`, ke skema hasil pemindaian objek S3 Amazon EventBridge (EventBridge). `s3Throttled` Bidang menunjukkan apakah ada penundaan dalam mengunggah atau mengambil penyimpanan dari bucket Amazon Simple Storage Service (Amazon S3) atau tidak. Untuk informasi selengkapnya, lihat [Memantau pemindaian objek S3 dengan Amazon EventBridge](#).

September 13, 2024

[Fungsionalitas yang diperbarui dalam Runtime Monitoring - Amazon EC2](#)

Runtime Monitoring merilis agen baru versi 1.3.1 untuk sumber daya Amazon EC2. Untuk informasi selengkapnya tentang catatan rilis, lihat [agen GuardDuty keamanan untuk Amazon EC2](#).

September 12, 2024

[Fungsionalitas yang diperbarui dalam Runtime Monitoring - Amazon ECS-Fargate](#)

Runtime Monitoring merilis agen baru versi 1.3.1 untuk sumber daya Amazon ECS-Fargate. Untuk informasi selengkapnya tentang catatan rilis, lihat [agen GuardDuty keamanan untuk AWS Fargate \(khusus Amazon ECS\)](#).

September 11, 2024

[GuardDuty Peran terkait layanan \(SLR\) yang diperbarui](#)

GuardDuty telah memperbarui SLR untuk menyertakan `ec2:Describe:Vpcs` izin dalam EC2 tindakan Amazon. Untuk informasi selengkapnya, lihat [Izin peran terkait layanan](#) untuk GuardDuty

Agustus 22, 2024

[Penambahan konten yang signifikan](#)

GuardDuty menambahkan pembaruan konten yang signifikan ke fitur Perlindungan Malware untuk S3.

Agustus 20, 2024

- Menambahkan contoh baru skema pemberitahuan sampel untuk menyiapkan EventBridge aturan Amazon agar menerima pemberitahuan terkait status sumber daya paket Perlindungan Malware dan hasil pemindaian objek S3. Untuk informasi selengkapnya, lihat [Memantau pemindaian objek S3 dengan Amazon EventBridge](#)
- Menambahkan informasi tentang [pemecahan masalah kegagalan tag pasca-pemindaian objek S3](#).

[Fungsionalitas yang diperbarui dalam GuardDuty Runtime Monitoring - Amazon EC2](#)

Runtime Monitoring merilis agen baru versi 1.3.0 untuk sumber daya Amazon EC2 . Untuk informasi selengkapnya tentang catatan rilis, lihat [agen GuardDuty keamanan untuk Amazon EC2](#).

Agustus 19, 2024

[Fungsionalitas yang diperbarui dalam GuardDuty Runtime Monitoring - Amazon EKS](#)

Runtime Monitoring merilis agen baru versi 1.7.0 untuk sumber daya Amazon EKS. Untuk informasi selengkapnya tentang catatan rilis, lihat [agen GuardDuty keamanan untuk klaster Amazon EKS](#).

Agustus 17, 2024

[Penambahan konten yang signifikan](#)

GuardDuty menambahkan informasi baru tentang metodologi deteksi malware dan mesin pemindaian yang digunakannya untuk Perlindungan Malware untuk S3 dan Perlindungan Malware untuk EC2 fitur. Untuk informasi selengkapnya, lihat [mesin pemindaian deteksi GuardDuty malware](#).

Agustus 15, 2024

[Fitur baru - Melindungi beban kerja AI](#)

GuardDuty deteksi ancaman dasar dan Perlindungan Lambda membantu Anda mengamankan dan mendeteksi ancaman terhadap beban kerja AI yang dibangun dengan lebih baik. AWS Untuk informasi selengkapnya, lihat [Melindungi beban kerja AI dengan GuardDuty.](#)

Agustus 14, 2024

[Fungsionalitas yang diperbarui dalam GuardDuty Runtime Monitoring - Fargate \(hanya Amazon ECS\)](#)

Runtime Monitoring merilis agen baru versi 1.3.0 untuk sumber daya (hanya AWS Fargate Amazon ECS). Untuk informasi selengkapnya tentang catatan rilis, lihat [agen GuardDuty keamanan untuk Fargate-ECS.](#)

Agustus 9, 2024

[Fungsionalitas yang diperbarui - Perlindungan Malware untuk S3](#)

GuardDuty Perlindungan Malware untuk S3 meningkatkan jumlah maksimum kuota bucket S3 dari 10 menjadi 25 bucket. Kuota ini berlaku untuk Akun AWS per masing-masing Wilayah AWS. Untuk informasi selengkapnya, lihat [Perlindungan Malware untuk S3.](#)

Agustus 8, 2024

[Diperbarui - Jenis temuan baru di Runtime Monitoring](#)

GuardDuty telah menambahkan dua jenis temuan Pemantauan Runtime baru yang akan membantu Anda mendeteksi ancaman yang melibatkan pembuatan shell yang mencurigakan pada sumber daya yang dipantau, dan eskalasi hak istimewa di mana suatu proses secara mencurigakan meningkatkan hak istimewanya untuk melakukan root.

Agustus 6, 2024

- [Execution:Runtime/SuspiciousShellCreated](#)
- [PrivilegeEscalation:Runtime/ElevationToRoot](#)

[Diperbarui - Integrasi dengan AWS Security Hub](#)

AWS Security Hub menyediakan daftar kontrol GuardDuty keamanan untuk mengevaluasi sumber daya Anda, dan memeriksa kepatuhan Anda terhadap standar industri keamanan dan praktik terbaik. Untuk informasi selengkapnya, lihat [Menggunakan GuardDuty kontrol di Security Hub](#).

Juli 11, 2024

[Skrip GuardDuty tester yang diperbarui untuk temuan](#)

GuardDuty sekarang mendukung lebih dari 100 temuan dengan AWS sumber daya yang berbeda dalam akun khusus. Untuk informasi lebih lanjut, lihat [GuardDuty Temuan uji di akun khusus](#).

Juni 28, 2024

Fungsionalitas yang diperbarui di Runtime Monitoring

Runtime Monitoring merilis agen keamanan baru versi 1.2.0 untuk sumber daya Amazon EC2 . Untuk informasi tentang catatan rilis, lihat [agen GuardDuty keamanan untuk EC2 instans Amazon](#). Untuk informasi tentang memperbarui agen keamanan ke versi rilis ini secara manual, lihat [Mengelola agen keamanan secara manual untuk EC2 instans Amazon](#).

Juni 13, 2024

Fitur baru - Perlindungan Malware untuk ketersediaan Wilayah S3

GuardDuty Perlindungan Malware untuk S3 sekarang tersedia di semua Wilayah komersial di mana GuardDuty tersedia. Fitur ini membantu Anda memindai objek yang baru diunggah ke bucket Amazon S3 untuk mencari potensi malware dan unggahan yang mencurigakan, dan mengambil tindakan untuk mengisolasinya sebelum dimasukkan ke dalam proses hilir. Untuk informasi tentang mengaktifkan Perlindungan Malware untuk S3, lihat [Perlindungan GuardDuty Malware untuk S3](#).

12 Juni 2024

[Fitur baru - Perlindungan Malware untuk S3](#)

Juni 11, 2024

GuardDuty mengumumkan ketersediaan umum Perlindungan Malware untuk S3 yang membantu Anda memindai objek yang baru diunggah ke bucket Amazon S3 untuk mencari potensi malware dan unggahan yang mencurigakan, dan mengambil tindakan untuk mengisolasi sebelum tertelan ke dalam proses hilir. Fitur ini sepenuhnya dikelola oleh AWS. GuardDuty menerbitkan hasil pemindaian objek S3 ke bus acara EventBridge default Anda. Anda dapat mengizinkan GuardDuty untuk menambahkan tag ke objek S3 yang dipindai. Anda dapat membuat alur kerja hilir, seperti isolasi ke bucket karantina, atau menentukan kebijakan bucket menggunakan tag yang mencegah pengguna atau aplikasi mengakses objek tertentu. Untuk informasi selengkapnya, lihat [Perlindungan GuardDuty Malware untuk S3](#). Saat ini, tersedia di Wilayah berikut:

- Timur AS (N. Virginia)
- AS Timur (Ohio)
- AS Barat (Oregon)
- Europe (Ireland)

- Eropa (Frankfurt)
- Eropa (Stockholm)
- Asia Pasifik (Sydney)
- Asia Pacific (Tokyo)
- Asia Pacific (Singapore)
(Asia Pacific (Singapore))

[AmazonGuardDutyFullAccessKebijakan yang diperbarui](#)

Menambahkan izin yang memungkinkan Anda meneruskan peran IAM GuardDuty saat Anda mengaktifkan Perlindungan Malware untuk S3. Untuk informasi selengkapnya tentang pembaruan kebijakan ini, lihat [GuardDuty pembaruan kebijakan AWS terkelola](#).

10 Juni 2024

[Fungsionalitas yang diperbarui dalam GuardDuty Perlindungan RDS](#)

Perlindungan RDS memperluas dukungan untuk memantau aktivitas login pada RDS Anda untuk database PostgreSQL. Sebagai bagian dari ekspansi ini, secara otomatis GuardDuty akan mulai memantau data login dari RDS untuk database PostgreSQL untuk akun yang telah mengaktifkan Perlindungan RDS. GuardDuty Untuk informasi lebih lanjut, lihat [Perlindungan RDS](#).

Juni 6, 2024

Fungsionalitas yang diperbarui dalam GuardDuty Runtime Monitoring - Fargate (hanya Amazon ECS)	Runtime Monitoring merilis agen baru versi 1.2.0 untuk sumber daya (hanya AWS Fargate Amazon ECS). Untuk informasi selengkapnya tentang catatan rilis, lihat agen GuardDuty keamanan untuk Fargate-ECS .	31 Mei 2024
Fungsionalitas yang diperbarui dalam Perlindungan GuardDuty Malware untuk EC2	Untuk setiap volume Amazon EBS yang dilampirkan ke EC2 instans Amazon dan beban kerja kontainer Anda, Perlindungan GuardDuty Malware untuk EC2 telah meningkatkan ukuran volume EBS yang dipindai hingga 2048 GB. Untuk informasi tentang pemindaian volume Amazon EBS yang dilampirkan ke instans Anda, lihat Perlindungan GuardDuty Malware untuk. EC2	29 Mei 2024
Fungsionalitas yang diperbarui di Runtime Monitoring	Runtime Monitoring untuk sumber daya Amazon ECS-Fargate sekarang mendukung pendeteksian potensi ancaman pada tugas yang diluncurkan oleh dan. AWS Batch AWS CodePipeline Untuk informasi selengkapnya, lihat Cara Runtime Monitoring bekerja dengan Fargate (hanya Amazon ECS) .	28 Mei 2024

[Fungsionalitas yang diperbarui di Runtime Monitoring](#)

Runtime Monitoring merilis agen baru versi 1.6.1 untuk sumber daya Amazon EKS. Untuk informasi tentang catatan rilis, lihat [riwayat rilis agen add-on EKS](#).

14 Mei 2024

[Dukungan Wilayah yang Diperluas untuk Runtime Monitoring](#)

GuardDuty memperluas dukungan untuk Runtime Monitoring ke Wilayah Kanada Barat (Calgary). Untuk informasi tentang memulai Runtime Monitoring, lihat [Mengaktifkan Runtime Monitoring](#).

7 Mei 2024

[Dukungan Wilayah yang Diperluas untuk Perlindungan RDS](#)

GuardDuty memperluas dukungan Perlindungan RDS menjadi berikut: Wilayah AWS

3 Mei 2024

- Kanada Barat (Calgary)
- Asia Pasifik (Hyderabad)
- Eropa (Spanyol)
- Eropa (Zürich)
- Timur Tengah (UEA)
- Israel (Tel Aviv)
- Asia Pasifik (Melbourne)

Untuk informasi tentang mengaktifkan fitur ini, lihat Perlindungan [RDS](#).

Fungsionalitas yang diperbarui di Runtime Monitoring	Runtime Monitoring merilis agen baru versi 1.1.0 untuk sumber daya (hanya AWS Fargate Amazon ECS). Untuk informasi selengkapnya tentang catatan rilis, lihat agen GuardDuty keamanan untuk Fargate-ECS .	1 Mei 2024
Fungsionalitas yang diperbarui di Runtime Monitoring	Runtime Monitoring merilis agen baru versi 1.6.0 untuk sumber daya Amazon EKS. Untuk informasi tentang catatan rilis, lihat riwayat rilis agen add-on EKS .	April 29, 2024
Support untuk IPAddressv6	GuardDuty telah menambahkan IPAddressv6 dukungan untuk detail IP lokal dan jarak jauh. Anda dapat menggunakan atribut Filter terkait untuk memfilter GuardDuty temuan atau membuat aturan penekanan .	April 18, 2024
Pengalaman konsol yang diperbarui untuk mengonfigurasi temuan ekspor	GuardDuty telah memperbaiki pengalaman konsol untuk mengeksport temuan yang dihasilkan di Akun AWS ember Amazon S3 Anda. Untuk informasi lebih lanjut, lihat Mengeksport GuardDuty temuan .	April 1, 2024

Fungsionalitas yang diperbarui di Runtime Monitoring

Runtime Monitoring merilis agen keamanan baru versi 1.1.0 untuk sumber daya Amazon EC2 . Versi ini mendukung konfigurasi agen GuardDuty otomatis dalam Runtime Monitoring untuk EC2 instans Amazon. Untuk informasi tentang catatan rilis, lihat [agen GuardDuty keamanan untuk EC2 instans Amazon](#).

Maret 28, 2024

[Ketersediaan umum Runtime Monitoring untuk instans Amazon EC2](#)

Maret 28, 2024

GuardDuty mengumumkan ketersediaan umum (GA) Runtime Monitoring untuk instans Amazon EC2 . Sekarang, Anda memiliki opsi untuk [mengaktifkan konfigurasi agen otomatis](#) yang memungkinkan GuardDuty untuk menginstal dan mengelola agen keamanan untuk EC2 instans Amazon Anda atas nama Anda. Dengan agen GuardDuty otomatis, Anda juga dapat menggunakan tag inklusi atau pengecualian untuk menginformasikan GuardDuty agar menginstal dan mengelola agen keamanan hanya pada EC2 instans Amazon tertentu. Untuk informasi selengkapnya, lihat [Cara kerja Runtime Monitoring dengan EC2 instans Amazon](#).

Daftar jenis temuan baru yang dirilis bersama dengan GA ini

- [Eksekusi:Runtime/SuspiciousTool](#)
- [Eksekusi:Runtime/SuspiciousCommand](#)
- [DefenseEvasion:Runtime/SuspiciousCommand](#)
- [DefenseEvasion:Runtime/PtraceAntiDebugging](#)

- [Eksekusi:Runtime/ Malicious FileExecuted](#)

[Amazon GuardDuty telah memperbarui peran terkait Layanan \(SLR\)](#)

26 Maret 2024

Gunakan AWS Systems Manager tindakan untuk mengelola asosiasi SSM di EC2 instans Amazon saat Anda mengaktifkan Pemantauan GuardDuty Waktu Proses dengan agen otomatis untuk Amazon. EC2 Ketika konfigurasi agen GuardDuty otomatis dinonaktifkan, GuardDuty pertimbangkan hanya EC2 instance yang memiliki tag inklusi (GuardDuty Managed :true).

- Daftar berikut menunjukkan izin baru:

```
"ssm:DescribeAssociation",  
"ssm:DeleteAssociation",  
"ssm:UpdateAssociation",  
"ssm:CreateAssociation",  
"ssm:StartAssociationsOnce",  
"ssm:AddTagsToResource",  
"ssm:CreateAssociation",  
"ssm:UpdateAssociation",  
"ssm:SendCommand",  
"ssm:GetCommandInvocation"
```

[Fungsionalitas yang diperbarui di Runtime Monitoring](#)

Dengan rilis v1.5.0 agen GuardDuty keamanan terbaru (add-on) untuk Amazon EKS, Runtime Monitoring sekarang mendukung konfigurasi parameter spesifik agen GuardDuty keamanan Anda, seperti pengaturan CPU dan memori, pengaturan, dan PriorityClass pengaturan kebijakan DNS. Untuk informasi selengkapnya, lihat [Mengonfigurasi GuardDuty parameter agen keamanan \(EKS add-on\)](#).

7 Maret 2024

[Fungsionalitas yang diperbarui di Runtime Monitoring](#)

Runtime Monitoring merilis agen baru versi 1.5.0 untuk sumber daya Amazon EKS. Untuk informasi tentang catatan rilis, lihat [riwayat rilis agen add-on EKS](#).

7 Maret 2024

[Dukungan untuk Kanada Barat \(Calgary\)](#)

Amazon sekarang GuardDuty tersedia di Wilayah Kanada Barat (Calgary). Beberapa rencana perlindungan di dalamnya GuardDuty mungkin tidak tersedia di Wilayah ini. Untuk informasi terbaru, lihat [Wilayah dan titik akhir](#).

6 Maret 2024

Fungsionalitas yang diperbarui di Runtime Monitoring

Agen GuardDuty keamanan versi 1.0.0 dan 1.1.0 untuk kluster Amazon EKS tidak akan lagi didukung mulai 14 Mei 2024. Untuk informasi tentang langkah-langkah apa yang dapat Anda ambil sebelum akhir dukungan standar, lihat [agen GuardDuty keamanan untuk kluster Amazon EKS](#).

Februari 16, 2024

Fungsionalitas yang diperbarui di Runtime Monitoring

Runtime Monitoring mendukung [Kubernetes versi 1.29 terbaru dengan agen keamanan versi 1.4.1](#) yang ada. Dukungan telah tersedia sejak peluncuran versi Kubernetes ini. Untuk informasi tentang versi Kubernetes yang didukung, lihat Versi [Kubernetes](#) yang didukung oleh agen keamanan. GuardDuty

Februari 16, 2024

[Fungsionalitas yang diperbarui dalam Runtime Monitoring - Ketersediaan regional](#)

GuardDuty Runtime Monitoring sekarang mendukung VPC Amazon bersama dalam hal yang sama. AWS Organizations [GuardDuty peran terkait layanan \(SLR\)](#) memiliki izin baru — `organizations:DescribeOrganization` yang membantu mengambil ID organisasi untuk akun VPC Amazon bersama untuk menetapkan kebijakan titik akhir. [Untuk informasi tentang prasyarat menggunakan endpoint Amazon VPC bersama di Runtime Monitoring](#), lihat [Support for shared Amazon VPC](#). Kemampuan ini tersedia di semua Wilayah yang GuardDuty mendukung Runtime Monitoring.

Februari 12, 2024

[Fungsionalitas yang diperbarui dalam Runtime Monitoring - Ketersediaan regional](#)

GuardDuty Runtime Monitoring sekarang mendukung VPC Amazon bersama dalam hal yang sama. AWS Organizations [GuardDuty peran terkait layanan \(SLR\)](#) memiliki izin baru — `organizations:DescribeOrganization` yang membantu mengambil ID organisasi untuk akun VPC Amazon bersama untuk menetapkan kebijakan titik akhir. [Untuk informasi tentang prasyarat menggunakan endpoint Amazon VPC bersama di Runtime Monitoring, lihat Support for shared Amazon VPC.](#) Saat ini, kemampuan ini tersedia di beberapa Wilayah AWS. Untuk informasi selengkapnya, lihat [Wilayah dan titik akhir.](#)

Februari 9, 2024

[Fungsionalitas yang diperbarui dengan dukungan untuk yang baru Wilayah AWS - Perlindungan Malware untuk EC2](#)

Perlindungan Malware untuk EC2 saat ini mendukung pemindaian volume EBS yang dienkripsi Kunci yang dikelola AWS di Wilayah AS Barat (Oregon).

Februari 6, 2024

Februari 5, 2024

[Fungsionalitas yang diperbarui dengan dukungan untuk yang baru Wilayah AWS - Perlindungan Malware untuk EC2](#)

[Perlindungan Malware untuk EC2 saat ini mendukung pemindaian volume EBS yang dienkripsi dengan berikut Kunci yang dikelola AWS ini: Wilayah AWS](#)

- Asia Pacific (Singapore) (ap-southeast-1)
- Europe (Frankfurt) (eu-central-1)
- Asia Pacific (Osaka) (ap-northeast-3)
- US East (Ohio) (us-east-2)
- Europe (Milan) (eu-south-1)
- Asia Pacific (Tokyo) (ap-northeast-1)
- Asia Pacific (Seoul) (ap-northeast-2)
- Canada (Central) (ca-central-1)
- Europe (Ireland) (eu-west-1)
- US East (N. Virginia) (us-east-1)

Fungsionalitas yang diperbarui di Runtime Monitoring

GuardDuty Runtime Monitoring telah merilis versi agen GuardDuty keamanan baru (v1.0.2) untuk instans Amazon EC2. Versi agen ini mencakup dukungan untuk Amazon ECS AMIs terbaru. Untuk informasi selengkapnya tentang riwayat rilis agen, lihat [agen GuardDuty keamanan untuk EC2 instans Amazon](#).

Februari 2, 2024

[Fungsionalitas yang diperbarui dengan dukungan untuk yang baru Wilayah AWS - Perlindungan Malware untuk EC2](#)

[Perlindungan Malware untuk EC2 saat ini mendukung pemindaian volume Amazon EBS yang dienkripsi dengan berikut Kunci yang dikelola AWS ini: Wilayah AWS](#)

Januari 31, 2024

- Europe (London) (eu-west-2)
- Europe (Stockholm) (eu-north-1)
- Asia Pacific (Hong Kong) (ap-east-1)
- Africa (Cape Town) (af-south-1)
- Middle East (Bahrain) (me-south-1)
- Asia Pasifik (Hyderabad) (ap-south-2)
- Eropa (Spanyol) (eu-south-2)
- Asia Pasifik (Melbourne) (ap-southeast-4)
- Asia Pacific (Sydney) (ap-southeast-2)
- Israel (Tel Aviv) (il-central-1)

[Mengelola akun yang diperbarui dengan AWS Organizations](#)

Menata ulang konten di bawah [Mengelola akun dengan AWS Organizations](#) , menambahkan langkah-langkah untuk mengubah akun GuardDuty administrator yang didelegasikan, dan diperbarui [Memahami hubungan antara akun GuardDuty administrator dan akun anggota](#).

Januari 30, 2024

[Fungsionalitas yang diperbarui dengan dukungan untuk yang baru Wilayah AWS](#)

[Perlindungan Malware untuk EC2 saat ini mendukung pemindaian volume EBS yang dienkripsi dengan berikut Kunci yang dikelola AWS ini: Wilayah AWS](#)

Januari 29, 2024

- Asia Pasifik (Jakarta) (ap-southeast-3)
- US West (N. California) (us-west-1)
- Timur Tengah (UEA) (me-central-1)
- Eropa (Zurich) () eu-central-2
- Asia Pacific (Mumbai) (ap-south-1)
- South America (São Paulo) (sa-east-1)

[Fungsionalitas yang diperbarui dalam Perlindungan Malware untuk EC2](#)

Perlindungan Malware untuk EC2 saat ini mendukung pemindaian volume EBS yang dienkripsi menggunakan Kunci yang dikelola AWS [Perlindungan Malware untuk peran EC2 terkait layanan \(SLR\)](#) memiliki dua izin baru — dan. GetSnapshotBlock ListSnapshots hotBlocks Izin ini akan membantu GuardDuty mengambil snapshot volume EBS (dienkripsi menggunakan Kunci yang dikelola AWS) dari Akun AWS dan menyalinnya ke [akun GuardDuty layanan](#) sebelum memulai pemindaian malware. Saat ini, fungsi ini hanya tersedia di Eropa (Paris) (eu-west-3). Untuk informasi selengkapnya, lihat [Volume yang didukung untuk pemindaian malware.](#)

Januari 25, 2024

[Fungsionalitas yang diperbarui di Runtime Monitoring](#)

GuardDuty Runtime Monitoring telah merilis versi agen GuardDuty keamanan baru (v1.0.1) dengan penyetelan dan peningkatan kinerja umum. Untuk informasi selengkapnya tentang riwayat rilis agen, lihat [agen GuardDuty keamanan untuk EC2 instans Amazon.](#)

23 Januari 2024

[Fungsionalitas yang diperbarui di Runtime Monitoring](#)

Runtime Monitoring merilis agen baru versi 1.4.1 untuk sumber daya Amazon EKS. Untuk informasi selengkapnya, lihat [riwayat rilis agen add-on EKS](#).

Januari 16, 2024

[Runtime Monitoring merilis agen baru v1.4.0 untuk sumber daya Amazon EKS](#)

Runtime Monitoring merilis agen baru versi 1.4.0 untuk sumber daya Amazon EKS. Untuk informasi selengkapnya, lihat [riwayat rilis agen add-on EKS](#).

21 Desember 2023

[Menambahkan jenis temuan berbasis S3 dan pembelajaran AWS CloudTrail mesin \(ML\) ke Eropa \(Zurich\), Eropa \(Spanyol\), Asia Pasifik \(Hyderabad\), Asia Pasifik \(Melbourne\), dan Israel \(Tel Aviv\)](#)

S3 berikut dan CloudTrail temuan yang mengidentifikasi perilaku anomali menggunakan model pembelajaran mesin deteksi anomali (ML) sekarang tersedia di Wilayah Eropa (Zurich), Eropa (Spanyol), Asia Pasifik (Hyderabad), Asia Pasifik (Melbourne), dan Israel (Tel Aviv): GuardDuty

21 Desember 2023

- [Discovery:S3/AnomalousBehavior](#)
- [Impact:S3/AnomalousBehavior.Write](#)
- [Impact:S3/AnomalousBehavior.Delete](#)
- [Impact:S3/AnomalousBehavior.Permission](#)
- [Exfiltration:S3/AnomalousBehavior](#)
- [Exfiltration:IAMUser/AnomalousBehavior](#)
- [Impact:IAMUser/AnomalousBehavior](#)
- [CredentialAccess:IAMUser/AnomalousBehavior](#)
- [DefenseEvasion:IAMUser/AnomalousBehavior](#)
- [InitialAccess:IAMUser/AnomalousBehavior](#)
- [Persistence:IAMUser/AnomalousBehavior](#)

- [PrivilegeEscalation:IAMUser/AnomalousBehavior](#)
- [Discovery:IAMUser/AnomalousBehavior](#)

[GuardDuty mendukung 50.000 akun anggota melalui AWS Organizations](#)

GuardDuty Administrator yang didelegasikan sekarang dapat mengelola maksimal 50.000 akun anggota melalui AWS Organizations. Ini juga termasuk maksimal 5000 akun anggota yang terkait dengan akun GuardDuty administrator melalui undangan.

20 Desember 2023

[GuardDuty Dukungan Runtime Monitoring diperluas menjadi 19 Wilayah AWS](#)

Runtime Monitoring sekarang tersedia di Asia Pasifik (Jakarta), Eropa (Paris), Asia Pasifik (Osaka), Asia Pasifik (Seoul), Timur Tengah (Bahrain), Eropa (Spanyol), Asia Pasifik (Hyderabad), Asia Pasifik (Melbourne), Israel (Tel Aviv), AS Barat (California N.), Eropa (London), Asia Pasifik (Hong Kong), Eropa (Milan), Timur Tengah (UEA), Amerika Selatan (São Paulo), Asia Pasifik (Mumbai), Kanada (Tengah), Afrika (Cape Town), Eropa (Zurich).

6 Desember 2023

[GuardDuty memperluas kemampuan Runtime Monitoring](#)

Selain mendeteksi ancaman terhadap kluster Amazon EKS Anda, GuardDuty mengumumkan ketersediaan umum Runtime Monitoring untuk mendeteksi ancaman terhadap beban kerja Amazon ECS Anda dan rilis pratinjau untuk mendeteksi ancaman terhadap instans Amazon Anda. EC2 Untuk informasi selengkapnya tentang yang Wilayah AWS saat ini mendukung Runtime Monitoring, lihat [Wilayah dan titik akhir](#).

26 November 2023

[Amazon GuardDuty telah memperbarui peran terkait Layanan \(SLR\)](#)

GuardDuty telah menambahkan izin baru untuk menggunakan tindakan Amazon ECS untuk mengelola dan mengambil informasi tentang kluster Amazon ECS, dan mengelola pengaturan akun Amazon ECS. `guardduty:Activate` Tindakan yang berkaitan dengan Amazon ECS juga mengambil informasi tentang tag yang terkait dengannya. GuardDuty

26 November 2023

- Izin berikut telah ditambahkan sebagai bagian dari GuardDuty perluasan kemampuan [Runtime Monitoring](#):

```
"ecs:ListClusters",  
"ecs:DescribeClusters",  
"ecs:PutAccountSettingDefault"
```

[Memperbarui kebijakan AWS terkelola](#)

GuardDuty menambahkan izin baru, `organizations:ListAccounts` ke [AmazonGuardDutyFullAccessPolicy](#) dan [AmazonGuardDutyReadOnlyAccess](#).

16 November 2023

[GuardDuty merilis jenis temuan baru yang menggunakan EKS Audit Log Monitoring.](#)

November 11, 2023

EKS Audit Log Monitoring sekarang mendukung jenis temuan berikut di Asia Pasifik (Melbourne) (ap-southeast-4).

- CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed
- PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated
- Execution:Kubernetes/AnomalousBehavior.ExecInPod
- PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer
- PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount
- Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed
- PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated
- Discovery:Kubernetes/AnomalousBehavior.PermissionChecked

[GuardDuty merilis jenis temuan baru yang menggunakan EKS Audit Log Monitoring.](#)

10 November 2023

EKS Audit Log Monitoring sekarang mendukung jenis temuan berikut di Asia Pasifik (Hyderabad) (ap-south-2), Eropa (Zurich) (eu-central-2), dan Eropa (Spanyol) (eu-south-2) Wilayah.

- CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed
- PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated
- Execution:Kubernetes/AnomalousBehavior.ExecInPod
- PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer
- PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount
- Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed
- PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated
- Discovery:Kubernetes/AnomalousBehavior.PermissionChecked

[GuardDuty merilis jenis temuan baru yang menggunakan EKS Audit Log Monitoring.](#)

8 November 2023

EKS Audit Log Monitoring sekarang mendukung jenis temuan berikut. Jenis temuan ini belum tersedia di Asia Pasifik (Hyderabad) (ap-south-2), Eropa (Zurich) (), Eropa (Spain) (eu-central-1-2) (), dan Asia Pasifik (Melbourne) (ap-southeast-4).

- CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed
- PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated
- Execution:Kubernetes/AnomalousBehavior.ExecInPod
- PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer
- PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount
- Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed
- PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated

- Discovery:Kubernetes/
AnomalousBehavior.PermissionChecked

[EKS Runtime Monitoring merilis agen baru v1.3.1](#)

EKS Runtime Monitoring merilis agen baru versi 1.3.1 yang mencakup tambalan dan pembaruan keamanan penting.

23 Oktober 2023

[Atribut filter baru untuk menemukan](#)

GuardDuty telah menambahkan kriteria baru untuk menyaring temuan yang dihasilkan. Akhirnya domain permintaan DNS menyediakan domain tingkat kedua dan teratas yang terlibat dalam aktivitas yang diminta GuardDuty untuk menghasilkan temuan.

17 Oktober 2023

[EKS Runtime Monitoring merilis agen baru v1.3.0 yang mendukung Kubernetes versi 1.28](#)

EKS Runtime Monitoring merilis agen baru versi 1.3.0 yang mendukung Kubernetes versi 1.28. Menambahkan dukungan untuk Ubuntu. Untuk informasi selengkapnya, lihat [riwayat rilis agen add-on EKS](#).

5 Oktober 2023

[Menambahkan jenis temuan berbasis S3 dan AWS CloudTrail machine learning \(ML\) ke Wilayah Asia Pasifik \(Jakarta\) dan Timur Tengah \(UEA\)](#)

20 September 2023

S3 berikut dan CloudTrail temuan yang mengidentifikasi perilaku anomali menggunakan model pembelajaran mesin deteksi anomali (ML) sekarang tersedia di Wilayah Asia Pasifik (Jakarta) dan Timur Tengah (UEA): GuardDuty

- [Discovery:S3/AnomalousBehavior](#)
- [Impact:S3/AnomalousBehavior.Write](#)
- [Impact:S3/AnomalousBehavior.Delete](#)
- [Impact:S3/AnomalousBehavior.Permission](#)
- [Exfiltration:S3/AnomalousBehavior](#)
- [Exfiltration:IAMUser/AnomalousBehavior](#)
- [Impact:IAMUser/AnomalousBehavior](#)
- [CredentialAccess:IAMUser/AnomalousBehavior](#)
- [DefenseEvasion:IAMUser/AnomalousBehavior](#)
- [InitialAccess:IAMUser/AnomalousBehavior](#)
- [Persistence:IAMUser/AnomalousBehavior](#)
- [PrivilegeEscalation:IAMUser/AnomalousBehavior](#)

- [Discovery:IAMUser/
AnomalousBehavior](#)

[GuardDuty EKS Runtime
Monitoring memperkenalkan
agen GuardDuty keamanan
pengelola di tingkat cluster](#)

EKS Runtime Monitoring menambahkan dukungan untuk mengelola agen GuardDuty keamanan untuk kluster EKS individu untuk memantau peristiwa runtime hanya dari cluster selektif ini. EKS Runtime Monitoring memperluas kemampuan ini dengan dukungan tag.

13 September 2023

[GuardDuty Perlindungan
Malware untuk EC2
memperluas dukungan ke
lebih Wilayah AWS](#)

Perlindungan Malware untuk sekarang EC2 tersedia di Asia Pasifik (Hyderabad), Asia Pasifik (Melbourne), Eropa (Zurich), dan Eropa (Spanyol).

11 September 2023

[GuardDuty sekarang tersedia di Israel \(Tel Aviv\) Region](#)

Menambahkan Wilayah Israel (Tel Aviv) ke daftar Wilayah AWS tempat sekarang GuardDuty tersedia. Rencana perlindungan berikut juga tersedia di Wilayah Israel (Tel Aviv):

24 Agustus 2023

- [Perlindungan EKS](#) mencakup Pemantauan Log Audit EKS dan Pemantauan Runtime EKS.
- [Perlindungan Lambda](#).
- [Perlindungan Malware untuk EC2](#).
- [Perlindungan S3](#).

Untuk informasi lebih lanjut tentang ketersediaan rencana perlindungan di Wilayah Israel (Tel Aviv), lihat [Wilayah dan titik akhir](#).

[GuardDuty menambahkan konfigurasi aktifkan otomatis untuk organisasi Anda di tingkat rencana perlindungan](#)

Perbarui konfigurasi organisasi untuk paket perlindungan di Wilayah Anda. Opsi konfigurasi yang memungkinkan adalah mengaktifkan semua akun, mengaktifkan otomatis untuk akun baru, atau tidak mengaktifkan otomatis untuk akun apa pun di organisasi Anda.

16 Agustus 2023

[Jenis temuan S3 yang mengidentifikasi perilaku anomali menggunakan GuardDuty model pembelajaran mesin deteksi anomali \(ML\) sekarang tersedia di Asia Pasifik \(Osaka\)](#)

Jenis temuan berikut sekarang tersedia di Wilayah Asia Pasifik (Osaka):

10 Agustus 2023

- [Discovery:S3/AnomalousBehavior](#)
- [Impact:S3/AnomalousBehavior.Write](#)
- [Impact:S3/AnomalousBehavior.Delete](#)
- [Impact:S3/AnomalousBehavior.Permission](#)
- [Exfiltration:S3/AnomalousBehavior](#)

[EKS Runtime Monitoring sekarang tersedia di Asia Pasifik \(Melbourne\)](#)

Pemantauan Runtime GuardDuty EKS dalam Perlindungan EKS menyediakan deteksi ancaman runtime untuk kluster Amazon EKS Anda di lingkungan. AWS Sekarang didukung di Wilayah Asia Pasifik (Melbourne).

8 Agustus 2023

[Memperbarui daftar GuardDuty temuan yang memanggil pemindaian malware GuardDuty yang dimulai](#)

Jenis temuan Pemantauan Runtime EKS tertentu sekarang dapat memanggil pemindaian malware GuardDuty yang dimulai di Anda. Akun AWS

Juli 19, 2023

[GuardDuty mendukung 10.000 akun anggota melalui AWS Organizations](#)

Akun GuardDuty administrator sekarang dapat mengelola maksimal 10.000 akun anggota AWS Organizations. Ini juga termasuk maksimal 5000 akun anggota yang terkait dengan akun GuardDuty administrator melalui undangan.

29 Juni 2023

[EKS Runtime Monitoring mengumumkan tiga jenis temuan baru.](#)

EKS Runtime Monitoring mendukung tiga jenis temuan baru yang didasarkan pada teknik injeksi proses. Jenis temuan baru adalah DefenseEvasion:Runtime/ProcessInjection.Proc, DefenseEvasion:Runtime/ProcessInjection.Ptrace, and DefenseEvasion:Runtime/ProcessInjection.VirtualMemoryWrite.

22 Juni 2023

[EKS Runtime Monitoring merilis agen baru v1.2.0 yang mendukung Kubernetes versi 1.27](#)

EKS Runtime Monitoring merilis agen baru versi 1.2.0 yang juga mendukung instance ARM64 berbasis. Ditambahkan dukungan untuk Bottlerocket. Untuk informasi selengkapnya, lihat [riwayat rilis agen add-on EKS](#).

Juni 16, 2023

[GuardDuty konsol memberikan pandangan yang diringkaskan dari temuan Anda.](#)

Dasbor ringkasan di GuardDuty konsol memberikan tampilan agregat GuardDuty temuan. Saat ini, dasbor menampilkan data melalui berbagai widget untuk 10.000 temuan terakhir yang dihasilkan untuk akun Anda (atau akun anggota jika Anda adalah akun GuardDuty administrator) untuk Wilayah saat ini.

12 Juni 2023

[EKS Audit Log Monitoring sekarang tersedia di Asia Pasifik \(Hyderabad\), Asia Pasifik \(Melbourne\), Eropa \(Zurich\), dan Eropa \(Spanyol\)](#)

Aktifkan Pemantauan Log Audit EKS (dalam Perlindungan EKS) untuk akun Anda untuk memantau log audit EKS dari kluster Amazon EKS Anda dan menganalisisnya untuk aktivitas yang berpotensi berbahaya dan mencurigakan.

1 Juni 2023

[Pemantauan Log Audit EKS sekarang tersedia di Timur Tengah \(UEA\)](#)

Pemantauan Log Audit EKS sekarang tersedia di Timur Tengah (UEA). Aktifkan Pemantauan Log Audit EKS untuk akun Anda untuk memantau log audit EKS dari kluster Amazon EKS Anda dan menganalisisnya untuk aktivitas yang berpotensi berbahaya dan mencurigakan.

3 Mei 2023

[GuardDuty Perlindungan Malware untuk EC2 mengumumkan pemindaian malware sesuai permintaan](#)

27 April 2023

Perlindungan Malware untuk EC2 membantu Anda mendeteksi potensi keberadaan malware dalam volume Amazon EBS yang dilampirkan ke EC2 instans Amazon dan beban kerja kontainer Anda. Sekarang menawarkan dua jenis pemindaian — GuardDuty dimulai dan sesuai permintaan. GuardDuty -initiated malware scan memulai pemindaian tanpa agen dalam volume Amazon EBS secara otomatis hanya ketika GuardDuty menghasilkan salah satu [Temuan](#) yang memanggil pemindaian malware yang dimulai. GuardDuty Anda dapat memulai pemindaian malware sesuai permintaan untuk EC2 instans Amazon di akun Anda dengan memberikan Nama Sumber Daya Amazon (ARN) yang terkait dengan instans Amazon tersebut. EC2 Untuk informasi selengkapnya tentang perbedaan kedua jenis pemindaian, lihat [Perlindungan Malware untuk EC2](#).

- [GuardDuty-pemindaian malware yang dimulai](#)
- [Pemindaian malware sesuai permintaan](#)

[GuardDuty mengumumkan Perlindungan Lambda](#)

Perlindungan Lambda membantu Anda mengidentifikasi potensi ancaman keamanan dalam fungsi Anda AWS Lambda .

20 April 2023

- [Jenis temuan Perlindungan Lambda](#)
- [Memperbaiki fungsi Lambda yang berpotensi dikompromikan](#)

[GuardDuty sekarang tersedia di Wilayah Asia Pasifik \(Melbourne\)](#)

Menambahkan Asia Pasifik (Melbourne) ke daftar Wilayah AWS tempat GuardDuty tersedia. Untuk informasi tentang fitur yang tersedia di Wilayah ini, lihat [Wilayah dan titik akhir](#).

19 April 2023

[GuardDuty menambahkan 3 jenis EC2 temuan baru](#)

GuardDuty memperkenalkan jenis temuan baru untuk mendeteksi penggunaan resolver DNS eksternal dan teknologi DNS terenkripsi. Untuk informasi tentang Wilayah AWS di mana jenis temuan ini didukung, lihat [Wilayah dan titik akhir](#).

5 April 2023

- [DefenseEvasion:EC2/UnusualDNSResolver](#)
- [DefenseEvasion:EC2/UnusualDoHActivity](#)
- [DefenseEvasion:EC2/UnusualDoTActivity](#)

[GuardDuty mengumumkan Pemantauan Runtime EKS di Perlindungan EKS](#)

Pemantauan Runtime EKS dalam Perlindungan EKS menyediakan deteksi ancaman runtime untuk kluster Amazon EKS Anda di lingkungan. AWS ini menggunakan agen add-on Amazon EKS (aws-guardduty-agent) yang mengumpulkan [peristiwa Runtime](#) dari beban kerja EKS Anda. Setelah GuardDuty menerima peristiwa runtime ini, ia memantau dan menganalisisnya untuk mengidentifikasi potensi ancaman keamanan yang mencurigakan. Untuk informasi selengkapnya, lihat [Menemukan detail](#) dan [jenis pencarian Pemantauan Waktu Jalan EKS](#).

30 Maret 2023

GuardDuty menambahkan fungsionalitas baru - autoEnableOrganizationMembers

Maret 23, 2023

Amazon GuardDuty menambahkan opsi konfigurasi organisasi baru yang membantu akun GuardDuty administrator mengaudit dan menegakkan (jika diperlukan) yang GuardDuty diaktifkan untuk ALL anggota organisasi mereka. Praktik terbaik sekarang adalah menggunakan autoEnableOrganizationMembers alih-alih autoEnable . autoEnable sudah usang tetapi masih didukung. Berikut ini APIs dipengaruhi oleh fungsionalitas baru ini:

- [DescribeOrganizationConfiguration](#)
- [UpdateOrganizationConfiguration](#)
- [DisassociateMembers](#)
- [DeleteMembers](#)
- [DisassociateFromAdministratorAccount](#)
- [StopMonitoringMembers](#)

[Fitur Perlindungan RDS di Amazon sekarang GuardDuty tersedia secara umum](#)

GuardDuty Perlindungan RDS memantau dan memprofilkan aktivitas login RDS untuk mengidentifikasi perilaku login yang mencurigakan pada instans database Amazon Aurora Anda. Untuk informasi tentang yang Wilayah AWS mendukung Perlindungan RDS, lihat [Wilayah dan titik akhir](#).

16 Maret 2023

[GuardDuty mengumumkan aktivasi fitur](#)

Secara historis, GuardDuty API mengizinkan konfigurasi fitur dan sumber data, tetapi sekarang, semua jenis GuardDuty perlindungan baru akan dikonfigurasi sebagai fitur dan bukan sebagai sumber data. GuardDuty masih mendukung sumber data melalui API tetapi tidak akan menambahkan API baru. Aktivasi fitur mempengaruhi perilaku yang APIs digunakan untuk mengaktifkan GuardDuty atau jenis perlindungan di dalamnya GuardDuty. Jika Anda mengelola GuardDuty akun Anda melalui template API, SDK, atau CFN, lihat [perubahan GuardDuty API pada Maret 2023](#).

16 Maret 2023

[GuardDuty Perlindungan
Malware untuk sekarang EC2
tersedia di Wilayah Timur
Tengah \(UEA\)](#)

Perlindungan Malware untuk EC2 fitur di GuardDuty didukung di Wilayah Timur Tengah (UEA). Untuk informasi selengkapnya, lihat [Wilayah dan titik akhir](#).

13 Maret 2023

[Amazon GuardDuty telah
memperbarui peran terkait
Layanan \(SLR\)](#)

GuardDuty menambahkan izin baru berikut untuk mendukung fitur GuardDuty EKS Runtime Monitoring yang akan datang.

8 Maret 2023

- Gunakan tindakan Amazon EKS untuk mengelola dan mengambil informasi tentang kluster EKS, dan mengelola add-on EKS di kluster EKS. Tindakan EKS juga mengambil informasi tentang tag yang terkait dengan GuardDuty.

```
"eks:ListClusters",  
"eks:DescribeCluster",  
"ec2:DescribeVpcEndpointServices",  
"ec2:DescribeSecurityGroups"
```

[Amazon GuardDuty telah
memperbarui peran terkait
Layanan \(SLR\)](#)

GuardDuty SLR telah diperbarui untuk memungkinkan pembuatan Perlindungan Malware untuk EC2 SLR setelah Perlindungan Malware untuk EC2 diaktifkan.

21 Februari 2023

[GuardDuty membutuhkan TLS v1.2 atau yang lebih baru](#)

Untuk berkomunikasi dengan AWS sumber daya, GuardDuty membutuhkan dan mendukung TLS v1.2 atau yang lebih baru. Untuk informasi selengkapnya, lihat [Perlindungan data](#) dan [Keamanan infrastruktur](#).

14 Februari 2023

[GuardDuty sekarang tersedia di Wilayah Asia Pasifik \(Hyderabad\)](#)

Menambahkan Wilayah Asia Pasifik (Hyderabad) ke daftar Wilayah AWS tempat GuardDuty tersedia. Untuk informasi selengkapnya, lihat [Wilayah dan titik akhir](#).

14 Februari 2023

[Panduan GuardDuty Pengguna Amazon selaras dengan praktik terbaik IAM](#)

Memperbarui panduan untuk menyelaraskan dengan praktik terbaik IAM. Untuk informasi lebih lanjut, lihat [Praktik terbaik keamanan di IAM](#).

Februari 10, 2023

[GuardDuty sekarang tersedia di Wilayah Eropa \(Spanyol\)](#)

Menambahkan Eropa (Spanyol) ke Wilayah AWS daftar GuardDuty di mana tersedia. Untuk informasi selengkapnya, lihat [Wilayah dan titik akhir](#).

Februari 8, 2023

[GuardDuty sekarang tersedia di Wilayah Eropa \(Zurich\)](#)

Menambahkan Eropa (Zurich) ke daftar Wilayah AWS di mana GuardDuty tersedia. Untuk informasi selengkapnya, lihat [Wilayah dan titik akhir](#).

12 Desember 2022

[Pratinjau rilis fitur baru -
Perlindungan GuardDuty RDS](#)

GuardDuty Perlindungan RDS memantau dan memprofilkan aktivitas login RDS untuk mengidentifikasi perilaku login yang mencurigakan pada instans database Amazon Aurora Anda. Saat ini, tersedia untuk rilis pratinjau dalam lima Wilayah AWS. Untuk informasi selengkapnya, lihat [Wilayah dan titik akhir](#).

30 November 2022

[GuardDuty sekarang tersedia
di Wilayah Timur Tengah
\(UEA\)](#)

Menambahkan Timur Tengah (UEA) ke daftar Wilayah AWS di mana GuardDuty tersedia. Untuk informasi selengkapnya, lihat [Wilayah dan titik akhir](#).

6 Oktober 2022

[Menambahkan konten untuk fitur baru - Perlindungan GuardDuty Malware untuk EC2](#)

26 Juli 2022

GuardDuty Perlindungan Malware for EC2 adalah peningkatan opsional untuk Amazon GuardDuty. Sementara GuardDuty mengidentifikasi sumber daya yang berisiko, Perlindungan Malware untuk EC2 mendeteksi malware yang mungkin menjadi sumber kompromi. Dengan Perlindungan Malware untuk EC2 diaktifkan, setiap kali GuardDuty mendeteksi perilaku mencurigakan pada EC2 instans Amazon atau beban kerja kontainer yang menunjukkan GuardDuty malware, Perlindungan Malware untuk EC2 memulai pemindaian tanpa agen pada volume EBS yang dilampirkan pada EC2 instans yang terkena dampak atau beban kerja kontainer untuk mendeteksi keberadaan malware. Untuk informasi tentang cara EC2 kerja Perlindungan Malware dan mengonfigurasi fitur ini, lihat [Perlindungan GuardDuty Malware untuk EC2](#).

- Untuk informasi tentang Perlindungan Malware

untuk EC2 temuan, lihat

[Menemukan detail](#).

- Untuk informasi tentang memulihkan EC2 instans yang dikompromikan dan wadah mandiri, lihat [Memperbaiki masalah keamanan yang ditemukan](#) oleh GuardDuty
- Untuk informasi tentang mengaudit CloudWatch log untuk pemindaian malware dan alasan melewatkan sumber daya selama pemindaian malware, lihat [Memahami CloudWatch Log dan](#) lewati alasannya.
- Untuk informasi tentang deteksi ancaman positif palsu, lihat [Melaporkan positif palsu di Perlindungan GuardDuty Malware](#) untuk EC2

[Pensiunan satu jenis temuan](#)

[Exfiltration:S3/ObjectRead.Unusua](#)l telah pensiun.

Juli 5, 2022

[Menambahkan jenis temuan S3 baru yang mengidentifikasi perilaku anomali menggunakan GuardDuty model pembelajaran mesin deteksi anomali \(ML\).](#)

Menambahkan jenis temuan S3 baru berikut. Jenis temuan ini mengidentifikasi apakah permintaan API memanggil entitas IAM dengan cara yang anomali. Model ML mengevaluasi semua permintaan API di akun Anda dan mengidentifikasi peristiwa anomali yang terkait dengan teknik yang digunakan oleh musuh. Untuk mempelajari lebih lanjut tentang masing-masing temuan baru ini, lihat [tipe temuan S3](#).

- [Discovery:S3/AnomalousBehavior](#)
- [Impact:S3/AnomalousBehavior.Write](#)
- [Impact:S3/AnomalousBehavior.Delete](#)
- [Impact:S3/AnomalousBehavior.Permission](#)
- [Exfiltration:S3/AnomalousBehavior](#)

Juli 5, 2022

[Menambahkan konten Perlindungan GuardDuty EKS untuk GuardDuty](#)

GuardDuty sekarang dapat menghasilkan temuan untuk sumber daya Amazon EKS Anda melalui pemantauan log audit EKS. Untuk mempelajari cara mengonfigurasi fitur ini, lihat [Perlindungan EKS di Amazon GuardDuty](#).

Untuk daftar temuan yang GuardDuty dapat dihasilkan untuk sumber daya Amazon EKS, lihat temuan [Kubernetes](#). Panduan remediasi baru telah ditambahkan untuk mendukung remediasi temuan ini dalam panduan remediasi temuan [Kubernetes](#).

Januari 25, 2022

[Ditambahkan 1 temuan baru](#)

Temuan baru UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS telah ditambahkan. Temuan ini memberi tahu Anda kapan kredensial instans Anda diakses oleh AWS akun di luar lingkungan Anda. AWS

20 Januari 2022

[Memperbarui jenis temuan untuk membantu mengidentifikasi masalah yang terkait dengan log4j](#)

Amazon GuardDuty telah memperbarui jenis temuan berikut untuk membantu mengidentifikasi dan memprioritaskan masalah yang terkait dengan CVE-2021-44228 dan CVE-2021-45046;;.
Backdoor:EC2/C&CAActivity.B
Backdoor:EC2/C&CAActivity.B!
DNS Behavior:EC2/NetworkPortUnusual

Desember 22, 2021

[Menemukan Perubahan](#)

UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration telah diubah menjadi UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS. Versi temuan yang disempurnakan ini mempelajari lokasi khas yang digunakan kredensial Anda untuk mengurangi temuan dari lalu lintas yang diarahkan melalui jaringan premis.
[UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS](#)

7 September 2021

[Perbarui ke GuardDuty SLR](#)

GuardDuty SLR telah diperbarui dengan tindakan baru untuk meningkatkan akurasi pencarian.

Agustus 3, 2021

Menambahkan informasi sumber data untuk setiap jenis temuan.	Menemukan deskripsi sekarang berisi informasi tentang sumber data yang GuardDuty digunakan untuk menghasilkan temuan itu.	10 Mei 2021
Pensiunan 13 jenis pencarian.	13 temuan telah pensiun untuk diganti dengan Anomalous Behaviour temuan baru. Persistence:IAMUser/NetworkPermissions , Persistence:IAMUser/ResourcePermissions , Persistence:IAMUser/UserPermissions , PrivilegeEscalation:IAMUser/AdministrativePermissions , Recon:IAMUser/NetworkPermissions , Recon:IAMUser/ResourcePermissions , Recon:IAMUser/UserPermissions , ResourceConsumption:IAMUser/ComputeResources , Stealth:IAMUser/LoggingConfigurationModified , Discovery:S3/BucketEnumeration.Unusual , Impact:S3/ObjectDelete.Unusual , Impact:S3/PermissionsModification.Unusual , dan UnauthorizedAccess:IAMUser/ConsoleLogin .	12 Maret 2021

Menambahkan 8 jenis temuan baru untuk perilaku anomali.

Menambahkan 8 jenis IAMUser temuan baru berdasarkan perilaku anomali untuk kepala sekolah IAM. [CredentialAccess:IAMUser/AnomalousBehavior](#), [DefenseEv](#)
[asion:IAMUser/AnomalousBehavior](#), [Discovery:IAMUser/AnomalousBehavior](#), [Exfiltration:IAMUser/AnomalousBehavior](#), [Impact:IA](#)
[MUser/AnomalousBeh](#)
[avior](#), [InitialAccess:IAMU](#)
[ser/AnomalousBehavior](#), [Persistence:IAMUser/AnomalousBehavior](#), [Privilege](#)
[Escalation:IAMUser/Anomalou](#)
[sBehavior](#).

12 Maret 2021

Menambahkan EC2 temuan berdasarkan reputasi domain.

Menambahkan 4 tipe temuan Impact yang baru berdasark an reputasi domain. [Impact:EC2/AbusedDomainRequ](#)
[est.Reputation](#) , [Impact:EC2/BitcoinDomainRequest.Repu](#)
[tation](#), [Impact:EC2/Malicio](#)
[usDomainRequest.Re](#)
[putation](#). Juga menambahk an EC2 temuan baru untuk C &CActivity. [Impact:EC2/SuspiciousDomainRequest.R](#)
[eputation](#)

27 Januari 2021

Ditambahkan 4 jenis temuan baru.	Menambahkan 3 IPCaller temuan berbahaya S3 baru. Discovery:S3/MaliciousIPCal ler , Exfiltration:S3/MaliciousIP Caller , Impact:S3/Maliciou sIPCaller . Juga menambahk an EC2 temuan baru untuk C &CActivity. Backdoor:EC2/ C&CActivity.B	21 Desember 2020
Pensiun tipe UnauthorizedAccess:EC2/TorIPCaller temuan.	Jenis UnauthorizedAccess :EC2/TorIPCaller temuan sekarang sudah pensiun dari GuardDuty. Pelajari selengkapnya .	1 Oktober 2020
Menambahkan jenis Impact:EC2/WinRmBruteForce temuan.	Menambahkan temuan Dampak baru,Impact:EC2/ WinRmBruteForce. Pelajari selengkapnya .	17 September 2020
Menambahkan jenis Impact:EC2/PortSweep temuan.	Menambahkan temuan Dampak baru,Impact:EC2/Po rtSweep. Pelajari selengkapnya .	17 September 2020
GuardDuty sekarang tersedia di Wilayah Afrika (Cape Town) dan Eropa (Milan).	Menambahkan Afrika (Cape Town) dan Eropa (Milan) ke daftar AWS Wilayah di mana GuardDuty tersedia. Pelajari selengkapnya	31 Juli 2020

[Menambahkan detail penggunaan baru untuk memantau GuardDuty biaya.](#)

Sekarang Anda dapat menggunakan metrik baru untuk menanyakan data biaya GuardDuty penggunaan untuk akun dan akun yang Anda kelola. Gambaran umum baru tentang biaya penggunaan tersedia di konsol di <https://console.aws.amazon.com/guardduty/>. Informasi selengkapnya dapat diakses melalui API.

31 Juli 2020

[Menambahkan konten yang mencakup perlindungan S3 melalui pemantauan peristiwa data S3 di GuardDuty](#)

GuardDuty Perlindungan S3 sekarang tersedia melalui pemantauan peristiwa pesawat data S3 sebagai sumber data baru. Akun baru akan mengaktifkan fitur ini secara otomatis. Jika Anda sudah menggunakan GuardDuty Anda dapat mengaktifkan sumber data baru untuk diri sendiri atau akun anggota Anda.

31 Juli 2020

[Menambahkan 14 Temuan S3 baru.](#)

14 tipe temuan S3 yang baru telah ditambahkan untuk bidang kendali S3 dan sumber bidang data.

31 Juli 2020

[Menambahkan dukungan tambahan untuk temuan S3 dan mengubah 2 nama tipe temuan yang ada.](#)

GuardDuty temuan sekarang mencakup rincian lebih lanjut untuk temuan yang melibatkan ember S3. Jenis temuan yang ada yang terkait dengan aktivitas S3 telah diganti namanya: Policy:IAMUser/S3BlockPublicAccessDisabled telah diubah menjadi. Policy:S3/BucketBlockPublicAccessDisabled Stealth:IAMUser/S3ServerAccessLoggingDisabled telah diubah menjadi Stealth:S3/ServerAccessLoggingDisabled .

28 Mei 2020

[Menambahkan konten untuk AWS Organizations integrasi.](#)

GuardDuty sekarang terintegrasi dengan administrator AWS Organizations yang didelegasikan untuk memungkinkan Anda mengelola GuardDuty akun dalam organisasi Anda. Ketika Anda menetapkan administrator yang didelegasikan sebagai akun GuardDuty administrator, Anda dapat secara otomatis mengaktifkan GuardDuty anggota organisasi mana pun yang akan dikelola oleh akun administrator yang didelegasikan. Anda juga dapat mengaktifkan secara otomatis GuardDuty di akun AWS Organizations anggota baru. [Pelajari selengkapnya.](#)

20 April 2020

Menambahkan konten untuk fitur temuan ekspor.	Menambahkan konten yang menjelaskan fitur Temuan Ekspor dari GuardDuty.	14 November 2019
Menambahkan jenis UnauthorizedAccess:EC2/MetadataDNSRebind temuan.	Menambahkan temuan Tidak Sah baru, UnauthorizedAccess:EC2/MetadataDNSRebind. Pelajari selengkapnya.	10 Oktober 2019
Menambahkan jenis Stealth:IAMUser/S3ServerAccessLoggingDisabled temuan.	Menambahkan temuan Stealth baru, Stealth:IAMUser/S3ServerAccessLoggingDisabled. Pelajari selengkapnya.	10 Oktober 2019
Menambahkan jenis Policy:IAMUser/S3BlockPublicAccessDisabled temuan.	Menambahkan temuan Kebijakan baru, Policy:IAMUser/S3BlockPublicAccessDisabled. Pelajari selengkapnya.	10 Oktober 2019
Pensiun tipe Backdoor:EC2/XORDDOS temuan.	Jenis Backdoor:EC2/XORDDOS temuan sekarang sudah pensiun dari GuardDuty. Pelajari lebih lanjut	12 Juni 2019
Menambahkan jenis PrivilegeEscalation temuan.	Jenis PrivilegeEscalation temuan mendeteksi ketika pengguna mencoba menetapkan hak istimewa yang meningkat dan lebih permisif ke akun mereka. Pelajari selengkapnya	14 Mei 2019
GuardDuty sekarang tersedia di Wilayah Eropa (Stockholm).	Menambahkan Europe (Stockholm) ke daftar AWS Wilayah di mana GuardDuty tersedia. Pelajari selengkapnya	9 Mei 2019

[Menambahkan jenis temuan baru, Recon:EC2/PortProbeEMRUnprotectedPort.](#)

Temuan ini memberi tahu Anda bahwa port sensitif terkait EMR pada EC2 Instance tidak diblokir dan sedang diselidiki secara aktif. [Pelajari selengkapnya](#)

8 Mei 2019

[Menambahkan 5 jenis temuan baru yang mendeteksi jika EC2 instans Anda berpotensi digunakan untuk serangan denial of service \(DoS\).](#)

Temuan ini memberi tahu Anda tentang EC2 kejadian di lingkungan Anda yang berperilaku dengan cara yang mungkin menunjukkan bahwa mereka digunakan untuk melakukan serangan Denial of Service (DoS). [Pelajari selengkapnya](#)

8 Maret 2019

[Menambahkan jenis temuan baru: Policy:IAMUser/RootCredentialUsage](#)

Policy:IAMUser/RootCredentialUsage jenis pencarian memberi tahu Anda bahwa kredensi masuk pengguna root Anda Akun AWS sedang digunakan untuk membuat permintaan terprogram ke layanan. AWS [Pelajari selengkapnya](#)

24 Januari 2019

[UnauthorizedAccess:IAMUser/UnusualASNCallertipe temuan telah pensiun](#)

Jenis UnauthorizedAccess:IAMUser/UnusualASNCaller temuan telah pensiun. Anda sekarang akan diberi tahu tentang aktivitas yang dipanggil dari jaringan yang tidak biasa melalui jenis GuardDuty temuan aktif lainnya. Tipe temuan yang dihasilkan akan didasarkan pada kategori API yang dipanggil dari jaringan yang tidak biasa. [Pelajari selengkapnya](#)

21 Desember 2018

[Menambahkan dua jenis temuan baru: PenTest:IAMUser/ParrotLinux dan PenTest:IAMUser/PentooLinux](#)

PenTest:IAMUser/ParrotLinux jenis pencarian memberi tahu Anda bahwa komputer yang menjalankan Parrot Security Linux melakukan panggilan API menggunakan kredensial milik akun Anda. AWS PenTest:IAMUser/PentooLinux jenis pencarian memberi tahu Anda bahwa mesin yang menjalankan Pentoo Linux melakukan panggilan API menggunakan kredensial milik akun Anda. AWS [Pelajari selengkapnya](#)

21 Desember 2018

[Menambahkan dukungan untuk topik SNS GuardDuty pengumuman Amazon](#)

Anda sekarang dapat berlangganan topik SNS GuardDuty pengumuman untuk menerima pemberitahuan tentang jenis temuan yang baru dirilis, pembaruan untuk jenis temuan yang ada, dan perubahan fungsionalitas lainnya. Notifikasi tersedia dalam semua format yang didukung Amazon SNS.

[Pelajari selengkapnya](#)

21 November 2018

[Menambahkan dua jenis temuan baru: UnauthorizedAccess:EC2/TorClient dan UnauthorizedAccess:EC2/TorRelay](#)

UnauthorizedAccess:EC2/TorClient jenis pencarian memberi tahu Anda bahwa sebuah EC2 instance di AWS lingkungan Anda membuat koneksi ke Tor Guard atau node Authority. UnauthorizedAccess:EC2/TorRelay jenis pencarian memberi tahu Anda bahwa sebuah EC2 instance di AWS lingkungan Anda membuat koneksi ke jaringan Tor dengan cara yang menunjukkan bahwa itu bertindak sebagai relai Tor.

[Pelajari selengkapnya](#)

16 November 2018

[Menambahkan jenis temuan baru: Cryptocurrency:EC2/BitcoinTool.B](#)

Temuan ini memberi tahu Anda bahwa sebuah EC2 instance di AWS lingkungan Anda menanyakan nama domain yang terkait dengan Bitcoin, atau aktivitas terkait cryptocurrency lainnya. [Pelajari selengkapnya](#)

9 November 2018

[Menambahkan dukungan untuk memperbarui frekuensi pemberitahuan yang dikirim ke CloudWatch Acara](#)

Anda sekarang dapat memperbarui frekuensi pemberitahuan yang dikirim ke CloudWatch Acara untuk kejadian berikutnya dari temuan yang ada. Nilai yang mungkin adalah 15 menit, 1 jam, atau default 6 jam. [Pelajari selengkapnya](#)

9 Oktober 2018

[Ditambahkan dukungan Wilayah](#)

Menambahkan dukungan Wilayah untuk AWS GovCloud (AS-Barat) [Pelajari lebih lanjut](#)

25 Juli 2018

[Ditambahkan dukungan untuk AWS CloudFormation StackSets di GuardDuty](#)

Anda dapat menggunakan GuardDuty template Aktifkan Amazon untuk mengaktifkan GuardDuty secara bersamaan di beberapa akun. [Pelajari selengkapnya](#)

25 Juni 2018

[Menambahkan dukungan untuk aturan GuardDuty arsip otomatis](#)

Pelanggan kini dapat membuat aturan pengarsipan otomatis granular untuk penekanan temuan. Untuk temuan yang cocok dengan aturan arsip otomatis, tandai GuardDuty secara otomatis sebagai diarsipkan. Hal ini memungkinkan pelanggan untuk lebih menyesuaikan GuardDuty untuk menyimpan hanya temuan yang relevan dalam tabel temuan saat ini.

[Pelajari selengkapnya](#)

4 Mei 2018

[GuardDuty tersedia di Wilayah Eropa \(Paris\)](#)

GuardDuty sekarang tersedia di Eropa (Paris), memungkinkan Anda untuk memperluas pemantauan keamanan berkelanjutan dan deteksi ancaman di Wilayah ini.

[Pelajari selengkapnya](#)

29 Maret 2018

[Membuat akun GuardDuty administrator dan akun anggota AWS CloudFormation sekarang didukung.](#)

Untuk informasi selengkapnya, lihat [AWS::GuardDuty::master](#) dan [AWS::GuardDuty::member](#).

6 Maret 2018

[Menambahkan sembilan deteksi anomali CloudTrail berbasis baru.](#)

Jenis temuan baru ini diaktifkan secara otomatis GuardDuty di semua Wilayah yang didukung. [Pelajari selengkapnya](#)

28 Februari 2018

[Menambahkan tiga deteksi intelijen ancaman baru \(tipe pencarian\).](#)

Jenis temuan baru ini diaktifkan secara otomatis GuardDuty di semua Wilayah yang didukung. [Pelajari lebih lanjut](#)

5 Februari 2018

[Batasi kenaikan untuk akun GuardDuty anggota.](#)

Dengan rilis ini, Anda dapat memiliki hingga 1000 akun GuardDuty anggota ditambahkan per AWS akun (akun akun GuardDuty administrator). [Pelajari selengkapnya](#)

25 Januari 2018

[Perubahan dalam unggahan dan pengelolaan lebih lanjut dari daftar IP tepercaya dan daftar ancaman untuk akun GuardDuty administrator dan akun anggota.](#)

Dengan rilis ini, Pengguna dari akun GuardDuty akun administrator dapat mengunggah dan mengelola daftar IP tepercaya dan daftar ancaman. Pengguna dari GuardDuty akun anggota tidak dapat mengunggah dan mengelola daftar. Daftar IP tepercaya dan daftar ancaman yang diunggah oleh akun akun administrator dikenakan pada GuardDuty fungsionalitas di akun anggotanya. [Pelajari selengkapnya](#)

25 Januari 2018

Pembaruan lebih awal

Perubahan	Deskripsi	Tanggal
Publikasi awal	Publikasi awal Panduan GuardDuty Pengguna Amazon.	28 November 2017

Terjemahan disediakan oleh mesin penerjemah. Jika konten terjemahan yang diberikan bertentangan dengan versi bahasa Inggris aslinya, utamakan versi bahasa Inggris.