Panduan Pengguna

AWS Security Hub

AWS Security Hub: Panduan Pengguna

Table of Contents

Apa itu AWS Security Hub?

AWSSecurity Hub memberi Anda pandangan komprehensif tentang keadaan keamanan Anda AWS dan membantu Anda menilai AWS lingkungan Anda berdasarkan standar industri keamanan dan praktik terbaik.

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

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

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

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

Topik

Keuntungan dari Security Hub

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

Mengurangi upaya mengumpulkan dan memprioritaskan temuan

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

Pemeriksaan keamanan otomatis terhadap praktik dan standar terbaik

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

Pandangan konsolidasi temuan di seluruh akun dan penyedia

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

Kemampuan untuk mengotomatiskan menemukan pembaruan dan remediasi

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

Mengakses Security Hub

Security Hub tersedia di sebagian besarWilayah AWS. Untuk daftar Wilayah di mana Security Hub saat ini tersedia, lihat titik akhir dan kuota AWS Security Hub di. Referensi Umum AWS Untuk informasi tentang mengelola Wilayah AWS akun AndaAkun AWS, lihat Menentukan Wilayah AWS akun mana yang dapat digunakan dalam Panduan AWS Account Management Referensi.

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

Konsol Security Hub

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

Security Hub API

Security Hub API memberi Anda akses terprogram ke akun, data, dan sumber daya Security Hub Anda. Dengan API, Anda dapat mengirim permintaan HTTPS langsung ke Security Hub. Untuk informasi tentang API, lihat Referensi API AWS Security Hub.

AWS CLI

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

SDK AWS

AWS menyediakan SDK yang terdiri atas pustaka dan kode sampel untuk berbagai bahasa dan platform pemrograman, misalnya Java, Go, Python, C++, dan .NET. SDK menyediakan akses terprogram yang nyaman ke Security Hub dan lainnya Layanan AWS dalam bahasa pilihan Anda. SDK menangani tugas seperti menandatangani permintaan secara kriptografis, mengelola kesalahan, dan mencoba kembali permintaan secara otomatis. Untuk informasi tentang menginstal dan menggunakan SDK AWS, lihat Alat untuk Membangun di AWS.

> **Important**
>
> Security Hub hanya mendeteksi dan mengkonsolidasikan temuan yang dihasilkan setelah Anda mengaktifkan Security Hub. Itu tidak secara retroaktif mendeteksi dan mengkonsolidasikan temuan keamanan yang dihasilkan sebelum Anda mengaktifkan Security Hub.
> Security Hub hanya menerima dan memproses temuan di Wilayah tempat Anda mengaktifkan Security Hub di akun Anda.
> Untuk kepatuhan penuh dengan pemeriksaan keamanan CIS AWS Foundations Benchmark, Anda harus mengaktifkan Security Hub di semua Wilayah yang didukungAWS.

Layanan terkait

Untuk lebih mengamankan AWS lingkungan Anda, pertimbangkan untuk menggunakan yang lain Layanan AWS dalam kombinasi dengan Security Hub.

Untuk daftar orang lain Layanan AWS yang mengirim atau menerima temuan Security Hub, lihatLayanan AWS Integrasi dengan AWS Security Hub.

Security Hub menggunakan aturan terkait layanan dari AWS Config untuk menjalankan pemeriksaan keamanan untuk sebagian besar kontrol. Anda harus mengaktifkan AWS Config dan merekam sumber daya di AWS Config Security Hub untuk menghasilkan sebagian besar temuan kontrol. Untuk informasi selengkapnya, lihat Mengkonfigurasi AWS Config.

Uji coba dan harga gratis Security Hub

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

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

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

> **Note**
>
> Uji coba gratis Security Hub tidak didukung di Wilayah China (Beijing).

Melihat detail penggunaan dan perkiraan biaya

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

Untuk menampilkan informasi penggunaan (konsol)

1. Buka konsol AWS Security Hub di https://console.aws.amazon.com/securityhub/.
2. Di panel navigasi, pilih Penggunaan di bawah Pengaturan.

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

Informasi penggunaan dan perkiraan biaya hanya untuk akun saat ini dan Wilayah saat ini. Di Wilayah agregasi, informasi penggunaan dan perkiraan biaya tidak termasuk Wilayah yang ditautkan. Untuk informasi selengkapnya tentang Wilayah tertaut, lihatthe section called “Cara kerja agregasi lintas wilayah”.

Detail harga

Untuk informasi selengkapnya tentang cara Security Hub mengenakan biaya untuk temuan tertelan dan pemeriksaan keamanan, lihat harga Security Hub.

Konsep Security Hub

Topik ini menjelaskan konsep dan terminologi kunci di AWS Security Hub untuk membantu Anda memulai layanan.

Akun

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

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

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

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

Untuk informasi selengkapnya, lihat Mengelola akun administrator dan anggota.

Akun Administrator

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

Akun menjadi akun administrator dengan salah satu cara berikut:

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

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

Wilayah Agregasi

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

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

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

Lihat Agregasi Lintas Wilayah.

Temuan yang diarsipkan

Temuan yang memiliki satu `RecordState` set ke`ARCHIVED`. Mengarsipkan temuan menunjukkan bahwa penyedia temuan percaya bahwa temuan tersebut tidak lagi relevan. Status rekaman terpisah dari status alur kerja, yang melacak status investigasi ke dalam temuan.

Penyedia pencarian dapat menggunakan `BatchImportFindings`pengoperasian Security Hub API untuk mengarsipkan temuan yang mereka buat. Security Hub secara otomatis mengarsipkan temuan untuk kontrol jika kontrol dinonaktifkan atau sumber daya terkait dihapus, berdasarkan salah satu kriteria berikut.

- Temuan ini tidak diperbarui dalam tiga hingga lima hari (perhatikan bahwa ini adalah upaya terbaik dan tidak dijamin).
- AWS Config Evaluasi terkait kembali`NOT_APPLICABLE`.

Secara default, temuan yang diarsipkan dikecualikan dari daftar temuan di konsol Security Hub. Anda dapat memperbarui filter untuk menyertakan temuan yang diarsipkan.

`GetFindings`Pengoperasian Security Hub API mengembalikan temuan aktif dan yang diarsipkan. Anda dapat menyertakan filter untuk status rekaman.

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

AWS Format Pencarian Keamanan (ASFF)

Format standar untuk konten temuan yang dikumpulkan atau dihasilkan oleh Security Hub. Format Pencarian AWS Keamanan memungkinkan Anda menggunakan Security Hub untuk melihat dan menganalisis temuan yang dihasilkan oleh layanan AWS keamanan, solusi pihak ketiga, atau Security Hub sendiri dari menjalankan pemeriksaan keamanan. Untuk informasi selengkapnya, lihat AWS Format Pencarian Keamanan (ASFF).

Kontrol

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

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

Tindakan kustom

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

Akun administrator yang didelegasikan (Organizations)

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

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

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

Temuan

Catatan yang dapat diamati dari pemeriksaan keamanan atau deteksi terkait keamanan. Security Hub menghasilkan temuan setelah menyelesaikan pemeriksaan keamanan kontrol. Ini disebut temuan kontrol. Temuan juga dapat berasal dari integrasi produk pihak ketiga.

Untuk informasi selengkapnya tentang temuan di Security Hub, lihatTemuan .

> **Note**
>
> Temuan dihapus 90 hari setelah pembaruan terbaru atau 90 hari setelah tanggal pembuatan jika tidak ada pembaruan yang terjadi. Untuk menyimpan temuan selama lebih dari 90 hari, Anda dapat mengonfigurasi aturan yang EventBridge merutekan temuan ke bucket Amazon S3 Anda.

Agregasi Lintas Wilayah

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

Lihat Agregasi Lintas Wilayah.

Menemukan konsumsi

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

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

Wawasan

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

Wilayah Tertaut

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

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

Lihat Agregasi Lintas Wilayah.

Akun anggota

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

Akun menjadi akun anggota dengan salah satu cara berikut:

- Akun menerima undangan dari akun lain.
- Untuk akun organisasi, akun administrator Security Hub mengaktifkan akun sebagai akun anggota.

Persyaratan terkait

Seperangkat persyaratan industri atau peraturan yang dipetakan ke kontrol.

Aturan

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

Pemeriksaan keamanan

point-in-time Evaluasi spesifik aturan terhadap sumber daya tunggal yang menghasilkan`PASSED`,`FAILED`,`WARNING`, atau `NOT_AVAILABLE` negara. Menjalankan pemeriksaan keamanan menghasilkan temuan.

Akun administrator Security Hub

Akun organisasi yang mengelola keanggotaan Security Hub untuk suatu organisasi.

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

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

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

Standar keamanan

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

Kepelikan

Tingkat keparahan yang ditetapkan ke kontrol Security Hub mengidentifikasi pentingnya kontrol. Tingkat keparahan kontrol dapat Kritis, Tinggi, Sedang, Rendah, atau Informasi. Tingkat keparahan yang ditugaskan untuk mengontrol temuan sama dengan tingkat keparahan kontrol itu sendiri. Untuk mempelajari tentang cara Security Hub menetapkan tingkat keparahan pada kontrol, lihatMenetapkan tingkat keparahan untuk mengontrol temuan.

Status alur kerja

Status investigasi terhadap sebuah temuan. Dilacak menggunakan `Workflow.Status` atribut.

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

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

Untuk `GetFindings`operasi, Anda dapat menyertakan filter untuk status alur kerja.

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

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

Rekomendasi sebelum mengaktifkan Security Hub

Rekomendasi berikut dapat membantu Anda memulai penggunaan AWS Security Hub.

Integrasi dengan AWS Organizations

AWS Organizations adalah layanan manajemen akun global yang memungkinkan AWS administrator untuk mengkonsolidasikan dan mengelola beberapa Akun AWS unit organisasi (OU) secara terpusat. 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 Security Hub, Amazon GuardDuty, dan Amazon Macie.

Untuk membantu mengotomatisasi dan merampingkan pengelolaan akun, kami sangat menyarankan untuk mengintegrasikan Security Hub dan. AWS Organizations Anda dapat berintegrasi dengan Organizations jika Anda memiliki lebih dari satu Akun AWS yang menggunakan Security Hub.

Untuk petunjuk tentang mengaktifkan integrasi, lihat[Mengintegrasikan Security Hub dengan AWS Organizations](#).

Menggunakan konfigurasi pusat

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

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

- Apakah Security Hub diaktifkan atau dinonaktifkan
- Standar keamanan mana yang diaktifkan dan dinonaktifkan
- Kontrol keamanan mana yang diaktifkan dan dinonaktifkan

- Apakah akan menyesuaikan parameter untuk kontrol tertentu

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

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

Untuk mempelajari lebih lanjut tentang konfigurasi pusat, lihatCara kerja konfigurasi pusat.

Mengkonfigurasi AWS Config

AWS Security Hub menggunakan AWS Config aturan terkait layanan untuk melakukan pemeriksaan keamanan untuk sebagian besar kontrol.

Untuk mendukung kontrol ini, AWS Config harus diaktifkan di semua akun—baik akun administrator maupun akun anggota—di masing-masing tempat Wilayah AWS Security Hub diaktifkan. Selain itu, untuk setiap standar yang diaktifkan AWS Config harus dikonfigurasi untuk merekam sumber daya yang diperlukan untuk kontrol yang diaktifkan.

Sebaiknya aktifkan perekaman sumber daya AWS Config sebelum mengaktifkan standar Security Hub. Jika Security Hub mencoba menjalankan pemeriksaan keamanan saat perekaman sumber daya dimatikan, pemeriksaan akan mengembalikan kesalahan.

Security Hub tidak mengelola AWS Config untuk Anda. Jika Anda sudah AWS Config mengaktifkan, Anda dapat mengonfigurasi pengaturannya melalui AWS Config konsol atau API.

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

- Pada hari Anda mengaktifkan standar
- Sehari setelah Anda mengaktifkan standar
- 3 hari setelah Anda mengaktifkan standar
- 7 hari setelah Anda mengaktifkan standar (dan terus menerus setiap 7 hari setelahnya)

Jika Anda menggunakan konfigurasi pusat, Security Hub juga mencoba membuat AWS Config aturan saat Anda menerapkan kembali kebijakan konfigurasi yang mengaktifkan satu atau beberapa standar.

Mengaktifkan AWS Config

Jika Anda belum AWS Config mengaktifkannya, Anda dapat mengaktifkannya dengan salah satu cara berikut:

- Konsol atau AWS CLI — Anda dapat mengaktifkan secara manual AWS Config menggunakan AWS Config konsol atau AWS CLI. Lihat Memulai AWS Config di Panduan AWS Config Pengembang.
- AWS CloudFormation template — Jika Anda ingin mengaktifkan AWS Config pada sejumlah besar akun, Anda dapat mengaktifkan AWS Config dengan CloudFormation template Aktifkan AWS Config. Untuk mengakses template ini, lihat AWS CloudFormation StackSets contoh template di Panduan AWS CloudFormation Pengguna.
- Skrip Github — Security Hub menawarkan GitHub skrip yang memungkinkan Security Hub untuk beberapa akun di seluruh Wilayah. Skrip ini berguna jika Anda belum terintegrasi dengan Organizations atau jika Anda memiliki akun yang bukan bagian dari organisasi Anda. Ketika Anda menggunakan skrip ini untuk mengaktifkan Security Hub, itu juga secara otomatis mengaktifkan AWS Config akun-akun ini.

Untuk informasi selengkapnya tentang mengaktifkan AWS Config untuk membantu Anda menjalankan pemeriksaan keamanan Security Hub, lihat Optimalkan AWS ConfigAWS Security Hub untuk mengelola postur keamanan cloud Anda secara efektif.

Mengaktifkan perekaman sumber daya di AWS Config

Ketika Anda mengaktifkan perekaman sumber daya AWS Config dengan pengaturan default, itu merekam semua jenis sumber daya Regional yang didukung yang AWS Config menemukan Wilayah AWS di mana ia berjalan. Anda juga dapat mengonfigurasi AWS Config untuk merekam jenis sumber daya global yang didukung. Anda hanya perlu merekam sumber daya global di satu Wilayah (kami sarankan ini menjadi Wilayah asal Anda jika Anda menggunakan konfigurasi pusat).

Jika Anda menggunakan CloudFormation StackSets untuk mengaktifkan AWS Config, kami sarankan Anda menjalankan dua yang berbeda StackSets. Jalankan satu StackSet untuk merekam semua sumber daya, termasuk sumber daya global, dalam satu Wilayah. Jalankan sedetik StackSet untuk merekam semua sumber daya kecuali sumber daya global di Wilayah lain.

Anda juga dapat menggunakan Quick Setup, kemampuan AWS Systems Manager, untuk mengonfigurasi perekaman sumber daya dengan cepat di AWS Config seluruh akun dan Wilayah Anda. Selama proses Quick Setup, Anda dapat memilih Wilayah mana yang ingin Anda rekam sumber daya global. Untuk informasi selengkapnya, lihat perekam AWS Config konfigurasi di Panduan AWS Systems Manager Pengguna.

Kontrol keamanan Config.1 menghasilkan temuan yang gagal untuk Wilayah selain Wilayah tertaut dalam agregator (Wilayah dan Wilayah asal tidak berada dalam agregator temuan sama sekali) jika Wilayah tersebut tidak merekam sumber daya global AWS Identity and Access Management (IAM) dan telah mengaktifkan kontrol yang memerlukan sumber daya global IAM untuk direkam. Di Wilayah tertaut, Config.1 tidak memeriksa apakah sumber daya global IAM direkam. Untuk daftar sumber daya yang dibutuhkan setiap kontrol, lihatAWS Config sumber daya yang dibutuhkan untuk menghasilkan temuan kontrol.

Jika Anda menggunakan skrip multi-akun untuk mengaktifkan Security Hub, secara otomatis mengaktifkan perekaman sumber daya untuk semua sumber daya, termasuk sumber daya global, di semua Wilayah. Anda kemudian dapat memperbarui konfigurasi untuk merekam sumber daya global hanya dalam satu Wilayah. Untuk selengkapnya, lihat Memilih sumber daya yang AWS Config direkam dalam Panduan AWS Config Pengembang.

Agar Security Hub dapat secara akurat melaporkan temuan untuk kontrol yang bergantung pada AWS Config aturan, Anda harus mengaktifkan perekaman untuk sumber daya yang relevan. Untuk daftar kontrol dan AWS Config sumber daya terkait, lihatAWS Config sumber daya yang dibutuhkan untuk menghasilkan temuan kontrol.AWS Config memungkinkan Anda memilih antara perekaman berkelanjutan dan perekaman harian perubahan status sumber daya. Jika Anda memilih perekaman harian, AWS Config mengirimkan data konfigurasi sumber daya pada akhir setiap periode 24 jam jika ada perubahan status sumber daya. Jika tidak ada perubahan, tidak ada data yang dikirimkan. Ini dapat menunda pembuatan temuan Security Hub untuk kontrol yang dipicu perubahan hingga periode 24 jam selesai.

> **Note**
>
> Untuk menghasilkan temuan baru setelah pemeriksaan keamanan dan menghindari temuan basi, Anda harus memiliki izin yang cukup untuk peran IAM yang dilampirkan ke perekam konfigurasi untuk mengevaluasi sumber daya yang mendasarinya.

Pertimbangan biaya

Untuk detail tentang biaya yang terkait dengan pencatatan sumber daya, lihat AWS Security Hub harga dan AWS Config harga.

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

Mengaktifkan Security Hub

Ada dua cara untuk mengaktifkan AWS Security Hub, dengan mengintegrasikan dengan AWS Organizations atau secara manual.

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

Memverifikasi izin yang diperlukan

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

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

Untuk informasi selengkapnya, lihat AWS kebijakan terkelola untuk AWS Security Hub.

Mengaktifkan Security Hub dengan Integrasi Organizations

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

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

Security Hub console

Untuk menunjuk administrator yang didelegasikan Security Hub saat melakukan orientasi

1. Buka konsol AWS Security Hub di https://console.aws.amazon.com/securityhub/.

2. Pilih Buka Security Hub. Anda diminta untuk masuk ke akun manajemen Organisasi.
3. Pada halaman Tentukan administrator yang didelegasikan, di bagian Akun administrator yang didelegasikan, tentukan akun administrator yang didelegasikan. Sebaiknya pilih administrator terdelegasi yang sama yang telah Anda tetapkan untuk layanan AWS keamanan dan kepatuhan lainnya.
4. Pilih Setel administrator yang didelegasikan.

Security Hub API

Memanggil `EnableOrganizationAdminAccount`API dari akun manajemen Organizations. Berikan Akun AWS ID akun administrator yang didelegasikan Security Hub.

AWS CLI

Jalankan `enable-organization-admin-account`perintah dari akun manajemen Organisasi. Berikan Akun AWS ID akun administrator yang didelegasikan Security Hub.

Contoh perintah:

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

Untuk informasi selengkapnya tentang integrasi dengan Organizations, lihatMengintegrasikan Security Hub dengan AWS Organizations.

Setelah menunjuk administrator yang didelegasikan, kami sarankan Anda melanjutkan pengaturan Security Hub dengan konfigurasi pusat. Konsol meminta Anda untuk melakukannya. Dengan menggunakan konfigurasi pusat, Anda dapat menyederhanakan proses mengaktifkan dan mengonfigurasi Security Hub untuk organisasi Anda dan memastikan bahwa organisasi Anda memiliki cakupan keamanan yang memadai.

Konfigurasi pusat memungkinkan administrator yang didelegasikan menyesuaikan Security Hub di beberapa akun organisasi dan Wilayah daripada mengonfigurasi Region-by-Region. Anda dapat membuat kebijakan konfigurasi untuk seluruh organisasi, atau membuat kebijakan konfigurasi yang berbeda untuk akun dan OU yang berbeda. Kebijakan menentukan apakah Security Hub diaktifkan atau dinonaktifkan di akun terkait serta standar dan kontrol keamanan mana yang diaktifkan.

Administrator yang didelegasikan dapat menetapkan akun sebagai dikelola secara terpusat atau dikelola sendiri. Akun yang dikelola secara terpusat hanya dapat dikonfigurasi oleh administrator yang didelegasikan. Akun yang dikelola sendiri dapat menentukan pengaturan mereka sendiri.

Jika Anda tidak menggunakan konfigurasi pusat, administrator yang didelegasikan memiliki kemampuan yang lebih terbatas untuk mengonfigurasi Security Hub. Untuk informasi selengkapnya, lihat Mengelola akun dengan AWS Organizations.

Mengaktifkan Security Hub secara manual

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

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

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

Security Hub console

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

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

   Anda dapat mengaktifkan atau menonaktifkan standar atau kontrol individualnya kapan saja. Untuk informasi tentang mengelola standar dan kontrol keamanan, lihat Kontrol dan standar keamanan di AWS Security Hub.
4. Pilih Aktifkan Security Hub.

Security Hub API

Memanggil `EnableSecurityHub`API. Saat Anda mengaktifkan Security Hub dari API, maka secara otomatis mengaktifkan standar keamanan default berikut:

- AWSPraktik Terbaik Keamanan Dasar

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

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

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

AWS CLI

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

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

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

Contoh

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

Skrip pengaktifan multi-akun

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

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

Skrip secara otomatis memungkinkan perekaman sumber daya untuk semua sumber daya, termasuk sumber daya global, di semua Wilayah. Ini tidak membatasi pencatatan sumber daya global ke satu Wilayah.

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

Langkah selanjutnya setelah mengaktifkan Security Hub

Setelah mengaktifkan Security Hub, sebaiknya aktifkan standar keamanan dan kontrol keamanan yang penting untuk kebutuhan keamanan Anda. Setelah Anda mengaktifkan kontrol, Security Hub mulai menjalankan pemeriksaan keamanan dan menghasilkan temuan kontrol. Anda juga dapat memanfaatkan integrasi antara Security Hub dan solusi pihak ketiga lainnya Layanan AWS untuk melihat temuan mereka di Security Hub.

Cara kerja konfigurasi pusat

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

Dari akun administrator Security Hub yang didelegasikan, Anda dapat menentukan cara layanan Security Hub, standar keamanan, dan kontrol keamanan dikonfigurasi di akun organisasi dan unit organisasi (OU) di seluruh Wilayah. Anda dapat mengonfigurasi pengaturan ini hanya dalam beberapa langkah dari satu Wilayah utama, yang disebut sebagai Wilayah asal. Jika Anda tidak menggunakan konfigurasi pusat, Anda harus mengonfigurasi Security Hub secara terpisah di setiap akun dan Wilayah.

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

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

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

Bagian ini memberikan gambaran umum tentang konfigurasi pusat.

Manfaat konfigurasi pusat

Manfaat konfigurasi pusat meliputi:

Menyederhanakan konfigurasi layanan dan kemampuan Security Hub

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

Konfigurasikan di seluruh akun dan Wilayah

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

Mengakomodasi konfigurasi yang berbeda di akun dan OU yang berbeda

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

Mencegah penyimpangan konfigurasi

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

Siapa yang harus menggunakan konfigurasi pusat?

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

Anda dapat menggunakan konfigurasi pusat untuk mengonfigurasi layanan Security Hub, standar keamanan, dan kontrol keamanan. Anda juga dapat menggunakannya untuk menyesuaikan parameter kontrol tertentu. Untuk informasi tentang standar dan kontrol, lihatKontrol dan standar keamanan di AWS Security Hub.

Istilah dan konsep konfigurasi pusat

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

Konfigurasi pusat

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

Beranda Wilayah

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

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

Wilayah yang AWS diperkenalkan pada atau setelah 20 Maret 2019 dikenal sebagai Wilayah opt-in. Wilayah keikutsertaan tidak bisa menjadi Wilayah asal, tetapi bisa menjadi Wilayah yang terhubung. Untuk daftar Wilayah keikutsertaan, lihat Pertimbangan sebelum mengaktifkan dan menonaktifkan Wilayah di Panduan Referensi Manajemen Akun.AWS

Wilayah Tertaut

An Wilayah AWS yang dapat dikonfigurasi dari Wilayah asal. Kebijakan konfigurasi dibuat oleh administrator yang didelegasikan di Wilayah beranda. Kebijakan tersebut berlaku di Wilayah asal dan semua Wilayah terkait. Anda harus menentukan setidaknya satu Wilayah tertaut untuk menggunakan konfigurasi pusat.

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

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

Kebijakan konfigurasi Security Hub

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

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

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

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

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

Untuk menerapkan setelan berbeda ke organisasi, atau menerapkan kebijakan konfigurasi yang berbeda ke akun dan OU yang berbeda, buat kebijakan konfigurasi khusus.

Konfigurasi lokal

Jenis konfigurasi default untuk organisasi, setelah mengintegrasikan Security Hub dan AWS Organizations. Dengan konfigurasi lokal, administrator yang didelegasikan dapat memilih untuk secara otomatis mengaktifkan Security Hub dan standar keamanan default di akun organisasi baru di Wilayah saat ini. Jika administrator yang didelegasikan secara otomatis mengaktifkan standar default, semua kontrol yang merupakan bagian dari standar ini juga diaktifkan secara otomatis dengan parameter default untuk akun organisasi baru. Pengaturan ini tidak berlaku untuk akun yang ada, jadi penyimpangan konfigurasi dimungkinkan setelah akun bergabung dengan organisasi. Menonaktifkan kontrol spesifik yang merupakan bagian dari standar default, dan mengonfigurasi standar dan kontrol tambahan, harus dilakukan secara terpisah di setiap akun dan Wilayah.

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

Manajemen akun manual

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

API konfigurasi pusat

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

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

API khusus akun

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

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

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

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

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

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

Unit organisasi (OU)

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

Anda dapat mengelola OU di AWS Organizations atau AWS Control Tower. Untuk informasi selengkapnya, lihat Mengelola unit organisasi dalam Panduan AWS Organizations Pengguna

atau Mengatur organisasi dan akun AWS Control Tower di Panduan AWS Control Tower Pengguna.

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

Dikelola secara terpusat

Akun, OU, atau root yang hanya dapat dikonfigurasi oleh administrator yang didelegasikan di seluruh Wilayah dengan menggunakan kebijakan konfigurasi.

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

Dikelola sendiri

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

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

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

Asosiasi kebijakan konfigurasi

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

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

Asosiasi ada sampai konfigurasi yang berbeda diterapkan atau diwariskan.

Kebijakan konfigurasi yang diterapkan

Jenis asosiasi kebijakan konfigurasi di mana administrator yang didelegasikan secara langsung menerapkan kebijakan konfigurasi ke akun target, OU, atau root. Target dikonfigurasi dengan cara yang ditentukan oleh kebijakan konfigurasi, dan hanya administrator yang didelegasikan yang dapat mengubah konfigurasinya. Jika diterapkan ke root, kebijakan konfigurasi memengaruhi semua akun dan OU di organisasi yang tidak menggunakan konfigurasi berbeda melalui aplikasi atau warisan dari induk terdekat.

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

Kebijakan konfigurasi yang diwariskan

Jenis asosiasi kebijakan konfigurasi di mana akun atau OU mengadopsi konfigurasi OU induk terdekat atau root. Jika kebijakan konfigurasi tidak langsung diterapkan ke akun atau OU, kebijakan tersebut mewarisi konfigurasi induk terdekat. Semua elemen kebijakan diwariskan. Dengan kata lain, akun atau OU tidak dapat memilih untuk secara selektif mewarisi hanya bagian dari kebijakan. Jika orang tua terdekat dikelola sendiri, akun anak atau OU mewarisi perilaku yang dikelola sendiri dari orang tua.

Warisan tidak dapat mengganti konfigurasi yang diterapkan. Artinya, jika kebijakan konfigurasi atau konfigurasi yang dikelola sendiri langsung diterapkan ke akun atau OU, ia menggunakan konfigurasi itu dan tidak mewarisi konfigurasi induk.

Akar

Di AWS Organizations dan Security Hub, node induk tingkat atas dalam suatu organisasi. Jika administrator yang didelegasikan menerapkan kebijakan konfigurasi ke root, kebijakan tersebut dikaitkan dengan semua akun dan OU di organisasi kecuali mereka menggunakan kebijakan yang berbeda, melalui aplikasi atau warisan, atau ditetapkan sebagai dikelola sendiri. Jika administrator menetapkan root sebagai dikelola sendiri, semua akun dan OU dalam organisasi dikelola sendiri kecuali mereka menggunakan kebijakan konfigurasi melalui aplikasi atau warisan. Jika root dikelola sendiri dan tidak ada kebijakan konfigurasi saat ini, semua akun baru di organisasi akan mempertahankan pengaturannya saat ini.

Akun baru yang bergabung dengan organisasi berada di bawah root sampai mereka ditugaskan ke OU tertentu. Jika akun baru tidak ditetapkan ke OU, akun tersebut mewarisi konfigurasi root kecuali administrator yang didelegasikan menetapkannya sebagai akun yang dikelola sendiri.

Mulai menggunakan konfigurasi pusat

Akun administrator AWS Security Hub yang didelegasikan dapat menggunakan konfigurasi pusat untuk mengonfigurasi Security Hub, standar, dan kontrol untuk beberapa akun dan unit organisasi (OU) secara keseluruhanWilayah AWS.

Bagian ini menjelaskan prasyarat untuk konfigurasi pusat dan cara mulai menggunakannya.

Prasyarat untuk konfigurasi pusat

Sebelum Anda dapat mulai menggunakan konfigurasi pusat, Anda harus mengintegrasikan Security Hub dengan AWS Organizations dan menunjuk Wilayah rumah. Jika Anda menggunakan konsol Security Hub, prasyarat ini disertakan dalam alur kerja opt-in untuk konfigurasi pusat.

Integrasi dengan Organizations

Anda harus mengintegrasikan Security Hub dan Organizations untuk menggunakan konfigurasi pusat.

Untuk mengintegrasikan layanan ini, Anda mulai dengan membuat organisasi di Organizations. Dari akun manajemen Organizations, Anda kemudian menetapkan akun administrator yang didelegasikan Security Hub. Untuk petunjuk, silakan lihat Mengintegrasikan Security Hub dengan AWS Organizations.

Pastikan Anda menunjuk administrator yang didelegasikan di Wilayah rumah yang dituju. Saat Anda mulai menggunakan konfigurasi pusat, administrator yang didelegasikan yang sama secara otomatis diatur di semua Wilayah yang ditautkan juga. Akun manajemen Organisasi tidak dapat ditetapkan sebagai akun administrator yang didelegasikan.

> **Important**
>
> Bila menggunakan konfigurasi pusat, Anda tidak dapat menggunakan konsol Security Hub atau Security Hub API untuk mengubah atau menghapus akun administrator yang didelegasikan. Jika akun manajemen Organizations menggunakan AWS Organizations API untuk mengubah atau menghapus administrator yang didelegasikan Security Hub, Security Hub secara otomatis menghentikan konfigurasi pusat. Kebijakan konfigurasi Anda juga dipisahkan dan dihapus. Akun anggota mempertahankan konfigurasi yang mereka miliki sebelum administrator yang didelegasikan diubah atau dihapus.

Tentukan Wilayah rumah

Anda harus menunjuk Wilayah rumah untuk menggunakan konfigurasi pusat. Wilayah asal adalah Wilayah tempat administrator yang didelegasikan mengkonfigurasi organisasi.

Untuk menggunakan konfigurasi pusat, Anda harus menentukan setidaknya satu Wilayah tertaut yang dapat dikonfigurasi dari Wilayah beranda.

> **Note**
>
> Wilayah asal tidak dapat menjadi Wilayah yang AWS telah ditetapkan sebagai Wilayah keikutsertaan. Wilayah keikutsertaan dinonaktifkan secara default. Untuk daftar Wilayah keikutsertaan, lihat Pertimbangan sebelum mengaktifkan dan menonaktifkan Wilayah di Panduan Referensi Manajemen Akun. AWS

Administrator yang didelegasikan dapat membuat dan mengelola kebijakan konfigurasi hanya dari Wilayah beranda. Kebijakan konfigurasi berlaku di Wilayah asal dan semua Wilayah yang ditautkan. Anda tidak dapat membuat kebijakan konfigurasi yang hanya berlaku untuk subset Wilayah ini, dan bukan yang lain.

Wilayah asal juga merupakan Wilayah agregasi Security Hub Anda yang menerima temuan, wawasan, dan data lainnya dari Wilayah tertaut.

Jika Anda telah menetapkan Region agregasi untuk agregasi Cross-region, maka itu adalah Region home default Anda untuk konfigurasi pusat. Anda dapat mengubah Wilayah rumah sebelum mulai menggunakan konfigurasi pusat dengan menghapus agregator temuan Anda saat ini dan membuat yang baru di Wilayah rumah yang Anda inginkan. Agregator temuan adalah sumber daya Security Hub yang menentukan Wilayah asal dan Wilayah terkait.

Untuk menunjuk Wilayah asal, ikuti langkah-langkah untuk menetapkan Wilayah agregasi. Jika Anda sudah memiliki Wilayah beranda, Anda dapat memanggil GetFindingAggregatorAPI untuk melihat detailnya, termasuk Wilayah mana yang saat ini ditautkan dengannya.

Mulai konfigurasi pusat

Pilih metode pilihan Anda, dan ikuti langkah-langkah untuk mulai menggunakan konfigurasi pusat untuk organisasi Anda.

Security Hub console

Untuk mengonfigurasi organisasi Anda secara terpusat

1. Buka AWS Security Hub konsol di https://console.aws.amazon.com/securityhub/.
2. Pada panel navigasi, pilih Pengaturan dan Konfigurasi. Kemudian, pilih Mulai konfigurasi pusat.

   Jika Anda melakukan onboarding ke Security Hub, pilih Buka Security Hub.
3. Pada halaman Administrator yang didelegasikan, pilih akun administrator yang didelegasikan atau masukkan ID akunnya. Jika berlaku, sebaiknya pilih administrator yang didelegasikan sama yang telah Anda tetapkan untuk layanan AWS keamanan dan kepatuhan lainnya. Pilih Setel administrator yang didelegasikan.
4. Pada halaman Sentralisasi organisasi, di bagian Wilayah, pilih Wilayah rumah Anda. Anda harus masuk ke Wilayah asal untuk melanjutkan. Jika Anda telah menetapkan Region agregasi untuk agregasi Lintas wilayah, itu akan ditampilkan sebagai Wilayah beranda. Untuk mengubah wilayah beranda, pilih Edit pengaturan Wilayah. Anda kemudian dapat memilih Wilayah rumah pilihan Anda dan kembali ke alur kerja ini.
5. Pilih setidaknya satu Wilayah untuk ditautkan ke Wilayah asal. Secara opsional, pilih apakah Anda ingin secara otomatis menautkan Wilayah yang didukung future ke Wilayah asal. Wilayah yang Anda pilih di sini akan dapat dikonfigurasi dari Wilayah asal oleh administrator yang didelegasikan. Kebijakan konfigurasi berlaku di Wilayah asal Anda dan semua Wilayah yang ditautkan.
6. Pilih Konfirmasi dan lanjutkan.
7. Anda sekarang dapat menggunakan konfigurasi pusat. Lanjutkan mengikuti petunjuk konsol untuk membuat kebijakan konfigurasi pertama Anda. Jika Anda belum siap untuk membuat kebijakan konfigurasi, pilih Saya belum siap untuk mengonfigurasi. Anda dapat membuat kebijakan nanti dengan memilih Pengaturan dan Konfigurasi di panel navigasi. Untuk petunjuk cara membuat kebijakan konfigurasi, lihatMembuat dan mengaitkan kebijakan konfigurasi Security Hub.

Security Hub API

Untuk mengonfigurasi Security Hub secara terpusat

1. Menggunakan kredensional akun administrator yang didelegasikan, panggil UpdateOrganizationConfigurationAPI dari Wilayah beranda.

2. Atur `AutoEnable` bidang ke`false`.
3. Atur `ConfigurationType` bidang di `OrganizationConfiguration` objek ke`CENTRAL`. Tindakan ini memiliki dampak sebagai berikut:

   - Menetapkan akun panggilan sebagai administrator yang didelegasikan Security Hub di semua Wilayah yang ditautkan.
   - Mengaktifkan Security Hub di akun administrator yang didelegasikan di semua Wilayah tertaut.
   - Menetapkan akun panggilan sebagai administrator yang didelegasikan Security Hub untuk akun baru dan yang sudah ada yang menggunakan Security Hub dan milik organisasi. Ini terjadi di Wilayah asal dan semua Wilayah terkait. Akun panggilan ditetapkan sebagai administrator yang didelegasikan untuk akun organisasi baru hanya jika akun tersebut dikaitkan dengan kebijakan konfigurasi yang mengaktifkan Security Hub. Akun panggilan ditetapkan sebagai administrator yang didelegasikan untuk akun organisasi yang ada hanya jika mereka sudah mengaktifkan Security Hub.
   - Setel AutoEnableke `false` semua Wilayah tertaut, dan disetel AutoEnableStandardske `NONE` Wilayah asal dan semua Wilayah yang ditautkan. Parameter ini tidak relevan di wilayah beranda dan terkait saat Anda menggunakan konfigurasi pusat, tetapi Anda dapat secara otomatis mengaktifkan Security Hub dan standar keamanan default di akun organisasi melalui penggunaan kebijakan konfigurasi.
4. Anda sekarang dapat menggunakan konfigurasi pusat. Administrator yang didelegasikan dapat membuat kebijakan konfigurasi untuk mengonfigurasi Security Hub di organisasi Anda. Untuk petunjuk cara membuat kebijakan konfigurasi, lihatMembuat dan mengaitkan kebijakan konfigurasi Security Hub.

Contoh permintaan API:

```
{
    "AutoEnable": false,
    "OrganizationConfiguration": {
        "ConfigurationType": "CENTRAL"
    }
}
```

AWS CLI

Untuk mengonfigurasi Security Hub secara terpusat

1. Menggunakan kredensi akun administrator yang didelegasikan, jalankan update-organization-configurationperintah dari wilayah rumah.
2. Sertakan `no-auto-enable` parameternya.
3. Atur `ConfigurationType` bidang di `organization-configuration` objek ke`CENTRAL`. Tindakan ini memiliki dampak sebagai berikut:

   - Menetapkan akun panggilan sebagai administrator yang didelegasikan Security Hub di semua Wilayah yang ditautkan.
   - Mengaktifkan Security Hub di akun administrator yang didelegasikan di semua Wilayah tertaut.
   - Menetapkan akun panggilan sebagai administrator yang didelegasikan Security Hub untuk akun baru dan yang sudah ada yang menggunakan Security Hub dan milik organisasi. Ini terjadi di Wilayah asal dan semua Wilayah terkait. Akun panggilan ditetapkan sebagai administrator yang didelegasikan untuk akun organisasi baru hanya jika akun tersebut dikaitkan dengan kebijakan konfigurasi yang mengaktifkan Security Hub. Akun panggilan ditetapkan sebagai administrator yang didelegasikan untuk akun organisasi yang ada hanya jika mereka sudah mengaktifkan Security Hub.
   - Menetapkan opsi pengaktifan otomatis ke no-auto-enablesemua Wilayah yang ditautkan, dan disetel auto-enable-standardske Wilayah `NONE` beranda dan semua Wilayah yang ditautkan. Parameter ini tidak relevan di wilayah beranda dan terkait saat Anda menggunakan konfigurasi pusat, tetapi Anda dapat secara otomatis mengaktifkan Security Hub dan standar keamanan default di akun organisasi melalui penggunaan kebijakan konfigurasi.
4. Anda sekarang dapat menggunakan konfigurasi pusat. Administrator yang didelegasikan dapat membuat kebijakan konfigurasi untuk mengonfigurasi Security Hub di organisasi Anda. Untuk petunjuk cara membuat kebijakan konfigurasi, lihatMembuat dan mengaitkan kebijakan konfigurasi Security Hub.

Contoh perintah:

```
aws securityhub --region us-east-1 update-organization-configuration \
--no-auto-enable \
--organization-configuration '{"ConfigurationType": "CENTRAL"}'
```

Memilih jenis manajemen akun dan OU

Bila Anda menggunakan konfigurasi pusat, administrator yang AWS Security Hub didelegasikan dapat menetapkan setiap akun organisasi dan unit organisasi (OU) sebagai dikelola secara terpusat atau dikelola sendiri. Jenis manajemen akun atau OU menentukan bagaimana Anda dapat menentukan dan mengubah pengaturan Security Hub.

Akun yang dikelola sendiri atau OU dapat mengonfigurasi pengaturan Security Hub sendiri secara terpisah di masing-masing Wilayah AWS. Administrator yang didelegasikan tidak dapat mengonfigurasi setelan Security Hub untuk akun atau OU yang dikelola sendiri, dan kebijakan konfigurasi tidak dapat dikaitkan dengannya. Sebaliknya, hanya administrator yang didelegasikan yang dapat mengonfigurasi setelan Security Hub untuk akun dan OU yang dikelola secara terpusat di seluruh Wilayah asal dan Wilayah yang ditautkan. Kebijakan konfigurasi dapat dikaitkan dengan akun dan OU yang dikelola secara terpusat.

Administrator yang didelegasikan dapat mengalihkan status akun atau OU antara dikelola sendiri dan dikelola secara terpusat. Secara default, semua akun dan OU dikelola sendiri saat Anda memulai konfigurasi pusat melalui Security Hub API. Di konsol, jenis manajemen bergantung pada kebijakan konfigurasi pertama Anda. Akun dan OU yang Anda kaitkan dengan kebijakan pertama Anda dikelola secara terpusat. Akun lain dan OU dikelola sendiri secara default.

Jika Anda mengaitkan kebijakan konfigurasi dengan akun yang dikelola sendiri, kebijakan akan mengesampingkan penunjukan yang dikelola sendiri. Akun menjadi dikelola secara terpusat dan mengadopsi pengaturan yang tercermin dalam kebijakan konfigurasi.

Akun anak dan OU dapat mewarisi perilaku yang dikelola sendiri dari induk yang dikelola sendiri, dengan cara yang sama seperti akun anak dan OU dapat mewarisi kebijakan konfigurasi dari induk yang dikelola secara terpusat. Untuk informasi selengkapnya, lihat Asosiasi kebijakan melalui aplikasi dan warisan.

Akun yang dikelola sendiri atau OU tidak dapat mewarisi kebijakan konfigurasi dari node induk atau dari root. Misalnya, jika Anda ingin semua akun dan OU di organisasi Anda mewarisi kebijakan konfigurasi dari root, Anda harus mengubah jenis manajemen node yang dikelola sendiri menjadi dikelola secara terpusat.

Menentukan pengaturan untuk akun yang dikelola sendiri

Akun yang dikelola sendiri harus mengonfigurasi pengaturannya sendiri secara terpisah di setiap Wilayah.

Pemilik akun yang dikelola sendiri dapat menjalankan operasi Security Hub API berikut di setiap Wilayah untuk mengonfigurasi setelannya:

- `EnableSecurityHub`dan `DisableSecurityHub` untuk mengaktifkan atau menonaktifkan layanan Security Hub
- `BatchEnableStandards`dan `BatchDisableStandards` untuk mengaktifkan atau menonaktifkan standar
- `BatchUpdateStandardsControlAssociations`atau `UpdateStandardsControl` untuk mengaktifkan atau menonaktifkan kontrol

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

Untuk deskripsi tindakan Security Hub API, lihat Referensi AWS Security Hub API.

Akun yang dikelola sendiri juga dapat menggunakan konsol Security Hub atau AWS CLI untuk mengonfigurasi pengaturannya di setiap Wilayah.

Akun yang dikelola sendiri tidak dapat menjalankan API apa pun yang terkait dengan kebijakan konfigurasi dan asosiasi kebijakan Security Hub. Hanya administrator yang didelegasikan yang dapat memanggil API konfigurasi pusat dan menggunakan kebijakan konfigurasi untuk mengonfigurasi akun yang dikelola secara terpusat.

Memilih jenis manajemen akun dan OU

Pilih metode pilihan Anda, dan ikuti langkah-langkah untuk menetapkan akun atau OU sebagai dikelola secara terpusat atau dikelola sendiri.

Security Hub console

Untuk memilih jenis manajemen akun atau OU

1. Buka AWS Security Hub konsol di https://console.aws.amazon.com/securityhub/.

Masuk menggunakan kredensional akun administrator yang didelegasikan Security Hub di Wilayah beranda.

2. Pilih Konfigurasi.
3. Pada tab Organisasi, pilih akun target atau OU. Pilih Edit.
4. Pada halaman Tentukan konfigurasi, untuk tipe Manajemen, pilih Dikelola secara terpusat jika Anda ingin administrator yang didelegasikan mengonfigurasi akun target atau OU. Kemudian, pilih Terapkan kebijakan tertentu jika Anda ingin mengaitkan kebijakan konfigurasi yang ada dengan target. Pilih Mewarisi dari organisasi saya jika Anda ingin target mewarisi konfigurasi induk terdekatnya. Pilih Self-managed jika Anda ingin akun atau OU untuk mengkonfigurasi pengaturan sendiri.
5. Pilih Selanjutnya. Tinjau perubahan Anda, dan pilih Simpan.

Security Hub API

Untuk memilih jenis manajemen akun atau OU

1. Memanggil StartConfigurationPolicyAssociationAPI dari akun administrator yang didelegasikan Security Hub di Wilayah beranda.
2. Untuk `ConfigurationPolicyIdentifier` bidang ini, berikan `SELF_MANAGED_SECURITY_HUB` jika Anda ingin akun atau OU mengontrol pengaturannya sendiri. Berikan Nama Sumber Daya Amazon (ARN) atau ID kebijakan konfigurasi yang relevan jika Anda ingin administrator yang didelegasikan mengontrol pengaturan untuk akun atau OU.
3. Untuk `Target` bidang, berikan Akun AWS ID, ID OU, atau ID root target yang tipe manajemennya ingin Anda ubah. Ini mengaitkan perilaku yang dikelola sendiri atau kebijakan konfigurasi tertentu dengan target. Akun anak dari target dapat mewarisi kebijakan perilaku atau konfigurasi yang dikelola sendiri.

Contoh permintaan API untuk menunjuk akun yang dikelola sendiri:

```
{
    "ConfigurationPolicyIdentifier": "SELF_MANAGED_SECURITY_HUB",
    "Target": {"AccountId": "123456789012"}
}
```

AWS CLI

Untuk memilih jenis manajemen akun atau OU

1. Jalankan start-configuration-policy-associationperintah dari akun administrator yang didelegasikan Security Hub di Wilayah rumah.
2. Untuk `configuration-policy-identifier` bidang, berikan `SELF_MANAGED_SECURITY_HUB` jika Anda ingin akun atau OU mengontrol pengaturannya sendiri. Berikan Nama Sumber Daya Amazon (ARN) atau ID kebijakan konfigurasi yang relevan jika Anda ingin administrator yang didelegasikan untuk mengontrol pengaturan untuk akun atau OU..
3. Untuk `target` bidang, berikan Akun AWS ID, ID OU, atau ID root target yang tipe manajemennya ingin Anda ubah. Ini mengaitkan perilaku yang dikelola sendiri atau kebijakan konfigurasi tertentu dengan target. Akun anak dari target dapat mewarisi kebijakan perilaku atau konfigurasi yang dikelola sendiri.

Contoh perintah untuk menunjuk akun yang dikelola sendiri:

```
aws securityhub --region us-east-1 start-configuration-policy-association \
--configuration-policy-identifier "SELF_MANAGED_SECURITY_HUB" \
--target '{"AccountId": "123456789012"}'
```

Cara kerja kebijakan konfigurasi Security Hub

Akun administrator yang didelegasikan dapat membuat kebijakan AWS Security Hub konfigurasi untuk mengonfigurasi Security Hub, standar keamanan, dan kontrol keamanan di organisasi Anda. Setelah membuat kebijakan konfigurasi, administrator yang didelegasikan dapat mengaitkannya dengan akun, unit organisasi (OU), atau root. Administrator yang didelegasikan juga dapat melihat, mengedit, atau menghapus kebijakan konfigurasi.

Pertimbangan kebijakan

Sebelum Anda membuat kebijakan konfigurasi di Security Hub, pertimbangkan detail berikut.

- Kebijakan konfigurasi harus dikaitkan agar berlaku — Setelah membuat kebijakan konfigurasi, Anda dapat mengaitkannya dengan satu atau beberapa akun, unit organisasi (OU), atau root.

Kebijakan konfigurasi dapat dikaitkan dengan akun atau OU melalui aplikasi langsung, atau melalui warisan dari OU induk.

- Akun atau OU hanya dapat dikaitkan dengan satu kebijakan konfigurasi — Untuk mencegah pengaturan yang bertentangan, akun atau OU hanya dapat dikaitkan dengan satu kebijakan konfigurasi pada waktu tertentu. Atau, akun atau OU dapat dikelola sendiri.
- Kebijakan konfigurasi selesai — Kebijakan konfigurasi menyediakan spesifikasi pengaturan yang lengkap. Misalnya, akun anak tidak dapat menerima pengaturan untuk beberapa kontrol dari satu kebijakan dan pengaturan untuk kontrol lain dari kebijakan lain. Saat Anda mengaitkan kebijakan dengan akun anak, pastikan kebijakan tersebut menentukan semua setelan yang ingin digunakan oleh akun anak tersebut.
- Kebijakan konfigurasi tidak dapat dikembalikan — Tidak ada opsi untuk mengembalikan kebijakan konfigurasi setelah Anda mengaitkannya dengan akun atau OU. Misalnya, jika Anda mengaitkan kebijakan konfigurasi yang menonaktifkan CloudWatch kontrol dengan akun tertentu, lalu memisahkan kebijakan tersebut, CloudWatch kontrol akan terus dinonaktifkan di akun tersebut. Untuk mengaktifkan CloudWatch kontrol lagi, Anda dapat mengaitkan akun dengan kebijakan baru yang memungkinkan kontrol. Atau, Anda dapat mengubah akun menjadi dikelola sendiri dan mengaktifkan setiap CloudWatch kontrol di akun.
- Kebijakan konfigurasi berlaku di Wilayah asal Anda dan semua Wilayah tertaut — Kebijakan konfigurasi memengaruhi semua akun terkait di Wilayah asal dan semua Wilayah yang ditautkan. Anda tidak dapat membuat kebijakan konfigurasi yang berlaku hanya di beberapa Wilayah ini dan bukan yang lain. Pengecualian untuk ini adalah kontrol yang melibatkan sumber daya global.

  Wilayah yang AWS diperkenalkan pada atau setelah 20 Maret 2019 dikenal sebagai Wilayah opt-in. Anda harus mengaktifkan Wilayah tersebut untuk akun sebelum kebijakan konfigurasi berlaku di sana. Akun manajemen Organisasi dapat mengaktifkan Wilayah keikutsertaan untuk akun anggota. Untuk petunjuk tentang mengaktifkan Wilayah keikutsertaan, lihat Menentukan Wilayah AWS akun mana yang dapat digunakan dalam Panduan Referensi Manajemen AWS Akun.

  Jika kebijakan Anda mengonfigurasi kontrol yang tidak tersedia di Wilayah beranda atau satu atau beberapa Wilayah tertaut, Security Hub akan melewatkan konfigurasi kontrol di Wilayah yang tidak tersedia, tetapi menerapkan konfigurasi di Wilayah tempat kontrol tersedia.
- Kebijakan konfigurasi adalah sumber daya — Sebagai sumber daya, kebijakan konfigurasi memiliki Nama Sumber Daya Amazon (ARN) dan pengenal unik universal (UUID). ARN menggunakan format berikut:. `arn:`*`partition:`*`securityhub:`*`region`*`:`*`delegated administrator account ID`*`:configuration-policy/`*`configuration policy UUID` Konfigurasi yang

dikelola sendiri tidak memiliki ARN atau UUID. Pengidentifikasi untuk konfigurasi yang dikelola sendiri adalah. `SELF_MANAGED_SECURITY_HUB`

Jenis kebijakan konfigurasi

Setiap kebijakan konfigurasi menentukan pengaturan berikut:

- Aktifkan atau nonaktifkan Security Hub.
- Aktifkan satu atau lebih standar keamanan.
- Tunjukkan kontrol keamanan mana yang diaktifkan di seluruh standar yang diaktifkan. Anda dapat melakukannya dengan memberikan daftar kontrol khusus yang harus diaktifkan, dan Security Hub menonaktifkan semua kontrol lainnya, termasuk kontrol baru saat dirilis. Atau, Anda dapat memberikan daftar kontrol khusus yang harus dinonaktifkan, dan Security Hub mengaktifkan semua kontrol lainnya, termasuk kontrol baru saat dirilis.
- Secara opsional, sesuaikan parameter untuk memilih kontrol yang diaktifkan di seluruh standar yang diaktifkan.

Kebijakan konfigurasi pusat tidak menyertakan pengaturan AWS Config perekam. Anda harus mengaktifkan AWS Config dan mengaktifkan perekaman secara terpisah untuk sumber daya yang diperlukan agar Security Hub menghasilkan temuan kontrol. Untuk informasi selengkapnya, lihat Mengkonfigurasi AWS Config.

Jika Anda menggunakan konfigurasi pusat, Security Hub secara otomatis menonaktifkan kontrol yang melibatkan sumber daya global di semua Wilayah kecuali Wilayah asal. Kontrol lain yang Anda pilih untuk diaktifkan meskipun kebijakan konfigurasi diaktifkan di semua Wilayah yang tersedia. Untuk membatasi temuan untuk kontrol ini hanya pada satu Wilayah, Anda dapat memperbarui pengaturan AWS Config perekam dan menonaktifkan perekaman sumber daya global di semua Wilayah kecuali Wilayah asal. Saat Anda menggunakan konfigurasi pusat, Anda tidak memiliki cakupan untuk kontrol yang tidak tersedia di Wilayah asal dan Wilayah yang ditautkan. Untuk daftar kontrol yang melibatkan sumber daya global, lihatKontrol yang berhubungan dengan sumber daya global.

Kebijakan konfigurasi yang disarankan

Saat membuat kebijakan konfigurasi untuk pertama kalinya di konsol Security Hub, Anda memiliki opsi untuk memilih kebijakan yang direkomendasikan Security Hub.

Kebijakan yang direkomendasikan memungkinkan Security Hub, standar AWS Foundational Security Best Practices (FSBP), dan semua kontrol FSBP yang ada dan yang baru. Kontrol yang menerima parameter menggunakan nilai default. Kebijakan yang disarankan berlaku untuk root (semua akun dan OU, baik yang baru maupun yang sudah ada). Setelah membuat kebijakan yang disarankan untuk organisasi, Anda dapat memodifikasinya dari akun administrator yang didelegasikan. Misalnya, Anda dapat mengaktifkan standar atau kontrol tambahan atau menonaktifkan kontrol FSBP tertentu. Untuk petunjuk tentang memodifikasi kebijakan konfigurasi, lihatMemperbarui kebijakan konfigurasi Security Hub.

Kebijakan konfigurasi khusus

Alih-alih kebijakan yang disarankan, administrator yang didelegasikan dapat membuat hingga 20 kebijakan konfigurasi kustom. Anda dapat mengaitkan satu kebijakan kustom dengan seluruh organisasi atau kebijakan kustom yang berbeda dengan akun dan OU yang berbeda. Untuk kebijakan konfigurasi kustom, Anda menentukan pengaturan yang diinginkan. Misalnya, Anda dapat membuat kebijakan khusus yang memungkinkan FSBP, Tolok Ukur AWS Yayasan Center for Internet Security (CIS) v1.4.0, dan semua kontrol dalam standar tersebut kecuali kontrol Amazon Redshift. Tingkat perincian yang Anda gunakan dalam kebijakan konfigurasi khusus bergantung pada cakupan cakupan keamanan yang dimaksudkan di seluruh organisasi Anda.

> **Note**
>
> Anda tidak dapat mengaitkan kebijakan konfigurasi yang menonaktifkan Security Hub dengan akun administrator yang didelegasikan. Kebijakan semacam itu dapat dikaitkan dengan akun lain tetapi melewatkan asosiasi dengan administrator yang didelegasikan. Akun administrator yang didelegasikan mempertahankan konfigurasi saat ini.

Setelah membuat kebijakan konfigurasi kustom, Anda dapat beralih ke kebijakan konfigurasi yang disarankan dengan memperbarui kebijakan konfigurasi untuk mencerminkan konfigurasi yang disarankan. Namun, Anda tidak melihat pilihan untuk membuat kebijakan konfigurasi yang disarankan di konsol Security Hub setelah kebijakan pertama Anda dibuat.

Asosiasi kebijakan melalui aplikasi dan warisan

Saat Anda pertama kali ikut serta dalam konfigurasi pusat, organisasi Anda tidak memiliki asosiasi dan berperilaku dengan cara yang sama seperti sebelum ikut serta. Administrator yang didelegasikan

kemudian dapat membuat asosiasi antara kebijakan konfigurasi atau perilaku dan akun yang dikelola sendiri, OU, atau root. Asosiasi dapat dibentuk melalui aplikasi atau warisan.

Dari akun administrator yang didelegasikan, Anda dapat langsung menerapkan kebijakan konfigurasi ke akun, OU, atau root. Atau, administrator yang didelegasikan dapat langsung menerapkan penunjukan yang dikelola sendiri ke akun, OU, atau root.

Dengan tidak adanya aplikasi langsung, akun atau OU mewarisi pengaturan induk terdekat yang memiliki kebijakan konfigurasi atau perilaku yang dikelola sendiri. Jika induk terdekat dikaitkan dengan kebijakan konfigurasi, anak mewarisi kebijakan tersebut dan hanya dapat dikonfigurasi oleh administrator yang didelegasikan dari Wilayah beranda. Jika orang tua terdekat dikelola sendiri, anak mewarisi perilaku yang dikelola sendiri dan memiliki kemampuan untuk menentukan pengaturannya sendiri di masing-masing. Wilayah AWS

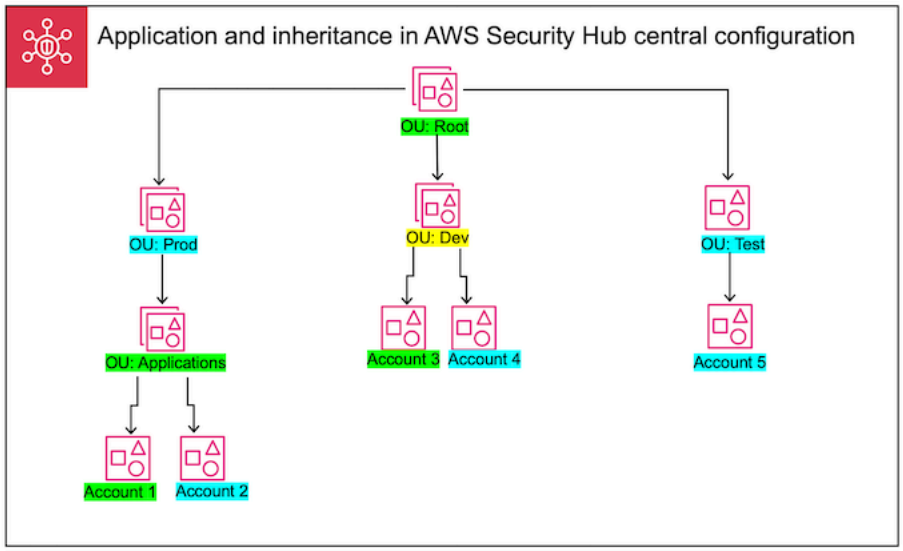
Aplikasi lebih diutamakan daripada warisan. Dengan kata lain, pewarisan tidak mengesampingkan kebijakan konfigurasi atau penunjukan yang dikelola sendiri yang telah diterapkan langsung oleh administrator yang didelegasikan ke akun atau OU.

Jika Anda langsung menerapkan kebijakan konfigurasi ke akun yang dikelola sendiri, kebijakan akan mengganti penunjukan yang dikelola sendiri. Akun menjadi dikelola secara terpusat dan mengadopsi pengaturan yang tercermin dalam kebijakan konfigurasi.

Kami merekomendasikan langsung menerapkan kebijakan konfigurasi ke root. Jika Anda menerapkan kebijakan ke root, maka akun baru yang bergabung dengan organisasi Anda akan secara otomatis mewarisi kebijakan root kecuali Anda mengaitkannya dengan kebijakan yang berbeda atau menunjuknya sebagai dikelola sendiri.

Hanya satu kebijakan konfigurasi yang dapat dikaitkan dengan akun atau OU pada waktu tertentu, baik melalui aplikasi atau warisan. Ini dirancang untuk mencegah pengaturan yang bertentangan.

Diagram berikut menggambarkan bagaimana aplikasi kebijakan dan pewarisan bekerja dalam konfigurasi pusat.



Dalam contoh ini, node yang disorot dengan warna hijau memiliki kebijakan konfigurasi yang telah diterapkan padanya. Node yang disorot dengan warna biru tidak memiliki kebijakan konfigurasi yang telah diterapkan padanya. Sebuah node yang disorot dengan warna kuning telah ditetapkan sebagai self-managed. Setiap akun dan OU menggunakan konfigurasi berikut:

- OU:root (Green) - OU ini menggunakan kebijakan konfigurasi yang telah diterapkan padanya.
- OU:prod (Blue) - OU ini mewarisi kebijakan konfigurasi dari ou:Root.
- OU: Aplikasi (Hijau) - OU ini menggunakan kebijakan konfigurasi yang telah diterapkan padanya.
- Akun 1 (Hijau) — Akun ini menggunakan kebijakan konfigurasi yang telah diterapkan padanya.
- Akun 2 (Biru) — Akun ini mewarisi kebijakan konfigurasi dari OU: Aplikasi.
- OU: dev (Kuning) - OU ini dikelola sendiri.
- Akun 3 (Hijau) — Akun ini menggunakan kebijakan konfigurasi yang telah diterapkan padanya.
- Akun 4 (Biru) — Akun ini mewarisi perilaku yang dikelola sendiri dari OU: dev.
- OU:test (Biru) - Akun ini mewarisi kebijakan konfigurasi dari OU:root.
- Akun 5 (Biru) — Akun ini mewarisi kebijakan konfigurasi dari OU:root karena induk langsungnya, ou:Test, tidak terkait dengan kebijakan konfigurasi.

Menguji kebijakan konfigurasi

Untuk menguji efek kebijakan konfigurasi, Anda dapat mengaitkannya dengan satu akun atau OU sebelum mengaitkannya secara lebih luas di seluruh organisasi Anda.

Untuk menguji kebijakan konfigurasi

1. Buat kebijakan konfigurasi khusus, tetapi jangan menerapkannya ke akun apa pun. Verifikasi bahwa pengaturan yang ditentukan untuk pemberdayaan, standar, dan kontrol Security Hub sudah benar.
2. Terapkan kebijakan konfigurasi ke akun pengujian atau OU yang tidak memiliki akun anak atau OU.
3. Verifikasi bahwa akun pengujian atau OU menggunakan kebijakan konfigurasi dengan cara yang diharapkan di Wilayah asal Anda dan semua Wilayah yang ditautkan. Anda juga dapat memverifikasi bahwa semua akun dan OU lain di organisasi Anda tetap dikelola sendiri dan dapat mengubah pengaturan mereka sendiri di setiap Wilayah.

Setelah menguji kebijakan konfigurasi dalam satu akun atau OU, Anda dapat mengaitkannya dengan akun lain dan OU. Untuk petunjuk tentang pembuatan dan asosiasi kebijakan, lihatMembuat dan mengaitkan kebijakan konfigurasi Security Hub. Anak-anak dari akun yang diterapkan mewarisi kebijakan kecuali mereka dikelola sendiri atau kebijakan konfigurasi yang berbeda berlaku untuk mereka. Anda juga dapat mengedit kebijakan konfigurasi dan membuat kebijakan konfigurasi tambahan jika diperlukan.

Membuat dan mengaitkan kebijakan konfigurasi Security Hub

Akun administrator yang didelegasikan dapat membuat kebijakan AWS Security Hub konfigurasi dan mengaitkannya dengan akun organisasi, unit organisasi (OU), atau root. Anda juga dapat mengaitkan konfigurasi yang dikelola sendiri dengan akun, OU, atau root.

Jika ini adalah pertama kalinya Anda membuat kebijakan konfigurasi, sebaiknya Cara kerja kebijakan konfigurasi Security Hub tinjau terlebih dahulu.

Pilih metode akses pilihan Anda, dan ikuti langkah-langkah untuk membuat dan mengaitkan kebijakan konfigurasi atau konfigurasi yang dikelola sendiri. Saat menggunakan konsol Security Hub, Anda dapat mengaitkan konfigurasi dengan beberapa akun atau OU secara bersamaan. Saat menggunakan Security Hub API atau AWS CLI, Anda dapat mengaitkan konfigurasi hanya dengan satu akun atau OU di setiap permintaan.

> **Note**
>
> Jika Anda menggunakan konfigurasi pusat, Security Hub secara otomatis menonaktifkan kontrol yang melibatkan sumber daya global di semua Wilayah kecuali Wilayah asal. Kontrol

lain yang Anda pilih untuk diaktifkan meskipun kebijakan konfigurasi diaktifkan di semua Wilayah yang tersedia. Untuk membatasi temuan untuk kontrol ini hanya pada satu Wilayah, Anda dapat memperbarui pengaturan AWS Config perekam dan menonaktifkan perekaman sumber daya global di semua Wilayah kecuali Wilayah asal. Saat Anda menggunakan konfigurasi pusat, Anda tidak memiliki cakupan untuk kontrol yang tidak tersedia di Wilayah asal dan Wilayah yang ditautkan. Untuk daftar kontrol yang melibatkan sumber daya global, lihatKontrol yang berhubungan dengan sumber daya global.

Security Hub console

Untuk membuat dan mengaitkan kebijakan konfigurasi

1. Buka AWS Security Hub konsol di https://console.aws.amazon.com/securityhub/.

   Masuk menggunakan kredensional akun administrator yang didelegasikan Security Hub di Wilayah beranda.
2. Di panel navigasi, pilih Konfigurasi dan tab Kebijakan. Kemudian, pilih Buat kebijakan.
3. Pada halaman Konfigurasi organisasi, jika ini adalah pertama kalinya Anda membuat kebijakan konfigurasi, Anda akan melihat tiga opsi di bawah Jenis konfigurasi. Jika Anda telah membuat setidaknya satu kebijakan konfigurasi, Anda hanya melihat opsi Kebijakan kustom.

   - Pilih Gunakan konfigurasi Security Hub yang AWS direkomendasikan di seluruh organisasi saya untuk menggunakan kebijakan yang kami rekomendasikan. Kebijakan yang direkomendasikan memungkinkan Security Hub di semua akun organisasi, mengaktifkan standar Praktik Terbaik Keamanan AWS Dasar (FSBP), dan memungkinkan semua kontrol FSBP baru dan yang sudah ada. Kontrol menggunakan nilai parameter default.
   - Pilih Saya belum siap untuk mengonfigurasi untuk membuat kebijakan konfigurasi nanti.
   - Pilih Kebijakan khusus untuk membuat kebijakan konfigurasi kustom. Tentukan apakah akan mengaktifkan atau menonaktifkan Security Hub, standar mana yang akan diaktifkan, dan kontrol mana yang akan diaktifkan di seluruh standar tersebut. Secara opsional, tentukan nilai parameter khusus untuk satu atau beberapa kontrol yang diaktifkan yang mendukung parameter kustom.
4. Di bagian Akun, pilih akun target, OU, atau root yang Anda inginkan untuk diterapkan oleh kebijakan konfigurasi Anda.

- Pilih Semua akun jika Anda ingin menerapkan kebijakan konfigurasi ke root. Ini termasuk semua akun dan OU di organisasi yang tidak memiliki kebijakan lain yang diterapkan atau diwariskan.
- Pilih Akun khusus jika Anda ingin menerapkan kebijakan konfigurasi ke akun atau OU tertentu. Masukkan ID akun, atau pilih akun dan OU dari struktur organisasi. Anda dapat menerapkan kebijakan ke maksimal 15 target (akun, OU, atau root) saat Anda membuatnya. Untuk menentukan angka yang lebih besar, edit kebijakan Anda setelah dibuat, dan terapkan ke target tambahan.
- Pilih Administrator yang didelegasikan hanya untuk menerapkan kebijakan konfigurasi ke akun administrator yang didelegasikan saat ini.

5. Pilih Selanjutnya.
6. Pada halaman Tinjau dan terapkan, tinjau detail kebijakan konfigurasi Anda. Kemudian, pilih Buat kebijakan dan terapkan. Di Wilayah beranda dan Wilayah tertaut, tindakan ini mengesampingkan setelan konfigurasi akun yang ada yang terkait dengan kebijakan konfigurasi ini. Akun dapat dikaitkan dengan kebijakan konfigurasi melalui aplikasi, atau warisan dari node induk. Akun turunan dan OU dari target yang diterapkan akan secara otomatis mewarisi kebijakan konfigurasi ini kecuali secara khusus dikecualikan, dikelola sendiri, atau menggunakan kebijakan konfigurasi yang berbeda.

Security Hub API

Untuk membuat dan mengaitkan kebijakan konfigurasi

1. Memanggil CreateConfigurationPolicyAPI dari akun administrator yang didelegasikan Security Hub di Wilayah beranda.
2. Untuk`Name`, berikan nama unik untuk kebijakan konfigurasi. Secara opsional, untuk`Description`, berikan deskripsi untuk kebijakan konfigurasi.
3. Untuk `ServiceEnabled` bidang, tentukan apakah Anda ingin Security Hub diaktifkan atau dinonaktifkan dalam kebijakan konfigurasi ini.
4. Untuk `EnabledStandardIdentifiers` bidang, tentukan standar Security Hub mana yang ingin Anda aktifkan dalam kebijakan konfigurasi ini.
5. Untuk `SecurityControlsConfiguration` objek, tentukan kontrol mana yang ingin Anda aktifkan atau nonaktifkan dalam kebijakan konfigurasi ini. Memilih `EnabledSecurityControlIdentifiers` berarti bahwa kontrol yang ditentukan

diaktifkan. Kontrol lain yang merupakan bagian dari standar Anda yang diaktifkan (termasuk kontrol yang baru dirilis) dinonaktifkan. Memilih `DisabledSecurityControlIdentifiers` berarti bahwa kontrol yang ditentukan dinonaktifkan. Kontrol lain yang merupakan bagian dari standar Anda yang diaktifkan (termasuk kontrol yang baru dirilis) diaktifkan.

6. Secara opsional, untuk `SecurityControlCustomParameters` bidang, tentukan kontrol yang diaktifkan yang ingin Anda sesuaikan parameternya. Berikan `CUSTOM` `ValueType` bidang dan nilai parameter khusus untuk `Value` bidang tersebut. Nilai harus tipe data yang benar dan dalam rentang valid yang ditentukan oleh Security Hub. Hanya kontrol pilih yang mendukung nilai parameter khusus. Untuk informasi selengkapnya, lihat Parameter kontrol khusus.
7. Untuk menerapkan kebijakan konfigurasi Anda ke akun atau OU, panggil StartConfigurationPolicyAssociationAPI dari akun administrator yang didelegasikan Security Hub di Wilayah beranda.
8. Untuk `ConfigurationPolicyIdentifier` bidang ini, berikan Nama Sumber Daya Amazon (ARN) atau pengenal unik universal (UUID) kebijakan. ARN dan UUID dikembalikan oleh API. `CreateConfigurationPolicy` Untuk konfigurasi yang dikelola sendiri, `ConfigurationPolicyIdentifier` bidangnya sama dengan`SELF_MANAGED_SECURITY_HUB`.
9. Untuk `Target` bidang, berikan OU, akun, atau ID root yang Anda inginkan untuk menerapkan kebijakan konfigurasi ini. Anda hanya dapat memberikan satu target di setiap permintaan API. Akun turunan dan OU dari target yang dipilih akan secara otomatis mewarisi kebijakan konfigurasi ini kecuali mereka dikelola sendiri atau menggunakan kebijakan konfigurasi yang berbeda.

Contoh permintaan API untuk membuat kebijakan konfigurasi:

```
{
    "Name": "SampleConfigurationPolicy",
    "Description": "Configuration policy for production accounts",
    "ConfigurationPolicy": {
        "SecurityHub": {
             "ServiceEnabled": true,
             "EnabledStandardIdentifiers": [
                    "arn:aws:securityhub:us-east-1::standards/aws-foundational-
security-best-practices/v/1.0.0",
                    "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0"
```

```
                ],
            "SecurityControlsConfiguration": {
                "DisabledSecurityControlIdentifiers": [
                    "CloudTrail.2"
                ],
                "SecurityControlCustomParameters": [
                    {
                        "SecurityControlId": "ACM.1",
                        "Parameters": {
                            "daysToExpiration": {
                                "ValueType": "CUSTOM",
                                "Value": {
                                    "Integer": 15
                                }
                            }
                        }
                    }
                ]
            }
        }
    }
}
```

Contoh permintaan API untuk mengaitkan kebijakan konfigurasi:

```
{
    "ConfigurationPolicyIdentifier": "arn:aws:securityhub:us-
east-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "Target": {"OrganizationalUnitId": "ou-examplerootid111-exampleouid111"}
}
```

AWS CLI

Untuk membuat dan mengaitkan kebijakan konfigurasi

1. Jalankan create-configuration-policyperintah dari akun administrator yang didelegasikan Security Hub di wilayah rumah.
2. Untuk`name`, berikan nama unik untuk kebijakan konfigurasi. Secara opsional, untuk`description`, berikan deskripsi untuk kebijakan konfigurasi.

3. Untuk `ServiceEnabled` bidang, tentukan apakah Anda ingin Security Hub diaktifkan atau dinonaktifkan dalam kebijakan konfigurasi ini.
4. Untuk `EnabledStandardIdentifiers` bidang, tentukan standar Security Hub mana yang ingin Anda aktifkan dalam kebijakan konfigurasi ini.
5. Untuk `SecurityControlsConfiguration` bidang, tentukan kontrol mana yang ingin Anda aktifkan atau nonaktifkan dalam kebijakan konfigurasi ini. Memilih `EnabledSecurityControlIdentifiers` berarti bahwa kontrol yang ditentukan diaktifkan. Kontrol lain yang merupakan bagian dari standar Anda yang diaktifkan (termasuk kontrol yang baru dirilis) dinonaktifkan. Memilih `DisabledSecurityControlIdentifiers` berarti bahwa kontrol yang ditentukan dinonaktifkan. Kontrol lain yang berlaku untuk standar Anda yang diaktifkan (termasuk kontrol yang baru dirilis) diaktifkan.
6. Secara opsional, untuk `SecurityControlCustomParameters` bidang, tentukan kontrol yang diaktifkan yang ingin Anda sesuaikan parameternya. Berikan `CUSTOM` `ValueType` bidang dan nilai parameter khusus untuk `Value` bidang tersebut. Nilai harus tipe data yang benar dan dalam rentang valid yang ditentukan oleh Security Hub. Hanya kontrol pilih yang mendukung nilai parameter khusus. Untuk informasi selengkapnya, lihat Parameter kontrol khusus.
7. Untuk menerapkan kebijakan konfigurasi ke akun atau OU, jalankan start-configuration-policy-associationperintah dari akun administrator yang didelegasikan Security Hub di Wilayah beranda.
8. Untuk `configuration-policy-identifier` bidang, berikan Nama Sumber Daya Amazon (ARN) atau ID kebijakan konfigurasi. ARN dan ID ini dikembalikan oleh perintah. `create-configuration-policy`
9. Untuk `target` bidang, berikan OU, akun, atau ID root yang Anda inginkan untuk menerapkan kebijakan konfigurasi ini. Anda hanya dapat memberikan satu target setiap kali Anda menjalankan perintah. Anak-anak dari target yang dipilih akan secara otomatis mewarisi kebijakan konfigurasi ini kecuali mereka dikelola sendiri atau menggunakan kebijakan konfigurasi yang berbeda.

Contoh perintah untuk membuat kebijakan konfigurasi:

```
aws securityhub --region us-east-1 create-configuration-policy \
--name "SampleConfigurationPolicy" \
--description "Configuration policy for production accounts" \
--configuration-policy '{"SecurityHub": {"ServiceEnabled": true,
 "EnabledStandardIdentifiers": ["arn:aws:securityhub:us-east-1::standards/aws-
```

```
foundational-security-best-practices/v/1.0.0","arn:aws:securityhub:::ruleset/
cis-aws-foundations-benchmark/v/1.2.0"],"SecurityControlsConfiguration":
{"DisabledSecurityControlIdentifiers": ["CloudTrail.2"],
 "SecurityControlCustomParameters": [{"SecurityControlId": "ACM.1", "Parameters":
 {"daysToExpiration": {"ValueType": "CUSTOM", "Value": {"Integer": 15}}}}]}}'
```

Contoh perintah untuk mengaitkan kebijakan konfigurasi:

```
aws securityhub --region us-east-1 start-configuration-policy-association \
--configuration-policy-identifier "arn:aws:securityhub:us-
east-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111" \
--target '{"OrganizationalUnitId": "ou-examplerootid111-exampleouid111"}'
```

`StartConfigurationPolicyAssociation`API mengembalikan bidang yang disebut`AssociationStatus`. Bidang ini memberi tahu Anda apakah asosiasi kebijakan sedang tertunda atau dalam keadaan berhasil atau gagal. Diperlukan waktu hingga 24 jam agar status berubah dari `PENDING` ke `SUCCESS` atau`FAILURE`. Untuk informasi selengkapnya tentang status asosiasi, lihatStatus asosiasi konfigurasi.

Melihat kebijakan konfigurasi Security Hub

Akun administrator yang didelegasikan dapat melihat kebijakan AWS Security Hub konfigurasi untuk organisasi dan detailnya.

Pilih metode pilihan Anda, dan ikuti langkah-langkah untuk melihat kebijakan konfigurasi Anda.

Console

Untuk melihat kebijakan konfigurasi

1. Buka AWS Security Hub konsol di https://console.aws.amazon.com/securityhub/.

   Masuk menggunakan kredensional akun administrator yang didelegasikan Security Hub di Wilayah beranda.
2. Di panel navigasi, pilih Pengaturan dan Konfigurasi.
3. Pilih tab Kebijakan untuk melihat ikhtisar kebijakan konfigurasi Anda.

4. Pilih kebijakan konfigurasi, dan pilih Lihat detail untuk melihat detail tambahan tentangnya.

API

Untuk melihat kebijakan konfigurasi

Untuk melihat daftar ringkasan semua kebijakan konfigurasi Anda, panggil `ListConfigurationPolicies`API dari akun administrator yang didelegasikan Security Hub di Wilayah rumah Anda. Anda dapat memberikan parameter pagination opsional

Contoh permintaan API:

```
{
    "MaxResults": 5,
    "NextToken": "U2FsdGVkX19nUI2zoh+Pou9YyutlYJHWpn9xnG4hqSOhvw3o2JqjI23QDxdf"
}
```

Untuk melihat detail tentang kebijakan konfigurasi tertentu, panggil `GetConfigurationPolicy`API dari akun administrator yang didelegasikan Security Hub di Wilayah rumah Anda. Berikan Nama Sumber Daya Amazon (ARN) atau ID kebijakan konfigurasi yang detailnya ingin Anda lihat.

Contoh permintaan API:

```
{
    "Identifier": "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
}
```

Untuk melihat daftar ringkasan semua kebijakan konfigurasi Anda dan asosiasinya, panggil `ListConfigurationPolicyAssociations`API dari akun administrator yang didelegasikan Security Hub di Wilayah asal Anda. Secara opsional, Anda dapat memberikan parameter pagination atau memfilter hasil berdasarkan ID kebijakan tertentu, jenis asosiasi, atau status asosiasi.

Contoh permintaan API:

```
{
```

```
    "AssociationType": "APPLIED"
}
```

Untuk melihat asosiasi untuk akun tertentu, OU, atau root, panggil [GetConfigurationPolicyAssociation](#)atau [BatchGetConfigurationPolicyAssociations](#)API dari akun administrator yang didelegasikan Security Hub di Wilayah asal Anda. Untuk`Target`, berikan nomor akun, ID OU, atau ID root.

```
{
    "Target": {"AccountId": "123456789012"}
}
```

AWS CLI

Untuk melihat kebijakan konfigurasi

Untuk melihat daftar ringkasan semua kebijakan konfigurasi Anda, jalankan [list-configuration-policies](#)perintah dari akun administrator yang didelegasikan Security Hub di Wilayah rumah Anda.

Contoh perintah:

```
aws securityhub --region us-east-1 list-configuration-policies \
--max-items 5 \
--starting-token U2FsdGVkX19nUI2zoh+Pou9YyutlYJHWpn9xnG4hqSOhvw3o2JqjI23QDxdf
```

Untuk melihat detail tentang kebijakan konfigurasi tertentu, jalankan [get-configuration-policy](#)perintah dari akun administrator yang didelegasikan Security Hub di Wilayah rumah Anda. Berikan Nama Sumber Daya Amazon (ARN) atau ID kebijakan konfigurasi yang detailnya ingin Anda lihat.

```
aws securityhub --region us-east-1 get-configuration-policy \
--identifier "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

Untuk melihat daftar ringkasan semua kebijakan konfigurasi Anda dan asosiasi akunnya, jalankan `list-configuration-policy-associations`perintah dari akun administrator yang didelegasikan Security Hub di Wilayah rumah Anda. Secara opsional, Anda dapat memberikan parameter pagination atau memfilter hasil berdasarkan ID kebijakan tertentu, jenis asosiasi, atau status asosiasi.

```
aws securityhub --region us-east-1 list-configuration-policy-associations \
--association-type "APPLIED"
```

Untuk melihat asosiasi untuk akun tertentu, jalankan `batch-get-configuration-policy-associations`perintah `get-configuration-policy-association`atau dari akun administrator yang didelegasikan Security Hub di Wilayah rumah Anda. Untuk`target`, berikan nomor akun, ID OU, atau ID root.

```
aws securityhub --region us-east-1 get-configuration-policy-association \
--target '{"AccountId": "123456789012"}'
```

Status asosiasi konfigurasi

Operasi API konfigurasi pusat berikut mengembalikan bidang yang disebut`AssociationStatus`:

- `BatchGetConfigurationPolicyAssociations`
- `GetConfigurationPolicyAssociation`
- `ListConfigurationPolicyAssociations`
- `StartConfigurationPolicyAssociation`

Bidang ini dikembalikan baik ketika konfigurasi yang mendasarinya adalah kebijakan konfigurasi dan ketika itu adalah perilaku yang dikelola sendiri.

Nilai `AssociationStatus` memberi tahu Anda apakah asosiasi kebijakan sedang tertunda atau dalam keadaan sukses atau gagal. Diperlukan waktu hingga 24 jam agar status berubah dari `PENDING` ke `SUCCESS` atau`FAILURE`. Status asosiasi OU orang tua atau root tergantung pada status anak-anaknya. Jika status asosiasi semua anak adalah`SUCCESS`, status asosiasi orang tua adalah`SUCCESS`. Jika status asosiasi satu atau lebih anak adalah`FAILED`, status asosiasi orang tua adalah`FAILED`.

Nilai `AssociationStatus` juga tergantung pada semua Wilayah. Jika asosiasi berhasil di Wilayah asal dan semua Daerah terkait, nilainya `AssociationStatus` adalah`SUCCESS`. Jika asosiasi gagal di satu atau lebih Wilayah ini, nilainya `AssociationStatus` adalah`FAILED`.

Perilaku berikut juga berdampak pada nilai`AssociationStatus`:

- Jika targetnya adalah OU orang tua atau root, ia memiliki `AssociationStatus` dari `SUCCESS` atau `FAILED` hanya ketika semua anak memiliki `FAILED` status `SUCCESS` atau. Jika status asosiasi akun turunan atau OU berubah (misalnya, saat Wilayah tertaut ditambahkan atau dihapus) setelah Anda pertama kali mengaitkan induk dengan konfigurasi, perubahan tersebut tidak akan memperbarui status asosiasi induk kecuali Anda menjalankan `StartConfigurationPolicyAssociation` API lagi.
- Jika targetnya adalah akun, ia memiliki `AssociationStatus` dari `SUCCESS` atau `FAILED` hanya jika asosiasi memiliki hasil dari `SUCCESS` atau `FAILED` di Wilayah asal dan semua Wilayah yang ditautkan. Jika status asosiasi akun target berubah (misalnya, saat Wilayah tertaut ditambahkan atau dihapus) setelah Anda pertama kali mengaitkannya dengan konfigurasi, status asosiasinya akan diperbarui. Namun, perubahan tidak memperbarui status asosiasi induk kecuali Anda memanggil `StartConfigurationPolicyAssociation` API lagi.

Jika Anda menambahkan Wilayah tertaut baru, Security Hub akan mereplikasi asosiasi Anda yang ada di `PENDING`SUCCESS,, atau `FAILED` status di Wilayah baru.

Alasan umum kegagalan asosiasi

Asosiasi kebijakan konfigurasi mungkin gagal karena alasan umum berikut:

- Akun manajemen Organisasi bukan anggota — Jika Anda ingin mengaitkan kebijakan konfigurasi dengan akun manajemen Organisasi, akun tersebut harus sudah mengaktifkan Security Hub. Ini membuat akun manajemen menjadi akun anggota dalam organisasi.
- AWS Configtidak diaktifkan atau dikonfigurasi dengan benar — Untuk mengaktifkan standar dalam kebijakan konfigurasi, AWS Config harus diaktifkan dan dikonfigurasi untuk merekam sumber daya yang relevan.
- Harus dikaitkan dari akun administrator yang didelegasikan — Anda hanya dapat mengaitkan kebijakan dengan akun target dan OU saat Anda masuk ke akun administrator yang didelegasikan.
- Harus dikaitkan dari wilayah asal — Anda hanya dapat mengaitkan kebijakan dengan akun target dan OU saat Anda masuk ke Wilayah asal.

- Keikutsertaan Wilayah tidak diaktifkan — Asosiasi kebijakan gagal untuk akun anggota atau OU di Wilayah tertaut jika itu adalah Wilayah keikutsertaan yang belum diaktifkan oleh administrator yang didelegasikan. Anda dapat mencoba lagi setelah mengaktifkan Region dari akun administrator yang didelegasikan.
- Akun anggota ditangguhkan — Asosiasi kebijakan gagal jika Anda mencoba mengaitkan kebijakan dengan akun anggota yang ditangguhkan.

Memperbarui kebijakan konfigurasi Security Hub

Akun administrator yang didelegasikan dapat memperbarui kebijakan AWS Security Hub konfigurasi sesuai kebutuhan. Administrator yang didelegasikan dapat memperbarui setelan kebijakan, akun atau OU yang terkait dengan kebijakan, atau keduanya. Ketika setelan kebijakan diperbarui, akun yang terkait dengan kebijakan konfigurasi secara otomatis mulai menggunakan kebijakan yang diperbarui.

Mirip dengan saat Anda membuat kebijakan konfigurasi, Anda dapat memperbarui setelan kebijakan berikut:

- Aktifkan atau nonaktifkan Security Hub.
- Aktifkan satu atau lebih standar keamanan.
- Tunjukkan kontrol keamanan mana yang diaktifkan di seluruh standar yang diaktifkan. Anda dapat melakukannya dengan memberikan daftar kontrol khusus yang harus diaktifkan, dan Security Hub menonaktifkan semua kontrol lainnya, termasuk kontrol baru saat dirilis. Atau, Anda dapat memberikan daftar kontrol khusus yang harus dinonaktifkan, dan Security Hub mengaktifkan semua kontrol lainnya, termasuk kontrol baru saat dirilis.
- Secara opsional, sesuaikan parameter untuk memilih kontrol yang diaktifkan di seluruh standar yang diaktifkan.

Pilih metode pilihan Anda, dan ikuti langkah-langkah untuk memperbarui kebijakan konfigurasi.

Jika Anda menggunakan konfigurasi pusat, Security Hub secara otomatis menonaktifkan kontrol yang melibatkan sumber daya global di semua Wilayah kecuali Wilayah asal. Kontrol lain yang Anda pilih untuk diaktifkan meskipun kebijakan konfigurasi diaktifkan di semua Wilayah yang tersedia. Untuk membatasi temuan untuk kontrol ini hanya pada satu Wilayah, Anda dapat memperbarui pengaturan AWS Config perekam dan menonaktifkan perekaman sumber daya global di semua Wilayah kecuali Wilayah asal. Saat Anda menggunakan konfigurasi pusat, Anda tidak memiliki cakupan untuk kontrol

yang tidak tersedia di Wilayah asal dan Wilayah yang ditautkan. Untuk daftar kontrol yang melibatkan sumber daya global, lihatKontrol yang berhubungan dengan sumber daya global.

Console

Untuk memperbarui kebijakan konfigurasi

1. Buka AWS Security Hub konsol di https://console.aws.amazon.com/securityhub/.

   Masuk menggunakan kredensional akun administrator yang didelegasikan Security Hub di Wilayah beranda.
2. Di panel navigasi, pilih Pengaturan dan Konfigurasi.
3. Pilih tab Kebijakan.
4. Pilih kebijakan konfigurasi yang ingin Anda edit, lalu pilih Edit. Jika diinginkan, edit pengaturan kebijakan. Biarkan bagian ini seolah-olah Anda ingin menjaga pengaturan kebijakan tidak berubah.
5. Pilih Berikutnya. Jika diinginkan, edit asosiasi kebijakan. Biarkan bagian ini seolah-olah Anda ingin menjaga agar asosiasi kebijakan tidak berubah. Anda dapat mengaitkan atau memisahkan kebijakan dengan maksimal 15 target (akun, OU, atau root) saat Anda memperbaruinya.
6. Pilih Selanjutnya.
7. Tinjau perubahan Anda, lalu pilih Simpan dan terapkan. Di Wilayah beranda dan Wilayah tertaut, tindakan ini mengesampingkan setelan konfigurasi akun yang ada yang terkait dengan kebijakan konfigurasi ini. Akun dapat dikaitkan dengan kebijakan konfigurasi melalui aplikasi, atau warisan dari node induk.

API

Untuk memperbarui kebijakan konfigurasi

1. Untuk memperbarui setelan dalam kebijakan konfigurasi, panggil UpdateConfigurationPolicyAPI dari akun administrator yang didelegasikan Security Hub di Wilayah beranda.
2. Berikan Nama Sumber Daya Amazon (ARN) atau ID kebijakan konfigurasi yang ingin Anda perbarui.
3. Berikan nilai yang diperbarui untuk bidang di bawah`ConfigurationPolicy`. Secara opsional, Anda juga dapat memberikan alasan untuk pembaruan.

4. Untuk menambahkan asosiasi baru untuk kebijakan konfigurasi ini, panggil StartConfigurationPolicyAssociationAPI dari akun administrator yang didelegasikan Security Hub di Wilayah beranda. Untuk menghapus satu atau beberapa asosiasi saat ini, panggil StartConfigurationPolicyDisassociationAPI dari akun administrator yang didelegasikan Security Hub di Wilayah beranda.
5. Untuk `ConfigurationPolicyIdentifier` bidang, berikan ARN atau ID kebijakan konfigurasi yang asosiasinya ingin Anda perbarui.
6. Untuk `Target` bidang, berikan akun, OU, atau ID root yang ingin Anda kaitkan atau lepaskan. Tindakan ini mengesampingkan asosiasi kebijakan sebelumnya untuk OU atau akun tertentu.

> **Note**
>
> Saat Anda menjalankan `UpdateConfigurationPolicy` API, Security Hub melakukan penggantian daftar lengkap untuk`EnabledStandardIdentifiers`,, `EnabledSecurityControlIdentifiersDisabledSecurityControlIdentifiers`, dan `SecurityControlCustomParameters` bidang. Setiap kali Anda menjalankan API ini, berikan daftar lengkap standar yang ingin Anda aktifkan dan daftar lengkap kontrol yang ingin Anda aktifkan atau nonaktifkan dan sesuaikan parameternya.

Contoh permintaan API untuk memperbarui kebijakan konfigurasi:

```
{
    "Identifier": "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "Description": "Updated configuration policy",
    "UpdatedReason": "Disabling CloudWatch.1",
    "ConfigurationPolicy": {
        "SecurityHub": {
             "ServiceEnabled": true,
             "EnabledStandardIdentifiers": [
                    "arn:aws:securityhub:us-east-1::standards/aws-foundational-
security-best-practices/v/1.0.0",
                    "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0"
                ],
            "SecurityControlsConfiguration": {
                "DisabledSecurityControlIdentifiers": [
```

```
                    "CloudTrail.2",
                    "CloudWatch.1"
                ],
                "SecurityControlCustomParameters": [
                    {
                        "SecurityControlId": "ACM.1",
                        "Parameters": {
                            "daysToExpiration": {
                                "ValueType": "CUSTOM",
                                "Value": {
                                    "Integer": 15
                                }
                            }
                        }
                    }
                ]
            }
        }
    }
}
```

AWS CLI

Untuk memperbarui kebijakan konfigurasi

1. Untuk memperbarui pengaturan dalam kebijakan konfigurasi, jalankan update-configuration-policyperintah dari akun administrator yang didelegasikan Security Hub di Wilayah beranda.
2. Berikan Nama Sumber Daya Amazon (ARN) atau ID kebijakan konfigurasi yang ingin Anda perbarui.
3. Berikan nilai yang diperbarui untuk bidang di bawah`configuration-policy`. Secara opsional, Anda juga dapat memberikan alasan untuk pembaruan.
4. Untuk menambahkan asosiasi baru untuk kebijakan konfigurasi ini, jalankan start-configuration-policy-associationperintah dari akun administrator yang didelegasikan Security Hub di Wilayah beranda. Untuk menghapus satu atau beberapa asosiasi saat ini, jalankan start-configuration-policy-disassociationperintah dari akun administrator yang didelegasikan Security Hub di Wilayah beranda.
5. Untuk `configuration-policy-identifier` bidang, berikan ARN atau ID kebijakan konfigurasi yang asosiasinya ingin Anda perbarui.

6. Untuk `target` bidang, berikan akun, OU, atau ID root yang ingin Anda kaitkan atau lepaskan. Tindakan ini mengesampingkan asosiasi kebijakan sebelumnya untuk OU atau akun tertentu.

> **Note**
>
> Saat Anda menjalankan `update-configuration-policy` perintah, Security Hub melakukan penggantian daftar lengkap untuk`EnabledStandardIdentifiers`,`EnabledSecurityControlIdentifiers`,`DisabledSe` dan `SecurityControlCustomParameters` bidang. Setiap kali Anda menjalankan perintah ini, berikan daftar lengkap standar yang ingin Anda aktifkan dan daftar lengkap kontrol yang ingin Anda aktifkan atau nonaktifkan dan sesuaikan parameternya.

Contoh perintah untuk memperbarui kebijakan konfigurasi:

```
aws securityhub update-configuration-policy \
--region us-east-1 \
--identifier "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111" \
--description "Updated configuration policy" \
--updated-reason "Disabling CloudWatch.1" \
--configuration-policy '{"SecurityHub": {"ServiceEnabled": true,
 "EnabledStandardIdentifiers": ["arn:aws:securityhub:us-east-1::standards/aws-
foundational-security-best-practices/v/1.0.0","arn:aws:securityhub:::ruleset/
cis-aws-foundations-benchmark/v/1.2.0"],"SecurityControlsConfiguration":
{"DisabledSecurityControlIdentifiers": ["CloudTrail.2","CloudWatch.1"],
 "SecurityControlCustomParameters": [{"SecurityControlId": "ACM.1", "Parameters":
 {"daysToExpiration": {"ValueType": "CUSTOM", "Value": {"Integer": 15}}}}]}}'
```

`StartConfigurationPolicyAssociation`API mengembalikan bidang yang disebut`AssociationStatus`. Bidang ini memberi tahu Anda apakah asosiasi kebijakan sedang tertunda atau dalam keadaan berhasil atau gagal. Diperlukan waktu hingga 24 jam agar status berubah dari `PENDING` ke `SUCCESS` atau`FAILURE`. Untuk informasi selengkapnya tentang status asosiasi, lihatStatus asosiasi konfigurasi.

Menghapus dan memutus kebijakan konfigurasi Security Hub

Akun administrator yang didelegasikan dapat menghapus kebijakan AWS Security Hub konfigurasi. Atau, akun administrator yang didelegasikan dapat mempertahankan kebijakan konfigurasi, tetapi memisahkannya dari akun tertentu atau unit organisasi (OU).

Bagian berikut menjelaskan kedua opsi ini.

Menghapus kebijakan konfigurasi

Saat Anda menghapus kebijakan konfigurasi, kebijakan tersebut tidak ada lagi untuk organisasi Anda. Akun target, OU, dan root organisasi tidak dapat lagi menggunakan kebijakan konfigurasi. Target yang dikaitkan dengan kebijakan konfigurasi yang dihapus mewarisi kebijakan konfigurasi induk terdekat, atau dikelola sendiri jika induk terdekat dikelola sendiri. Jika Anda ingin target menggunakan konfigurasi yang berbeda, Anda dapat mengaitkan target dengan kebijakan konfigurasi baru. Untuk informasi selengkapnya, lihat Membuat dan mengaitkan kebijakan konfigurasi Security Hub.

Sebaiknya buat dan kaitkan setidaknya satu kebijakan konfigurasi dengan organisasi Anda untuk menyediakan cakupan keamanan yang memadai.

Sebelum Anda dapat menghapus kebijakan konfigurasi, Anda harus memisahkan kebijakan dari akun, OU, atau root yang saat ini berlaku.

Pilih metode pilihan Anda, dan ikuti langkah-langkah untuk menghapus kebijakan konfigurasi.

Console

Untuk menghapus kebijakan konfigurasi

1. Buka AWS Security Hub konsol di https://console.aws.amazon.com/securityhub/.

   Masuk menggunakan kredensional akun administrator yang didelegasikan Security Hub di Wilayah beranda.
2. Di panel navigasi, pilih Pengaturan dan Konfigurasi.
3. Pilih tab Kebijakan. Pilih kebijakan konfigurasi yang ingin Anda hapus, lalu pilih Hapus. Jika kebijakan konfigurasi masih terkait dengan akun atau OU apa pun, Anda diminta untuk terlebih dahulu memisahkan kebijakan dari target tersebut sebelum dapat menghapusnya.
4. Tinjau pesan konfirmasi. Masukkan**`confirm`**, dan pilih Hapus.

API

Untuk menghapus kebijakan konfigurasi

Memanggil DeleteConfigurationPolicyAPI dari akun administrator yang didelegasikan Security Hub di Wilayah beranda.

Berikan Nama Sumber Daya Amazon (ARN) atau ID kebijakan konfigurasi yang ingin Anda hapus. Jika Anda menerima `ConflictException` kesalahan, kebijakan konfigurasi masih berlaku untuk akun atau OU di organisasi Anda. Untuk mengatasi kesalahan, putuskan kebijakan konfigurasi dari akun ini atau OU sebelum mencoba menghapusnya.

Contoh permintaan API untuk menghapus kebijakan konfigurasi:

```
{
    "Identifier": "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
}
```

AWS CLI

Untuk menghapus kebijakan konfigurasi

Jalankan delete-configuration-policyperintah dari akun administrator yang didelegasikan Security Hub di Wilayah rumah.

Berikan Nama Sumber Daya Amazon (ARN) atau ID kebijakan konfigurasi yang ingin Anda hapus. Jika Anda menerima `ConflictException` kesalahan, kebijakan konfigurasi masih berlaku untuk akun atau OU di organisasi Anda. Untuk mengatasi kesalahan, putuskan kebijakan konfigurasi dari akun ini atau OU sebelum mencoba menghapusnya.

```
aws securityhub --region us-east-1 delete-configuration-policy \
--identifier "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

Memutuskan konfigurasi dari akun dan OU

Dari akun administrator yang didelegasikan, Anda dapat memisahkan akun target, OU, atau root dari kebijakan konfigurasi yang saat ini berlaku untuknya atau dari konfigurasi yang dikelola sendiri.

Anda dapat memisahkan target hanya dari konfigurasi yang diterapkan, bukan dari konfigurasi yang diwariskan. Untuk mengubah konfigurasi yang diwariskan, Anda dapat menerapkan kebijakan konfigurasi atau perilaku yang dikelola sendiri ke akun atau OU yang terpengaruh. Anda juga dapat menerapkan kebijakan konfigurasi baru, yang mencakup modifikasi yang Anda inginkan, ke induk terdekat.

Disassociation tidak menghapus kebijakan konfigurasi. Kebijakan ini disimpan di akun Anda, sehingga Anda dapat mengaitkannya dengan target lain di organisasi Anda. Ketika disasosiasi selesai, target yang terpengaruh mewarisi kebijakan konfigurasi atau perilaku yang dikelola sendiri dari induk terdekat. Jika tidak ada konfigurasi yang dapat diwariskan, target mempertahankan pengaturan yang dimilikinya sebelum disasosiasi tetapi menjadi dikelola sendiri.

Pilih metode pilihan Anda, dan ikuti langkah-langkah untuk memisahkan akun, OU, atau root dari konfigurasi saat ini.

Console

Untuk memisahkan akun atau OU dari konfigurasi saat ini

1. Buka AWS Security Hub konsol di https://console.aws.amazon.com/securityhub/.

   Masuk menggunakan kredensional akun administrator yang didelegasikan Security Hub di Wilayah beranda.
2. Di panel navigasi, pilih Pengaturan dan Konfigurasi.
3. Pada tab Organizations, pilih akun, OU, atau root yang ingin Anda putuskan dari konfigurasi saat ini. Pilih Edit.
4. Pada halaman Tentukan konfigurasi, untuk Manajemen, pilih Kebijakan diterapkan jika Anda ingin administrator yang didelegasikan dapat menerapkan kebijakan secara langsung ke target. Pilih Inherited jika Anda ingin target mewarisi konfigurasi induk terdekatnya. Dalam salah satu kasus ini, administrator yang didelegasikan mengontrol pengaturan untuk target. Pilih Self-managed jika Anda ingin akun atau OU mengontrol pengaturannya sendiri.
5. Setelah meninjau perubahan Anda, pilih Berikutnya dan Terapkan. Tindakan ini mengesampingkan konfigurasi akun atau OU yang ada dalam cakupan, jika konfigurasi tersebut bertentangan dengan pilihan Anda saat ini.

API

Untuk memisahkan akun atau OU dari konfigurasi saat ini

1. Memanggil StartConfigurationPolicyDisassociationAPI dari akun administrator yang didelegasikan Security Hub di Wilayah beranda.
2. Untuk`ConfigurationPolicyIdentifier`, berikan Nama Sumber Daya Amazon (ARN) atau ID kebijakan konfigurasi yang ingin Anda putuskan. Sediakan bidang ini `SELF_MANAGED_SECURITY_HUB` untuk memisahkan perilaku yang dikelola sendiri.
3. Untuk`Target`, berikan akun, OU, atau root yang ingin Anda memisahkan dari kebijakan konfigurasi ini.

Contoh permintaan API untuk memisahkan kebijakan konfigurasi:

```
{
    "ConfigurationPolicyIdentifier": "arn:aws:securityhub:us-
east-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "Target": {"RootId": "r-f6g7h8i9j0example"}
}
```

AWS CLI

Untuk memisahkan akun atau OU dari konfigurasi saat ini

1. Jalankan start-configuration-policy-disassociationperintah dari akun administrator yang didelegasikan Security Hub di Wilayah rumah.
2. Untuk`configuration-policy-identifier`, berikan Nama Sumber Daya Amazon (ARN) atau ID kebijakan konfigurasi yang ingin Anda putuskan. Sediakan bidang ini `SELF_MANAGED_SECURITY_HUB` untuk memisahkan perilaku yang dikelola sendiri.
3. Untuk`target`, berikan akun, OU, atau root yang ingin Anda memisahkan dari kebijakan konfigurasi ini.

Contoh perintah untuk memisahkan kebijakan konfigurasi:

```
aws securityhub --region us-east-1 start-configuration-policy-disassociation \
--configuration-policy-identifier "arn:aws:securityhub:us-
east-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111" \
```

```
--target '{"RootId": "r-f6g7h8i9j0example"}'
```

Konfigurasi sentral dalam konteks standar atau kontrol

Anda dapat menggunakan konfigurasi pusat dari halaman Konfigurasi AWS Security Hub konsol, atau dalam konteks standar keamanan atau kontrol keamanan tertentu. Menggunakan fitur ini dalam konteks memungkinkan Anda mengonfigurasi standar dan kontrol di seluruh organisasi Anda dengan cara yang terintegrasi dengan alur kerja yang ada. Selain itu, saat Anda melihat temuan, Anda dapat menemukan standar dan kontrol mana yang paling relevan dengan lingkungan Anda dan mengonfigurasinya pada saat yang bersamaan.

Konfigurasi dalam konteks hanya tersedia di konsol Security Hub. Secara terprogram, Anda harus memanggil UpdateConfigurationPolicyAPI untuk mengubah cara standar atau kontrol tertentu dikonfigurasi di organisasi Anda.

Mengkonfigurasi standar keamanan dalam konteks

Ikuti langkah-langkah untuk mengonfigurasi standar keamanan dalam konteks melalui konfigurasi pusat.

Untuk mengonfigurasi standar keamanan dalam konteks (hanya konsol)

1. Buka AWS Security Hub konsol di https://console.aws.amazon.com/securityhub/.

   Masuk menggunakan kredensional akun administrator yang didelegasikan Security Hub di Wilayah beranda.
2. Di panel navigasi, pilih Standar keamanan.
3. Untuk standar yang ingin Anda konfigurasikan, pilih Konfigurasi. Anda juga dapat memilih standar tertentu dan kemudian memilih Konfigurasi dari halaman detail standar. Konsol mencantumkan kebijakan konfigurasi Security Hub yang ada (kebijakan konfigurasi) dan status standar ini di masing-masing kebijakan.
4. Pilih opsi untuk mengaktifkan atau menonaktifkan standar di setiap kebijakan konfigurasi.
5. Setelah melakukan perubahan, pilih Berikutnya.
6. Tinjau perubahan Anda, dan pilih Terapkan. Tindakan ini memengaruhi semua akun dan OU yang terkait dengan kebijakan konfigurasi. Konfigurasi Anda berlaku di Wilayah asal dan semua Wilayah yang ditautkan.

Mengkonfigurasi kontrol keamanan dalam konteks

Ikuti langkah-langkah untuk mengonfigurasi kontrol keamanan dalam konteks melalui konfigurasi pusat.

Untuk mengonfigurasi kontrol keamanan dalam konteks (hanya konsol)

1. Buka AWS Security Hub konsol di https://console.aws.amazon.com/securityhub/.

   Masuk menggunakan kredensional akun administrator yang didelegasikan Security Hub di Wilayah beranda.
2. Di panel navigasi, pilih Kontrol.
3. Pilih kontrol tertentu, lalu pilih Konfigurasi. Konsol mencantumkan kebijakan konfigurasi Anda saat ini dan status kontrol ini di masing-masing kebijakan konfigurasi.
4. Pilih opsi untuk mengaktifkan atau menonaktifkan kontrol di setiap kebijakan konfigurasi. Anda juga dapat memilih untuk menyesuaikan parameter kontrol.
5. Setelah melakukan perubahan, pilih Berikutnya.
6. Tinjau perubahan Anda, dan pilih Terapkan. Tindakan ini memengaruhi semua akun dan OU yang terkait dengan kebijakan konfigurasi. Konfigurasi Anda berlaku di Wilayah asal dan semua Wilayah yang ditautkan.

Berhenti menggunakan konfigurasi pusat

Saat Anda berhenti menggunakan konfigurasi pusatAWS Security Hub, administrator yang didelegasikan kehilangan kemampuan untuk mengonfigurasi Security Hub, standar keamanan, dan kontrol keamanan di beberapa Akun AWS unit organisasi (OU), danWilayah AWS. Sebagai gantinya, akun organisasi harus mengonfigurasi sebagian besar pengaturannya sendiri secara terpisah di setiap Wilayah.

> **Important**
>
> Sebelum Anda dapat berhenti menggunakan konfigurasi pusat, Anda harus terlebih dahulu memisahkan akun dan OU Anda dari konfigurasi mereka saat ini, apakah itu kebijakan konfigurasi atau perilaku yang dikelola sendiri.
> Sebelum Anda dapat berhenti menggunakan konfigurasi pusat, Anda juga harus menghapus kebijakan konfigurasi Anda.

Ketika Anda menghentikan konfigurasi pusat, perubahan berikut terjadi:

- Administrator yang didelegasikan tidak dapat lagi membuat kebijakan konfigurasi untuk organisasi.
- Akun yang memiliki kebijakan konfigurasi yang diterapkan atau diwariskan mempertahankan pengaturan mereka saat ini, tetapi menjadi dikelola sendiri.
- Organisasi Anda beralih ke konfigurasi lokal. Di bawah konfigurasi lokal, sebagian besar pengaturan Security Hub harus dikonfigurasi secara terpisah di setiap akun organisasi dan Wilayah. Administrator yang didelegasikan dapat memilih untuk secara otomatis mengaktifkan Security Hub, standar keamanan default, dan semua kontrol yang merupakan bagian dari standar default di akun organisasi baru. Standar default adalah AWS Foundational Security Best Practices (FSBP) dan Center for Internet Security (CIS) AWS Foundations Benchmark v1.2.0. Pengaturan ini hanya berlaku di Wilayah saat ini dan hanya memengaruhi akun organisasi baru. Administrator yang didelegasikan tidak dapat mengubah standar mana yang default. Konfigurasi lokal tidak mendukung penggunaan kebijakan konfigurasi atau konfigurasi di tingkat OU.

Identitas akun administrator yang didelegasikan tetap sama ketika Anda berhenti menggunakan konfigurasi pusat. Wilayah asal Anda dan Wilayah terkait juga tetap sama (Wilayah asal Anda sekarang disebut Wilayah agregasi, dan dapat digunakan untuk menemukan agregasi).

Pilih metode pilihan Anda, dan ikuti langkah-langkah untuk berhenti menggunakan konfigurasi pusat dan beralih ke konfigurasi lokal.

Security Hub console

Untuk berhenti menggunakan konfigurasi pusat

1. Buka AWS Security Hub konsol di https://console.aws.amazon.com/securityhub/.

   Masuk menggunakan kredensil akun administrator yang didelegasikan Security Hub di Wilayah beranda.
2. Pada panel navigasi, pilih Pengaturan dan Konfigurasi.
3. Di bagian Ikhtisar, pilih Edit.
4. Di kotak Edit konfigurasi organisasi, pilih Konfigurasi lokal. Jika belum melakukannya, Anda diminta untuk memisahkan dan menghapus kebijakan konfigurasi Anda saat ini sebelum Anda dapat menghentikan konfigurasi pusat. Akun atau OU yang ditetapkan sebagai dikelola sendiri harus dipisahkan dari konfigurasi yang dikelola sendiri. Anda dapat melakukan ini

di konsol dengan mengubah jenis manajemen setiap akun yang dikelola sendiri atau OU menjadi dikelola secara terpusat dan Mewarisi dari organisasi saya.

5. Secara opsional, pilih pengaturan default konfigurasi lokal untuk akun organisasi baru.
6. Pilih Konfirmasi.

Security Hub API

Untuk berhenti menggunakan konfigurasi pusat

1. Memanggil UpdateOrganizationConfigurationAPI.
2. Atur `ConfigurationType` bidang di `OrganizationConfiguration` objek ke`LOCAL`. API menampilkan kesalahan jika Anda memiliki kebijakan konfigurasi atau asosiasi kebijakan yang ada. Untuk memisahkan kebijakan konfigurasi, panggil API. `StartConfigurationPolicyDisassociation` Untuk menghapus kebijakan konfigurasi, panggil `DeleteConfigurationPolicy` API.
3. Jika Anda ingin mengaktifkan Security Hub secara otomatis di akun organisasi baru, setel `AutoEnable` bidang tersebut`true`. Secara default, nilai bidang ini adalah`false`, dan Security Hub tidak diaktifkan secara otomatis di akun organisasi baru. Secara opsional, jika Anda ingin mengaktifkan standar keamanan default secara otomatis di akun organisasi baru, setel `AutoEnableStandards` bidang ke`DEFAULT`. Ini nilai default. Jika Anda tidak ingin mengaktifkan standar keamanan default secara otomatis di akun organisasi baru, setel `AutoEnableStandards` bidang tersebut`NONE`.

Contoh permintaan API:

```
{
    "AutoEnable": true,
    "OrganizationConfiguration": {
        "ConfigurationType" : "LOCAL"
    }
}
```

AWS CLI

Untuk berhenti menggunakan konfigurasi pusat

1. Jalankan perintah update-organization-configuration.

2. Atur `ConfigurationType` bidang di `organization-configuration` objek ke`LOCAL`. Perintah mengembalikan kesalahan jika Anda memiliki kebijakan konfigurasi atau asosiasi kebijakan yang ada. Untuk memisahkan kebijakan konfigurasi, jalankan `start-configuration-policy-disassociation` perintah. Untuk menghapus kebijakan konfigurasi, jalankan `delete-configuration-policy` perintah.
3. Jika Anda ingin mengaktifkan Security Hub secara otomatis di akun organisasi baru, sertakan `auto-enable` parameternya. Secara default, nilai parameter ini adalahno`-auto-enable`, dan Security Hub tidak diaktifkan secara otomatis di akun organisasi baru. Secara opsional, jika Anda ingin mengaktifkan standar keamanan default secara otomatis di akun organisasi baru, setel `auto-enable-standards` bidang ke`DEFAULT`. Ini nilai default. Jika Anda tidak ingin mengaktifkan standar keamanan default secara otomatis di akun organisasi baru, setel `auto-enable-standards` bidang tersebut`NONE`.

```
aws securityhub --region us-east-1 update-organization-configuration \
--auto-enable \
--organization-configuration '{"ConfigurationType": "LOCAL"}'
```

Mengelola akun administrator dan anggota

Jika AWS lingkungan Anda memiliki beberapa akun, Anda dapat memperlakukan akun yang menggunakan AWS Security Hub sebagai akun anggota dan mengaitkannya dengan satu akun administrator. Administrator dapat memantau postur keamanan Anda secara keseluruhan dan mengambil tindakan yang diizinkan pada akun anggota. Administrator juga dapat melakukan berbagai tugas manajemen akun dan administrasi dalam skala besar, seperti memantau perkiraan biaya penggunaan dan menilai kuota akun.

Anda dapat mengaitkan akun anggota dengan administrator dalam dua cara, dengan mengintegrasikan Security Hub dengan AWS Organizations atau dengan mengirim dan menerima undangan keanggotaan secara manual di Security Hub.

Mengelola akun dengan AWS Organizations

AWS Organizationsadalah layanan manajemen akun global yang memungkinkan AWS administrator untuk mengkonsolidasikan dan mengelola beberapa. Akun AWS Ini menyediakan manajemen akun dan fitur penagihan terkonsolidasi yang dirancang untuk mendukung kebutuhan anggaran, keamanan, dan kepatuhan. Ini ditawarkan tanpa biaya tambahan, dan terintegrasi dengan beberapa, termasuk AWS Security HubLayanan AWS, Amazon Macie, dan Amazon. GuardDuty Untuk informasi selengkapnya, silakan lihat Panduan Pengguna AWS Organizations.

Saat Anda mengintegrasikan Security Hub danAWS Organizations, akun manajemen Organizations menunjuk administrator yang didelegasikan Security Hub. Security Hub secara otomatis diaktifkan di akun administrator yang didelegasikan Wilayah AWS di mana ia ditunjuk.

Setelah menunjuk administrator yang didelegasikan, kami sarankan mengelola akun di Security Hub dengan konfigurasi pusat. Ini adalah cara paling efisien untuk menyesuaikan Security Hub dan memastikan cakupan keamanan yang memadai untuk organisasi Anda.

Konfigurasi pusat memungkinkan administrator yang didelegasikan menyesuaikan Security Hub di beberapa akun organisasi dan Wilayah daripada mengonfigurasi Region-by-Region. Anda dapat membuat kebijakan konfigurasi untuk seluruh organisasi, atau membuat kebijakan konfigurasi yang berbeda untuk akun dan OU yang berbeda. Kebijakan menentukan apakah Security Hub diaktifkan atau dinonaktifkan di akun terkait serta standar dan kontrol keamanan mana yang diaktifkan.

Administrator yang didelegasikan dapat menetapkan akun sebagai dikelola secara terpusat atau dikelola sendiri. Akun yang dikelola secara terpusat hanya dapat dikonfigurasi oleh administrator yang didelegasikan. Akun yang dikelola sendiri dapat menentukan pengaturan mereka sendiri.

Jika Anda tidak ikut serta dalam konfigurasi pusat, administrator yang didelegasikan memiliki kemampuan yang lebih terbatas untuk mengonfigurasi Security Hub, yang disebut konfigurasi lokal. Di bawah konfigurasi lokal, administrator yang didelegasikan dapat secara otomatis mengaktifkan Security Hub dan standar keamanan default di akun organisasi baru di Wilayah saat ini. Namun, akun yang ada tidak menggunakan pengaturan ini, sehingga penyimpangan konfigurasi dapat terjadi setelah akun bergabung dengan organisasi.

Selain pengaturan akun baru ini, konfigurasi lokal bersifat spesifik akun dan spesifik Wilayah. Setiap akun organisasi harus mengonfigurasi layanan, standar, dan kontrol Security Hub secara terpisah di setiap Wilayah. Konfigurasi lokal juga tidak mendukung penggunaan kebijakan konfigurasi.

Mengelola akun secara manual dengan undangan

Anda harus mengelola akun anggota secara manual berdasarkan undangan di Security Hub jika Anda memiliki akun mandiri atau jika Anda tidak berintegrasi dengan Organizations. Akun mandiri tidak dapat diintegrasikan dengan Organizations, jadi Anda perlu mengelolanya secara manual. Kami merekomendasikan untuk mengintegrasikan dengan AWS Organizations dan menggunakan konfigurasi pusat jika Anda menambahkan akun tambahan di masa mendatang.

Saat Anda menggunakan manajemen akun manual, Anda menetapkan akun untuk menjadi administrator Security Hub. Akun administrator dapat melihat data di akun anggota dan mengambil tindakan tertentu pada temuan akun anggota. Administrator Security Hub mengundang akun lain untuk menjadi akun anggota, dan hubungan administrator-anggota terbentuk ketika akun calon anggota menerima undangan.

Manajemen akun manual tidak mendukung penggunaan kebijakan konfigurasi. Tanpa kebijakan konfigurasi, administrator tidak dapat menyesuaikan Security Hub secara terpusat dengan mengonfigurasi setelan variabel untuk akun yang berbeda. Sebagai gantinya, setiap akun organisasi harus mengaktifkan dan mengonfigurasi Security Hub untuk dirinya sendiri secara terpisah di setiap Wilayah. Ini dapat membuatnya lebih sulit dan memakan waktu untuk memastikan cakupan keamanan yang memadai di semua akun dan Wilayah tempat Anda menggunakan Security Hub. Ini juga dapat menyebabkan penyimpangan konfigurasi karena akun anggota dapat menentukan pengaturan mereka sendiri tanpa masukan dari administrator.

Untuk mengelola akun berdasarkan undangan, lihatMengelola akun dengan undangan.

Mengelola akun dengan AWS Organizations

Anda dapat mengintegrasikan AWS Security Hub dengan AWS Organizations, dan kemudian mengelola Security Hub untuk akun di organisasi Anda.

Untuk mengintegrasikan Security Hub dengan AWS Organizations, Anda membuat organisasi di AWS Organizations. Akun manajemen Organizations menetapkan satu akun sebagai administrator yang didelegasikan Security Hub untuk organisasi. Administrator yang didelegasikan kemudian dapat mengaktifkan Security Hub untuk akun lain di organisasi, menambahkan akun tersebut sebagai akun anggota Security Hub, dan mengambil tindakan yang diizinkan pada akun anggota. Administrator yang didelegasikan Security Hub dapat mengaktifkan dan mengelola Security Hub hingga 10.000 akun anggota.

Tingkat kemampuan konfigurasi administrator yang didelegasikan bergantung pada apakah Anda menggunakan konfigurasi pusat. Dengan konfigurasi pusat diaktifkan, Anda tidak perlu mengonfigurasi Security Hub secara terpisah di setiap akun anggota dan Wilayah AWS. Administrator yang didelegasikan dapat menerapkan pengaturan Security Hub tertentu di akun anggota dan unit organisasi (OU) tertentu di seluruh Wilayah.

Akun administrator yang didelegasikan Security Hub dapat melakukan tindakan berikut pada akun anggota:

- Jika menggunakan konfigurasi pusat, konfigurasikan Security Hub secara terpusat untuk akun anggota dan OU dengan membuat kebijakan konfigurasi Security Hub. Kebijakan konfigurasi dapat digunakan untuk mengaktifkan dan menonaktifkan Security Hub, mengaktifkan dan menonaktifkan standar, serta mengaktifkan dan menonaktifkan kontrol.
- Secara otomatis memperlakukan akun baru sebagai akun anggota Security Hub saat mereka bergabung dengan organisasi. Jika Anda menggunakan konfigurasi pusat, kebijakan konfigurasi yang terkait dengan OU mencakup akun yang ada dan baru yang merupakan bagian dari OU.
- Perlakukan akun organisasi yang ada sebagai akun anggota Security Hub. Ini terjadi secara otomatis jika Anda menggunakan konfigurasi pusat.
- Putuskan akun anggota yang termasuk dalam organisasi. Jika Anda menggunakan konfigurasi pusat, Anda dapat memisahkan akun anggota hanya setelah menetapkannya sebagai dikelola sendiri. Atau, Anda dapat mengaitkan kebijakan konfigurasi yang menonaktifkan Security Hub dengan akun anggota tertentu yang dikelola secara terpusat.

Untuk daftar lengkap tindakan yang dapat dilakukan administrator yang didelegasikan pada akun anggota, lihatTindakan yang diizinkan untuk akun.

Topik di bagian ini menjelaskan cara mengintegrasikan Security Hub dengan AWS Organizations dan cara mengelola Security Hub untuk akun dalam suatu organisasi. Jika relevan, setiap bagian mengidentifikasi manfaat dan perbedaan manajemen untuk pengguna konfigurasi pusat.

Topik

Mengintegrasikan Security Hub dengan AWS Organizations

Untuk mengintegrasikan AWS Security Hub dan AWS Organizations, Anda membuat organisasi di Organizations dan menggunakan akun manajemen organisasi untuk menunjuk akun administrator Security Hub yang didelegasikan. Hal ini memungkinkan Security Hub sebagai layanan terpercaya di Organizations. Ini juga memungkinkan Security Hub saat ini Wilayah AWS untuk akun administrator yang didelegasikan, dan memungkinkan administrator yang didelegasikan untuk mengaktifkan Security Hub untuk akun anggota, melihat data di akun anggota, dan melakukan tindakan lain yang diizinkan pada akun anggota.

Jika Anda menggunakan konfigurasi pusat, administrator yang didelegasikan juga dapat membuat kebijakan konfigurasi Security Hub yang menentukan bagaimana layanan, standar, dan kontrol Security Hub harus dikonfigurasi di akun organisasi.

Membuat organisasi

Organisasi adalah entitas yang Anda buat untuk mengkonsolidasikan Anda Akun AWS sehingga Anda dapat mengelolanya sebagai satu kesatuan.

Anda dapat membuat organisasi dengan menggunakan AWS Organizations konsol atau dengan menggunakan perintah dari AWS CLI atau salah satu SDK API. Untuk petunjuk mendetail, lihat Membuat organisasi di Panduan AWS Organizations Pengguna.

Anda dapat menggunakan AWS Organizations untuk melihat dan mengelola semua akun dalam organisasi secara terpusat. Sebuah organisasi memiliki satu akun manajemen bersama dengan nol

atau lebih akun anggota. Anda dapat mengatur akun dalam struktur hierarkis seperti pohon dengan root di bagian atas dan unit organisasi (OU) bersarang di bawah root. Setiap akun dapat langsung di bawah root, atau ditempatkan di salah satu OU dalam hierarki. OU adalah wadah untuk akun tertentu. Misalnya, Anda dapat membuat OU keuangan yang mencakup semua akun yang terkait dengan operasi keuangan.

Rekomendasi untuk memilih administrator Security Hub yang didelegasikan

Jika Anda memiliki akun administrator dari proses undangan manual dan sedang beralih ke manajemen akun AWS Organizations, sebaiknya tentukan akun tersebut sebagai administrator Security Hub yang didelegasikan.

Meskipun API dan konsol Security Hub memungkinkan akun manajemen organisasi menjadi administrator Security Hub yang didelegasikan, sebaiknya pilih dua akun yang berbeda. Ini karena pengguna yang memiliki akses ke akun manajemen organisasi untuk mengelola penagihan cenderung berbeda dari pengguna yang membutuhkan akses ke Security Hub untuk manajemen keamanan.

Sebaiknya gunakan administrator yang didelegasikan sama di seluruh Wilayah. Jika Anda ikut serta dalam konfigurasi pusat, Security Hub secara otomatis menetapkan administrator yang didelegasikan yang sama di Wilayah asal Anda dan Wilayah yang ditautkan.

Verifikasi izin untuk mengonfigurasi administrator yang didelegasikan

Untuk menetapkan dan menghapus akun administrator Security Hub yang didelegasikan, akun manajemen organisasi harus memiliki izin untuk `DisableOrganizationAdminAccount` tindakan `EnableOrganizationAdminAccount` dan tindakan di Security Hub. Akun manajemen Organizations juga harus memiliki izin administratif untuk Organizations.

Untuk memberikan semua izin yang diperlukan, lampirkan kebijakan terkelola Security Hub berikut ke prinsipal IAM untuk akun manajemen organisasi:

- AWSSecurityHubFullAccess
- AWSSecurityHubOrganizationsAccess

Menunjuk administrator yang didelegasikan

Untuk menetapkan akun administrator Security Hub yang didelegasikan, Anda dapat menggunakan konsol Security Hub, Security Hub API, atau. AWS CLI Security Hub menetapkan administrator yang

didelegasikan Wilayah AWS hanya di saat ini, dan Anda harus mengulangi tindakan di Wilayah lain. Jika Anda mulai menggunakan konfigurasi pusat, maka Security Hub secara otomatis menetapkan administrator yang didelegasikan yang sama di Wilayah beranda dan Wilayah yang ditautkan.

Akun manajemen organisasi tidak harus mengaktifkan Security Hub untuk menetapkan akun administrator Security Hub yang didelegasikan.

Kami menyarankan agar akun manajemen organisasi bukan akun administrator Security Hub yang didelegasikan. Namun, jika Anda memilih akun manajemen organisasi sebagai administrator yang didelegasikan Security Hub, akun manajemen harus mengaktifkan Security Hub. Jika akun manajemen tidak mengaktifkan Security Hub, Anda harus mengaktifkan Security Hub secara manual. Security Hub tidak dapat diaktifkan secara otomatis untuk akun manajemen organisasi.

> **Note**
>
> Anda harus menunjuk administrator Security Hub yang didelegasikan menggunakan salah satu metode berikut. Menunjuk administrator Security Hub yang didelegasikan dengan Organizations API tidak tercermin di Security Hub.
> Pilih metode yang Anda inginkan, dan ikuti langkah-langkah untuk menetapkan akun administrator Security Hub yang didelegasikan.

Security Hub console

Untuk menunjuk administrator Security Hub yang didelegasikan saat melakukan orientasi

1. Buka AWS Security Hub konsol di https://console.aws.amazon.com/securityhub/.
2. Pilih Buka Security Hub. Anda diminta untuk masuk ke akun manajemen organisasi.
3. Pada halaman Tentukan administrator yang didelegasikan, di bagian Akun administrator yang didelegasikan, tentukan akun administrator yang didelegasikan. Sebaiknya pilih administrator yang didelegasikan sama yang telah Anda tetapkan untuk layanan AWS keamanan dan kepatuhan lainnya.
4. Pilih Setel administrator yang didelegasikan. Anda diminta untuk masuk ke akun administrator yang didelegasikan (jika belum) untuk melanjutkan orientasi dengan konfigurasi pusat. Jika Anda tidak ingin memulai konfigurasi pusat, pilih Batal. Administrator yang didelegasikan Anda disetel, tetapi Anda belum menggunakan konfigurasi pusat.

Untuk menunjuk administrator Security Hub yang didelegasikan dari halaman Pengaturan

1. Buka AWS Security Hub konsol di https://console.aws.amazon.com/securityhub/.
2. Di panel navigasi Security Hub, pilih Pengaturan. Kemudian pilih Umum.
3. Jika akun administrator Security Hub saat ini ditetapkan, maka sebelum Anda dapat menunjuk akun baru, Anda harus menghapus akun saat ini.

   Di bawah Administrator Delegasi, untuk menghapus akun saat ini, pilih Hapus.
4. Masukkan ID akun akun yang ingin Anda tetapkan sebagai akun administrator Security Hub.

   Anda harus menetapkan akun administrator Security Hub yang sama di semua Wilayah. Jika Anda menetapkan akun yang berbeda dari akun yang ditunjuk di Wilayah lain, konsol mengembalikan kesalahan.
5. Pilih Delegasikan.

Security Hub API, AWS CLI

Dari akun manajemen organisasi, gunakan EnableOrganizationAdminAccountpengoperasian Security Hub API. Jika Anda menggunakan AWS CLI, jalankan enable-organization-admin-accountperintah. Berikan Akun AWS ID administrator Security Hub yang didelegasikan.

Contoh berikut menunjuk administrator Security Hub yang didelegasikan. Contoh ini diformat untuk Linux, macOS, atau Unix, dan menggunakan karakter garis miring terbalik (\) untuk meningkatkan keterbacaan.

```
$ aws securityhub enable-organization-admin-account --admin-account-id 123456789012
```

Menghapus atau mengubah administrator yang didelegasikan

Warning

Bila menggunakan konfigurasi pusat, Anda tidak dapat menggunakan konsol Security Hub atau Security Hub API untuk mengubah atau menghapus akun administrator yang didelegasikan. Jika akun manajemen organisasi menggunakan AWS Organizations konsol atau AWS Organizations API untuk mengubah atau menghapus administrator Security Hub yang didelegasikan, Security Hub secara otomatis menghentikan konfigurasi pusat, dan menghapus kebijakan konfigurasi dan asosiasi kebijakan Anda. Akun anggota

mempertahankan konfigurasi yang mereka miliki sebelum administrator yang didelegasikan diubah atau dihapus.

Hanya akun manajemen organisasi yang dapat menghapus akun administrator Security Hub yang didelegasikan.

Untuk mengubah administrator Security Hub yang didelegasikan, Anda harus terlebih dahulu menghapus akun administrator yang didelegasikan saat ini dan kemudian menunjuk yang baru.

Jika Anda menggunakan konsol Security Hub untuk menghapus administrator yang didelegasikan di satu Wilayah, maka secara otomatis dihapus di semua Wilayah.

Security Hub API hanya menghapus akun administrator Security Hub yang didelegasikan dari Wilayah tempat panggilan atau perintah API dikeluarkan. Anda harus mengulangi tindakan di Wilayah lain.

Jika Anda menggunakan Organizations API untuk menghapus akun administrator Security Hub yang didelegasikan, akun tersebut akan dihapus secara otomatis di semua Wilayah.

Menghapus administrator yang didelegasikan (Organizations API, AWS CLI)

Anda dapat menggunakan Organizations untuk menghapus administrator Security Hub yang didelegasikan di semua Wilayah.

Jika Anda menggunakan konfigurasi pusat untuk mengelola akun, menghapus akun administrator yang didelegasikan akan mengakibatkan penghapusan kebijakan konfigurasi dan asosiasi kebijakan Anda. Akun anggota mempertahankan konfigurasi yang mereka miliki sebelum administrator yang didelegasikan diubah atau dihapus. Namun, akun ini tidak dapat dikelola lagi oleh akun administrator yang didelegasikan yang dihapus. Mereka menjadi akun yang dikelola sendiri yang harus dikonfigurasi secara terpisah di setiap Wilayah.

Pilih metode yang Anda inginkan, dan ikuti petunjuk untuk menghapus akun administrator Security Hub yang didelegasikan. AWS Organizations

Organizations API, AWS CLI

Untuk menghapus administrator Security Hub yang didelegasikan

Dari akun manajemen organisasi, gunakan DeregisterDelegatedAdministratorpengoperasian API Organizations. Jika Anda menggunakan AWS CLI, jalankan deregister-delegated-

administratorperintah. Berikan ID akun administrator yang didelegasikan, dan kepala layanan untuk Security Hub, yaitu`securityhub.amazonaws.com`.

Contoh berikut menghapus administrator Security Hub yang didelegasikan. Contoh ini diformat untuk Linux, macOS, atau Unix, dan menggunakan karakter garis miring terbalik (\) untuk meningkatkan keterbacaan.

```
$ aws organizations deregister-delegated-administrator --account-id 123456789012 --
service-principal securityhub.amazonaws.com
```

Menghapus administrator yang didelegasikan (konsol Security Hub)

Anda dapat menggunakan konsol Security Hub untuk menghapus administrator Security Hub yang didelegasikan di semua Wilayah.

Ketika akun administrator Security Hub yang didelegasikan dihapus, akun anggota akan dipisahkan dari akun administrator Security Hub yang didelegasikan yang dihapus.

Security Hub masih diaktifkan di akun anggota. Mereka menjadi akun mandiri sampai administrator Security Hub baru mengaktifkannya sebagai akun anggota.

Jika akun manajemen organisasi bukan akun yang diaktifkan di Security Hub, gunakan opsi di halaman Selamat Datang di Security Hub.

Untuk menghapus akun administrator Security Hub yang didelegasikan dari halaman Selamat Datang di Security Hub

1. Buka AWS Security Hub konsol di https://console.aws.amazon.com/securityhub/.
2. Pilih Buka Security Hub.
3. Di bawah Administrator Delegasi, pilih Hapus.

Jika akun manajemen organisasi adalah akun yang diaktifkan di Security Hub, maka gunakan opsi pada tab Umum pada halaman Pengaturan.

Untuk menghapus akun administrator Security Hub yang didelegasikan dari halaman Pengaturan

1. Buka AWS Security Hub konsol di https://console.aws.amazon.com/securityhub/.
2. Di panel navigasi Security Hub, pilih Pengaturan. Kemudian pilih Umum.
3. Di bawah Administrator Delegasi, pilih Hapus.

Menghapus administrator yang didelegasikan (Security Hub API, AWS CLI)

Anda dapat menggunakan Security Hub API atau operasi Security Hub AWS CLI untuk menghapus administrator Security Hub yang didelegasikan. Saat Anda menghapus administrator yang didelegasikan dengan salah satu metode ini, administrator hanya akan dihapus di Wilayah tempat panggilan atau perintah API dikeluarkan. Security Hub tidak memperbarui Wilayah lain, dan tidak menghapus akun administrator yang didelegasikan. AWS Organizations

Pilih metode yang Anda inginkan, dan ikuti langkah-langkah berikut untuk menghapus akun administrator Security Hub yang didelegasikan dengan Security Hub.

Security Hub API, AWS CLI

Untuk menghapus administrator Security Hub yang didelegasikan

Dari akun manajemen organisasi, gunakan DisableOrganizationAdminAccountpengoperasian Security Hub API. Jika Anda menggunakan AWS CLI, jalankan disable-organization-admin-accountperintah. Berikan ID akun administrator Security Hub yang didelegasikan.

Contoh berikut menghapus administrator Security Hub yang didelegasikan. Contoh ini diformat untuk Linux, macOS, atau Unix, dan menggunakan karakter garis miring terbalik (\) untuk meningkatkan keterbacaan.

```
$ aws securityhub disable-organization-admin-account --admin-account-id 123456789012
```

Menonaktifkan integrasi Security Hub dengan AWS Organizations

Setelah AWS Organizations organisasi terintegrasi AWS Security Hub, akun manajemen Organizations selanjutnya dapat menonaktifkan integrasi. Sebagai pengguna akun manajemen Organizations, Anda dapat melakukannya dengan menonaktifkan akses tepercaya untuk Security Hub di. AWS Organizations

Saat Anda menonaktifkan akses tepercaya untuk Security Hub, hal berikut akan terjadi:

- Security Hub kehilangan statusnya sebagai layanan tepercaya di AWS Organizations.
- Akun administrator yang didelegasikan Security Hub kehilangan akses ke setelan, data, dan sumber daya Security Hub untuk semua akun anggota Security Hub secara keseluruhan Wilayah AWS.

- Jika Anda menggunakan konfigurasi pusat, Security Hub secara otomatis berhenti menggunakannya untuk organisasi Anda. Kebijakan konfigurasi dan asosiasi kebijakan Anda akan dihapus. Akun mempertahankan konfigurasi yang mereka miliki sebelum Anda menonaktifkan akses tepercaya.
- Semua akun anggota Security Hub menjadi akun mandiri dan mempertahankan pengaturan mereka saat ini. Jika Security Hub diaktifkan untuk akun anggota di satu atau beberapa Wilayah, Security Hub terus diaktifkan untuk akun di Wilayah tersebut. Standar dan kontrol yang diaktifkan juga tidak berubah. Anda dapat mengubah pengaturan ini secara terpisah di setiap akun dan Wilayah. Namun, akun tidak lagi dikaitkan dengan administrator yang didelegasikan di Wilayah mana pun.

Untuk informasi tambahan tentang hasil menonaktifkan akses layanan tepercaya, lihat Menggunakan AWS Organizations dengan yang lain Layanan AWS di AWS Organizations Panduan Pengguna.

Untuk menonaktifkan akses tepercaya, Anda dapat menggunakan AWS Organizations konsol, Organizations API, atau file AWS CLI. Hanya pengguna akun manajemen Organizations yang dapat menonaktifkan akses layanan tepercaya untuk Security Hub. Untuk detail tentang izin yang Anda perlukan, lihat Izin yang diperlukan untuk menonaktifkan akses tepercaya di AWS Organizations Panduan Pengguna.

Sebelum Anda menonaktifkan akses tepercaya, sebaiknya Anda bekerja sama dengan administrator yang didelegasikan untuk organisasi Anda untuk menonaktifkan Security Hub di akun anggota dan membersihkan sumber daya Security Hub di akun tersebut.

Pilih metode pilihan Anda, dan ikuti langkah-langkah untuk menonaktifkan akses tepercaya untuk Security Hub.

Organizations console

Untuk menonaktifkan akses tepercaya untuk Security Hub

1. Masuk ke AWS Management Console menggunakan kredensi akun AWS Organizations manajemen.
2. Buka konsol Organizations di https://console.aws.amazon.com/organizations/.
3. Pada panel navigasi, silakan pilih Layanan.
4. Di bawah Layanan terintegrasi, pilih AWS Security Hub.
5. Pilih Menonaktifkan akses terpercaya.

6. Konfirmasikan bahwa Anda ingin menonaktifkan akses tepercaya.

Organizations API

Untuk menonaktifkan akses tepercaya untuk Security Hub

Memanggil AWSServiceAccess operasi Nonaktifkan AWS Organizations API. Untuk `ServicePrincipal` parameter, tentukan prinsip layanan Security Hub (`securityhub.amazonaws.com`).

AWS CLI

Untuk menonaktifkan akses tepercaya untuk Security Hub

Jalankan disable-aws-service-accessperintah AWS Organizations API. Untuk `service-principal` parameter, tentukan prinsip layanan Security Hub (`securityhub.amazonaws.com`).

Contoh:

```
aws organizations disable-aws-service-access --service-principal
 securityhub.amazonaws.com
```

Mengaktifkan Security Hub secara otomatis di akun organisasi baru

Saat akun baru bergabung dengan organisasi Anda, akun tersebut ditambahkan ke daftar di halaman Akun AWS Security Hub konsol. Untuk akun organisasi, Type is By Organization. Secara default, akun baru tidak menjadi anggota Security Hub saat mereka bergabung dengan organisasi. Status mereka bukan anggota. Akun administrator yang didelegasikan dapat secara otomatis menambahkan akun baru sebagai anggota dan mengaktifkan Security Hub di akun ini saat mereka bergabung dengan organisasi.

> **Note**
>
> Meskipun banyak Wilayah AWS yang aktif secara default untuk Anda Akun AWS, Anda harus mengaktifkan Wilayah tertentu secara manual. Wilayah ini disebut Wilayah keikutsertaan dalam dokumen ini. Untuk mengaktifkan Security Hub secara otomatis di akun baru di Region opt-in, akun tersebut harus mengaktifkan Region tersebut terlebih dahulu. Hanya pemilik

akun yang dapat mengaktifkan Wilayah keikutsertaan. Untuk informasi selengkapnya tentang opt-in Regions, lihat Menentukan yang dapat digunakan akun Wilayah AWS Anda.

Proses ini berbeda berdasarkan apakah Anda menggunakan konfigurasi pusat (disarankan) atau konfigurasi lokal.

Mengaktifkan akun organisasi baru secara otomatis (konfigurasi pusat)

Jika Anda menggunakan konfigurasi pusat, Anda dapat secara otomatis mengaktifkan Security Hub di akun organisasi baru dan yang sudah ada dengan membuat kebijakan konfigurasi di mana Security Hub diaktifkan. Anda kemudian dapat mengaitkan kebijakan dengan root organisasi atau unit organisasi tertentu (OU).

Jika Anda mengaitkan kebijakan konfigurasi di mana Security Hub diaktifkan dengan OU tertentu, Security Hub secara otomatis diaktifkan di semua akun (yang ada dan baru) milik OU tersebut. Akun baru yang bukan milik OU dikelola sendiri dan tidak secara otomatis mengaktifkan Security Hub. Jika Anda mengaitkan kebijakan konfigurasi di mana Security Hub diaktifkan dengan root, Security Hub secara otomatis diaktifkan di semua akun (yang ada dan baru) yang bergabung dengan organisasi. Pengecualian adalah jika akun menggunakan kebijakan yang berbeda melalui aplikasi atau warisan, atau dikelola sendiri.

Dalam kebijakan konfigurasi, Anda juga dapat menentukan standar dan kontrol keamanan mana yang harus diaktifkan di OU. Untuk menghasilkan temuan kontrol untuk standar yang diaktifkan, akun di OU harus AWS Config diaktifkan dan dikonfigurasi untuk mencatat sumber daya yang diperlukan. Untuk informasi selengkapnya tentang AWS Config perekaman, lihat Mengaktifkan dan mengonfigurasi AWS Config.

Untuk petunjuk cara membuat kebijakan konfigurasi, lihatMembuat dan mengaitkan kebijakan konfigurasi Security Hub.

Mengaktifkan akun organisasi baru secara otomatis (konfigurasi lokal)

Saat Anda menggunakan konfigurasi lokal dan mengaktifkan pengaktifan otomatis, Security Hub menambahkan akun organisasi baru sebagai anggota dan mengaktifkan Security Hub di dalamnya di Wilayah saat ini. Wilayah lain tidak terpengaruh. Selain itu, mengaktifkan pengaktifan otomatis tidak mengaktifkan Security Hub di akun organisasi yang ada kecuali akun tersebut telah ditambahkan sebagai akun anggota.

Setelah mengaktifkan pengaktifan otomatis, standar keamanan default juga diaktifkan secara otomatis untuk akun baru di Wilayah saat ini ketika mereka bergabung dengan organisasi. Standar default adalah AWS Foundational Security Best Practices (FSBP) dan Center for Internet Security (CIS) AWS Foundations Benchmark v1.2.0. Anda tidak dapat mengubah standar default. Jika Anda ingin mengaktifkan standar lain di seluruh organisasi Anda, atau mengaktifkan standar untuk akun dan OU tertentu, sebaiknya gunakan konfigurasi pusat.

Untuk menghasilkan temuan kontrol untuk standar default (dan standar lain yang diaktifkan), akun di organisasi Anda harus telah AWS Config diaktifkan dan dikonfigurasi untuk merekam sumber daya yang diperlukan. Untuk informasi selengkapnya tentang AWS Config perekaman, lihat Mengaktifkan dan mengonfigurasi AWS Config.

Pilih metode yang Anda inginkan, dan ikuti langkah-langkah untuk mengaktifkan Security Hub secara otomatis di akun organisasi baru. Petunjuk ini hanya berlaku jika Anda menggunakan konfigurasi lokal.

Security Hub console

Untuk mengaktifkan akun organisasi baru secara otomatis sebagai anggota Security Hub

1. Buka AWS Security Hub konsol di https://console.aws.amazon.com/securityhub/.

   Tanda menggunakan kredensi akun administrator yang didelegasikan.
2. Di panel navigasi Security Hub, di bawah Pengaturan, pilih Konfigurasi.
3. Di bagian Akun, nyalakan Akun Aktifkan otomatis.

Security Hub API

Untuk mengaktifkan akun organisasi baru secara otomatis sebagai anggota Security Hub

Memanggil `UpdateOrganizationConfiguration`API dari akun administrator yang didelegasikan. Setel `AutoEnable` bidang `true` untuk mengaktifkan Security Hub secara otomatis di akun organisasi baru.

AWS CLI

Untuk mengaktifkan akun organisasi baru secara otomatis sebagai anggota Security Hub

Jalankan `update-organization-configuration`perintah dari akun administrator yang didelegasikan. Sertakan `auto-enable` parameter untuk mengaktifkan Security Hub secara otomatis di akun organisasi baru.

```
aws securityhub update-organization-configuration --auto-enable
```

Mengaktifkan Security Hub secara manual di akun organisasi baru

Jika Anda tidak secara otomatis mengaktifkan Security Hub di akun organisasi baru saat mereka bergabung dengan organisasi, Anda dapat menambahkan akun tersebut sebagai anggota dan mengaktifkan Security Hub di dalamnya secara manual setelah mereka bergabung dengan organisasi. Anda juga harus mengaktifkan Security Hub secara manual di Akun AWS mana Anda sebelumnya terputus dari organisasi.

> **Note**
>
> Bagian ini tidak berlaku untuk Anda jika Anda menggunakan konfigurasi pusat. Jika Anda menggunakan konfigurasi pusat, Anda dapat membuat kebijakan konfigurasi yang mengaktifkan Security Hub di akun anggota tertentu dan unit organisasi (OU). Anda juga dapat mengaktifkan standar dan kontrol tertentu di akun dan OU tersebut.

Anda tidak dapat mengaktifkan Security Hub di akun jika sudah menjadi akun anggota dalam organisasi lain.

Anda juga tidak dapat mengaktifkan Security Hub di akun yang saat ini ditangguhkan. Jika Anda mencoba mengaktifkan layanan di akun yang ditangguhkan, status akun berubah menjadi Akun Ditangguhkan.

- Jika akun tidak mengaktifkan Security Hub, Security Hub diaktifkan di akun tersebut. Standar AWS Foundational Security Best Practices (FSBP) dan CIS AWS Foundations Benchmark v1.2.0 juga diaktifkan di akun kecuali Anda mematikan standar keamanan default.

  Pengecualian untuk ini adalah akun manajemen Organizations. Security Hub tidak dapat diaktifkan secara otomatis di akun manajemen Organisasi. Anda harus mengaktifkan Security Hub secara manual di akun manajemen Organisasi sebelum dapat menambahkannya sebagai akun anggota.
- Jika akun sudah mengaktifkan Security Hub, Security Hub tidak membuat perubahan lain pada akun tersebut. Ini hanya memungkinkan keanggotaan.

Agar Security Hub menghasilkan temuan kontrol, akun anggota harus telah AWS Config diaktifkan dan dikonfigurasi untuk merekam sumber daya yang diperlukan. Untuk informasi selengkapnya, lihat Mengaktifkan dan mengonfigurasi AWS Config.

Pilih metode yang Anda inginkan, dan ikuti langkah-langkah untuk mengaktifkan akun organisasi sebagai akun anggota Security Hub.

Security Hub console

Mengaktifkan akun organisasi secara manual sebagai anggota Security Hub

1. Buka AWS Security Hub konsol di https://console.aws.amazon.com/securityhub/.

   Masuk menggunakan kredensi akun administrator yang didelegasikan.
2. Di panel navigasi Security Hub, di bawah Pengaturan, pilih Konfigurasi.
3. Dalam daftar Akun, pilih setiap akun organisasi yang ingin Anda aktifkan.
4. Pilih Tindakan, lalu pilih Tambah anggota.

Security Hub API

Mengaktifkan akun organisasi secara manual sebagai anggota Security Hub

Memanggil `CreateMembers`API dari akun administrator yang didelegasikan. Agar setiap akun dapat diaktifkan, berikan ID akun.

Tidak seperti proses undangan manual, ketika Anda memanggil `CreateMembers` untuk mengaktifkan akun organisasi, Anda tidak perlu mengirim undangan.

AWS CLI

Mengaktifkan akun organisasi secara manual sebagai anggota Security Hub

Jalankan `create-members`perintah dari akun administrator yang didelegasikan. Agar setiap akun dapat diaktifkan, berikan ID akun.

Berbeda dengan proses undangan manual, ketika Anda menjalankan `create-members` untuk mengaktifkan akun organisasi, Anda tidak perlu mengirim undangan.

```
aws securityhub create-members --account-details '[{"AccountId": "<accountId>"}]'
```

Contoh

```
aws securityhub create-members --account-details '[{"AccountId": "123456789111"},
 {"AccountId": "123456789222"}]'
```

Memutuskan akun anggota dari organisasi Anda

Untuk berhenti menerima dan melihat temuan dari akun AWS Security Hub anggota, Anda dapat memisahkan akun anggota dari organisasi Anda.

> **Note**
>
> Jika Anda menggunakan konfigurasi pusat, disasosiasi bekerja secara berbeda. Anda dapat membuat kebijakan konfigurasi yang menonaktifkan Security Hub di satu atau beberapa akun anggota yang dikelola secara terpusat. Setelah itu, akun-akun ini masih menjadi bagian dari organisasi, tetapi tidak akan menghasilkan temuan Security Hub. Jika Anda menggunakan konfigurasi pusat tetapi juga memiliki akun anggota yang diundang secara manual, Anda dapat memisahkan satu atau beberapa akun yang diundang secara manual.

Akun anggota yang dikelola menggunakan tidak AWS Organizations dapat memisahkan akun mereka dari akun administrator. Hanya akun administrator yang dapat memisahkan akun anggota.

Memutuskan hubungan akun anggota tidak menutup akun. Sebaliknya, itu menghapus akun anggota dari organisasi. Akun anggota yang terputus menjadi mandiri Akun AWS yang tidak lagi dikelola oleh integrasi Security Hub dengan. AWS Organizations

Pilih metode pilihan Anda, dan ikuti langkah-langkah untuk memisahkan akun anggota dari organisasi.

Security Hub console

Untuk memisahkan akun anggota dari organisasi

1. Buka AWS Security Hub konsol di https://console.aws.amazon.com/securityhub/.

   Masuk menggunakan kredensi akun administrator yang didelegasikan.
2. Di panel navigasi, di bawah Pengaturan, pilih Konfigurasi.

3. Di bagian Akun, pilih akun yang ingin Anda pisahkan. Jika Anda menggunakan konfigurasi pusat, Anda dapat memilih akun yang diundang secara manual untuk dipisahkan dari tab. `Invitation accounts` Tab ini hanya terlihat jika Anda menggunakan konfigurasi pusat.
4. Pilih Tindakan, lalu pilih Putuskan akun.

Security Hub API

Untuk memisahkan akun anggota dari organisasi

Memanggil `DisassociateMembers`API dari akun administrator yang didelegasikan. Anda harus memberikan Akun AWS ID untuk akun anggota untuk dipisahkan. Untuk melihat daftar akun anggota, panggil `ListMembers`API.

AWS CLI

Untuk memisahkan akun anggota dari organisasi

Jalankan `disassociate-members`perintah> dari akun administrator yang didelegasikan. Anda harus memberikan Akun AWS ID untuk akun anggota untuk dipisahkan. Untuk melihat daftar akun anggota, jalankan `list-members`perintah>.

```
aws securityhub disassociate-members --account-ids "<accountIds>"
```

Contoh

```
aws securityhub disassociate-members --account-ids "123456789111" "123456789222"
```

Anda juga dapat menggunakan AWS Organizations konsol, AWS CLI, atau AWS SDK untuk memisahkan akun anggota dari organisasi Anda. Untuk informasi selengkapnya, lihat Menghapus akun anggota dari organisasi Anda di Panduan AWS Organizations Pengguna.

Mengelola akun dengan undangan

Anda dapat mengelola beberapa AWS Security Hub akun secara terpusat dengan dua cara, dengan mengintegrasikan Security Hub dengan AWS Organizations atau dengan mengirim dan menerima undangan keanggotaan secara manual. Anda harus menggunakan proses manual jika Anda memiliki akun mandiri atau jika Anda tidak berintegrasi dengan Organizations. Dalam manajemen

akun manual, administrator Security Hub mengundang akun untuk menjadi anggota. Hubungan administrator-anggota terjalin ketika calon anggota menerima undangan. Akun administrator Security Hub dapat mengelola Security Hub hingga 1.000 akun anggota berbasis undangan.

> **Tip**
>
> Jika Anda membuat organisasi berbasis undangan di Security Hub, Anda selanjutnya dapat beralih menggunakan. AWS Organizations Jika Anda memiliki lebih dari satu akun anggota, kami sarankan untuk mengelola akun melalui AWS Organizations.

Agregasi temuan Lintas Wilayah dan data lainnya tersedia untuk akun yang Anda undang melalui proses undangan manual. Namun, administrator harus mengundang akun anggota dari Wilayah agregasi dan semua Wilayah yang ditautkan agar agregasi lintas wilayah berfungsi. Selain itu, akun anggota harus mengaktifkan Security Hub di Wilayah agregasi dan semua Wilayah tertaut untuk memberikan administrator kemampuan untuk melihat temuan dari akun anggota.

Kebijakan konfigurasi tidak didukung untuk akun anggota yang diundang secara manual. Sebagai gantinya, Anda harus mengonfigurasi pengaturan Security Hub secara terpisah di setiap akun anggota dan Wilayah AWS saat Anda menggunakan proses undangan manual.

Anda juga harus menggunakan proses berbasis undangan manual untuk akun yang bukan milik organisasi Anda. Misalnya, Anda mungkin tidak menyertakan akun pengujian di organisasi Anda. Atau, Anda mungkin ingin menggabungkan akun dari beberapa organisasi di bawah satu akun administrator Security Hub. Akun administrator Security Hub harus mengirim undangan ke akun milik organisasi lain.

Pada halaman Konfigurasi konsol Security Hub, akun yang ditambahkan melalui undangan tercantum di tab Akun undangan. Jika Anda menggunakanCara kerja konfigurasi pusat, tetapi juga mengundang akun di luar organisasi, Anda dapat melihat temuan dari akun berbasis undangan di tab ini. Namun, administrator Security Hub tidak dapat mengonfigurasi akun berbasis undangan di seluruh Wilayah melalui penggunaan kebijakan konfigurasi.

Topik di bagian ini menjelaskan cara mengelola akun anggota melalui undangan.

Topik

- Menambahkan dan mengundang akun anggota
- Menanggapi undangan untuk menjadi akun anggota

- Memutuskan akun anggota
- Menghapus akun anggota
- Memutuskan hubungan dari akun administrator Anda
- Transisi ke manajemen AWS Organizations akun

Menambahkan dan mengundang akun anggota

Akun Anda menjadi AWS Security Hub administrator untuk akun yang menerima undangan Anda.

Ketika Anda menerima undangan dari akun lain, akun Anda menjadi akun anggota, dan akun itu menjadi administrator Anda.

Jika akun Anda adalah akun administrator, Anda tidak dapat menerima undangan untuk menjadi akun anggota.

Menambahkan akun anggota terdiri dari langkah-langkah berikut:

1. Akun administrator menambahkan akun anggota ke daftar akun anggota mereka.
2. Akun administrator mengirimkan undangan ke akun anggota.
3. Akun anggota menerima undangan.

Tambahkan akun anggota

Dari konsol Security Hub, Anda dapat menambahkan akun ke daftar akun anggota Anda. Di konsol Security Hub, Anda dapat memilih akun satu per satu, atau mengunggah `.csv` file yang berisi informasi akun.

Untuk setiap akun, Anda harus memberikan ID akun dan alamat email. Alamat email harus berupa alamat email untuk dihubungi tentang masalah keamanan di akun. Ini tidak digunakan untuk memverifikasi akun.

Pilih metode pilihan Anda, dan ikuti langkah-langkah untuk menambahkan akun anggota.

Security Hub console

Untuk menambahkan akun ke daftar akun anggota Anda

1. Buka AWS Security Hub konsol di https://console.aws.amazon.com/securityhub/.

Masuk menggunakan kredensi akun administrator.

2. Di panel kiri, pilih Pengaturan.
3. Pada halaman Pengaturan, pilih Akun, lalu pilih Tambah akun. Anda kemudian dapat menambahkan akun satu per satu atau mengunggah `.csv` file yang berisi daftar akun.
4. Untuk memilih akun, lakukan salah satu hal berikut:

   - Untuk menambahkan akun satu per satu, di bawah Masukkan akun, masukkan ID akun dan alamat email akun yang akan ditambahkan, lalu pilih Tambah.

     Ulangi proses ini untuk setiap akun.

   - Untuk menggunakan file nilai yang dipisahkan koma (.csv) untuk menambahkan beberapa akun, buat file terlebih dahulu. File harus berisi ID akun dan alamat email untuk ditambahkan setiap akun.

     Dalam `.csv` daftar Anda, akun harus muncul satu per baris. Baris pertama `.csv` file harus berisi header. Di header, kolom pertama adalah **`Account ID`** dan kolom kedua adalah**`Email`**.

     Setiap baris berikutnya harus berisi ID akun dan alamat email yang valid untuk ditambahkan akun.

     Berikut adalah contoh `.csv` file ketika dilihat di editor teks.

     ```
     Account ID,Email
     111111111111,user@example.com
     ```

     Dalam program spreadsheet, bidang muncul di kolom terpisah. Format yang mendasarinya masih dipisahkan koma. Anda harus memformat ID akun sebagai angka non-desimal. Misalnya, ID akun 444455556666 tidak dapat diformat sebagai 444455556666.0. Pastikan juga bahwa pemformatan angka tidak menghapus nol di depan dari ID akun.

     Untuk memilih file, di konsol, pilih Unggah daftar (.csv). Kemudian pilih Browse.

     Setelah Anda memilih file, pilih Tambah akun.

5. Setelah Anda selesai menambahkan akun, di bawah Akun yang akan ditambahkan, pilih Berikutnya.

Security Hub API

Untuk menambahkan akun ke daftar akun anggota Anda

Memanggil `CreateMembers`API dari akun administrator. Untuk setiap akun anggota untuk ditambahkan, Anda harus memberikan Akun AWS ID.

AWS CLI

Untuk menambahkan akun ke daftar akun anggota Anda

Jalankan `create-members`perintah dari akun administrator. Untuk setiap akun anggota untuk ditambahkan, Anda harus memberikan Akun AWS ID.

```
aws securityhub create-members --account-details '[{"AccountId": "<accountID1>"}]'
```

Contoh

```
aws securityhub create-members --account-details '[{"AccountId": "123456789111"},
 {"AccountId": "123456789222"}]'
```

Undang akun anggota

Setelah Anda menambahkan akun anggota, Anda mengirim undangan ke akun anggota. Anda juga dapat mengirim ulang undangan ke akun yang Anda lepaskan dari administrator.

Security Hub console

Mengundang akun calon member

1. Buka AWS Security Hub konsol di https://console.aws.amazon.com/securityhub/.

   Masuk menggunakan kredensi akun administrator.
2. Di panel navigasi, pilih Pengaturan, lalu pilih Akun.
3. Untuk akun yang akan diundang, pilih Undang di kolom Status.
4. Saat diminta untuk mengonfirmasi, pilih Undang.

> **Note**
>
> Untuk mengirim ulang undangan ke akun yang tidak terkait, pilih setiap akun yang tidak terkait di halaman Akun. Untuk Tindakan, pilih Kirim ulang undangan.

Security Hub API

Mengundang akun calon member

Memanggil `InviteMembers`API dari akun administrator. Untuk setiap akun yang akan diundang, Anda harus memberikan Akun AWS ID.

AWS CLI

Mengundang akun calon member

Jalankan `invite-members`perintah dari akun administrator. Untuk setiap akun yang akan diundang, Anda harus memberikan Akun AWS ID.

```
aws securityhub invite-members --account-ids <accountIDs>
```

Contoh

```
aws securityhub invite-members --account-ids "123456789111" "123456789222"
```

Menanggapi undangan untuk menjadi akun anggota

Anda dapat menerima atau menolak undangan untuk menjadi akun anggota.

Setelah Anda menerima undangan, akun Anda menjadi akun AWS Security Hub anggota. Akun yang mengirim undangan menjadi akun administrator Security Hub Anda. Pengguna akun administrator dapat melihat temuan untuk akun anggota Anda di Security Hub.

Jika Anda menolak undangan, maka akun Anda ditandai sebagai Mengundurkan diri pada daftar akun anggota akun administrator.

Anda hanya dapat menerima satu undangan untuk menjadi akun anggota.

Sebelum Anda dapat menerima atau menolak undangan, Anda harus mengaktifkan Security Hub.

Ingat bahwa semua akun Security Hub harus AWS Config diaktifkan dan dikonfigurasi untuk merekam semua sumber daya. Untuk detail tentang persyaratan AWS Config, lihat Mengaktifkan dan mengonfigurasi AWS Config.

Terima undangan

Pilih metode pilihan Anda, dan ikuti langkah-langkah untuk menerima undangan untuk menjadi akun anggota.

Security Hub console

Untuk menerima undangan keanggotaan

1. Buka AWS Security Hub konsol di https://console.aws.amazon.com/securityhub/.
2. Di panel navigasi, pilih Pengaturan, lalu pilih Akun.
3. Di bagian Akun Administrator, aktifkan Terima, lalu pilih Terima undangan.

Security Hub API

Untuk menerima undangan keanggotaan

Memanggil `AcceptAdministratorInvitation`API. Anda harus memberikan pengenal undangan dan Akun AWS ID akun administrator. Untuk mengambil detail tentang undangan, gunakan `ListInvitations`operasi.

AWS CLI

Untuk menerima undangan keanggotaan

Jalankan perintah `accept-administrator-invitation`. Anda harus memberikan pengenal undangan dan Akun AWS ID akun administrator. Untuk mengambil detail tentang undangan, jalankan `list-invitations`perintah.

```
aws securityhub accept-administrator-invitation --administrator-
id <administratorAccountID> --invitation-id <invitationID>
```

Contoh

```
aws securityhub accept-administrator-invitation --administrator-id 123456789012 --
invitation-id 7ab938c5d52d7904ad09f9e7c20cc4eb
```

> **Note**
>
> Konsol Security Hub terus digunakan`AcceptInvitation`. Pada akhirnya akan berubah untuk digunakan`AcceptAdministratorInvitation`. Setiap kebijakan IAM yang secara khusus mengontrol akses ke fungsi ini harus terus digunakan`AcceptInvitation`. Anda juga harus menambahkan kebijakan Anda `AcceptAdministratorInvitation` untuk memastikan bahwa izin yang benar diberlakukan setelah konsol mulai digunakan`AcceptAdministratorInvitation`.

Tolak undangan

Anda dapat menolak undangan untuk menjadi akun anggota. Saat Anda menolak undangan di konsol Security Hub, akun Anda ditandai sebagai Mengundurkan diri pada daftar akun anggota akun administrator.

Ketika Anda menolak undangan, Anda harus masuk ke akun anggota yang menerima undangan.

Pilih metode pilihan Anda, dan ikuti langkah-langkah untuk menolak undangan menjadi akun anggota.

Security Hub console

Untuk menolak undangan keanggotaan

1. Buka AWS Security Hub konsol di https://console.aws.amazon.com/securityhub/.
2. Di panel navigasi, pilih Pengaturan, lalu pilih Akun.
3. Di bagian Akun Administrator, pilih Tolak undangan.

Security Hub API

Untuk menolak undangan keanggotaan

Memanggil `DeclineInvitations`API. Anda harus memberikan Akun AWS ID akun administrator yang mengeluarkan undangan. Untuk melihat informasi tentang undangan Anda, gunakan operasi. `ListInvitations`

AWS CLI

Untuk menolak undangan keanggotaan

Jalankan perintah `decline-invitations`. Anda harus memberikan Akun AWS ID akun administrator yang mengeluarkan undangan. Untuk melihat informasi tentang undangan Anda, jalankan perintah. `list-invitations`

```
aws securityhub decline-invitations --account-ids "<administratorAccountId>"
```

Contoh

```
aws securityhub decline-invitations --account-ids "123456789012"
```

Memutuskan akun anggota

Akun AWS Security Hub administrator dapat memisahkan akun anggota untuk berhenti menerima dan melihat temuan dari akun tersebut. Anda harus memisahkan akun anggota sebelum Anda dapat menghapusnya.

Saat Anda memisahkan akun anggota, akun tersebut tetap ada dalam daftar akun anggota Anda dengan status Dihapus (Terputus). Akun Anda dihapus dari informasi akun administrator untuk akun anggota.

Untuk melanjutkan menerima temuan untuk akun, Anda dapat mengirim ulang undangan. Untuk menghapus akun anggota sepenuhnya, Anda dapat menghapus akun anggota.

Pilih metode pilihan Anda, dan ikuti langkah-langkah untuk memisahkan akun anggota yang diundang secara manual dari akun administrator.

Security Hub console

Untuk memisahkan akun anggota yang diundang secara manual

1. Buka AWS Security Hub konsol di https://console.aws.amazon.com/securityhub/.

   Masuk menggunakan kredensi akun administrator.
2. Di panel navigasi, di bawah Pengaturan, pilih Konfigurasi.
3. Di bagian Akun, pilih akun yang ingin Anda pisahkan.
4. Pilih Tindakan, lalu pilih Disassociate account.

Security Hub API

Untuk memisahkan akun anggota yang diundang secara manual

Memanggil `DisassociateMembers`API dari akun administrator. Anda harus memberikan Akun AWS ID akun anggota yang ingin Anda pisahkan. Untuk melihat daftar akun anggota, gunakan `ListMembers`operasi.

AWS CLI

Untuk memisahkan akun anggota yang diundang secara manual

Jalankan `disassociate-members`perintah dari akun administrator. Anda harus memberikan Akun AWS ID akun anggota yang ingin Anda pisahkan. Untuk melihat daftar akun anggota, jalankan `list-members`perintah.

```
aws securityhub disassociate-members --account-ids <accountIds>
```

Contoh

```
aws securityhub disassociate-members --account-ids "123456789111" "123456789222"
```

Menghapus akun anggota

Sebagai akun AWS Security Hub administrator, Anda dapat menghapus akun anggota yang ditambahkan melalui undangan. Sebelum Anda dapat menghapus akun yang diaktifkan, Anda harus memisahkannya.

Ketika Anda menghapus akun anggota, itu sepenuhnya dihapus dari daftar. Untuk memulihkan keanggotaan akun, Anda harus menambahkan dan mengundangnya lagi seolah-olah itu adalah akun anggota yang sama sekali baru.

Anda tidak dapat menghapus akun milik organisasi dan yang dikelola menggunakan integrasi dengan AWS Organizations.

Pilih metode pilihan Anda, dan ikuti langkah-langkah untuk menghapus akun anggota yang diundang secara manual.

Security Hub console

Untuk menghapus akun anggota yang diundang secara manual

1. Buka AWS Security Hub konsol di https://console.aws.amazon.com/securityhub/.

   Masuk menggunakan akun administrator.
2. Di panel navigasi, pilih Pengaturan, lalu pilih Konfigurasi.
3. Pilih tab Akun undangan. Kemudian, pilih akun yang akan dihapus.
4. Pilih Tindakan, lalu pilih Hapus. Opsi ini hanya tersedia jika Anda telah memisahkan akun. Anda harus memisahkan akun anggota sebelum dapat dihapus.

Security Hub API

Untuk menghapus akun anggota yang diundang secara manual

Memanggil `DeleteMembers`API dari akun administrator. Anda harus memberikan Akun AWS ID akun anggota yang ingin Anda hapus. Untuk mengambil daftar akun anggota, panggil API. `ListMembers`

AWS CLI

Untuk menghapus akun anggota yang diundang secara manual

Jalankan `delete-members`perintah dari akun administrator. Anda harus memberikan Akun AWS ID akun anggota yang ingin Anda hapus. Untuk mengambil daftar akun anggota, jalankan `list-members`perintah.

```
aws securityhub delete-members --account-ids <memberAccountIDs>
```

Contoh

```
aws securityhub delete-members --account-ids "123456789111" "123456789222"
```

Memutuskan hubungan dari akun administrator Anda

Jika akun Anda ditambahkan sebagai akun AWS Security Hub anggota melalui undangan, Anda dapat memisahkan akun anggota dari akun administrator. Setelah Anda memisahkan akun anggota, Security Hub tidak mengirimkan temuan dari akun ke akun administrator.

Akun anggota yang dikelola menggunakan integrasi dengan tidak AWS Organizations dapat memisahkan akun mereka dari akun administrator. Hanya administrator yang didelegasikan Security Hub yang dapat memisahkan akun anggota yang dikelola dengan Organizations.

Ketika Anda memisahkan diri dari akun administrator Anda, akun Anda tetap berada dalam daftar anggota akun administrator dengan status Mengundurkan diri. Namun, akun administrator tidak menerima temuan apa pun untuk akun Anda.

Setelah Anda memisahkan diri dari akun administrator, undangan untuk menjadi anggota masih tetap ada. Anda dapat menerima undangan lagi di masa depan.

Security Hub console

Untuk memisahkan diri dari akun administrator Anda

1. Buka AWS Security Hub konsol di https://console.aws.amazon.com/securityhub/.
2. Di panel navigasi, pilih Pengaturan, lalu pilih Akun.
3. Di bagian Akun Administrator, matikan Terima, lalu pilih Perbarui.

Security Hub API

Untuk memisahkan diri dari akun administrator Anda

Memanggil `DisassociateFromAdministratorAccount`API.

AWS CLI

Untuk memisahkan diri dari akun administrator Anda

Jalankan perintah `disassociate-from-administrator-account`.

```
aws securityhub disassociate-from-administrator-account
```

> **Note**
>
> Konsol Security Hub terus digunakan`DisassociateFromMasterAccount`. Pada akhirnya akan berubah untuk digunakan`DisassociateFromAdministratorAccount`. Setiap kebijakan IAM yang secara khusus mengontrol akses ke fungsi ini harus terus digunakan`DisassociateFromMasterAccount`. Anda juga harus

menambahkan kebijakan Anda `DisassociateFromAdministratorAccount` untuk memastikan bahwa izin yang benar diberlakukan setelah konsol mulai digunakan`DisassociateFromAdministratorAccount`.

Transisi ke manajemen AWS Organizations akun

Saat Anda mengelola akun secara manualAWS Security Hub, Anda harus mengundang akun calon anggota dan mengonfigurasi setiap akun anggota secara terpisah di masing-masing Wilayah AWS akun.

Dengan mengintegrasikan Security Hub danAWS Organizations, Anda dapat menghilangkan kebutuhan untuk mengirim undangan dan mendapatkan kontrol lebih besar atas cara Security Hub dikonfigurasi dan disesuaikan di organisasi Anda.

Anda dapat menggunakan pendekatan gabungan di mana Anda menggunakan AWS Organizations integrasi, tetapi juga mengundang akun secara manual di luar organisasi Anda. Namun, kami merekomendasikan secara eksklusif menggunakan integrasi Organizations. Konfigurasi pusat, fitur yang membantu Anda mengelola Security Hub di beberapa akun dan Wilayah, hanya tersedia saat Anda berintegrasi dengan Organizations.

Bagian ini mencakup bagaimana Anda dapat beralih dari manajemen akun berbasis undangan manual ke mengelola akun dengan. AWS Organizations

Mengintegrasikan Security Hub dengan AWS Organizations

Pertama, Anda harus mengintegrasikan Security Hub danAWS Organizations.

Anda dapat mengintegrasikan layanan ini dengan menyelesaikan langkah-langkah berikut:

- Buat organisasi diAWS Organizations. Untuk petunjuk, lihat Membuat organisasi di Panduan AWS Organizations Pengguna.
- Dari akun manajemen Organizations, tentukan akun administrator yang didelegasikan Security Hub.

> **Note**
>
> Akun manajemen organisasi tidak dapat ditetapkan sebagai akun DA.

Untuk instruksi detail, lihat Mengintegrasikan Security Hub dengan AWS Organizations.

Dengan menyelesaikan langkah-langkah sebelumnya, Anda memberikan akses tepercaya untuk Security Hub di. AWS Organizations Ini juga memungkinkan Security Hub saat ini Wilayah AWS untuk akun administrator yang didelegasikan.

Administrator yang didelegasikan dapat mengelola organisasi di Security Hub, terutama dengan menambahkan akun organisasi sebagai akun anggota Security Hub. Administrator juga dapat mengakses pengaturan, data, dan sumber daya Security Hub tertentu untuk akun tersebut.

Saat Anda beralih ke manajemen akun menggunakan Organizations, akun berbasis undangan tidak otomatis menjadi anggota Security Hub. Hanya akun yang Anda tambahkan ke organisasi baru yang dapat menjadi anggota Security Hub.

Konfigurasi pusat vs. konfigurasi lokal

Setelah mengaktifkan integrasi, Anda dapat mengelola akun dengan Organizations. Untuk informasi, lihat Mengelola akun dengan AWS Organizations. Manajemen akun bervariasi berdasarkan jenis konfigurasi organisasi Anda.

Ada dua jenis konfigurasi yang mungkin untuk organisasi Anda, lokal dan pusat. Jenis konfigurasi default Anda adalah konfigurasi lokal. Untuk melihat jenis konfigurasi Anda saat ini, pilih Pengaturan pada panel navigasi konsol Security Hub dan kemudian Konfigurasi. Anda juga dapat memanggil `DescribeOrganizationConfiguration`API untuk melihat jenis konfigurasi Anda.

Di bawah konfigurasi lokal, akun administrator yang didelegasikan dapat memilih untuk secara otomatis mengaktifkan Security Hub dan standar keamanan default di akun baru saat mereka bergabung dengan organisasi. Pengaturan akun baru ini berlaku di Wilayah saat ini. Pengaturan Security Hub lainnya harus dikonfigurasi secara terpisah oleh setiap akun anggota di setiap Wilayah.

Sebaiknya gunakan konfigurasi pusat alih-alih konfigurasi lokal. Di bawah konfigurasi pusat, akun administrator yang didelegasikan dapat membuat kebijakan konfigurasi Security Hub yang berlaku di beberapa Wilayah dan menentukan kapabilitas Security Hub di berbagai akun dan unit organisasi (OU) organisasi Anda. Anda dapat menerapkan kebijakan konfigurasi tunggal ke seluruh organisasi, atau kebijakan konfigurasi yang berbeda ke akun dan OU yang berbeda. Misalnya, Anda dapat mengaktifkan satu set standar dan kontrol dalam akun produksi dan serangkaian standar dan kontrol yang berbeda dalam akun pengujian. DA dapat mengedit kebijakan konfigurasi sesuai kebutuhan.

Untuk informasi selengkapnya tentang cara kerja konfigurasi pusat, lihatCara kerja konfigurasi pusat.

Untuk petunjuk tentang beralih dari konfigurasi lokal ke pusat, lihatMulai menggunakan konfigurasi pusat.

Tindakan yang diizinkan untuk akun

Akun administrator dan anggota memiliki akses ke AWS Security Hub tindakan yang dicatat dalam tabel berikut. Dalam tabel, nilainya memiliki arti sebagai berikut:

- Apa saja — Akun dapat melakukan tindakan untuk akun anggota mana pun di bawah administrator yang sama.
- Saat ini — Akun dapat melakukan tindakan hanya untuk dirinya sendiri (akun yang saat ini Anda masuki).
- Dash — Menunjukkan bahwa akun tidak dapat melakukan tindakan.

Sebagaimana dicatat dalam tabel, tindakan yang diizinkan berbeda berdasarkan apakah Anda berintegrasi dengan AWS Organizations dan jenis konfigurasi yang digunakan organisasi Anda. Untuk informasi tentang perbedaan antara konfigurasi pusat dan lokal, lihatMengelola akun dengan AWS Organizations.

Security Hub tidak menyalin temuan akun anggota ke akun administrator. Di Security Hub, semua temuan dicerna ke Wilayah tertentu untuk akun tertentu. Di setiap Wilayah, akun administrator dapat melihat dan mengelola temuan untuk akun anggota mereka di Wilayah tersebut.

Jika Anda menetapkan Wilayah agregasi, akun administrator dapat melihat dan mengelola temuan akun anggota dari Wilayah tertaut yang direplikasi ke Wilayah agregasi. Untuk informasi selengkapnya tentang agregasi lintas wilayah, lihat agregasi Lintas Wilayah.

Tabel ini mencerminkan izin default untuk akun administrator dan anggota. Anda dapat menggunakan kebijakan IAM khusus untuk membatasi akses lebih lanjut ke fitur dan fungsi Security Hub. Untuk panduan dan contoh, lihat posting blog Menyelaraskan kebijakan IAM ke persona pengguna. AWS Security Hub

Tindakan yang diizinkan jika Anda berintegrasi dengan Organizations dan menggunakan konfigurasi pusat

Akun administrator dan anggota dapat mengakses tindakan Security Hub sebagai berikut jika Anda berintegrasi dengan Organizations dan menggunakan konfigurasi pusat.

Tindakan	Akun administrator yang didelegasikan Security Hub	Akun anggota yang dikelola secara terpusat	Akun anggota yang dikelola sendiri
Membuat dan mengelola kebijakan konfigurasi Security Hub	Untuk akun yang dikelola sendiri dan terpusat	–	–
Lihat akun organisasi	Setiap	–	–
Putuskan akun anggota	Setiap	–	–
Hapus akun anggota	Akun non-organisasi	–	–
Nonaktifkan Security Hub	Untuk akun saat ini dan akun yang dikelola secara terpusat	–	Saat ini
Lihat temuan dan temukan sejarah	Setiap	Saat ini	Saat ini
Perbarui temuan	Setiap	Saat ini	Saat ini
Lihat hasil wawasan	Setiap	Saat ini	Saat ini
Lihat detail kontrol	Setiap	Saat ini	Saat ini
Mengaktifkan atau menonaktifkan temuan kontrol terkonsolidasi	Setiap	–	–
Aktifkan dan nonaktifkan standar	Untuk akun saat ini dan akun yang dikelola secara terpusat	–	Saat ini

Tindakan	Akun administrator yang didelegasikan Security Hub	Akun anggota yang dikelola secara terpusat	Akun anggota yang dikelola sendiri
Aktifkan dan nonaktifkan kontrol	Untuk akun saat ini dan akun yang dikelola secara terpusat	–	Saat ini
Aktifkan dan nonaktifkan integrasi	Saat ini	Saat ini	Saat ini
Konfigurasikan agregasi lintas wilayah	Setiap	–	–
Pilih beranda Wilayah dan terkait Wilayah	Apa saja (harus berhenti dan memulai ulang konfigurasi pusat untuk mengubah Wilayah rumah)	–	–
Konfigurasikan tindakan khusus	Saat ini	Saat ini	Saat ini
Konfigurasikan aturan otomatisasi	Setiap	–	–
Konfigurasikan wawasan khusus	Saat ini	Saat ini	Saat ini

Tindakan yang diizinkan jika Anda berintegrasi dengan Organizations dan menggunakan konfigurasi lokal

Akun administrator dan anggota dapat mengakses tindakan Security Hub sebagai berikut jika Anda berintegrasi dengan Organizations dan menggunakan konfigurasi lokal.

Tindakan	Akun administrator yang didelegasikan Security Hub	Akun anggota
Membuat dan mengelola kebijakan konfigurasi Security Hub	–	–
Lihat akun organisasi	Setiap	–
Putuskan akun anggota	Setiap	–
Hapus akun anggota	–	–
Nonaktifkan Security Hub	–	Saat ini (jika akun dipisahkan dari administrator yang didelegasikan)
Lihat temuan dan temukan sejarah	Setiap	Saat ini
Perbarui temuan	Setiap	Saat ini
Lihat hasil wawasan	Setiap	Saat ini
Lihat detail kontrol	Setiap	Saat ini
Mengaktifkan atau menonaktifkan temuan kontrol terkonsolidasi	Setiap	–
Aktifkan dan nonaktifkan standar	Saat ini	Saat ini
Secara otomatis mengaktifkan Security Hub dan standar default di akun organisasi baru	Untuk akun saat ini dan akun organisasi baru	–
Aktifkan dan nonaktifkan kontrol	Saat ini	Saat ini

Tindakan	Akun administrator yang didelegasikan Security Hub	Akun anggota
Aktifkan dan nonaktifkan integrasi	Saat ini	Saat ini
Konfigurasikan agregasi lintas wilayah	Setiap	–
Konfigurasikan tindakan khusus	Saat ini	Saat ini
Konfigurasikan aturan otomatisasi	Setiap	–
Konfigurasikan wawasan khusus	Saat ini	Saat ini

Tindakan yang diizinkan untuk akun berbasis undangan

Akun administrator dan anggota dapat mengakses tindakan Security Hub sebagai berikut jika Anda menggunakan metode berbasis undangan untuk mengelola akun secara manual, bukan mengintegrasikan dengan. AWS Organizations

Tindakan	Akun administrator Security Hub	Akun anggota
Membuat dan mengelola kebijakan konfigurasi Security Hub	–	–
Lihat akun organisasi	Setiap	–
Putuskan akun anggota	Setiap	Saat ini
Hapus akun anggota	Setiap	–

Tindakan	Akun administrator Security Hub	Akun anggota
Nonaktifkan Security Hub	Saat ini (jika tidak ada akun anggota yang diaktifkan)	Saat ini (jika akun dipisahkan dari akun administrator)
Lihat temuan dan temukan sejarah	Setiap	Saat ini
Perbarui temuan	Setiap	Saat ini
Lihat hasil wawasan	Setiap	Saat ini
Lihat detail kontrol	Setiap	Saat ini
Mengaktifkan atau menonakti fkan temuan kontrol terkonsol idasi	Setiap	–
Aktifkan dan nonaktifkan standar	Saat ini	Saat ini
Secara otomatis mengaktif kan Security Hub dan standar default di akun organisasi baru	–	–
Aktifkan dan nonaktifkan kontrol	Saat ini	Saat ini
Aktifkan dan nonaktifkan integrasi	Saat ini	Saat ini
Konfigurasikan agregasi lintas wilayah	Setiap	–
Konfigurasikan tindakan khusus	Saat ini	Saat ini
Konfigurasikan aturan otomatisasi	Setiap	–

Tindakan	Akun administrator Security Hub	Akun anggota
Konfigurasikan wawasan khusus	Saat ini	Saat ini

Pembatasan dan rekomendasi tentang manajemen akun

Bagian berikut merangkum beberapa batasan dan rekomendasi yang perlu diingat saat mengelola akun anggota di AWS Security Hub.

Jumlah maksimum akun anggota

Jika Anda menggunakan integrasi dengan AWS Organizations, Security Hub mendukung hingga 10.000 akun anggota per akun administrator yang didelegasikan di masing-masing Wilayah AWSakun. Jika Anda mengaktifkan dan mengelola Security Hub secara manual, Security Hub mendukung hingga 1.000 undangan akun anggota per akun administrator di setiap Wilayah.

Akun dan Wilayah

Keanggotaan menurut organisasi

Jika Anda mengintegrasikan Security Hub dengan AWS Organizations, akun manajemen Organisasi dapat menunjuk akun administrator yang didelegasikan (DA) untuk Security Hub. Akun manajemen organisasi tidak dapat ditetapkan sebagai DA di Organizations. Meskipun ini diizinkan di Security Hub, kami menyarankan agar akun manajemen Organisasi tidak boleh menjadi DA.

Kami menyarankan Anda memilih akun DA yang sama di semua Wilayah. Jika Anda menggunakan konfigurasi pusat, maka Security Hub menetapkan akun DA yang sama di semua Wilayah tempat Anda mengonfigurasi Security Hub untuk organisasi Anda.

Kami juga menyarankan Anda memilih akun DA yang sama di seluruh layanan AWS keamanan dan kepatuhan untuk membantu Anda mengelola masalah terkait keamanan dalam satu panel kaca.

Keanggotaan berdasarkan undangan

Untuk akun anggota yang dibuat berdasarkan undangan, asosiasi akun administrator-anggota dibuat hanya di Wilayah tempat undangan dikirim. Akun administrator harus mengaktifkan Security Hub

di setiap Wilayah tempat Anda ingin menggunakannya. Akun administrator kemudian mengundang setiap akun untuk menjadi akun anggota di Wilayah tersebut.

Pembatasan hubungan administrator-anggota

> **Note**
>
> Jika Anda menggunakan integrasi Security Hub dengan AWS Organizations, dan belum mengundang akun anggota secara manual, bagian ini tidak berlaku untuk Anda.

Akun tidak dapat berupa akun administrator dan akun anggota secara bersamaan.

Akun anggota hanya dapat dikaitkan dengan satu akun administrator. Jika akun organisasi diaktifkan oleh akun administrator Security Hub, akun tidak dapat menerima undangan dari akun lain. Jika akun telah menerima undangan, akun tidak dapat diaktifkan oleh akun administrator Security Hub untuk organisasi tersebut. Itu juga tidak dapat menerima undangan dari akun lain.

Untuk proses undangan manual, menerima undangan keanggotaan adalah opsional.

Mengkoordinasikan akun administrator di seluruh layanan

Security Hub mengumpulkan temuan dari berbagai AWS layanan, seperti Amazon, Amazon Inspector GuardDuty, dan Amazon Macie. Security Hub juga memungkinkan pengguna untuk beralih dari GuardDuty temuan untuk memulai penyelidikan di Amazon Detective.

Namun, hubungan administrator-anggota yang Anda atur di layanan lain ini tidak berlaku secara otomatis ke Security Hub. Security Hub merekomendasikan agar Anda menggunakan akun yang sama dengan akun administrator untuk semua layanan ini. Akun administrator ini harus menjadi akun yang bertanggung jawab atas alat keamanan. Akun yang sama juga harus menjadi akun agregator untuk AWS Config.

Misalnya, pengguna dari akun GuardDuty administrator A dapat melihat temuan untuk akun GuardDuty anggota B dan C di GuardDuty konsol. Jika akun A kemudian mengaktifkan Security Hub, pengguna dari akun A tidak secara otomatis melihat GuardDuty temuan untuk akun B dan C di Security Hub. Hubungan administrator-anggota Security Hub juga diperlukan untuk akun ini.

Untuk melakukan ini, buat akun A sebagai akun administrator Security Hub dan aktifkan akun B dan C untuk menjadi akun anggota Security Hub.

Pengaruh tindakan akun pada data Security Hub

Tindakan akun ini memiliki efek berikut pada AWS Security Hub data.

Security Hub dinonaktifkan

Jika Anda menggunakan konfigurasi pusat, administrator yang didelegasikan (DA) dapat membuat kebijakan konfigurasi Security Hub yang menonaktifkan AWS Security Hub di akun tertentu dan unit organisasi (OU). Dalam hal ini, Security Hub dinonaktifkan di akun tertentu dan OU di Wilayah asal Anda dan Wilayah yang ditautkan.

Jika tidak menggunakan konfigurasi pusat, Anda harus menonaktifkan Security Hub secara terpisah di setiap akun dan Wilayah tempat Anda mengaktifkannya.

Tidak ada temuan baru yang dihasilkan untuk akun administrator jika Security Hub dinonaktifkan di akun administrator. Anda juga tidak dapat menggunakan konfigurasi pusat jika Security Hub dinonaktifkan di akun DA. Temuan yang ada dihapus setelah 90 hari.

Integrasi dengan Layanan AWS yang lain dihapus.

Standar dan kontrol keamanan yang diaktifkan dinonaktifkan.

Data dan setelan Security Hub lainnya, termasuk tindakan kustom, wawasan, dan langganan produk pihak ketiga dipertahankan.

Akun anggota dipisahkan dari akun administrator

Ketika akun anggota dipisahkan dari akun administrator, akun administrator kehilangan izin untuk melihat temuan di akun anggota. Namun, Security Hub masih diaktifkan di kedua akun.

Jika Anda menggunakan konfigurasi pusat, DA tidak dapat mengonfigurasi Security Hub untuk akun anggota yang dipisahkan dari akun DA.

Pengaturan atau integrasi khusus yang ditentukan untuk akun administrator tidak diterapkan pada temuan dari akun anggota sebelumnya. Misalnya, setelah akun dipisahkan, Anda mungkin memiliki tindakan kustom di akun administrator yang digunakan sebagai pola peristiwa dalam EventBridge aturan Amazon. Namun, tindakan kustom ini tidak dapat digunakan di akun anggota.

Dalam daftar Akun untuk akun administrator Security Hub, akun yang dihapus memiliki status Terputus.

Akun anggota dihapus dari organisasi

Ketika akun anggota dihapus dari organisasi, akun administrator Security Hub kehilangan izin untuk melihat temuan di akun anggota. Namun, Security Hub masih diaktifkan di kedua akun dengan pengaturan yang sama sebelum dihapus.

Jika Anda menggunakan konfigurasi pusat, Anda tidak dapat mengonfigurasi Security Hub untuk akun anggota setelah dihapus dari organisasi tempat administrator yang didelegasikan berada. Namun, akun mempertahankan pengaturan yang dimilikinya sebelum dihapus kecuali Anda mengubahnya secara manual.

Dalam daftar Akun untuk akun administrator Security Hub, akun yang dihapus memiliki status Dihapus.

Akun ditangguhkan

Ketika akun ditangguhkanAWS, akun kehilangan izin untuk melihat temuan mereka di Security Hub. Tidak ada temuan baru yang dihasilkan untuk akun itu. Akun administrator untuk akun yang ditangguhkan dapat melihat temuan akun yang ada.

Untuk akun organisasi, status akun anggota juga dapat berubah menjadi Akun Ditangguhkan. Ini terjadi jika akun ditangguhkan pada saat yang sama ketika akun administrator mencoba mengaktifkan akun. Akun administrator untuk akun yang Ditangguhkan Akun tidak dapat melihat temuan untuk akun tersebut. Jika tidak, status yang ditangguhkan tidak akan memengaruhi status akun anggota.

Jika Anda menggunakan konfigurasi pusat, asosiasi kebijakan gagal jika administrator yang didelegasikan mencoba mengaitkan kebijakan konfigurasi dengan akun yang ditangguhkan.

Setelah 90 hari, akun dihentikan atau diaktifkan kembali. Ketika akun diaktifkan kembali, izin Security Hub dipulihkan. Jika status akun anggota adalah Akun Ditangguhkan, akun administrator harus mengaktifkan akun secara manual.

Akun ditutup

Ketika Akun AWS ditutup, Security Hub merespons penutupan sebagai berikut.

Security Hub menyimpan temuan untuk akun selama 90 hari sejak tanggal efektif penutupan akun. Pada akhir periode 90 hari, Security Hub secara permanen menghapus semua temuan untuk akun tersebut.

- Untuk mempertahankan temuan selama lebih dari 90 hari, Anda dapat menggunakan tindakan kustom dengan EventBridge aturan untuk menyimpan temuan di bucket Amazon S3. Selama Security Hub mempertahankan temuan, saat Anda membuka kembali akun yang ditutup, Security Hub mengembalikan temuan untuk akun tersebut.
- Jika akun tersebut adalah akun administrator Security Hub, akun tersebut dihapus sebagai administrator dan semua akun anggota dihapus. Jika akun tersebut adalah akun anggota, akun tersebut dipisahkan dan dihapus sebagai anggota dari akun administrator Security Hub.
- Untuk informasi selengkapnya, lihat Menutup akun di Panduan Pengguna AWS Billing and Cost Management.

Important

Untuk pelanggan di Wilayah AWS GovCloud (US):

- Sebelum menutup akun Anda, cadangkan, lalu hapus data kebijakan dan sumber daya akun lainnya. Anda tidak akan lagi memiliki akses ke mereka setelah Anda menutup akun.

Agregasi Lintas Wilayah

Dengan agregasi lintas wilayah, Anda dapat mengumpulkan temuan, menemukan pembaruan, wawasan, mengontrol status kepatuhan, dan skor keamanan dari beberapa Wilayah ke Wilayah agregasi tunggal. Anda kemudian dapat mengelola semua data ini dari Wilayah agregasi.

> **Note**
>
> Di AWS GovCloud (US), agregasi lintas wilayah hanya didukung untuk temuan, menemukan pembaruan, dan wawasan di seluruh wilayah. AWS GovCloud (US) Secara khusus, Anda hanya dapat mengumpulkan temuan, menemukan pembaruan, dan wawasan antara AWS GovCloud (AS-Timur) dan AWS GovCloud (AS-Barat). Di Wilayah China, agregasi lintas wilayah hanya didukung untuk temuan, menemukan pembaruan, dan wawasan di seluruh Wilayah China. Secara khusus, Anda hanya dapat mengumpulkan temuan, menemukan pembaruan, dan wawasan antara China (Beijing) dan China (Ningxia).

Misalkan Anda menetapkan US East (Virginia N.) sebagai Wilayah agregasi, dan US West (Oregon) dan US West (California N.) sebagai Wilayah terkait Anda. Ketika Anda melihat halaman Temuan di AS Timur (Virginia N.), Anda melihat temuan dari ketiga Wilayah. Pembaruan temuan tersebut juga tercermin di ketiga Wilayah.

Status pemberdayaan kontrol harus dimodifikasi di setiap Wilayah. Jika kontrol diaktifkan di Wilayah tertaut tetapi dinonaktifkan di Wilayah agregasi, Anda dapat melihat status kepatuhan kontrol dari Wilayah agregasi, tetapi Anda tidak dapat mengaktifkan atau menonaktifkan kontrol tersebut dari Wilayah agregasi.

Untuk melihat skor keamanan lintas wilayah dan status kepatuhan, tambahkan izin berikut ke peran IAM Anda yang menggunakan Security Hub:

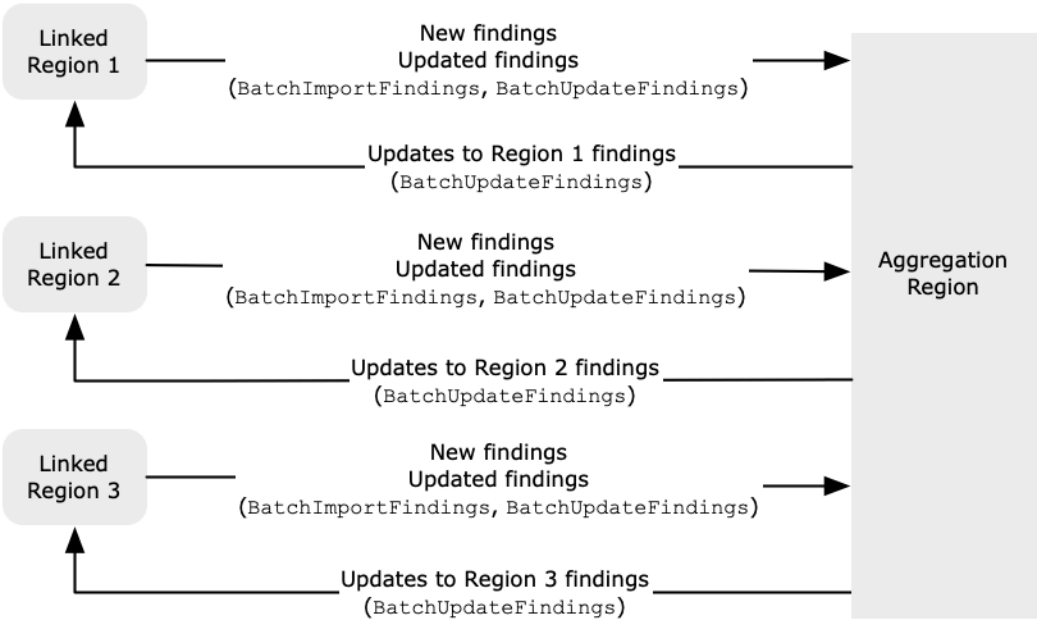
- `ListSecurityControlDefinitions`
- `BatchGetStandardsControlAssociations`
- `BatchUpdateStandardsControlAssociations`

Cara kerja agregasi lintas wilayah

Saat agregasi lintas wilayah diaktifkan, Security Hub mereplikasi data berikut dari Wilayah tertaut ke Wilayah agregasi. Ini terjadi di setiap akun yang mengaktifkan agregasi lintas wilayah.

- Temuan
- Wawasan
- Mengontrol status kepatuhan
- Skor keamanan

Selain data baru dalam daftar sebelumnya, Security Hub juga mereplikasi pembaruan data ini antara Wilayah tertaut dan Wilayah agregasi. Pembaruan yang terjadi di Wilayah tertaut direplikasi ke Wilayah agregasi. Pembaruan yang terjadi di Wilayah agregasi direplikasi kembali ke Wilayah yang ditautkan.



Jika ada pembaruan yang bertentangan di Wilayah agregasi dan Wilayah yang ditautkan, maka pembaruan terbaru akan digunakan.

Agregasi Lintas Wilayah tidak menambah biaya Security Hub. Anda tidak dikenakan biaya saat Security Hub mereplikasi data atau pembaruan baru.

Di Wilayah agregasi, halaman Ringkasan memberikan tampilan temuan aktif Anda di seluruh Wilayah tertaut. Untuk informasi, lihat Melihat ringkasan temuan lintas wilayah berdasarkan tingkat keparahan.

Panel halaman Ringkasan lainnya yang menganalisis temuan juga menampilkan informasi dari seluruh Wilayah terkait.

Skor keamanan Anda di Wilayah agregasi dihitung dengan membandingkan jumlah kontrol yang diteruskan dengan jumlah kontrol yang diaktifkan di semua Wilayah tertaut. Selain itu, jika kontrol diaktifkan di setidaknya satu Wilayah tertaut, kontrol akan terlihat di halaman detail standar Keamanan Wilayah agregasi. Status kepatuhan kontrol pada halaman detail standar mencerminkan temuan di seluruh Wilayah terkait. Jika pemeriksaan keamanan yang terkait dengan kontrol gagal di satu atau beberapa Wilayah tertaut, status kepatuhan kontrol tersebut ditampilkan sebagai Gagal pada halaman detail standar Wilayah agregasi. Jumlah pemeriksaan keamanan mencakup temuan dari semua Wilayah terkait.

Security Hub hanya mengumpulkan data dari Wilayah yang mengaktifkan Security Hub akun. Security Hub tidak diaktifkan secara otomatis untuk akun berdasarkan konfigurasi agregasi lintas wilayah.

Agregasi untuk akun administrator dan anggota

Akun mandiri, akun anggota, dan akun administrator dapat mengonfigurasi agregasi lintas wilayah. Jika dikonfigurasi oleh administrator, keberadaan akun administrator sangat penting agar agregasi lintas wilayah berfungsi di akun yang dikelola. Jika akun administrator dihapus atau dipisahkan dari akun anggota, agregasi lintas wilayah untuk akun anggota akan berhenti. Hal ini berlaku bahkan jika akun telah mengaktifkan agregasi lintas wilayah sebelum hubungan administrator-anggota dimulai.

Saat akun administrator mengaktifkan agregasi Lintas wilayah, Security Hub mereplikasi data yang dihasilkan akun administrator di semua Wilayah tertaut ke Wilayah agregasi. Selain itu, Security Hub mengidentifikasi akun anggota yang terkait dengan administrator tersebut, dan setiap akun anggota mewarisi pengaturan agregasi lintas wilayah administrator. Security Hub mereplikasi data yang dihasilkan akun anggota di semua Wilayah tertaut ke Wilayah agregasi.

Administrator dapat mengakses dan mengelola temuan keamanan dari semua akun anggota dalam wilayah yang dikelola. Namun, sebagai administrator Security Hub, Anda harus masuk ke Wilayah agregasi untuk melihat data gabungan dari semua akun anggota dan Wilayah tertaut.

Sebagai akun anggota Security Hub, Anda harus masuk ke Wilayah agregasi untuk melihat data agregat dari akun Anda dari semua Wilayah yang ditautkan. Akun anggota tidak memiliki izin untuk melihat data dari akun anggota lainnya.

Akun administrator dapat mengundang akun anggota secara manual atau berfungsi sebagai administrator yang didelegasikan dari organisasi yang terintegrasi dengannya AWS Organizations. Untuk akun anggota yang diundang secara manual, administrator harus mengundang akun dari Wilayah agregasi dan semua Wilayah yang ditautkan agar agregasi lintas wilayah berfungsi. Selain itu, akun anggota harus mengaktifkan Security Hub di Wilayah agregasi dan semua Wilayah tertaut untuk memberikan administrator kemampuan untuk melihat temuan dari akun anggota. Jika Anda tidak menggunakan Wilayah agregasi untuk tujuan lain, Anda dapat menonaktifkan standar dan integrasi Security Hub di Wilayah tersebut untuk mencegah tagihan.

Jika Anda berencana untuk menggunakan agregasi lintas wilayah, dan memiliki beberapa akun administrator, sebaiknya ikuti praktik terbaik berikut ini:

- Setiap akun administrator memiliki akun anggota yang berbeda.
- Setiap akun administrator memiliki akun anggota yang sama di seluruh Wilayah.
- Setiap akun administrator menggunakan Wilayah agregasi yang berbeda.

> **Note**
>
> Untuk memahami bagaimana agregasi lintas wilayah memengaruhi konfigurasi pusat, lihat. Konfigurasi pusat dan agregasi lintas wilayah

Konfigurasi pusat dan agregasi lintas wilayah

Konfigurasi pusat adalah fitur opt-in di Security Hub yang dapat Anda gunakan jika Anda berintegrasi dengannya AWS Organizations. Jika Anda menggunakan konfigurasi pusat, akun administrator yang didelegasikan dapat mengonfigurasi layanan, standar, dan kontrol Security Hub untuk akun dan unit organisasi (OU) dalam organisasi. Untuk mengonfigurasi akun dan OU, administrator yang didelegasikan membuat kebijakan konfigurasi Security Hub. Kebijakan konfigurasi dapat digunakan untuk menentukan apakah Security Hub diaktifkan atau dinonaktifkan, dan standar dan kontrol mana yang diaktifkan. Administrator yang didelegasikan mengaitkan kebijakan konfigurasi dengan akun tertentu, OU, atau root (seluruh organisasi).

Administrator yang didelegasikan dapat membuat dan mengelola kebijakan konfigurasi untuk organisasi hanya dari Wilayah agregasi. Selain itu, kebijakan konfigurasi berlaku di Wilayah agregasi dan semua Wilayah yang ditautkan. Anda tidak dapat membuat kebijakan konfigurasi yang hanya berlaku di beberapa Wilayah tertaut dan bukan yang lain. Dalam konfigurasi pusat, Wilayah agregasi

disebut Wilayah asal. Wilayah yang sama harus berfungsi sebagai Wilayah asal untuk tujuan konfigurasi pusat dan sebagai Wilayah agregasi untuk tujuan agregasi Lintas wilayah. Untuk informasi tentang agregasi lintas wilayah, lihat Agregasi Lintas Wilayah.

Untuk menggunakan konfigurasi pusat, Anda harus menunjuk Wilayah rumah dan setidaknya satu Wilayah yang ditautkan.

Mengubah setelan agregasi lintas wilayah dapat memengaruhi kebijakan konfigurasi Anda. Saat Anda menambahkan Wilayah tertaut, kebijakan konfigurasi Anda akan berlaku di Wilayah tersebut. Jika Region adalah Region opt-in, Region harus diaktifkan agar kebijakan konfigurasi Anda berlaku di sana. Sebaliknya, saat Anda menghapus Wilayah tertaut, kebijakan konfigurasi tidak lagi berlaku di Wilayah tersebut. Di Wilayah itu, akun mempertahankan pengaturan yang mereka miliki saat Wilayah yang ditautkan dihapus. Anda dapat mengubah pengaturan tersebut, tetapi harus melakukannya secara terpisah di setiap akun dan Wilayah.

Jika Anda menghapus atau mengubah Wilayah beranda, kebijakan konfigurasi dan asosiasi kebijakan Anda akan dihapus. Anda tidak dapat lagi menggunakan konfigurasi pusat atau membuat kebijakan konfigurasi di Wilayah mana pun. Akun mempertahankan pengaturan yang mereka miliki sebelum Wilayah asal diubah atau dihapus. Anda dapat mengubah pengaturan tersebut kapan saja, tetapi karena Anda tidak lagi menggunakan konfigurasi pusat, pengaturan harus dimodifikasi secara terpisah di setiap akun dan Wilayah. Anda dapat menggunakan konfigurasi pusat dan membuat kebijakan konfigurasi lagi jika Anda menunjuk Wilayah rumah baru.

Untuk informasi selengkapnya tentang konfigurasi pusat, lihatCara kerja konfigurasi pusat.

Mengaktifkan agregasi lintas wilayah

Anda harus mengaktifkan agregasi lintas wilayah dari Wilayah AWS yang ingin Anda tetapkan sebagai Wilayah agregasi.

Anda tidak dapat menggunakan Wilayah yang dinonaktifkan secara default sebagai Wilayah agregasi Anda. Untuk daftar Wilayah yang dinonaktifkan secara default, lihat Mengaktifkan Wilayah di. Referensi Umum AWS

Mengaktifkan agregasi lintas wilayah (konsol)

Saat mengaktifkan agregasi Lintas wilayah, Anda memilih Wilayah tertaut. Anda juga memilih apakah akan secara otomatis menautkan Wilayah baru saat Security Hub mulai mendukungnya dan Anda telah memilihnya.

Untuk mengaktifkan agregasi lintas wilayah

1. Buka AWS Security Hub konsol di https://console.aws.amazon.com/securityhub/.
2. Menggunakan Wilayah AWS pemilih, masuk ke Wilayah yang ingin Anda gunakan sebagai Wilayah agregasi.
3. Di menu navigasi Security Hub, pilih Pengaturan dan kemudian Wilayah.
4. Untuk Menemukan agregasi, pilih Konfigurasikan agregasi pencarian.

   Secara default, Region agregasi diatur ke No agregasi Region.
5. Di bawah Wilayah Agregasi, pilih opsi untuk menetapkan Wilayah saat ini sebagai Wilayah agregasi.
6. Secara opsional, untuk Wilayah Tertaut, pilih Wilayah untuk mengumpulkan data.
7. Untuk secara otomatis menggabungkan data dari Wilayah baru di partisi karena Security Hub mendukungnya dan Anda memilihnya, pilih Tautkan Wilayah masa depan.
8. Pilih Simpan.

Mengaktifkan agregasi lintas wilayah (Security Hub API,) AWS CLI

Anda dapat menggunakan Security Hub API untuk mengaktifkan agregasi lintas wilayah.

Untuk mengaktifkan agregasi lintas wilayah dari Security Hub API, Anda membuat agregator pencarian. Anda harus membuat agregator temuan dari Wilayah yang ingin Anda gunakan sebagai Wilayah agregasi.

Untuk membuat agregator temuan (Security Hub API, AWS CLI)

- Security Hub API: Dari Region yang ingin Anda gunakan sebagai Region agregasi, gunakan `CreateFindingAggregator`operasi. Untuk`RegionLinkingMode`, Anda memilih dari opsi berikut:
  - `ALL_REGIONS`— Security Hub mengumpulkan data dari semua Wilayah. Security Hub juga mengumpulkan data dari Wilayah baru saat didukung dan Anda memilihnya.
  - `ALL_REGIONS_EXCEPT_SPECIFIED`Security Hub mengumpulkan data dari semua Wilayah kecuali untuk Wilayah yang ingin Anda kecualikan. Security Hub juga mengumpulkan data dari Wilayah baru saat didukung dan Anda memilihnya. Gunakan `Regions` untuk menyediakan daftar Wilayah untuk dikecualikan dari agregasi.

  - `SPECIFIED_REGIONS`— Security Hub mengumpulkan data dari daftar Wilayah yang dipilih. Security Hub tidak mengumpulkan data secara otomatis dari Wilayah baru. Gunakan `Regions` untuk menyediakan daftar Wilayah untuk dikumpulkan dari.
- AWS CLI: Pada baris perintah, jalankan `create-finding-aggregator`perintah. Pisahkan setiap Wilayah dengan spasi.

```
aws securityhub create-finding-aggregator --region <aggregation Region> --region-
linking-mode ALL_REGIONS | ALL_REGIONS_EXCEPT_SPECIFIED | SPECIFIED_REGIONS --
regions <Region list>
```

  Dalam contoh berikut, agregasi lintas wilayah dikonfigurasi untuk Wilayah yang dipilih. Wilayah agregasi adalah US East (Virginia N.). Wilayah yang terhubung adalah US West (California N.) dan US West (Oregon).

```
aws securityhub create-finding-aggregator --region us-east-1 --region-linking-mode
 SPECIFIED_REGIONS --regions us-west-1 us-west-2
```

Melihat pengaturan agregasi lintas wilayah

Anda dapat melihat konfigurasi agregasi Lintas wilayah saat ini dari Wilayah mana pun. Konfigurasi mencakup Wilayah agregasi, Wilayah tertaut, dan apakah akan secara otomatis menautkan Wilayah baru.

Melihat konfigurasi agregasi lintas wilayah (konsol)

Tab Wilayah pada halaman Pengaturan menampilkan konfigurasi agregasi lintas wilayah saat ini. Anda dapat melihat konfigurasi dari Wilayah mana pun. Akun anggota juga dapat melihat konfigurasi Lintas wilayah yang dikonfigurasi oleh akun administrator.

Jika agregasi lintas wilayah tidak diaktifkan, maka tab Wilayah menampilkan opsi untuk mengaktifkan agregasi lintas wilayah. Lihat the section called “Mengaktifkan agregasi lintas wilayah”. Hanya akun administrator dan akun mandiri yang dapat mengaktifkan agregasi lintas wilayah.

Jika agregasi lintas wilayah diaktifkan, maka tab Wilayah menampilkan informasi berikut:

- Wilayah agregasi
- Apakah akan secara otomatis menggabungkan temuan, wawasan, status kontrol, dan skor keamanan dari Wilayah baru yang didukung Security Hub dan yang Anda pilih

- Daftar Wilayah tertaut

Melihat konfigurasi agregasi Lintas wilayah saat ini (Security Hub API,) AWS CLI

Anda dapat menggunakan Security Hub API atau AWS CLI untuk melihat konfigurasi agregasi lintas wilayah saat ini. Anda dapat melihat konfigurasi agregasi lintas wilayah dari Wilayah mana pun.

Untuk melihat konfigurasi agregasi Lintas wilayah saat ini (Security Hub API,) AWS CLI

- Security Hub API: Gunakan `GetFindingAggregator`API. Ketika Anda membuat permintaan, Anda harus memberikan agregator temuan ARN. Untuk mendapatkan ARN agregator temuan, gunakan. `ListFindingAggregators`
- AWS CLI: Pada baris perintah, jalankan `get-finding-aggregator`perintah. Untuk mendapatkan ARN agregator temuan, gunakan. `list-finding-aggregators`

```
aws securityhub get-finding-aggregator --finding-aggregator-arn <finding aggregator
 ARN>
```

Memperbarui konfigurasi agregasi lintas wilayah

Anda dapat memperbarui konfigurasi agregasi lintas wilayah untuk mengubah tautan Wilayah AWS untuk Wilayah agregasi saat ini. Anda juga dapat mengubah apakah akan secara otomatis mengumpulkan temuan, wawasan, status kontrol, dan skor keamanan dari Wilayah baru.

Perubahan pada agregasi Lintas wilayah tidak diterapkan untuk Wilayah keikutsertaan hingga Wilayah diaktifkan di. Akun AWS Wilayah yang AWS diperkenalkan pada atau setelah hingga 20 Maret 2019 adalah Wilayah yang ikut serta.

Bila Anda berhenti menggabungkan data dari Wilayah tertaut, Security Hub tidak menghapus data agregat yang ada dari Wilayah agregasi.

Anda tidak dapat menggunakan proses pembaruan untuk mengubah Wilayah agregasi. Untuk mengubah Wilayah agregasi, Anda harus melakukan hal berikut:

1. Hentikan agregasi lintas wilayah. Lihat the section called “Menghentikan agregasi lintas wilayah”.
2. Ubah ke Region yang Anda inginkan menjadi Region agregasi baru.

3. Aktifkan agregasi lintas wilayah. Lihat the section called “Mengaktifkan agregasi lintas wilayah”.

Memperbarui konfigurasi agregasi lintas wilayah (konsol)

Anda harus memperbarui konfigurasi agregasi lintas wilayah dari Wilayah agregasi saat ini.

Di Wilayah AWS selain Wilayah agregasi, panel agregasi Menemukan menampilkan pesan bahwa Anda harus mengedit konfigurasi di Wilayah agregasi. Pilih pesan ini untuk menampilkan tautan untuk menavigasi ke Wilayah agregasi.

Untuk mengubah Wilayah tertaut untuk Wilayah agregasi saat ini

1. Buka AWS Security Hub konsol di https://console.aws.amazon.com/securityhub/.
2. Ubah ke Wilayah agregasi saat ini.
3. Di menu navigasi Security Hub, pilih Pengaturan, lalu pilih Wilayah.
4. Di bawah Menemukan agregasi, pilih Edit.
5. Di bawah Wilayah Tertaut, perbarui Wilayah tertaut yang dipilih.
6. Jika perlu, ubah apakah Link future Regions dipilih. Pengaturan ini menentukan apakah Security Hub secara otomatis menautkan Wilayah baru karena menambahkan dukungan untuk mereka dan Anda memilihnya.
7. Pilih Simpan.

Memperbarui konfigurasi agregasi lintas wilayah (Security Hub API,) AWS CLI

Anda dapat menggunakan Security Hub API atau AWS CLI memperbarui konfigurasi agregasi lintas wilayah. Anda harus memperbarui agregasi lintas wilayah dari Wilayah agregasi saat ini.

Anda dapat mengubah mode penautan Wilayah. Jika mode penautan adalah `ALL_REGIONS_EXCEPT_SPECIFIED` atau`SPECIFIED_REGIONS`, Anda dapat mengubah daftar Wilayah yang dikecualikan atau disertakan.

Ketika Anda mengubah daftar Wilayah yang dikecualikan atau disertakan, Anda harus memberikan daftar lengkap dengan pembaruan. Misalnya, Anda saat ini mengumpulkan temuan dari US East (Ohio), dan ingin juga mengumpulkan temuan dari US West (Oregon). Saat Anda menelepon `UpdateFindingAggregator`, Anda memberikan `Regions` daftar yang berisi US East (Ohio) dan US West (Oregon).

Untuk memperbarui agregasi Lintas wilayah (Security Hub API,) AWS CLI

- Security Hub API: Gunakan operasi UpdateFindingAggregatorAPI. Untuk mengidentifikasi agregator temuan, Anda harus memberikan agregator temuan ARN. Untuk mendapatkan ARN agregator temuan, gunakan. ListFindingAggregators

  Anda menyediakan mode penautan Wilayah dan daftar Wilayah yang dikecualikan atau disertakan yang diperbarui.
- AWS CLI: Pada baris perintah, jalankan update-finding-aggregatorperintah. Pisahkan setiap Wilayah dengan spasi.

  ```
  aws securityhub update-finding-aggregator --region <aggregation Region> --finding-
  aggregator-arn <finding aggregator ARN> --region-linking-mode ALL_REGIONS |
   ALL_REGIONS_EXCEPT_SPECIFIED | SPECIFIED_REGIONS --regions <Region list>
  ```

  Dalam contoh berikut, konfigurasi agregasi lintas wilayah diubah menjadi agregasi untuk Wilayah yang dipilih. Perintah dijalankan dari Wilayah agregasi saat ini, yaitu US East (Virginia N.). Wilayah yang terhubung adalah US West (California N.) dan US West (Oregon).

  ```
  aws securityhub update-finding-aggregator --region us-east-1 --finding-aggregator-arn
   arn:aws:securityhub:us-east-1:222222222222:finding-aggregator/123e4567-e89b-12d3-
  a456-426652340000 --region-linking-mode SPECIFIED_REGIONS --regions us-west-1 us-
  west-2
  ```

Menghentikan agregasi lintas wilayah

Hentikan agregasi lintas wilayah jika Anda tidak lagi ingin mengumpulkan data atau jika Anda ingin mengubah Wilayah agregasi.

Saat Anda menghentikan agregasi Lintas wilayah, Security Hub berhenti menggabungkan data. Itu tidak menghapus data agregat yang ada dari Wilayah agregasi.

Menghentikan agregasi lintas wilayah (konsol)

Anda harus menghentikan agregasi lintas wilayah dari Wilayah agregasi saat ini.

Di Wilayah selain Wilayah agregasi, panel agregasi Menemukan menampilkan pesan bahwa Anda harus mengedit konfigurasi di Wilayah agregasi. Pilih pesan ini untuk menampilkan tautan untuk beralih ke Wilayah agregasi.

Untuk menghentikan agregasi lintas wilayah

1. Buka AWS Security Hub konsol di https://console.aws.amazon.com/securityhub/.
2. Ubah ke Wilayah agregasi saat ini.
3. Di menu navigasi Security Hub, pilih Pengaturan, lalu pilih Wilayah.
4. Di bawah Menemukan agregasi, pilih Edit.
5. Di bawah Wilayah Agregasi, pilih Tidak ada Wilayah agregasi.
6. Pilih Simpan.
7. Pada dialog konfirmasi, di bidang konfirmasi, ketik**`Confirm`**.
8. Pilih Konfirmasi.

Menghentikan agregasi lintas wilayah (Security Hub API,) AWS CLI

Anda dapat menggunakan Security Hub API untuk menghentikan agregasi lintas wilayah. Anda harus menghentikan agregasi lintas wilayah dari Wilayah agregasi.

Untuk menghentikan agregasi lintas wilayah (Security Hub API,) AWS CLI

- Security Hub API: Gunakan `DeleteFindingAggregator`operasi. Untuk mengidentifikasi agregator temuan yang akan dihapus, Anda memberikan ARN agregator temuan. Untuk mendapatkan ARN agregator temuan, gunakan. `ListFindingAggregators`
- AWS CLI: Pada baris perintah, jalankan `delete-finding-aggregator`perintah.

```
aws securityhub delete-finding-aggregator <finding aggregator ARN> --
region <aggregation Region>
```

Temuan di AWS Security Hub

AWS Security Hub menghilangkan kompleksitas dalam menangani sejumlah besar temuan dari beberapa penyedia. Ini mengurangi upaya yang diperlukan untuk mengelola dan meningkatkan keamanan semua sumber daya Akun AWS, dan beban kerja Anda.

Security Hub menerima temuan dari sumber-sumber berikut.

- Security Hub memeriksa kontrol yang diaktifkan. Lihat the section called “Menghasilkan dan memperbarui temuan kontrol”.
- Integrasi dengan Layanan AWS yang Anda aktifkan. Lihat the section called “Layanan AWS integrasi”.
- Integrasi dengan produk pihak ketiga yang Anda aktifkan. Lihat the section called “Integrasi produk pihak ketiga”.
- Integrasi kustom yang Anda konfigurasikan. Lihat the section called “Menggunakan integrasi produk khusus”.

Security Hub mengkonsumsi temuan menggunakan format temuan standar yang disebut AWS Security Finding Format. Untuk informasi selengkapnya tentang format temuan, lihatthe section called “Menemukan format”.

Security Hub menghubungkan temuan di seluruh produk terintegrasi untuk memprioritaskan yang paling penting.

Penyedia pencarian dapat memperbarui temuan untuk mencerminkan contoh tambahan dari temuan tersebut. Anda dapat memperbarui temuan untuk memberikan rincian tentang penyelidikan Anda dan hasilnya.

Security Hub juga memungkinkan Anda untuk mengumpulkan temuan di seluruh Wilayah, sehingga Anda dapat melihat semua temuan Anda dari satu tempat. Lihat Agregasi Lintas Wilayah.

Topik

- Membuat dan memperbarui temuan di AWS Security Hub
- Mengelola dan meninjau detail dan riwayat penemuan
- Mengambil tindakan atas temuan di AWS Security Hub
- AWS Format Pencarian Keamanan (ASFF)

Membuat dan memperbarui temuan di AWS Security Hub

Pada tahun AWS Security Hub, temuan dapat berasal dari salah satu jenis penyedia pencarian berikut.

- Kontrol keamanan yang diaktifkan di Security Hub
- Integrasi yang diaktifkan dengan yang lain Layanan AWS
- Integrasi yang diaktifkan dengan produk pihak ketiga

Setelah temuan dibuat, itu dapat diperbarui oleh penyedia temuan atau oleh pelanggan.

- Penyedia temuan menggunakan operasi `BatchImportFindings`API untuk memperbarui informasi umum tentang temuan. Penyedia pencarian hanya dapat memperbarui temuan yang mereka buat.
- Pelanggan menggunakan operasi `BatchUpdateFindings`API untuk memperbarui status investigasi menjadi temuan. `BatchUpdateFindings`juga dapat digunakan oleh tiket, manajemen insiden, orkestrasi, remediasi, atau alat SIEM atas nama pelanggan.

  Dari konsol Security Hub, pelanggan dapat mengelola status alur kerja temuan dan mengirim temuan ke tindakan khusus. Lihat the section called “Mengambil tindakan atas temuan”.

Security Hub juga secara otomatis memperbarui dan menghapus temuan. Semua temuan dihapus secara otomatis jika tidak diperbarui dalam 90 hari terakhir.

Jika Anda mengaktifkan agregasi Lintas wilayah, maka Security Hub secara otomatis mengumpulkan temuan baru dari Wilayah tertaut ke Wilayah agregasi. Security Hub juga mereplikasi pembaruan temuan. Pembaruan yang terjadi di Wilayah tertaut direplikasi ke Wilayah agregasi. Pembaruan yang terjadi di Wilayah agregasi direplikasi ke Wilayah yang ditautkan. Untuk informasi selengkapnya tentang agregasi lintas wilayah, lihat. Agregasi Lintas Wilayah

Topik

Menggunakan BatchImportFindings untuk membuat dan memperbarui temuan

Penyedia pencarian menggunakan operasi `BatchImportFindings`API untuk membuat temuan baru dan memperbarui informasi tentang temuan yang mereka buat. Mereka tidak dapat memperbarui temuan yang tidak mereka buat.

Pelanggan, SIEM, alat tiket, dan alat SOAR digunakan `BatchUpdateFindings`untuk membuat pembaruan terkait penyelidikan temuan mereka dari penyedia pencarian. Lihat the section called “Menggunakan BatchUpdateFindings”.

Setiap kali AWS Security Hub menerima `BatchImportFindings` permintaan untuk membuat atau memperbarui temuan, secara otomatis menghasilkan Security Hub Findings - Importedacara di Amazon EventBridge. Lihat the section called “Respon dan remediasi otomatis”.

Persyaratan untuk akun dan ukuran batch

`BatchImportFindings`harus dipanggil oleh salah satu dari berikut ini:

- Akun yang terkait dengan temuan. Pengidentifikasi akun terkait adalah nilai `AwsAccountId` atribut untuk temuan tersebut.
- Akun yang diizinkan terdaftar untuk integrasi mitra Security Hub resmi.

Security Hub hanya dapat menerima pembaruan pencarian untuk akun yang mengaktifkan Security Hub. Penyedia temuan juga harus diaktifkan. Jika Security Hub dinonaktifkan, atau integrasi penyedia pencarian tidak diaktifkan, maka temuan akan dikembalikan dalam `FailedFindings` daftar, dengan `InvalidAccess` kesalahan.

`BatchImportFindings`menerima hingga 100 temuan per batch, hingga 240 KB per temuan, dan hingga 6 MB per batch. Batas kecepatan throttle adalah 10 TPS per akun per Wilayah, dengan ledakan 30 TPS.

Menentukan apakah akan membuat atau memperbarui temuan

Untuk menentukan apakah akan membuat atau memperbarui temuan, Security Hub memeriksa `ID` bidang tersebut. Jika nilai `ID` tidak sesuai dengan temuan yang ada, maka temuan baru dibuat.

Jika `ID` tidak cocok dengan temuan yang ada, maka Security Hub memeriksa `UpdatedAt` bidang untuk pembaruan.

- Jika `UpdatedAt` pada pembaruan cocok atau terjadi sebelumnya `UpdatedAt` pada temuan yang ada, maka pembaruan diabaikan.
- Jika `UpdatedAt` pada pembaruan terjadi setelah `UpdatedAt` pada temuan yang ada, maka temuan yang ada diperbarui.

Atribut terbatas untuk BatchImportFindings

Untuk temuan yang ada, penyedia pencarian tidak dapat digunakan `BatchImportFindings` untuk memperbarui atribut dan objek berikut. Atribut ini hanya dapat diperbarui menggunakan`BatchUpdateFindings`.

- `Note`
- `UserDefinedFields`
- `VerificationState`
- `Workflow`

Security Hub mengabaikan konten apa pun yang disediakan dalam `BatchImportFindings` permintaan atribut dan objek tersebut. Pelanggan, atau penyedia lain yang bertindak atas nama mereka, gunakan `BatchUpdateFindings` untuk memperbaruinya.

Menggunakan FindingProviderFields

Mencari penyedia juga tidak boleh digunakan `BatchImportFindings` untuk memperbarui atribut berikut.

- `Confidence`
- `Criticality`
- `RelatedFindings`
- `Severity`
- `Types`

Sebaliknya, menemukan penyedia menggunakan `FindingProviderFields`objek untuk memberikan nilai untuk atribut ini.

Contoh

```
"FindingProviderFields": {
    "Confidence": 42,
    "Criticality": 99,
    "RelatedFindings":[
      {
        "ProductArn": "arn:aws:securityhub:us-west-2::product/aws/guardduty",
        "Id": "123e4567-e89b-12d3-a456-426655440000"
      }
    ],
    "Severity": {
        "Label": "MEDIUM",
        "Original": "MEDIUM"
    },
    "Types": [ "Software and Configuration Checks/Vulnerabilities/CVE" ]
}
```

Untuk `BatchImportFindings` permintaan, Security Hub menangani nilai di atribut tingkat atas dan `FindingProviderFields`sebagai berikut.

(Preferred) **`BatchImportFindings`** memberikan nilai untuk atribut di **`FindingProviderFields`**, tetapi tidak memberikan nilai untuk atribut tingkat atas yang sesuai.

Misalnya, `BatchImportFindings` menyediakan`FindingProviderFields.Confidence`, tetapi tidak menyediakan`Confidence`. Ini adalah opsi yang lebih disukai untuk `BatchImportFindings` permintaan.

Security Hub memperbarui nilai atribut di`FindingProviderFields`.

Ini mereplikasi nilai ke atribut tingkat atas hanya jika atribut belum diperbarui oleh. `BatchUpdateFindings`

`BatchImportFindings`memberikan nilai untuk atribut tingkat atas, tetapi tidak memberikan nilai untuk atribut yang sesuai di**`FindingProviderFields`**.

Misalnya, `BatchImportFindings` menyediakan`Confidence`, tetapi tidak menyediakan`FindingProviderFields.Confidence`.

Security Hub menggunakan nilai untuk memperbarui atribut di`FindingProviderFields`. Ini menimpa nilai yang ada.

Security Hub memperbarui atribut tingkat atas hanya jika atribut belum diperbarui oleh`BatchUpdateFindings`.

`BatchImportFindings`memberikan nilai untuk atribut tingkat atas dan atribut yang sesuai di**`FindingProviderFields`**.

Misalnya, `BatchImportFindings` menyediakan keduanya `Confidence` dan`FindingProviderFields.Confidence`.

Untuk temuan baru, Security Hub menggunakan nilai dalam `FindingProviderFields` untuk mengisi atribut tingkat atas dan atribut yang sesuai. `FindingProviderFields` Itu tidak menggunakan nilai atribut tingkat atas yang disediakan.

Untuk temuan yang ada, Security Hub menggunakan kedua nilai. Namun, itu memperbarui nilai atribut tingkat atas hanya jika atribut belum diperbarui oleh`BatchUpdateFindings`.

Menggunakan batch-import-findings perintah dari AWS CLI

Di AWS Command Line Interface, Anda menggunakan [`batch-import-findings`](#)perintah untuk membuat atau memperbarui temuan.

Anda memberikan setiap temuan sebagai objek JSON.

Contoh

```
aws securityhub batch-import-findings --findings
    [{
        "AwsAccountId": "123456789012",
        "CreatedAt": "2019-08-07T17:05:54.832Z",
        "Description": "Vulnerability in a CloudTrail trail",
        "GeneratorId": "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0/rule/2.2",
        "Id": "Id1",
        "ProductArn": "arn:aws:securityhub:us-west-1:123456789012:product/123456789012/
default",
        "Resources": [
            {
                "Id": "arn:aws:cloudtrail:us-west-1:123456789012:trail/TrailName",
                "Partition": "aws",
                "Region": "us-west-1",
                "Type": "AwsCloudTrailTrail"
            }
        ],
        "SchemaVersion": "2018-10-08",
        "Title": "CloudTrail trail vulnerability",
```

```
        "UpdatedAt": "2020-06-02T16:05:54.832Z",
        "Types": [
            "Software and Configuration Checks/Vulnerabilities/CVE"
        ],
        "Severity": {
            "Label": "INFORMATIONAL",
            "Original": "0"
        }
    }]'
```

Menggunakan BatchUpdateFindings untuk memperbarui temuan

`BatchUpdateFindings`Tindakan ini digunakan untuk memperbarui informasi yang terkait dengan pemrosesan temuan pelanggan dari penyedia pencarian. Ini dapat digunakan oleh pelanggan atau oleh SIEM, tiket, manajemen insiden, atau alat SOAR yang bekerja atas nama pelanggan. Anda dapat menggunakan `BatchUpdateFindings` untuk memperbarui bidang tertentu dalam AWS Security Finding Format (ASFF).

Anda tidak dapat menggunakan `BatchUpdateFindings` untuk membuat temuan baru. Anda dapat menggunakannya untuk memperbarui hingga 100 temuan sekaligus.

Setiap kali Security Hub menerima `BatchUpdateFindings` permintaan untuk memperbarui temuan, secara otomatis menghasilkan Security Hub Findings - Importedperistiwa di Amazon EventBridge. Lihat the section called “Respon dan remediasi otomatis”.

`BatchUpdateFindings`tidak mengubah `UpdatedAt` bidang untuk temuan. `UpdatedAt`hanya mencerminkan pembaruan terbaru dari penyedia temuan.

Bidang yang tersedia untuk BatchUpdateFindings

Akun administrator dapat menggunakan> `BatchUpdateFindings` untuk memperbarui temuan untuk akun mereka atau untuk akun anggota mereka. Akun anggota dapat menggunakan> `BatchUpdateFindings` untuk memperbarui temuan untuk akun mereka.

Pelanggan hanya dapat menggunakan> `BatchUpdateFindings` untuk memperbarui bidang dan objek berikut.

- `Confidence`
- `Criticality`
- `Note`

- `RelatedFindings`
- `Severity`
- `Types`
- `UserDefinedFields`
- `VerificationState`
- `Workflow`

Secara default, akun administrator dan anggota memiliki akses ke semua bidang dan nilai bidang di atas. Security Hub juga menyediakan kunci konteks untuk memungkinkan Anda membatasi akses ke bidang dan nilai bidang.

Misalnya, Anda mungkin hanya mengizinkan akun anggota `Workflow.Status` untuk disetel`RESOLVED`. Atau Anda mungkin tidak ingin mengizinkan akun anggota berubah`Severity.Label`.

Mengkonfigurasi akses ke BatchUpdateFindings

Anda dapat mengonfigurasi kebijakan IAM untuk membatasi akses penggunaan `BatchUpdateFindings` untuk memperbarui bidang dan nilai bidang.

Dalam pernyataan untuk membatasi akses ke`BatchUpdateFindings`, gunakan nilai-nilai berikut:

- `Action`adalah `securityhub:BatchUpdateFindings`
- `Effect`adalah `Deny`
- Untuk`Condition`, Anda dapat menolak `BatchUpdateFindings` permintaan berdasarkan hal berikut:
  - Temuan ini mencakup bidang tertentu.
  - Temuan ini mencakup nilai bidang tertentu.

Kunci syarat

Ini adalah kunci kondisi untuk membatasi akses ke`BatchUpdateFindings`.

Bidang ASFF

Kunci kondisi untuk bidang ASFF adalah sebagai berikut:

```
securityhub:ASFFSyntaxPath/<fieldName>
```

Ganti *<fieldName>* dengan bidang ASFF. Saat mengonfigurasi akses ke`BatchUpdateFindings`, sertakan satu atau lebih bidang ASFF spesifik dalam kebijakan IAM Anda, bukan bidang tingkat induk. Misalnya, untuk membatasi akses ke `Workflow.Status` bidang, Anda harus menyertakan `securityhub:ASFFSyntaxPath/Workflow.Status` dalam kebijakan, bukan bidang tingkat `Workflow` induk.

Melarangi semua pembaruan ke bidang

Untuk mencegah pengguna melakukan pembaruan apa pun ke bidang tertentu, gunakan kondisi seperti ini:

```
 "Condition": {
                "Null": {
                    "securityhub:ASFFSyntaxPath/<fieldName>": "false"
               }
}
```

Misalnya, pernyataan berikut menunjukkan bahwa tidak `BatchUpdateFindings` dapat digunakan untuk memperbarui status alur kerja.

```
{
    "Sid": "VisualEditor0",
    "Effect": "Deny",
    "Action": "securityhub:BatchUpdateFindings",
    "Resource": "*",
    "Condition": {
        "Null": {
            "securityhub:ASFFSyntaxPath/Workflow.Status": "false"
        }
    }
}
```

Melarangi nilai bidang tertentu

Untuk mencegah pengguna menyetel bidang ke nilai tertentu, gunakan kondisi seperti ini:

```
"Condition": {
```

```
                "StringEquals": {
                    "securityhub:ASFFSyntaxPath/<fieldName>": "<fieldValue>"
                }
}
```

Misalnya, pernyataan berikut menunjukkan bahwa tidak `BatchUpdateFindings` dapat digunakan untuk mengatur `Workflow.Status` ke`SUPPRESSED`.

```
{
    "Sid": "VisualEditor0",
    "Effect": "Deny",
    "Action": "securityhub:BatchUpdateFindings",
    "Resource": "*",
    "Condition": {
    "StringEquals": {
        "securityhub:ASFFSyntaxPath/Workflow.Status": "SUPPRESSED"
    }
}
```

Anda juga dapat memberikan daftar nilai yang tidak diizinkan.

```
 "Condition": {
                "StringEquals": {
                    "securityhub:ASFFSyntaxPath/<fieldName>": [ "<fieldValue1>",
 "<fieldValue2>", "<fieldValuen>" ]
                }
}
```

Misalnya, pernyataan berikut menunjukkan bahwa tidak `BatchUpdateFindings` dapat digunakan untuk menyetel `Workflow.Status` ke salah satu `RESOLVED` atau`SUPPRESSED`.

```
{
    "Sid": "VisualEditor0",
    "Effect": "Deny",
    "Action": "securityhub:BatchUpdateFindings",
    "Resource": "*",
    "Condition": {
    "StringEquals": {
        "securityhub:ASFFSyntaxPath/Workflow.Status": [
            "RESOLVED",
            "NOTIFIED"
        ]
```

```
    }
}
```

Menggunakan batch-update-findings perintah dari AWS CLI

Di AWS Command Line Interface, Anda menggunakan `batch-update-findings`perintah untuk memperbarui temuan.

Untuk setiap temuan untuk diperbarui, Anda memberikan ID temuan dan ARN dari produk yang menghasilkan temuan.

```
--finding-identifiers ID="<findingID1>",ProductArn="<productARN>"
 ID="<findingID2>",ProductArn="<productARN2>"
```

Saat Anda memberikan atribut untuk diperbarui, Anda dapat menggunakan format JSON atau format pintasan.

Berikut adalah contoh pembaruan ke `Note` objek yang menggunakan format JSON:

```
--note '{"Text": "Known issue that is not a risk.", "UpdatedBy": "user1"}'
```

Berikut adalah pembaruan yang sama yang menggunakan format pintasan:

```
--note Text="Known issue that is not a risk.",UpdatedBy="user1"
```

AWS CLI Command Reference menyediakan sintaks JSON dan shortcut untuk setiap bidang.

`batch-update-findings`Contoh > berikut memperbarui dua temuan untuk menambahkan catatan, mengubah label keparahan, dan menyelesaikannya.

```
aws securityhub batch-update-findings --finding-identifiers Id="arn:aws:securityhub:us-
west-1:123456789012:subscription/pci-dss/v/3.2.1/PCI.Lambda.2/finding/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",ProductArn="arn:aws:securityhub:us-
west-2::product/aws/securityhub" Id="arn:aws:securityhub:us-
west-1:123456789012:subscription/pci-dss/v/3.2.1/PCI.Lambda.2/finding/
a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",ProductArn="arn:aws:securityhub:us-
west-1::product/aws/securityhub" --note '{"Text": "Known issue that is not a
 risk.", "UpdatedBy": "user1"}' --severity '{"Label": "LOW"}' --workflow '{"Status":
 "RESOLVED"}'
```

Ini adalah contoh yang sama, tetapi menggunakan pintasan alih-alih JSON.

```
aws securityhub batch-update-findings --finding-identifiers Id="arn:aws:securityhub:us-
west-1:123456789012:subscription/pci-dss/v/3.2.1/PCI.Lambda.2/finding/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",ProductArn="arn:aws:securityhub:us-
west-1::product/aws/securityhub" Id="arn:aws:securityhub:us-
west-1:123456789012:subscription/pci-dss/v/3.2.1/PCI.Lambda.2/finding/
a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",ProductArn="arn:aws:securityhub:us-
west-1::product/aws/securityhub" --note Text="Known issue that is not a
 risk.",UpdatedBy="user1" --severity Label="LOW" --workflow Status="RESOLVED"
```

Mengelola dan meninjau detail dan riwayat penemuan

Ada beberapa cara untuk melihat daftar pencarian di AWS Security Hub konsol:

- Halaman temuan - Menampilkan daftar lengkap temuan dari semua kontrol yang diaktifkan dan integrasi produk. Secara default, temuan aktif dengan status `NOTIFIED` alur kerja `NEW` atau ditampilkan.
- Halaman detail kontrol - Menampilkan daftar temuan yang dihasilkan dalam 24 jam terakhir untuk kontrol tertentu.
- Halaman Wawasan - Menampilkan daftar temuan untuk wawasan yang cocok. Wawasan adalah koleksi temuan spesifik. Untuk informasi selengkapnya, lihat the section called “Melihat hasil dan temuan wawasan”.
- Halaman Integrasi - Menampilkan daftar temuan yang dihasilkan oleh produk terintegrasi Layanan AWS atau pihak ketiga.

Anda dapat memfilter dan mengelompokkan temuan pada daftar ini untuk fokus pada jenis temuan tertentu. Anda juga dapat memilih temuan tertentu di halaman sebelumnya untuk melihat detailnya.

Untuk melihat daftar temuan secara terprogram, gunakan `GetFindings`pengoperasian Security Hub API. Anda dapat menyertakan filter untuk mengambil jenis temuan tertentu.

Jika Anda mengaktifkan agregasi lintas wilayah, Anda dapat mengambil status kontrol, skor keamanan, wawasan, dan temuan dari seluruh Wilayah. Di Wilayah agregasi, menemukan data mencakup data dari Wilayah agregasi dan Wilayah terkait. Di Wilayah lain, menemukan data khusus untuk Wilayah itu saja. Untuk informasi tentang mengonfigurasi agregasi lintas wilayah, lihat. Agregasi Lintas Wilayah

Penyaringan dan pengelompokan temuan (konsol)

Saat Anda menampilkan daftar temuan di halaman Temuan, halaman Integrasi, atau halaman Wawasan di konsol Security Hub, daftar tersebut telah difilter sebelumnya berdasarkan status rekaman dan status alur kerja. Ini adalah tambahan untuk filter untuk wawasan atau integrasi.

Status rekaman menunjukkan apakah temuan aktif atau diarsipkan. Secara default, daftar temuan hanya menampilkan temuan aktif.Temuan dapat diarsipkan oleh penyedia temuan. AWS Security Hub juga secara otomatis mengarsipkan temuan kontrol jika sumber daya terkait dihapus.

Status alur kerja menunjukkan status investigasi terhadap suatu temuan. Secara default, daftar temuan hanya menampilkan temuan dengan status alur kerja `NEW` atau`NOTIFIED`. Anda dapat memperbarui status alur kerja temuan.

Jika Anda mengaktifkan pencarian agregasi dan masuk ke Wilayah agregasi, Anda dapat memfilter temuan berdasarkan Wilayah di halaman Temuan dan Wawasan.

Untuk informasi tentang bekerja dengan temuan kontrol, lihatthe section called “Memfilter dan menyortir temuan”. Informasi di halaman ini berlaku untuk menemukan daftar di halaman Temuan, Wawasan, dan Integrasi.

Menambahkan filter

Untuk mengubah cakupan daftar, Anda dapat menambahkan filter ke dalamnya.

Anda dapat memfilter hingga 10 atribut. Untuk setiap atribut, Anda dapat memberikan hingga 20 nilai filter.

Saat memfilter daftar temuan, Security Hub menerapkan logika AND ke kumpulan filter. Dengan kata lain, temuan hanya cocok jika cocok dengan semua filter yang disediakan. Misalnya, jika Anda menambahkan GuardDuty sebagai filter untuk nama produk, dan `AwsS3Bucket` sebagai filter untuk jenis sumber daya, maka temuan yang cocok harus cocok dengan kedua kriteria ini.

Namun, Security Hub menerapkan logika OR ke filter yang menggunakan atribut yang sama tetapi nilainya berbeda. Misalnya, Anda menambahkan keduanya GuardDuty dan Amazon Inspector sebagai nilai filter untuk nama produk. Dalam hal ini, temuan cocok jika itu dihasilkan oleh salah satu GuardDuty atau Amazon Inspector.

Untuk menambahkan filter ke daftar temuan

1. Buka AWS Security Hub konsol di https://console.aws.amazon.com/securityhub/.

2. Untuk menampilkan daftar temuan, lakukan salah satu hal berikut:

   - Di panel navigasi Security Hub, pilih Temuan.
   - Di panel navigasi Security Hub, pilih Wawasan. Pilih wawasan. Kemudian pada daftar hasil, pilih hasil wawasan.
   - Di panel navigasi Security Hub, pilih Integrasi. Pilih Lihat temuan untuk integrasi.

3. Di kotak Tambahkan filter, untuk Filter, pilih filter.

   Saat Anda memfilter berdasarkan nama Perusahaan atau Nama Produk, konsol menggunakan tingkat atas `CompanyName` dan `ProductName` bidang. API menggunakan nilai-nilai yang ada di`ProductFields`.

4. Pilih jenis kecocokan filter.

   Untuk filter string, Anda dapat memilih dari opsi perbandingan berikut:

   - is — Temukan nilai yang sama persis dengan nilai filter.
   - dimulai dengan - Temukan nilai yang dimulai dengan nilai filter.
   - is not — Temukan nilai yang tidak cocok dengan nilai filter.
   - tidak dimulai dengan — Temukan nilai yang tidak dimulai dengan nilai filter.

   Untuk filter numerik, Anda dapat memilih apakah akan memberikan nomor tunggal (Sederhana) atau rentang angka (Rentang).

   Untuk filter tanggal atau waktu, Anda dapat memilih apakah akan memberikan jangka waktu dari tanggal dan waktu saat ini (Jendela bergulir) atau rentang tanggal tertentu (Rentang tetap).

   Menambahkan beberapa filter memiliki interaksi berikut:

   - adalah dan dimulai dengan filter bergabung dengan OR. Nilai cocok jika berisi salah satu nilai filter. Misalnya, jika Anda menentukan label Keparahan adalah KRITIS dan label Keparahan TINGGI, hasilnya mencakup temuan tingkat keparahan kritis dan tinggi.
   - tidak dan tidak dimulai dengan filter bergabung dengan AND. Nilai hanya cocok jika tidak mengandung salah satu nilai filter tersebut. Misalnya, jika Anda menentukan label Keparahan tidak RENDAH dan label Keparahan tidak SEDANG, hasilnya tidak termasuk temuan tingkat keparahan rendah atau sedang.

Jika Anda memiliki filter is di bidang, Anda tidak dapat memiliki is not atau tidak dimulai dengan filter pada bidang yang sama.

5. Tentukan nilai filter.

   Untuk filter string, nilai filter peka huruf besar/kecil.

   Misalnya, untuk temuan dari Security Hub, nama Produk adalah Security Hub. Jika Anda menggunakan operator EQUALS untuk melihat temuan dari Security Hub, Anda harus memasukkan **`Security Hub`** sebagai nilai filter. Jika Anda masuk**`security hub`**, tidak ada temuan yang ditampilkan.

   Demikian pula, jika Anda menggunakan operator PREFIX, dan enter**`Sec`**, temuan Security Hub akan ditampilkan. Jika Anda masuk**`sec`**, tidak ada temuan Security Hub yang ditampilkan.

6. Pilih Terapkan.

Temuan pengelompokan

Selain mengubah filter, Anda dapat mengelompokkan temuan berdasarkan nilai atribut yang dipilih.

Saat Anda mengelompokkan temuan, daftar temuan diganti dengan daftar nilai untuk atribut yang dipilih dalam temuan yang cocok. Untuk setiap nilai, daftar menampilkan jumlah temuan yang cocok dengan kriteria filter lainnya.

Misalnya, jika Anda mengelompokkan temuan berdasarkan Akun AWS ID, Anda akan melihat daftar pengidentifikasi akun, dengan jumlah temuan yang cocok untuk setiap akun.

Perhatikan bahwa Security Hub hanya dapat menampilkan 100 nilai. Jika ada lebih dari 100 nilai pengelompokan, Anda hanya melihat 100 yang pertama.

Saat Anda memilih nilai atribut, daftar temuan yang cocok untuk nilai tersebut ditampilkan.

Untuk mengelompokkan temuan dalam daftar temuan

1. Pada daftar temuan, pilih kotak Tambahkan filter.
2. Untuk Pengelompokan, pilih Grup menurut.
3. Dalam daftar, pilih atribut yang akan digunakan untuk pengelompokan.
4. Pilih Terapkan.

Mengubah nilai filter atau atribut pengelompokan

Untuk filter yang ada, Anda dapat mengubah nilai filter. Anda juga dapat mengubah atribut pengelompokan.

Misalnya, Anda dapat mengubah filter status Rekam untuk mencari `ARCHIVED` temuan alih-alih `ACTIVE` temuan.

Untuk mengedit atribut filter atau pengelompokan

1. Pada daftar temuan yang difilter, pilih atribut filter atau pengelompokan.
2. Untuk Group by, pilih atribut baru, lalu pilih Terapkan.
3. Untuk filter, pilih nilai baru, lalu pilih Terapkan.

Menghapus atribut filter atau pengelompokan

Untuk menghapus atribut filter atau pengelompokan, pilih ikon x.

Daftar diperbarui secara otomatis untuk mencerminkan perubahan. Saat Anda menghapus atribut pengelompokan, daftar berubah dari daftar nilai bidang kembali ke daftar temuan.

Informasi pencarian yang tersedia

Anda bisa mendapatkan berbagai detail temuan di konsol Security Hub atau dengan memanggil GetFindingspengoperasian Security Hub API. Berikut adalah sebagian daftar jenis detail temuan yang bisa Anda dapatkan.

- Metadata aplikasi — Menyediakan nama dan Nama Sumber Daya Amazon (ARN) aplikasi yang terlibat dalam temuan jika Anda membuat aplikasi. dan menambahkan tag aplikasi ke dalamnya. AWS Kami merekomendasikan membuat aplikasi di AWS Service Catalog AppRegistry.
- Menemukan sejarah — Memberikan sejarah temuan dalam 90 hari terakhir.
- Menemukan investigasi di Detektif (hanya konsol) - Menyediakan tautan untuk menyelidiki lebih lanjut temuan di Detektif menggunakan pengumpulan log otomatis, analitik keamanan, dan Layanan AWS alat eksplorasi sumber daya. Informasi ini hanya disertakan untuk temuan Security Hub yang diterima dari pihak lain Layanan AWS jika Anda mengaktifkan Detective.
- Menemukan bidang penyedia — menampilkan nilai dari penyedia temuan untuk kepercayaan diri, kekritisan, temuan terkait, tingkat keparahan, dan jenis temuan.

- Parameter — Menunjukkan nilai parameter saat ini untuk kontrol keamanan. Security Hub menggunakan nilai parameter ini saat melakukan pemeriksaan keamanan kontrol.
- Remediasi — Menyediakan tautan ke instruksi untuk memulihkan temuan kontrol yang gagal.
- Sumber daya — Memberikan informasi tentang AWS sumber daya yang terlibat dalam temuan.
- Tag sumber daya — Menyediakan kunci tag dan informasi nilai untuk sumber daya yang terlibat dalam temuan. Anda dapat menandai sumber daya yang didukung oleh `GetResources` pengoperasian API AWS Resource Groups Tagging. Security Hub memanggil operasi ini melalui peran terkait layanan dan mengambil tag sumber daya jika `Resource.Id` bidang AWS Security Finding Format (ASFF) diisi dengan ARN sumber daya. AWS ID sumber daya yang tidak valid diabaikan. Untuk informasi lebih lanjut tentang penyertaan tag sumber daya dalam temuan, lihatTanda.
- Jenis dan temuan terkait - Berisi informasi tentang jenis temuan.
- Detail kerentanan — Informasi tentang kerentanan yang terdeteksi dalam temuan dan paket yang terpengaruh. Detail ini tersedia jika Anda mengaktifkan Amazon Inspector untuk temuan yang dikirim Amazon Inspector ke Security Hub.

Tinjau bagian berikut untuk memahami cara mengakses detail ini untuk sebuah temuan.

Meninjau riwayat penemuan

Menemukan riwayat adalah fitur Security Hub yang memungkinkan Anda melacak perubahan yang dibuat pada temuan selama 90 hari terakhir. Ini tersedia untuk temuan aktif dan diarsipkan. Menemukan riwayat memberikan jejak perubahan yang tidak dapat diubah yang dibuat pada temuan dari waktu ke waktu, termasuk apa perubahan itu, kapan itu terjadi, dan oleh pengguna mana.

Secara khusus, Anda dapat melacak perubahan yang dibuat pada bidang diAWS Format Pencarian Keamanan (ASFF). Security Hub melacak perubahan yang Anda buat secara manual dan dengan aturan otomatisasi.

Riwayat pencarian tersedia di konsol Security Hub, API, dan AWS CLI.

Jika Anda masuk ke akun administrator Security Hub, Anda bisa mendapatkan riwayat pencarian untuk akun administrator dan semua akun anggota.

Pilih metode pilihan Anda, dan ikuti langkah-langkah untuk meninjau riwayat penemuan.

Security Hub console

Meninjau riwayat penemuan

1. Buka AWS Security Hub konsol di https://console.aws.amazon.com/securityhub/.
2. Di panel navigasi kiri, pilih Temuan.
3. Pilih temuan. Di panel yang muncul, pilih tab Riwayat.

Security Hub API

Meninjau riwayat penemuan

1. Jalankan GetFindings, atau jika Anda menggunakan AWS CLI, jalankan get-findingsperintah. menggunakan filter yang sesuai sesuai kebutuhan, untuk mengidentifikasi temuan yang ingin Anda lihat histori. Respons API akan memberi Anda `ProductArn` dan `Id` untuk temuan tersebut. Anda memerlukan nilai untuk bidang ini di langkah ketiga.
2. Jalankan GetFindingHistory, atau jika Anda menggunakan AWS CLI, jalankan get-finding-historyperintah.
3. Identifikasi temuan yang ingin Anda dapatkan riwayat dengan `Id` bidang `ProductArn` dan. Untuk informasi lebih lanjut tentang bidang ini, lihat AwsSecurityFindingIdentifier. Anda hanya bisa mendapatkan riwayat untuk satu temuan per permintaan.
4. Berikan nilai untuk`StartTime`. dan `EndTime` untuk membatasi riwayat penemuan pada periode waktu tertentu.
5. Berikan nilai `MaxResults` untuk membatasi riwayat penemuan ke sejumlah hasil tertentu. Jika tidak disediakan, respons API mengembalikan 100 hasil pertama dari riwayat pencarian.
6. Berikan nilai `NextToken` untuk melihat 100 hasil berikutnya (jika ada) untuk sebuah temuan. Dalam permintaan API awal Anda, nilai `NextToken` harus`NULL`.

Perintah CLI berikut mengambil riwayat untuk temuan yang ditentukan. Contoh ini diformat untuk Linux, macOS, atau Unix, dan menggunakan karakter garis miring terbalik (\) untuk meningkatkan keterbacaan.

```
$ aws securityhub get-finding-history \
--region us-west-2 \
--finding-identifier Id="a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111",ProductArn="arn:aws:securityhub:us-
west-2:123456789012:product/123456789012/default" \
```

```
--max-results 2 \
--start-time "2021-09-30T15:53:35.573Z" \
--end-time "2021-09-31T15:53:35.573Z"
```

Meninjau detail temuan

Pilih metode yang Anda inginkan, dan ikuti langkah-langkah untuk melihat detail pencarian di Security Hub.

Security Hub console

Meninjau detail temuan

1. Buka AWS Security Hub konsol di https://console.aws.amazon.com/securityhub/.
2. Untuk menampilkan daftar temuan, lakukan salah satu tindakan berikut:
   - Di panel navigasi Security Hub, pilih Temuan. Tambahkan filter pencarian seperlunya untuk mempersempit daftar temuan.
   - Di panel navigasi Security Hub, pilih Wawasan. Pilih wawasan. Kemudian pada daftar hasil, pilih hasil wawasan.
   - Di panel navigasi Security Hub, pilih Integrasi. Pilih Lihat temuan untuk integrasi.
3. Pilih judul temuan.
4. Dari panel detail temuan, Anda dapat mengambil tindakan tambahan sebagai berikut:
   - Untuk menampilkan JSON lengkap untuk temuan, pilih ID temuan. Dari Finding JSON, unduh temuan JSON.
   - Untuk temuan yang didasarkan pada AWS Config aturan, untuk menampilkan daftar aturan yang berlaku, pilih Aturan.
   - Pilih Selidiki dengan Macie untuk menyelidiki data sensitif yang ditemukan dalam temuan di konsol Macie. Opsi ini hanya tersedia jika Anda mengaktifkan Amazon Macie dan fitur penemuan data sensitif otomatisnya.
   - Pilih Sumber Daya untuk melihat informasi tentang sumber daya yang terlibat dalam temuan.
   - Pilih Selidiki di Amazon Detective untuk menyelidiki temuan di konsol Detektif. Opsi ini hanya tersedia jika Anda mengaktifkan Amazon Detective.
   - Pilih tab Riwayat untuk melihat riwayat penemuan hingga 90 hari.

> **Note**
>
> Bagian atas panel detail temuan berisi informasi ikhtisar tentang temuan, termasuk akun, tingkat keparahan, tanggal, dan status. Jika Anda mengintegrasikan AWS Organizations dan akun yang Anda masuki adalah akun anggota organisasi, maka panel detail menyertakan nama akun. Untuk akun anggota yang diundang secara manual dan bukan melalui integrasi Organizations, panel detail hanya menyertakan ID akun.

Security Hub API

Meninjau detail temuan

Gunakan `GetFindings`pengoperasian Security Hub API, atau jika Anda menggunakan AWS CLI, jalankan perintah get-findings.

Anda dapat memberikan satu atau lebih nilai untuk `Filters` parameter untuk mempersempit temuan yang ingin Anda ambil.

Jika volume hasil terlalu besar, Anda dapat menggunakan `MaxResults` parameter untuk membatasi temuan ke angka tertentu dan `NextToken` parameter untuk membuat halaman temuan. Gunakan `SortCriteria` parameter untuk mengurutkan temuan berdasarkan bidang tertentu.

Jika Anda telah mengaktifkan agregasi lintas wilayah dan menjalankan operasi ini dari Wilayah agregasi, hasilnya menyertakan temuan dari agregasi dan Wilayah tertaut.

Perintah CLI berikut mengambil temuan yang cocok dengan filter yang disediakan dan mengurutkannya dalam urutan bidang yang menurun. `LastObservedAt` Contoh ini diformat untuk Linux, macOS, atau Unix, dan menggunakan karakter garis miring terbalik (\) untuk meningkatkan keterbacaan.

```
$ aws securityhub get-findings \
--filters '{"GeneratorId":[{"Value": "aws-
foundational","Comparison":"PREFIX"}],"WorkflowStatus": [{"Value":
 "NEW","Comparison":"EQUALS"}],"Confidence": [{"Gte": 85}]}' --sort-criteria
 '{"Field": "LastObservedAt","SortOrder": "desc"}' --page-size 5 --max-items 100
```

PowerShell

Meninjau detail temuan

1. Gunakan `Get-SHUBFinding` cmdlet.
2. Secara opsional, isi `Filter` parameter untuk mempersempit temuan yang ingin Anda ambil.

Contoh

```
Get-SHUBFinding -Filter @{AwsAccountId =
 [Amazon.SecurityHub.Model.StringFilter]@{Comparison = "EQUALS"; Value =
 "XXX"};ComplianceStatus = [Amazon.SecurityHub.Model.StringFilter]@{Comparison =
 "EQUALS"; Value = 'FAILED'}}
```

> **Note**
>
> Saat Anda memfilter temuan berdasarkan `CompanyName` atau`ProductName`, Security Hub menggunakan nilai yang merupakan bagian dari objek `ProductFields` ASFF. Security Hub tidak menggunakan top-level `CompanyName` dan `ProductName` field.

Mengambil tindakan atas temuan di AWS Security Hub

AWS Security Hub memungkinkan Anda untuk melacak status penyelidikan Anda saat ini ke dalam sebuah temuan.

Anda juga dapat mengirim temuan ke tindakan khusus untuk diproses.

Topik

- Mengatur status alur kerja temuan
- Mengirim temuan ke tindakan khusus

Mengatur status alur kerja temuan

Status alur kerja melacak kemajuan penyelidikan Anda ke dalam sebuah temuan. Status alur kerja khusus untuk temuan individu. Itu tidak mempengaruhi generasi temuan baru. Misalnya, menyetel

status alur kerja temuan ke SUPPRESSED atau RESOLVED tidak AWS Security Hub mencegah menghasilkan temuan baru untuk masalah yang sama.

Status alur kerja dapat memiliki nilai-nilai berikut:

NEW

Keadaan awal temuan sebelum Anda memeriksanya.

Temuan yang dicerna dari terintegrasi Layanan AWS, seperti AWS Config, memiliki NEW status awal mereka.

Security Hub juga mengatur ulang status alur kerja dari salah satu NOTIFIED atau RESOLVED ke NEW dalam kasus berikut:

- RecordStateperubahan dari ARCHIVED keACTIVE.
- Compliance.Statusperubahan dari PASSED keFAILED,WARNING, atauNOT_AVAILABLE.

Perubahan ini menyiratkan bahwa penyelidikan tambahan diperlukan.

NOTIFIED

Menunjukkan bahwa Anda memberi tahu pemilik sumber daya tentang masalah keamanan. Anda dapat menggunakan status ini ketika Anda bukan pemilik sumber daya, dan Anda memerlukan intervensi dari pemilik sumber daya untuk menyelesaikan masalah keamanan.

Jika salah satu hal berikut terjadi, status alur kerja diubah secara otomatis dari NOTIFIED menjadiNEW:

- RecordStateperubahan dari ARCHIVED keACTIVE.
- Compliance.Statusperubahan dari PASSED keFAILED,WARNING, atauNOT_AVAILABLE.

SUPPRESSED

Menunjukkan bahwa Anda meninjau temuan dan tidak percaya bahwa tindakan apa pun diperlukan.

Status alur kerja SUPPRESSED temuan tidak berubah jika RecordState berubah dari ARCHIVED keACTIVE.

RESOLVED

Temuan ini ditinjau dan diperbaiki dan sekarang dianggap telah diselesaikan.

Temuan tetap ada RESOLVED kecuali salah satu dari berikut ini terjadi:

- `RecordState`perubahan dari `ARCHIVED` ke`ACTIVE`.
- `Compliance.Status`perubahan dari `PASSED` ke`FAILED`,`WARNING`, atau`NOT_AVAILABLE`.

Dalam kasus tersebut, status alur kerja diatur ulang secara otomatis. `NEW`

Untuk temuan dari kontrol, jika `Compliance.Status` ada`PASSED`, maka Security Hub secara otomatis menyetel status alur kerja ke`RESOLVED`.

Mengatur status alur kerja temuan

Pilih metode pilihan Anda, dan ikuti langkah-langkah untuk mengatur status alur kerja dari satu atau beberapa temuan.

Untuk memperbarui status alur kerja temuan tertentu secara otomatis, lihatAturan otomatisasi.

Security Hub console

Untuk mengatur status alur kerja temuan

1. Buka AWS Security Hub konsol di https://console.aws.amazon.com/securityhub/.
2. Untuk menampilkan daftar temuan, lakukan salah satu hal berikut:
   - Di panel navigasi Security Hub, pilih Temuan.
   - Di panel navigasi Security Hub, pilih Wawasan. Pilih wawasan. Kemudian pada daftar hasil, pilih hasil wawasan.
   - Di panel navigasi Security Hub, pilih Integrasi. Pilih Lihat temuan untuk integrasi.
   - Di panel navigasi Security Hub, pilih Standar keamanan. Pilih Lihat hasil untuk menampilkan daftar kontrol. Kemudian, pilih kontrol untuk melihat daftar temuan untuk kontrol itu.
3. Dalam daftar temuan, pilih kotak centang untuk setiap temuan yang ingin Anda perbarui.
4. Di bagian atas daftar, untuk status Alur Kerja, pilih status.
5. Dalam kotak dialog Setel status alur kerja, berikan catatan opsional yang merinci alasan untuk memperbarui status alur kerja. Pilih Tetapkan status.

Security Hub API

Memanggil `BatchUpdateFindings`API. Berikan ID temuan dan ARN dari produk yang menghasilkan temuan. Anda bisa mendapatkan detail ini dengan menjalankan `GetFindings`API.

AWS CLI

Jalankan perintah `batch-update-findings`. Berikan ID temuan dan ARN dari produk yang menghasilkan temuan. Anda bisa mendapatkan detail ini dengan menjalankan `get-findings`perintah.

```
batch-update-findings --finding-identifiers
 Id="<findingID>",ProductArn="<productARN>" --workflow Status="<workflowStatus>"
```

Contoh

```
aws securityhub batch-update-findings --finding-identifiers
 Id="arn:aws:securityhub:us-west-1:123456789012:subscription/
pci-dss/v/3.2.1/PCI.Lambda.2/finding/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111",ProductArn="arn:aws:securityhub:us-west-1::product/aws/securityhub" --
workflow Status="RESOLVED"
```

Mengirim temuan ke tindakan khusus

Anda dapat membuat tindakan AWS Security Hub khusus untuk mengotomatiskan Security Hub dengan Amazon EventBridge. Untuk tindakan kustom, jenis acara adalah Security Hub Findings - Custom Action.

Untuk informasi selengkapnya dan langkah-langkah mendetail dalam membuat tindakan kustom, lihatthe section called “Respon dan remediasi otomatis”.

Setelah menyiapkan tindakan kustom, Anda dapat mengirim temuan ke sana.

Untuk mengirim temuan ke tindakan kustom (konsol)

1. Buka AWS Security Hub konsol di https://console.aws.amazon.com/securityhub/.
2. Untuk menampilkan daftar temuan, lakukan salah satu hal berikut:

   - Di panel navigasi Security Hub, pilih Temuan.
   - Di panel navigasi Security Hub, pilih Wawasan. Pilih wawasan. Kemudian pada daftar hasil, pilih hasil wawasan.
   - Di panel navigasi Security Hub, pilih Integrasi. Pilih Lihat temuan untuk integrasi.
   - Di panel navigasi Security Hub, pilih Standar keamanan. Pilih Lihat hasil untuk menampilkan daftar kontrol. Kemudian pilih nama kontrol.

3. Dalam daftar temuan, pilih kotak centang untuk setiap temuan untuk dikirim ke tindakan kustom.

   Anda dapat mengirim hingga 20 temuan sekaligus.
4. Untuk Tindakan, pilih tindakan kustom.

AWS Format Pencarian Keamanan (ASFF)

AWS Security Hub mengkonsumsi, mengumpulkan, mengatur, dan memprioritaskan temuan dari layanan AWS keamanan dan dari integrasi produk pihak ketiga. Security Hub memproses temuan ini menggunakan format temuan standar yang disebut AWS Security Finding Format (ASFF), yang menghilangkan kebutuhan akan upaya konversi data yang memakan waktu. Kemudian itu menghubungkan temuan yang dicerna di seluruh produk untuk memprioritaskan yang paling penting.

Topik

- AWS Sintaks Security Finding Format (ASFF)
- Dampak konsolidasi pada bidang dan nilai ASFF
- Contoh ASFF

AWS Sintaks Security Finding Format (ASFF)

Halaman ini memberikan garis besar lengkap JSON untuk temuan di AWS Security Finding Format (ASFF). Formatnya berasal dari Skema JSON. Pilih nama objek tertaut untuk melihat contoh temuan untuk objek itu. Anda dapat membandingkan temuan Security Hub Anda dengan sumber daya dan contoh yang ditampilkan di sini untuk membantu Anda menafsirkan temuan Anda.

Untuk melihat deskripsi atribut ASFF yang diperlukan, lihat. the section called “Atribut tingkat atas yang diperlukan”

Untuk melihat deskripsi atribut ASFF tingkat atas lainnya, lihat. the section called “Atribut tingkat atas opsional”

```
"Findings": [
    {
     "Action": {
      "ActionType": "string",
      "AwsApiCallAction": {
       "AffectedResources": {
        "string": "string"
```

```
        },
        "Api": "string",
        "CallerType": "string",
        "DomainDetails": {
         "Domain": "string"
        },
        "FirstSeen": "string",
        "LastSeen": "string",
        "RemoteIpDetails": {
         "City": {
          "CityName": "string"
         },
         "Country": {
          "CountryCode": "string",
          "CountryName": "string"
         },
         "IpAddressV4": "string",
         "Geolocation": {
          "Lat": number,
          "Lon": number
         },
         "Organization": {
          "Asn": number,
          "AsnOrg": "string",
          "Isp": "string",
          "Org": "string"
         }
        },
        "ServiceName": "string"
       },
       "DnsRequestAction": {
        "Blocked": boolean,
        "Domain": "string",
        "Protocol": "string"
       },
       "NetworkConnectionAction": {
        "Blocked": boolean,
        "ConnectionDirection": "string",
        "LocalPortDetails": {
         "Port": number,
         "PortName": "string"
        },
        "Protocol": "string",
        "RemoteIpDetails": {
```

```
        "City": {
         "CityName": "string"
        },
        "Country": {
         "CountryCode": "string",
         "CountryName": "string"
        },
        "IpAddressV4": "string",
        "Geolocation": {
         "Lat": number,
         "Lon": number
        },
        "Organization": {
         "Asn": number,
         "AsnOrg": "string",
         "Isp": "string",
         "Org": "string"
        }
       },
       "RemotePortDetails": {
        "Port": number,
        "PortName": "string"
       }
      },
      "PortProbeAction": {
       "Blocked": boolean,
       "PortProbeDetails": [{
        "LocalIpDetails": {
         "IpAddressV4": "string"
        },
        "LocalPortDetails": {
         "Port": number,
         "PortName": "string"
        },
        "RemoteIpDetails": {
         "City": {
          "CityName": "string"
         },
         "Country": {
          "CountryCode": "string",
          "CountryName": "string"
         },
         "GeoLocation": {
          "Lat": number,
```

```
          "Lon": number
         },
         "IpAddressV4": "string",
         "Organization": {
          "Asn": number,
          "AsnOrg": "string",
          "Isp": "string",
          "Org": "string"
         }
        }
       }]
      }
     },
     "AwsAccountId": "string",
     "AwsAccountName": "string",
     "CompanyName": "string",
     "Compliance": {
      "AssociatedStandards": [{
       "StandardsId": "string"
      }],
      "RelatedRequirements": ["string"],
      "SecurityControlId": "string",
      "SecurityControlParameters": [
       {
        "Name": "string",
        "Value": ["string"]
       }
     ],
      "Status": "string",
      "StatusReasons": [
       {
        "Description": "string",
        "ReasonCode": "string"
       }
      ]
     },
     "Confidence": number,
     "CreatedAt": "string",
     "Criticality": number,
     "Description": "string",
     "FindingProviderFields": {
      "Confidence": number,
      "Criticality": number,
      "RelatedFindings": [{
```

```
        "ProductArn": "string",
        "Id": "string"
       }],
       "Severity": {
        "Label": "string",
        "Normalized": number,
        "Original": "string"
       },
       "Types": ["string"]
      },
      "FirstObservedAt": "string",
      "GeneratorId": "string",
      "Id": "string",
      "LastObservedAt": "string",
      "Malware": [{
       "Name": "string",
       "Path": "string",
       "State": "string",
       "Type": "string"
      }],
      "Network": {
       "DestinationDomain": "string",
       "DestinationIpV4": "string",
       "DestinationIpV6": "string",
       "DestinationPort": number,
       "Direction": "string",
       "OpenPortRange": {
        "Begin": integer,
        "End": integer
       },
       "Protocol": "string",
       "SourceDomain": "string",
       "SourceIpV4": "string",
       "SourceIpV6": "string",
       "SourceMac": "string",
       "SourcePort": number
      },
      "NetworkPath": [{
       "ComponentId": "string",
       "ComponentType": "string",
       "Egress": {
        "Destination": {
         "Address": ["string"],
         "PortRanges": [{
```

```
          "Begin": integer,
          "End": integer
         }]
        },
        "Protocol": "string",
        "Source": {
         "Address": ["string"],
         "PortRanges": [{
          "Begin": integer,
          "End": integer
         }]
        }
       },
       "Ingress": {
        "Destination": {
         "Address": ["string"],
         "PortRanges": [{
          "Begin": integer,
          "End": integer
         }]
        },
        "Protocol": "string",
        "Source": {
         "Address": ["string"],
         "PortRanges": [{
          "Begin": integer,
          "End": integer
         }]
        }
       }
      }],
      "Note": {
       "Text": "string",
       "UpdatedAt": "string",
       "UpdatedBy": "string"
      },
      "PatchSummary": {
       "FailedCount": number,
       "Id": "string",
       "InstalledCount": number,
       "InstalledOtherCount": number,
       "InstalledPendingReboot": number,
       "InstalledRejectedCount": number,
       "MissingCount": number,
```

```
      "Operation": "string",
      "OperationEndTime": "string",
      "OperationStartTime": "string",
      "RebootOption": "string"
    },
    "Process": {
      "LaunchedAt": "string",
      "Name": "string",
      "ParentPid": number,
      "Path": "string",
      "Pid": number,
      "TerminatedAt": "string"
    },
    "ProductArn": "string",
    "ProductFields": {
      "string": "string"
    },
    "ProductName": "string",
    "RecordState": "string",
    "Region": "string",
    "RelatedFindings": [{
      "Id": "string",
      "ProductArn": "string"
    }],
    "Remediation": {
      "Recommendation": {
        "Text": "string",
        "Url": "string"
      }
    },
    "Resources": [{
      "ApplicationArn": "string",
      "ApplicationName": "string",
      "DataClassification": {
        "DetailedResultsLocation": "string",
        "Result": {
          "AdditionalOccurrences": boolean,
          "CustomDataIdentifiers": {
            "Detections": [{
              "Arn": "string",
              "Count": integer,
              "Name": "string",
              "Occurrences": {
                "Cells": [{
```

```
            "CellReference": "string",
            "Column": integer,
            "ColumnName": "string",
            "Row": integer
           }],
           "LineRanges": [{
            "End": integer,
            "Start": integer,
            "StartColumn": integer
           }],
           "OffsetRanges": [{
            "End": integer,
            "Start": integer,
            "StartColumn": integer
           }],
           "Pages": [{
            "LineRange": {
             "End": integer,
             "Start": integer,
             "StartColumn": integer
            },
            "OffsetRange": {
             "End": integer,
             "Start": integer,
             "StartColumn": integer
            },
            "PageNumber": integer
           }],
           "Records": [{
            "JsonPath": "string",
            "RecordIndex": integer
           }]
          }
         }],
         "TotalCount": integer
        },
        "MimeType": "string",
        "SensitiveData": [{
         "Category": "string",
         "Detections": [{
          "Count": integer,
          "Occurrences": {
           "Cells": [{
            "CellReference": "string",
```

```
            "Column": integer,
            "ColumnName": "string",
            "Row": integer
           }],
           "LineRanges": [{
            "End": integer,
            "Start": integer,
            "StartColumn": integer
           }],
           "OffsetRanges": [{
            "End": integer,
            "Start": integer,
            "StartColumn": integer
           }],
           "Pages": [{
            "LineRange": {
             "End": integer,
             "Start": integer,
             "StartColumn": integer
            },
            "OffsetRange": {
             "End": integer,
             "Start": integer,
             "StartColumn": integer
            },
            "PageNumber": integer
           }],
           "Records": [{
            "JsonPath": "string",
            "RecordIndex": integer
           }]
          },
          "Type": "string"
         }],
         "TotalCount": integer
        }],
        "SizeClassified": integer,
        "Status": {
         "Code": "string",
         "Reason": "string"
        }
       }
      },
      "Details": {
```

```
        "AwsAmazonMQBroker": {
         "AutoMinorVersionUpgrade": boolean,
         "BrokerArn": "string",
         "BrokerId": "string",
         "BrokerName": "string",
         "Configuration": {
          "Id": "string",
          "Revision": integer
         },
         "DeploymentMode": "string",
         "EncryptionOptions": {
          "UseAwsOwnedKey": boolean
         },
         "EngineType": "string",
         "EngineVersion": "string",
         "HostInstanceType": "string",
         "Logs": {
          "Audit": boolean,
          "AuditLogGroup": "string",
          "General": boolean,
          "GeneralLogGroup": "string"
         },
         "MaintenanceWindowStartTime": {
          "DayOfWeek": "string",
          "TimeOfDay": "string",
          "TimeZone": "string"
         },
         "PubliclyAccessible": boolean,
         "SecurityGroups": [
          "string"
         ],
         "StorageType": "string",
         "SubnetIds": [
          "string",
          "string"
         ],
         "Users": [{
          "Username": "string"
         }]
        },
        "AwsApiGatewayRestApi": {
         "ApiKeySource": "string",
         "BinaryMediaTypes": [" string"],
         "CreatedDate": "string",
```

```
        "Description": "string",
        "EndpointConfiguration": {
         "Types": ["string"]
        },
        "Id": "string",
        "MinimumCompressionSize": number,
        "Name": "string",
        "Version": "string"
       },
       "AwsApiGatewayStage": {
        "AccessLogSettings": {
         "DestinationArn": "string",
         "Format": "string"
        },
        "CacheClusterEnabled": boolean,
        "CacheClusterSize": "string",
        "CacheClusterStatus": "string",
        "CanarySettings": {
         "DeploymentId": "string",
         "PercentTraffic": number,
         "StageVariableOverrides": [{
          "string": "string"
         }],
         "UseStageCache": boolean
        },
        "ClientCertificateId": "string",
        "CreatedDate": "string",
        "DeploymentId": "string",
        "Description": "string",
        "DocumentationVersion": "string",
        "LastUpdatedDate": "string",
        "MethodSettings": [{
         "CacheDataEncrypted": boolean,
         "CachingEnabled": boolean,
         "CacheTtlInSeconds": number,
         "DataTraceEnabled": boolean,
         "HttpMethod": "string",
         "LoggingLevel": "string",
         "MetricsEnabled": boolean,
         "RequireAuthorizationForCacheControl": boolean,
         "ResourcePath": "string",
         "ThrottlingBurstLimit": number,
         "ThrottlingRateLimit": number,
         "UnauthorizedCacheControlHeaderStrategy": "string"
```

```
        }],
        "StageName": "string",
        "TracingEnabled": boolean,
        "Variables": {
         "string": "string"
        },
        "WebAclArn": "string"
       },
       "AwsApiGatewayV2Api": {
        "ApiEndpoint": "string",
        "ApiId": "string",
        "ApiKeySelectionExpression": "string",
        "CorsConfiguration": {
         "AllowCredentials": boolean,
         "AllowHeaders": ["string"],
         "AllowMethods": ["string"],
         "AllowOrigins": ["string"],
         "ExposeHeaders": ["string"],
         "MaxAge": number
        },
        "CreatedDate": "string",
        "Description": "string",
        "Name": "string",
        "ProtocolType": "string",
        "RouteSelectionExpression": "string",
        "Version": "string"
       },
       "AwsApiGatewayV2Stage": {
        "AccessLogSettings": {
         "DestinationArn": "string",
         "Format": "string"
        },
        "ApiGatewayManaged": boolean,
        "AutoDeploy": boolean,
        "ClientCertificateId": "string",
        "CreatedDate": "string",
        "DefaultRouteSettings": {
         "DataTraceEnabled": boolean,
         "DetailedMetricsEnabled": boolean,
         "LoggingLevel": "string",
         "ThrottlingBurstLimit": number,
         "ThrottlingRateLimit": number
        },
        "DeploymentId": "string",
```

```
        "Description": "string",
        "LastDeploymentStatusMessage": "string",
        "LastUpdatedDate": "string",
        "RouteSettings": {
         "DetailedMetricsEnabled": boolean,
         "LoggingLevel": "string",
         "DataTraceEnabled": boolean,
         "ThrottlingBurstLimit": number,
         "ThrottlingRateLimit": number
        },
        "StageName": "string",
        "StageVariables": [{
         "string": "string"
        }]
       },
       "AwsAppSyncGraphQLApi": {
        "AwsAppSyncGraphQlApi": {
         "AdditionalAuthenticationProviders": [
         {
          "AuthenticationType": "string",
          "LambdaAuthorizerConfig": {
           "AuthorizerResultTtlInSeconds": integer,
           "AuthorizerUri": "string"
          }
         },
         {
          "AuthenticationType": "string"
         }
         ],
         "ApiId": "string",
         "Arn": "string",
         "AuthenticationType": "string",
         "Id": "string",
         "LogConfig": {
          "CloudWatchLogsRoleArn": "string",
          "ExcludeVerboseContent": boolean,
          "FieldLogLevel": "string"
         },
         "Name": "string",
         "XrayEnabled": boolean
        }
       },
       "AwsAthenaWorkGroup": {
        "Description": "string",
```

```
        "Name": "string",
        "WorkgroupConfiguration": {
         "ResultConfiguration": {
          "EncryptionConfiguration": {
           "EncryptionOption": "string",
           "KmsKey": "string"
          }
         }
        },
        "State": "string"
       },
       "AwsAutoScalingAutoScalingGroup": {
        "AvailabilityZones": [{
         "Value": "string"
        }],
        "CreatedTime": "string",
        "HealthCheckGracePeriod": integer,
        "HealthCheckType": "string",
        "LaunchConfigurationName": "string",
        "LoadBalancerNames": ["string"],
        "LaunchTemplate": {
                       "LaunchTemplateId": "string",
                       "LaunchTemplateName": "string",
                       "Version": "string"
                   },
        "MixedInstancesPolicy": {
         "InstancesDistribution": {
          "OnDemandAllocationStrategy": "string",
          "OnDemandBaseCapacity": number,
          "OnDemandPercentageAboveBaseCapacity": number,
          "SpotAllocationStrategy": "string",
          "SpotInstancePools": number,
          "SpotMaxPrice": "string"
         },
         "LaunchTemplate": {
          "LaunchTemplateSpecification": {
           "LaunchTemplateId": "string",
           "LaunchTemplateName": "string",
           "Version": "string"
          },
          "CapacityRebalance": boolean,
          "Overrides": [{
           "InstanceType": "string",
           "WeightedCapacity": "string"
```

```
          }]
         }
        }
       },
       "AwsAutoScalingLaunchConfiguration": {
        "AssociatePublicIpAddress": boolean,
        "BlockDeviceMappings": [{
         "DeviceName": "string",
         "Ebs": {
          "DeleteOnTermination": boolean,
          "Encrypted": boolean,
          "Iops": number,
          "SnapshotId": "string",
          "VolumeSize": number,
          "VolumeType": "string"
         },
         "NoDevice": boolean,
         "VirtualName": "string"
        }],
        "ClassicLinkVpcId": "string",
        "ClassicLinkVpcSecurityGroups": ["string"],
        "CreatedTime": "string",
        "EbsOptimized": boolean,
        "IamInstanceProfile": "string"
       },
       "ImageId": "string",
       "InstanceMonitoring": {
        "Enabled": boolean
       },
       "InstanceType": "string",
       "KernelId": "string",
       "KeyName": "string",
       "LaunchConfigurationName": "string",
       "MetadataOptions": {
        "HttpEndPoint": "string",
        "HttpPutReponseHopLimit": number,
        "HttpTokens": "string"
       },
       "PlacementTenancy": "string",
       "RamdiskId": "string",
       "SecurityGroups": ["string"],
       "SpotPrice": "string",
       "UserData": "string"
      },
```

```
      "AwsBackupBackupPlan": {
       "BackupPlan": {
        "AdvancedBackupSettings": [{
         "BackupOptions": {
          "WindowsVSS":"string"
         },
         "ResourceType":"string"
        }],
        "BackupPlanName": "string",
        "BackupPlanRule": [{
         "CompletionWindowMinutes": integer,
         "CopyActions": [{
          "DestinationBackupVaultArn": "string",
          "Lifecycle": {
           "DeleteAfterDays": integer,
           "MoveToColdStorageAfterDays": integer
          }
         }],
         "Lifecycle": {
          "DeleteAfterDays": integer
         },
         "RuleName": "string",
         "ScheduleExpression": "string",
         "StartWindowMinutes": integer,
         "TargetBackupVault": "string"
        }]
       },
       "BackupPlanArn": "string",
       "BackupPlanId": "string",
       "VersionId": "string"
      },
      "AwsBackupBackupVault": {
       "AccessPolicy": {
        "Statement": [{
         "Action": ["string"],
         "Effect": "string",
         "Principal": {
          "AWS": "string"
         },
         "Resource": "string"
        }],
        "Version": "string"
       },
       "BackupVaultArn": "string",
```

```
        "BackupVaultName": "string",
        "EncryptionKeyArn": "string",
        "Notifications": {
         "BackupVaultEvents": ["string"],
         "SNSTopicArn": "string"
        }
       },
       "AwsBackupRecoveryPoint": {
        "BackupSizeInBytes": integer,
        "BackupVaultName": "string",
        "BackupVaultArn": "string",
        "CalculatedLifecycle": {
         "DeleteAt": "string",
         "MoveToColdStorageAt": "string"
        },
        "CompletionDate": "string",
        "CreatedBy": {
         "BackupPlanArn": "string",
         "BackupPlanId": "string",
         "BackupPlanVersion": "string",
         "BackupRuleId": "string"
        },
        "CreationDate": "string",
        "EncryptionKeyArn": "string",
        "IamRoleArn": "string",
        "IsEncrypted": boolean,
        "LastRestoreTime": "string",
        "Lifecycle": {
         "DeleteAfterDays": integer,
         "MoveToColdStorageAfterDays": integer
        },
        "RecoveryPointArn": "string",
        "ResourceArn": "string",
        "ResourceType": "string",
        "SourceBackupVaultArn": "string",
        "Status": "string",
        "StatusMessage": "string",
        "StorageClass": "string"
       },
       "AwsCertificateManagerCertificate": {
        "CertificateAuthorityArn": "string",
        "CreatedAt": "string",
        "DomainName": "string",
        "DomainValidationOptions": [{
```

```
        "DomainName": "string",
        "ResourceRecord": {
         "Name": "string",
         "Type": "string",
         "Value": "string"
        },
        "ValidationDomain": "string",
        "ValidationEmails": ["string"],
        "ValidationMethod": "string",
        "ValidationStatus": "string"
       }],
       "ExtendedKeyUsages": [{
        "Name": "string",
        "OId": "string"
       }],
       "FailureReason": "string",
       "ImportedAt": "string",
       "InUseBy": ["string"],
       "IssuedAt": "string",
       "Issuer": "string",
       "KeyAlgorithm": "string",
       "KeyUsages": [{
        "Name": "string"
       }],
       "NotAfter": "string",
       "NotBefore": "string",
       "Options": {
        "CertificateTransparencyLoggingPreference": "string"
       },
       "RenewalEligibility": "string",
       "RenewalSummary": {
        "DomainValidationOptions": [{
         "DomainName": "string",
         "ResourceRecord": {
          "Name": "string",
          "Type": "string",
          "Value": "string"
         },
         "ValidationDomain": "string",
         "ValidationEmails": ["string"],
         "ValidationMethod": "string",
         "ValidationStatus": "string"
        }],
        "RenewalStatus": "string",
```

```
        "RenewalStatusReason": "string",
        "UpdatedAt": "string"
       },
       "Serial": "string",
       "SignatureAlgorithm": "string",
       "Status": "string",
       "Subject": "string",
       "SubjectAlternativeNames": ["string"],
       "Type": "string"
      },
      "AwsCloudFormationStack": {
       "Capabilities": ["string"],
       "CreationTime": "string",
       "Description": "string",
       "DisableRollback": boolean,
       "DriftInformation": {
        "StackDriftStatus": "string"
       },
       "EnableTerminationProtection": boolean,
       "LastUpdatedTime": "string",
       "NotificationArns": ["string"],
       "Outputs": [{
        "Description": "string",
        "OutputKey": "string",
        "OutputValue": "string"
       }],
       "RoleArn": "string",
       "StackId": "string",
       "StackName": "string",
       "StackStatus": "string",
       "StackStatusReason": "string",
       "TimeoutInMinutes": number
      },
      "AwsCloudFrontDistribution": {
       "CacheBehaviors": {
        "Items": [{
         "ViewerProtocolPolicy": "string"
        }]
       },
       "DefaultCacheBehavior": {
        "ViewerProtocolPolicy": "string"
       },
       "DefaultRootObject": "string",
       "DomainName": "string",
```

```
        "Etag": "string",
        "LastModifiedTime": "string",
        "Logging": {
         "Bucket": "string",
         "Enabled": boolean,
         "IncludeCookies": boolean,
         "Prefix": "string"
        },
        "OriginGroups": {
         "Items": [{
          "FailoverCriteria": {
           "StatusCodes": {
            "Items": [number],
            "Quantity": number
           }
          }
         }]
        },
        "Origins": {
         "Items": [{
          "CustomOriginConfig": {
           "HttpPort": number,
           "HttpsPort": number,
           "OriginKeepaliveTimeout": number,
           "OriginProtocolPolicy": "string",
           "OriginReadTimeout": number,
           "OriginSslProtocols": {
            "Items": ["string"],
            "Quantity": number
           }
          },
          "DomainName": "string",
          "Id": "string",
          "OriginPath": "string",
          "S3OriginConfig": {
           "OriginAccessIdentity": "string"
          }
         }]
        },
        "Status": "string",
        "ViewerCertificate": {
         "AcmCertificateArn": "string",
         "Certificate": "string",
         "CertificateSource": "string",
```

```
        "CloudFrontDefaultCertificate": boolean,
        "IamCertificateId": "string",
        "MinimumProtocolVersion": "string",
        "SslSupportMethod": "string"
       },
       "WebAclId": "string"
      },
      "AwsCloudTrailTrail": {
       "CloudWatchLogsLogGroupArn": "string",
       "CloudWatchLogsRoleArn": "string",
       "HasCustomEventSelectors": boolean,
       "HomeRegion": "string",
       "IncludeGlobalServiceEvents": boolean,
       "IsMultiRegionTrail": boolean,
       "IsOrganizationTrail": boolean,
       "KmsKeyId": "string",
       "LogFileValidationEnabled": boolean,
       "Name": "string",
       "S3BucketName": "string",
       "S3KeyPrefix": "string",
       "SnsTopicArn": "string",
       "SnsTopicName": "string",
       "TrailArn": "string"
      },
      "AwsCloudWatchAlarm": {
       "ActionsEnabled": boolean,
       "AlarmActions": ["string"],
       "AlarmArn": "string",
       "AlarmConfigurationUpdatedTimestamp": "string",
       "AlarmDescription": "string",
       "AlarmName": "string",
       "ComparisonOperator": "string",
       "DatapointsToAlarm": number,
       "Dimensions": [{
        "Name": "string",
        "Value": "string"
       }],
       "EvaluateLowSampleCountPercentile": "string",
       "EvaluationPeriods": number,
       "ExtendedStatistic": "string",
       "InsufficientDataActions": ["string"],
       "MetricName": "string",
       "Namespace": "string",
       "OkActions": ["string"],
```

```
        "Period": number,
        "Statistic": "string",
        "Threshold": number,
        "ThresholdMetricId": "string",
        "TreatMissingData": "string",
        "Unit": "string"
       },
       "AwsCodeBuildProject": {
        "Artifacts": [{
         "ArtifactIdentifier": "string",
         "EncryptionDisabled": boolean,
         "Location": "string",
         "Name": "string",
         "NamespaceType": "string",
         "OverrideArtifactName": boolean,
         "Packaging": "string",
         "Path": "string",
         "Type": "string"
        }],
        "SecondaryArtifacts": [{
                    "ArtifactIdentifier": "string",
                    "Type": "string",
                    "Location": "string",
                    "Name": "string",
                    "NamespaceType": "string",
                    "Packaging": "string",
                    "Path": "string",
                    "EncryptionDisabled": boolean,
                    "OverrideArtifactName": boolean
                }],
        "EncryptionKey": "string",
        "Certificate": "string",
        "Environment": {
         "Certificate": "string",
         "EnvironmentVariables": [{
          "Name": "string",
          "Type": "string",
          "Value": "string"
         }],
         "ImagePullCredentialsType": "string",
         "PrivilegedMode": boolean,
         "RegistryCredential": {
          "Credential": "string",
          "CredentialProvider": "string"
```

```
        },
        "Type": "string"
       },
       "LogsConfig": {
        "CloudWatchLogs": {
         "GroupName": "string",
         "Status": "string",
         "StreamName": "string"
        },
        "S3Logs": {
         "EncryptionDisabled": boolean,
         "Location": "string",
         "Status": "string"
        }
       },
       "Name": "string",
       "ServiceRole": "string",
       "Source": {
        "Type": "string",
        "Location": "string",
        "GitCloneDepth": integer
       },
       "VpcConfig": {
        "VpcId": "string",
        "Subnets": ["string"],
        "SecurityGroupIds": ["string"]
       }
      },
      "AwsDmsEndpoint": {
       "CertificateArn": "string",
       "DatabaseName": "string",
       "EndpointArn": "string",
       "EndpointIdentifier": "string",
       "EndpointType": "string",
       "EngineName": "string",
       "KmsKeyId": "string",
       "Port": integer,
       "ServerName": "string",
       "SslMode": "string",
       "Username": "string"
      },
      "AwsDmsReplicationInstance": {
       "AllocatedStorage": integer,
       "AutoMinorVersionUpgrade": boolean,
```

```
        "AvailabilityZone": "string",
        "EngineVersion": "string",
        "KmsKeyId": "string",
        "MultiAZ": boolean,
        "PreferredMaintenanceWindow": "string",
        "PubliclyAccessible": boolean,
        "ReplicationInstanceClass": "string",
        "ReplicationInstanceIdentifier": "string",
        "ReplicationSubnetGroup": {
            "ReplicationSubnetGroupIdentifier": "string"
        },
        "VpcSecurityGroups": [
            {
                "VpcSecurityGroupId": "string"
            }
        ]
      },
      "AwsDmsReplicationTask": {
        "CdcStartPosition": "string",
        "Id": "string",
        "MigrationType": "string",
        "ReplicationInstanceArn": "string",
        "ReplicationTaskIdentifier": "string",
        "ReplicationTaskSettings": {
          "string": "string"
        },
        "SourceEndpointArn": "string",
        "TableMappings": {
          "string": "string"
        },
        "TargetEndpointArn": "string"
      },
      "AwsDynamoDbTable": {
        "AttributeDefinitions": [{
          "AttributeName": "string",
          "AttributeType": "string"
        }],
        "BillingModeSummary": {
          "BillingMode": "string",
          "LastUpdateToPayPerRequestDateTime": "string"
        },
        "CreationDateTime": "string",
        "DeletionProtectionEnabled": boolean,
        "GlobalSecondaryIndexes": [{
```

```
        "Backfilling": boolean,
        "IndexArn": "string",
        "IndexName": "string",
        "IndexSizeBytes": number,
        "IndexStatus": "string",
        "ItemCount": number,
        "KeySchema": [{
         "AttributeName": "string",
         "KeyType": "string"
        }],
        "Projection": {
         "NonKeyAttributes": ["string"],
         "ProjectionType": "string"
        },
        "ProvisionedThroughput": {
         "LastDecreaseDateTime": "string",
         "LastIncreaseDateTime": "string",
         "NumberOfDecreasesToday": number,
         "ReadCapacityUnits": number,
         "WriteCapacityUnits": number
        }
       }],
       "GlobalTableVersion": "string",
       "ItemCount": number,
       "KeySchema": [{
        "AttributeName": "string",
        "KeyType": "string"
       }],
       "LatestStreamArn": "string",
       "LatestStreamLabel": "string",
       "LocalSecondaryIndexes": [{
        "IndexArn": "string",
        "IndexName": "string",
        "KeySchema": [{
         "AttributeName": "string",
         "KeyType": "string"
        }],
        "Projection": {
         "NonKeyAttributes": ["string"],
         "ProjectionType": "string"
        }
       }],
       "ProvisionedThroughput": {
        "LastDecreaseDateTime": "string",
```

```
        "LastIncreaseDateTime": "string",
        "NumberOfDecreasesToday": number,
        "ReadCapacityUnits": number,
        "WriteCapacityUnits": number
       },
       "Replicas": [{
        "GlobalSecondaryIndexes": [{
         "IndexName": "string",
         "ProvisionedThroughputOverride": {
          "ReadCapacityUnits": number
         }
        }],
        "KmsMasterKeyId": "string",
        "ProvisionedThroughputOverride": {
         "ReadCapacityUnits": number
        },
        "RegionName": "string",
        "ReplicaStatus": "string",
        "ReplicaStatusDescription": "string"
       }],
       "RestoreSummary": {
        "RestoreDateTime": "string",
        "RestoreInProgress": boolean,
        "SourceBackupArn": "string",
        "SourceTableArn": "string"
       },
       "SseDescription": {
        "InaccessibleEncryptionDateTime": "string",
        "KmsMasterKeyArn": "string",
        "SseType": "string",
        "Status": "string"
       },
       "StreamSpecification": {
        "StreamEnabled": boolean,
        "StreamViewType": "string"
       },
       "TableId": "string",
       "TableName": "string",
       "TableSizeBytes": number,
       "TableStatus": "string"
      },
      "AwsEc2ClientVpnEndpoint": {
       "AuthenticationOptions": [
        {
```

```
          "MutualAuthentication": {
           "ClientRootCertificateChainArn": "string"
          },
          "Type": "string"
         }
        ],
        "ClientCidrBlock": "string",
        "ClientConnectOptions": {
         "Enabled": boolean
        },
        "ClientLoginBannerOptions": {
         "Enabled": boolean
        },
        "ClientVpnEndpointId": "string",
        "ConnectionLogOptions": {
         "Enabled": boolean
        },
        "Description": "string",
        "DnsServer": ["string"],
        "ServerCertificateArn": "string",
        "SecurityGroupIdSet": [
         "string"
        ],
        "SelfServicePortalUrl": "string",
        "SessionTimeoutHours": "integer",
        "SplitTunnel": boolean,
        "TransportProtocol": "string",
        "VpcId": "string",
        "VpnPort": integer
       },
       "AwsEc2Eip": {
        "AllocationId": "string",
        "AssociationId": "string",
        "Domain": "string",
        "InstanceId": "string",
        "NetworkBorderGroup": "string",
        "NetworkInterfaceId": "string",
        "NetworkInterfaceOwnerId": "string",
        "PrivateIpAddress": "string",
        "PublicIp": "string",
        "PublicIpv4Pool": "string"
       },
       "AwsEc2Instance": {
        "IamInstanceProfileArn": "string",
```

```
        "ImageId": "string",
        "IpV4Addresses": ["string"],
        "IpV6Addresses": ["string"],
        "KeyName": "string",
        "LaunchedAt": "string",
        "MetadataOptions": {
         "HttpEndpoint": "string",
         "HttpProtocolIpv6": "string",
         "HttpPutResponseHopLimit": number,
         "HttpTokens": "string",
         "InstanceMetadataTags": "string"
        },
        "Monitoring": {
         "State": "string"
        },
        "NetworkInterfaces": [{
         "NetworkInterfaceId": "string"
        }],
        "SubnetId": "string",
        "Type": "string",
        "VirtualizationType": "string",
        "VpcId": "string"
       },
       "AwsEc2LaunchTemplate": {
        "DefaultVersionNumber": "string",
        "ElasticGpuSpecifications": ["string"],
        "ElasticInferenceAccelerators": ["string"],
        "Id": "string",
        "ImageId": "string",
        "LatestVersionNumber": "string",
        "LaunchTemplateData": {
         "BlockDeviceMappings": [{
          "DeviceName": "string",
          "Ebs": {
           "DeleteonTermination": boolean,
           "Encrypted": boolean,
           "SnapshotId": "string",
           "VolumeSize": number,
           "VolumeType": "string"
          }
         }],
         "MetadataOptions": {
          "HttpTokens": "string",
          "HttpPutResponseHopLimit" : number
```

```
        },
        "Monitoring": {
         "Enabled": boolean
        },
        "NetworkInterfaces": [{
         "AssociatePublicIpAddress" : boolean
        }]
       },
       "LaunchTemplateName": "string",
       "LicenseSpecifications": ["string"],
       "SecurityGroupIds": ["string"],
       "SecurityGroups": ["string"],
       "TagSpecifications": ["string"]
      },
      "AwsEc2NetworkAcl": {
       "Associations": [{
        "NetworkAclAssociationId": "string",
        "NetworkAclId": "string",
        "SubnetId": "string"
       }],
       "Entries": [{
        "CidrBlock": "string",
        "Egress": boolean,
        "IcmpTypeCode": {
         "Code": number,
         "Type": number
        },
        "Ipv6CidrBlock": "string",
        "PortRange": {
         "From": number,
         "To": number
        },
        "Protocol": "string",
        "RuleAction": "string",
        "RuleNumber": number
       }],
       "IsDefault": boolean,
       "NetworkAclId": "string",
       "OwnerId": "string",
       "VpcId": "string"
      },
      "AwsEc2NetworkInterface": {
       "Attachment": {
        "AttachmentId": "string",
```

```
        "AttachTime": "string",
        "DeleteOnTermination": boolean,
        "DeviceIndex": number,
        "InstanceId": "string",
        "InstanceOwnerId": "string",
        "Status": "string"
       },
       "Ipv6Addresses": [{
        "Ipv6Address": "string"
       }],
       "NetworkInterfaceId": "string",
       "PrivateIpAddresses": [{
        "PrivateDnsName": "string",
        "PrivateIpAddress": "string"
       }],
       "PublicDnsName": "string",
       "PublicIp": "string",
       "SecurityGroups": [{
        "GroupId": "string",
        "GroupName": "string"
       }],
       "SourceDestCheck": boolean
      },
      "AwsEc2RouteTable": {
       "AssociationSet": [{
        "AssociationState": {
         "State": "string"
        },
        "Main": boolean,
        "RouteTableAssociationId": "string",
        "RouteTableId": "string"
       }],
       "PropogatingVgwSet": [],
       "RouteTableId": "string",
       "RouteSet": [
        {
         "DestinationCidrBlock": "string",
         "GatewayId": "string",
         "Origin": "string",
         "State": "string"
        },
        {
         "DestinationCidrBlock": "string",
         "GatewayId": "string",
```

```
          "Origin": "string",
          "State": "string"
         }
        ],
        "VpcId": "string"
       },
       "AwsEc2SecurityGroup": {
        "GroupId": "string",
        "GroupName": "string",
        "IpPermissions": [{
         "FromPort": number,
         "IpProtocol": "string",
         "IpRanges": [{
          "CidrIp": "string"
         }],
         "Ipv6Ranges": [{
          "CidrIpv6": "string"
         }],
         "PrefixListIds": [{
          "PrefixListId": "string"
         }],
         "ToPort": number,
         "UserIdGroupPairs": [{
          "GroupId": "string",
          "GroupName": "string",
          "PeeringStatus": "string",
          "UserId": "string",
          "VpcId": "string",
          "VpcPeeringConnectionId": "string"
         }]
        }],
        "IpPermissionsEgress": [{
         "FromPort": number,
         "IpProtocol": "string",
         "IpRanges": [{
          "CidrIp": "string"
         }],
         "Ipv6Ranges": [{
          "CidrIpv6": "string"
         }],
         "PrefixListIds": [{
          "PrefixListId": "string"
         }],
         "ToPort": number,
```

```
        "UserIdGroupPairs": [{
         "GroupId": "string",
         "GroupName": "string",
         "PeeringStatus": "string",
         "UserId": "string",
         "VpcId": "string",
         "VpcPeeringConnectionId": "string"
        }]
       }],
       "OwnerId": "string",
       "VpcId": "string"
      },
      "AwsEc2Subnet": {
       "AssignIpv6AddressOnCreation": boolean,
       "AvailabilityZone": "string",
       "AvailabilityZoneId": "string",
       "AvailableIpAddressCount": number,
       "CidrBlock": "string",
       "DefaultForAz": boolean,
       "Ipv6CidrBlockAssociationSet": [{
        "AssociationId": "string",
        "Ipv6CidrBlock": "string",
        "CidrBlockState": "string"
       }],
       "MapPublicIpOnLaunch": boolean,
       "OwnerId": "string",
       "State": "string",
       "SubnetArn": "string",
       "SubnetId": "string",
       "VpcId": "string"
      },
      "AwsEc2TransitGateway": {
       "AmazonSideAsn": number,
       "AssociationDefaultRouteTableId": "string",
       "AutoAcceptSharedAttachments": "string",
       "DefaultRouteTableAssociation": "string",
       "DefaultRouteTablePropagation": "string",
       "Description": "string",
       "DnsSupport": "string",
       "Id": "string",
       "MulticastSupport": "string",
       "PropagationDefaultRouteTableId": "string",
       "TransitGatewayCidrBlocks": ["string"],
       "VpnEcmpSupport": "string"
```

```
      },
      "AwsEc2Volume": {
       "Attachments": [{
        "AttachTime": "string",
        "DeleteOnTermination": boolean,
        "InstanceId": "string",
        "Status": "string"
       }],
       "CreateTime": "string",
       "DeviceName": "string",
       "Encrypted": boolean,
       "KmsKeyId": "string",
       "Size": number,
       "SnapshotId": "string",
       "Status": "string",
       "VolumeId": "string",
       "VolumeScanStatus": "string",
       "VolumeType": "string"
      },
      "AwsEc2Vpc": {
       "CidrBlockAssociationSet": [{
        "AssociationId": "string",
        "CidrBlock": "string",
        "CidrBlockState": "string"
       }],
       "DhcpOptionsId": "string",
       "Ipv6CidrBlockAssociationSet": [{
        "AssociationId": "string",
        "CidrBlockState": "string",
        "Ipv6CidrBlock": "string"
       }],
       "State": "string"
      },
      "AwsEc2VpcEndpointService": {
       "AcceptanceRequired": boolean,
       "AvailabilityZones": ["string"],
       "BaseEndpointDnsNames": ["string"],
       "ManagesVpcEndpoints": boolean,
       "GatewayLoadBalancerArns": ["string"],
       "NetworkLoadBalancerArns": ["string"],
       "PrivateDnsName": "string",
       "ServiceId": "string",
       "ServiceName": "string",
       "ServiceState": "string",
```

```
        "ServiceType": [{
         "ServiceType": "string"
        }]
       },
       "AwsEc2VpcPeeringConnection": {
        "AccepterVpcInfo": {
         "CidrBlock": "string",
         "CidrBlockSet": [{
          "CidrBlock": "string"
         }],
         "Ipv6CidrBlockSet": [{
          "Ipv6CidrBlock": "string"
         }],
         "OwnerId": "string",
         "PeeringOptions": {
          "AllowDnsResolutionFromRemoteVpc": boolean,
          "AllowEgressFromLocalClassicLinkToRemoteVpc": boolean,
          "AllowEgressFromLocalVpcToRemoteClassicLink": boolean
         },
         "Region": "string",
         "VpcId": "string"
        },
        "ExpirationTime": "string",
        "RequesterVpcInfo": {
         "CidrBlock": "string",
         "CidrBlockSet": [{
          "CidrBlock": "string"
         }],
         "Ipv6CidrBlockSet": [{
          "Ipv6CidrBlock": "string"
         }],
         "OwnerId": "string",
         "PeeringOptions": {
          "AllowDnsResolutionFromRemoteVpc": boolean,
          "AllowEgressFromLocalClassicLinkToRemoteVpc": boolean,
          "AllowEgressFromLocalVpcToRemoteClassicLink": boolean
         },
         "Region": "string",
         "VpcId": "string"
        },
        "Status": {
         "Code": "string",
         "Message": "string"
        },
```

```
        "VpcPeeringConnectionId": "string"
      },
      "AwsEc2VpnConnection": {
       "Category": "string",
       "CustomerGatewayConfiguration": "string",
       "CustomerGatewayId": "string",
       "Options": {
        "StaticRoutesOnly": boolean,
        "TunnelOptions": [{
         "DpdTimeoutSeconds": number,
         "IkeVersions": ["string"],
         "OutsideIpAddress": "string",
         "Phase1DhGroupNumbers": [number],
         "Phase1EncryptionAlgorithms": ["string"],
         "Phase1IntegrityAlgorithms": ["string"],
         "Phase1LifetimeSeconds": number,
         "Phase2DhGroupNumbers": [number],
         "Phase2EncryptionAlgorithms": ["string"],
         "Phase2IntegrityAlgorithms": ["string"],
         "Phase2LifetimeSeconds": number,
         "PreSharedKey": "string",
         "RekeyFuzzPercentage": number,
         "RekeyMarginTimeSeconds": number,
         "ReplayWindowSize": number,
         "TunnelInsideCidr": "string"
        }]
       },
       "Routes": [{
        "DestinationCidrBlock": "string",
        "State": "string"
       }],
       "State": "string",
       "TransitGatewayId": "string",
       "Type": "string",
       "VgwTelemetry": [{
        "AcceptedRouteCount": number,
        "CertificateArn": "string",
        "LastStatusChange": "string",
        "OutsideIpAddress": "string",
        "Status": "string",
        "StatusMessage": "string"
       }],
       "VpnConnectionId": "string",
       "VpnGatewayId": "string"
```

```
      },
      "AwsEcrContainerImage": {
       "Architecture": "string",
       "ImageDigest": "string",
       "ImagePublishedAt": "string",
       "ImageTags": ["string"],
       "RegistryId": "string",
       "RepositoryName": "string"
      },
      "AwsEcrRepository": {
       "Arn": "string",
       "ImageScanningConfiguration": {
        "ScanOnPush": boolean
       },
       "ImageTagMutability": "string",
       "LifecyclePolicy": {
        "LifecyclePolicyText": "string",
        "RegistryId": "string"
       },
       "RepositoryName": "string",
       "RepositoryPolicyText": "string"
      },
      "AwsEcsCluster": {
       "ActiveServicesCount": number,
       "CapacityProviders": ["string"],
       "ClusterArn": "string",
       "ClusterName": "string",
       "ClusterSettings": [{
        "Name": "string",
        "Value": "string"
       }],
       "Configuration": {
        "ExecuteCommandConfiguration": {
         "KmsKeyId": "string",
         "LogConfiguration": {
          "CloudWatchEncryptionEnabled": boolean,
          "CloudWatchLogGroupName": "string",
          "S3BucketName": "string",
          "S3EncryptionEnabled": boolean,
          "S3KeyPrefix": "string"
         },
         "Logging": "string"
        }
       },
```

```
        "DefaultCapacityProviderStrategy": [{
         "Base": number,
         "CapacityProvider": "string",
         "Weight": number
        }],
        "RegisteredContainerInstancesCount": number,
        "RunningTasksCount": number,
        "Status": "string"
       },
       "AwsEcsContainer": {
        "Image": "string",
        "MountPoints": [{
         "ContainerPath": "string",
         "SourceVolume": "string"
        }],
        "Name": "string",
        "Privileged": boolean
       },
       "AwsEcsService": {
        "CapacityProviderStrategy": [{
         "Base": number,
         "CapacityProvider": "string",
         "Weight": number
        }],
        "Cluster": "string",
        "DeploymentConfiguration": {
         "DeploymentCircuitBreaker": {
          "Enable": boolean,
          "Rollback": boolean
         },
         "MaximumPercent": number,
         "MinimumHealthyPercent": number
        },
        "DeploymentController": {
         "Type": "string"
        },
        "DesiredCount": number,
        "EnableEcsManagedTags": boolean,
        "EnableExecuteCommand": boolean,
        "HealthCheckGracePeriodSeconds": number,
        "LaunchType": "string",
        "LoadBalancers": [{
         "ContainerName": "string",
         "ContainerPort": number,
```

```
        "LoadBalancerName": "string",
        "TargetGroupArn": "string"
       }],
       "Name": "string",
       "NetworkConfiguration": {
        "AwsVpcConfiguration": {
         "AssignPublicIp": "string",
         "SecurityGroups": ["string"],
         "Subnets": ["string"]
        }
       },
       "PlacementConstraints": [{
        "Expression": "string",
        "Type": "string"
       }],
       "PlacementStrategies": [{
        "Field": "string",
        "Type": "string"
       }],
       "PlatformVersion": "string",
       "PropagateTags": "string",
       "Role": "string",
       "SchedulingStrategy": "string",
       "ServiceArn": "string",
       "ServiceName": "string",
       "ServiceRegistries": [{
        "ContainerName": "string",
        "ContainerPort": number,
        "Port": number,
        "RegistryArn": "string"
       }],
       "TaskDefinition": "string"
      },
      "AwsEcsTask": {
       "CreatedAt": "string",
       "ClusterArn": "string",
       "Group": "string",
       "StartedAt": "string",
       "StartedBy": "string",
       "TaskDefinitionArn": "string",
       "Version": number,
       "Volumes": [{
        "Name": "string",
        "Host": {
```

```
          "SourcePath": "string"
         }
        }],
        "Containers": [{
         "Image": "string",
         "MountPoints": [{
          "ContainerPath": "string",
          "SourceVolume": "string"
         }],
         "Name": "string",
         "Privileged": boolean
        }]
       },
       "AwsEcsTaskDefinition": {
        "ContainerDefinitions": [{
         "Command": ["string"],
         "Cpu": number,
         "DependsOn": [{
          "Condition": "string",
          "ContainerName": "string"
         }],
         "DisableNetworking": boolean,
         "DnsSearchDomains": ["string"],
         "DnsServers": ["string"],
         "DockerLabels": {
          "string": "string"
         },
         "DockerSecurityOptions": ["string"],
         "EntryPoint": ["string"],
         "Environment": [{
          "Name": "string",
          "Value": "string"
         }],
         "EnvironmentFiles": [{
          "Type": "string",
          "Value": "string"
         }],
         "Essential": boolean,
         "ExtraHosts": [{
          "Hostname": "string",
          "IpAddress": "string"
         }],
         "FirelensConfiguration": {
          "Options": {
```

```
          "string": "string"
         },
         "Type": "string"
        },
        "HealthCheck": {
         "Command": ["string"],
         "Interval": number,
         "Retries": number,
         "StartPeriod": number,
         "Timeout": number
        },
        "Hostname": "string",
        "Image": "string",
        "Interactive": boolean,
        "Links": ["string"],
        "LinuxParameters": {
         "Capabilities": {
          "Add": ["string"],
          "Drop": ["string"]
         },
         "Devices": [{
          "ContainerPath": "string",
          "HostPath": "string",
          "Permissions": ["string"]
         }],
         "InitProcessEnabled": boolean,
         "MaxSwap": number,
         "SharedMemorySize": number,
         "Swappiness": number,
         "Tmpfs": [{
          "ContainerPath": "string",
          "MountOptions": ["string"],
          "Size": number
         }]
        },
        "LogConfiguration": {
         "LogDriver": "string",
         "Options": {
          "string": "string"
         },
         "SecretOptions": [{
          "Name": "string",
          "ValueFrom": "string"
         }]
```

```
        },
        "Memory": number,
        "MemoryReservation": number,
        "MountPoints": [{
         "ContainerPath": "string",
         "ReadOnly": boolean,
         "SourceVolume": "string"
        }],
        "Name": "string",
        "PortMappings": [{
         "ContainerPort": number,
         "HostPort": number,
         "Protocol": "string"
        }],
        "Privileged": boolean,
        "PseudoTerminal": boolean,
        "ReadonlyRootFilesystem": boolean,
        "RepositoryCredentials": {
         "CredentialsParameter": "string"
        },
        "ResourceRequirements": [{
         "Type": "string",
         "Value": "string"
        }],
        "Secrets": [{
         "Name": "string",
         "ValueFrom": "string"
        }],
        "StartTimeout": number,
        "StopTimeout": number,
        "SystemControls": [{
         "Namespace": "string",
         "Value": "string"
        }],
        "Ulimits": [{
         "HardLimit": number,
         "Name": "string",
         "SoftLimit": number
        }],
        "User": "string",
        "VolumesFrom": [{
         "ReadOnly": boolean,
         "SourceContainer": "string"
        }],
```

```
        "WorkingDirectory": "string"
       }],
       "Cpu": "string",
       "ExecutionRoleArn": "string",
       "Family": "string",
       "InferenceAccelerators": [{
        "DeviceName": "string",
        "DeviceType": "string"
       }],
       "IpcMode": "string",
       "Memory": "string",
       "NetworkMode": "string",
       "PidMode": "string",
       "PlacementConstraints": [{
        "Expression": "string",
        "Type": "string"
       }],
       "ProxyConfiguration": {
        "ContainerName": "string",
        "ProxyConfigurationProperties": [{
         "Name": "string",
         "Value": "string"
        }],
        "Type": "string"
       },
       "RequiresCompatibilities": ["string"],
       "Status": "string",
       "TaskRoleArn": "string",
       "Volumes": [{
        "DockerVolumeConfiguration": {
         "Autoprovision": boolean,
         "Driver": "string",
         "DriverOpts": {
          "string": "string"
         },
         "Labels": {
          "string": "string"
         },
         "Scope": "string"
        },
        "EfsVolumeConfiguration": {
         "AuthorizationConfig": {
          "AccessPointId": "string",
          "Iam": "string"
```

```
        },
        "FilesystemId": "string",
        "RootDirectory": "string",
        "TransitEncryption": "string",
        "TransitEncryptionPort": number
       },
       "Host": {
        "SourcePath": "string"
       },
       "Name": "string"
      }]
     },
     "AwsEfsAccessPoint": {
      "AccessPointId": "string",
      "Arn": "string",
      "ClientToken": "string",
      "FileSystemId": "string",
      "PosixUser": {
       "Gid": "string",
       "SecondaryGids": ["string"],
       "Uid": "string"
      },
      "RootDirectory": {
       "CreationInfo": {
        "OwnerGid": "string",
        "OwnerUid": "string",
        "Permissions": "string"
       },
       "Path": "string"
      }
     },
     "AwsEksCluster": {
      "Arn": "string",
      "CertificateAuthorityData": "string",
      "ClusterStatus": "string",
      "Endpoint": "string",
      "Logging": {
       "ClusterLogging": [{
        "Enabled": boolean,
        "Types": ["string"]
       }]
      },
      "Name": "string",
      "ResourcesVpcConfig": {
```

```
        "EndpointPublicAccess": boolean,
        "SecurityGroupIds": ["string"],
        "SubnetIds": ["string"]
       },
       "RoleArn": "string",
       "Version": "string"
      },
      "AwsElasticBeanstalkEnvironment": {
       "ApplicationName": "string",
       "Cname": "string",
       "DateCreated": "string",
       "DateUpdated": "string",
       "Description": "string",
       "EndpointUrl": "string",
       "EnvironmentArn": "string",
       "EnvironmentId": "string",
       "EnvironmentLinks": [{
        "EnvironmentName": "string",
        "LinkName": "string"
       }],
       "EnvironmentName": "string",
       "OptionSettings": [{
        "Namespace": "string",
        "OptionName": "string",
        "ResourceName": "string",
        "Value": "string"
       }],
       "PlatformArn": "string",
       "SolutionStackName": "string",
       "Status": "string",
       "Tier": {
        "Name": "string",
        "Type": "string",
        "Version": "string"
       },
       "VersionLabel": "string"
      },
      "AwsElasticSearchDomain": {
       "AccessPolicies": "string",
       "DomainStatus": {
        "DomainId": "string",
        "DomainName": "string",
        "Endpoint": "string",
        "Endpoints": {
```

```
          "string": "string"
         }
        },
        "DomainEndpointOptions": {
         "EnforceHTTPS": boolean,
         "TLSSecurityPolicy": "string"
        },
        "ElasticsearchClusterConfig": {
         "DedicatedMasterCount": number,
         "DedicatedMasterEnabled": boolean,
         "DedicatedMasterType": "string",
         "InstanceCount": number,
         "InstanceType": "string",
         "ZoneAwarenessConfig": {
          "AvailabilityZoneCount": number
         },
         "ZoneAwarenessEnabled": boolean
        },
        "ElasticsearchVersion": "string",
        "EncryptionAtRestOptions": {
         "Enabled": boolean,
         "KmsKeyId": "string"
        },
        "LogPublishingOptions": {
         "AuditLogs": {
          "CloudWatchLogsLogGroupArn": "string",
          "Enabled": boolean
         },
         "IndexSlowLogs": {
          "CloudWatchLogsLogGroupArn": "string",
          "Enabled": boolean
         },
         "SearchSlowLogs": {
          "CloudWatchLogsLogGroupArn": "string",
          "Enabled": boolean
         }
        },
        "NodeToNodeEncryptionOptions": {
         "Enabled": boolean
        },
        "ServiceSoftwareOptions": {
         "AutomatedUpdateDate": "string",
         "Cancellable": boolean,
         "CurrentVersion": "string",
```

```
        "Description": "string",
        "NewVersion": "string",
        "UpdateAvailable": boolean,
        "UpdateStatus": "string"
       },
       "VPCOptions": {
        "AvailabilityZones": [
         "string"
        ],
        "SecurityGroupIds": [
         "string"
        ],
        "SubnetIds": [
         "string"
        ],
        "VPCId": "string"
       }
      },
      "AwsElbLoadBalancer": {
       "AvailabilityZones": ["string"],
       "BackendServerDescriptions": [{
        "InstancePort": number,
        "PolicyNames": ["string"]
       }],
       "CanonicalHostedZoneName": "string",
       "CanonicalHostedZoneNameID": "string",
       "CreatedTime": "string",
       "DnsName": "string",
       "HealthCheck": {
        "HealthyThreshold": number,
        "Interval": number,
        "Target": "string",
        "Timeout": number,
        "UnhealthyThreshold": number
       },
       "Instances": [{
        "InstanceId": "string"
       }],
       "ListenerDescriptions": [{
        "Listener": {
         "InstancePort": number,
         "InstanceProtocol": "string",
         "LoadBalancerPort": number,
         "Protocol": "string",
```

```
          "SslCertificateId": "string"
         },
         "PolicyNames": ["string"]
        }],
        "LoadBalancerAttributes": {
         "AccessLog": {
          "EmitInterval": number,
          "Enabled": boolean,
          "S3BucketName": "string",
          "S3BucketPrefix": "string"
         },
         "ConnectionDraining": {
          "Enabled": boolean,
          "Timeout": number
         },
         "ConnectionSettings": {
          "IdleTimeout": number
         },
         "CrossZoneLoadBalancing": {
          "Enabled": boolean
         },
         "AdditionalAttributes": [{
                        "Key": "string",
                        "Value": "string"
                    }]
        },
        "LoadBalancerName": "string",
        "Policies": {
         "AppCookieStickinessPolicies": [{
          "CookieName": "string",
          "PolicyName": "string"
         }],
         "LbCookieStickinessPolicies": [{
          "CookieExpirationPeriod": number,
          "PolicyName": "string"
         }],
         "OtherPolicies": ["string"]
        },
        "Scheme": "string",
        "SecurityGroups": ["string"],
        "SourceSecurityGroup": {
         "GroupName": "string",
         "OwnerAlias": "string"
        },
```

```
        "Subnets": ["string"],
        "VpcId": "string"
      },
      "AwsElbv2LoadBalancer": {
        "AvailabilityZones": {
          "SubnetId": "string",
          "ZoneName": "string"
        },
        "CanonicalHostedZoneId": "string",
        "CreatedTime": "string",
        "DNSName": "string",
        "IpAddressType": "string",
        "LoadBalancerAttributes": [{
          "Key": "string",
          "Value": "string"
        }],
        "Scheme": "string",
        "SecurityGroups": ["string"],
        "State": {
          "Code": "string",
          "Reason": "string"
        },
        "Type": "string",
        "VpcId": "string"
      },
      "AwsEventSchemasRegistry": {
        "Description": "string",
        "RegistryArn": "string",
        "RegistryName": "string"
      },
      "AwsEventsEndpoint": {
        "Arn": "string",
        "Description": "string",
        "EndpointId": "string",
        "EndpointUrl": "string",
        "EventBuses": [
            {
                "EventBusArn": "string"
            },
            {
                "EventBusArn": "string"
            }
        ],
        "Name": "string",
```

```
        "ReplicationConfig": {
            "State": "string"
        },
        "RoleArn": "string",
        "RoutingConfig": {
            "FailoverConfig": {
                "Primary": {
                    "HealthCheck": "string"
                },
                "Secondary": {
                    "Route": "string"
                }
            }
        },
        "State": "string"
      },
      "AwsEventsEventBus": {
        "Arn": "string",
        "Name": "string",
        "Policy": "string"
      },
      "AwsGuardDutyDetector": {
        "FindingPublishingFrequency": "string",
        "ServiceRole": "string",
        "Status": "string",
        "DataSources": {
          "CloudTrail": {
            "Status": "string"
          },
          "DnsLogs": {
            "Status": "string"
          },
          "FlowLogs": {
            "Status": "string"
          },
          "S3Logs": {
            "Status": "string"
          },
          "Kubernetes": {
            "AuditLogs": {
              "Status": "string"
            }
          },
          "MalwareProtection": {
```

```
          "ScanEc2InstanceWithFindings": {
           "EbsVolumes": {
            "Status": "string"
           }
          },
          "ServiceRole": "string"
         }
        }
       },
       "AwsIamAccessKey": {
        "AccessKeyId": "string",
        "AccountId": "string",
        "CreatedAt": "string",
        "PrincipalId": "string",
        "PrincipalName": "string",
        "PrincipalType": "string",
        "SessionContext": {
         "Attributes": {
          "CreationDate": "string",
          "MfaAuthenticated": boolean
         },
         "SessionIssuer": {
          "AccountId": "string",
          "Arn": "string",
          "PrincipalId": "string",
          "Type": "string",
          "UserName": "string"
         }
        },
        "Status": "string"
       },
       "AwsIamGroup": {
        "AttachedManagedPolicies": [{
         "PolicyArn": "string",
         "PolicyName": "string"
        }],
        "CreateDate": "string",
        "GroupId": "string",
        "GroupName": "string",
        "GroupPolicyList": [{
         "PolicyName": "string"
        }],
        "Path": "string"
       },
```

```
      "AwsIamPolicy": {
       "AttachmentCount": number,
       "CreateDate": "string",
       "DefaultVersionId": "string",
       "Description": "string",
       "IsAttachable": boolean,
       "Path": "string",
       "PermissionsBoundaryUsageCount": number,
       "PolicyId": "string",
       "PolicyName": "string",
       "PolicyVersionList": [{
        "CreateDate": "string",
        "IsDefaultVersion": boolean,
        "VersionId": "string"
       }],
       "UpdateDate": "string"
      },
      "AwsIamRole": {
       "AssumeRolePolicyDocument": "string",
       "AttachedManagedPolicies": [{
        "PolicyArn": "string",
        "PolicyName": "string"
       }],
       "CreateDate": "string",
       "InstanceProfileList": [{
        "Arn": "string",
        "CreateDate": "string",
        "InstanceProfileId": "string",
        "InstanceProfileName": "string",
        "Path": "string",
        "Roles": [{
         "Arn": "string",
         "AssumeRolePolicyDocument": "string",
         "CreateDate": "string",
         "Path": "string",
         "RoleId": "string",
         "RoleName": "string"
        }]
       }],
       "MaxSessionDuration": number,
       "Path": "string",
       "PermissionsBoundary": {
        "PermissionsBoundaryArn": "string",
        "PermissionsBoundaryType": "string"
```

```
        },
        "RoleId": "string",
        "RoleName": "string",
        "RolePolicyList": [{
         "PolicyName": "string"
        }]
       },
       "AwsIamUser": {
        "AttachedManagedPolicies": [{
         "PolicyArn": "string",
         "PolicyName": "string"
        }],
        "CreateDate": "string",
        "GroupList": ["string"],
        "Path": "string",
        "PermissionsBoundary": {
         "PermissionsBoundaryArn": "string",
         "PermissionsBoundaryType": "string"
        },
        "UserId": "string",
        "UserName": "string",
        "UserPolicyList": [{
         "PolicyName": "string"
        }]
       },
       "AwsKinesisStream": {
        "Arn": "string",
        "Name": "string",
        "RetentionPeriodHours": number,
        "ShardCount": number,
        "StreamEncryption": {
         "EncryptionType": "string",
         "KeyId": "string"
        }
       },
       "AwsKmsKey": {
        "AWSAccountId": "string",
        "CreationDate": "string",
        "Description": "string",
        "KeyId": "string",
        "KeyManager": "string",
        "KeyRotationStatus": boolean,
        "KeyState": "string",
        "Origin": "string"
```

```
      },
      "AwsLambdaFunction": {
       "Architectures": [
        "string"
       ],
       "Code": {
        "S3Bucket": "string",
        "S3Key": "string",
        "S3ObjectVersion": "string",
        "ZipFile": "string"
       },
       "CodeSha256": "string",
       "DeadLetterConfig": {
        "TargetArn": "string"
       },
       "Environment": {
        "Variables": {
         "Stage": "string"
        },
        "Error": {
         "ErrorCode": "string",
         "Message": "string"
        }
       },
       "FunctionName": "string",
       "Handler": "string",
       "KmsKeyArn": "string",
       "LastModified": "string",
       "Layers": {
        "Arn": "string",
        "CodeSize": number
       },
       "PackageType": "string",
       "RevisionId": "string",
       "Role": "string",
       "Runtime": "string",
       "Timeout": integer,
       "TracingConfig": {
        "Mode": "string"
       },
       "Version": "string",
       "VpcConfig": {
        "SecurityGroupIds": ["string"],
        "SubnetIds": ["string"]
```

```
        },
        "MasterArn": "string",
        "MemorySize": number
       },
       "AwsLambdaLayerVersion": {
        "CompatibleRuntimes": [
         "string"
        ],
        "CreatedDate": "string",
        "Version": number
       },
       "AwsMskCluster": {
        "ClusterInfo": {
         "ClientAuthentication": {
          "Sasl": {
           "Scram": {
            "Enabled": boolean
           },
           "Iam": {
            "Enabled": boolean
           }
          },
          "Tls": {
           "CertificateAuthorityArnList": [],
           "Enabled": boolean
          },
          "Unauthenticated": {
           "Enabled": boolean
          }
         },
         "ClusterName": "string",
         "CurrentVersion": "string",
         "EncryptionInfo": {
          "EncryptionAtRest": {
           "DataVolumeKMSKeyId": "string"
          },
          "EncryptionInTransit": {
           "ClientBroker": "string",
           "InCluster": boolean
          }
         },
         "EnhancedMonitoring": "string",
         "NumberOfBrokerNodes": integer
        }
```

```
      },
      "AwsNetworkFirewallFirewall": {
       "DeleteProtection": boolean,
       "Description": "string",
       "FirewallArn": "string",
       "FirewallId": "string",
       "FirewallName": "string",
       "FirewallPolicyArn": "string",
       "FirewallPolicyChangeProtection": boolean,
       "SubnetChangeProtection": boolean,
       "SubnetMappings": [{
        "SubnetId": "string"
       }],
       "VpcId": "string"
      },
      "AwsNetworkFirewallFirewallPolicy": {
       "Description": "string",
       "FirewallPolicy": {
        "StatefulRuleGroupReferences": [{
         "ResourceArn": "string"
        }],
        "StatelessCustomActions": [{
         "ActionDefinition": {
          "PublishMetricAction": {
           "Dimensions": [{
            "Value": "string"
           }]
          }
         },
         "ActionName": "string"
        }],
        "StatelessDefaultActions": ["string"],
        "StatelessFragmentDefaultActions": ["string"],
        "StatelessRuleGroupReferences": [{
         "Priority": number,
         "ResourceArn": "string"
        }]
       },
       "FirewallPolicyArn": "string",
       "FirewallPolicyId": "string",
       "FirewallPolicyName": "string"
      },
      "AwsNetworkFirewallRuleGroup": {
       "Capacity": number,
```

```
        "Description": "string",
        "RuleGroup": {
         "RulesSource": {
          "RulesSourceList": {
           "GeneratedRulesType": "string",
           "Targets": ["string"],
           "TargetTypes": ["string"]
          },
          "RulesString": "string",
          "StatefulRules": [{
           "Action": "string",
           "Header": {
            "Destination": "string",
            "DestinationPort": "string",
            "Direction": "string",
            "Protocol": "string",
            "Source": "string",
            "SourcePort": "string"
           },
           "RuleOptions": [{
            "Keyword": "string",
            "Settings": ["string"]
           }]
          }],
          "StatelessRulesAndCustomActions": {
           "CustomActions": [{
            "ActionDefinition": {
             "PublishMetricAction": {
              "Dimensions": [{
               "Value": "string"
              }]
             }
            },
            "ActionName": "string"
           }],
           "StatelessRules": [{
            "Priority": number,
            "RuleDefinition": {
             "Actions": ["string"],
             "MatchAttributes": {
              "DestinationPorts": [{
               "FromPort": number,
               "ToPort": number
              }],
```

```
            "Destinations": [{
             "AddressDefinition": "string"
            }],
            "Protocols": [number],
            "SourcePorts": [{
             "FromPort": number,
             "ToPort": number
            }],
            "Sources": [{
             "AddressDefinition": "string"
            }],
            "TcpFlags": [{
             "Flags": ["string"],
             "Masks": ["string"]
            }]
           }
          }
         }]
        }
       },
       "RuleVariables": {
        "IpSets": {
         "Definition": ["string"]
        },
        "PortSets": {
         "Definition": ["string"]
        }
       }
      },
      "RuleGroupArn": "string",
      "RuleGroupId": "string",
      "RuleGroupName": "string",
      "Type": "string"
     },
     "AwsOpenSearchServiceDomain": {
      "AccessPolicies": "string",
      "AdvancedSecurityOptions": {
       "Enabled": boolean,
       "InternalUserDatabaseEnabled": boolean,
       "MasterUserOptions": {
        "MasterUserArn": "string",
        "MasterUserName": "string",
        "MasterUserPassword": "string"
       }
```

```
        },
        "Arn": "string",
        "ClusterConfig": {
         "DedicatedMasterCount": number,
         "DedicatedMasterEnabled": boolean,
         "DedicatedMasterType": "string",
         "InstanceCount": number,
         "InstanceType": "string",
         "WarmCount": number,
         "WarmEnabled": boolean,
         "WarmType": "string",
         "ZoneAwarenessConfig": {
          "AvailabilityZoneCount": number
         },
         "ZoneAwarenessEnabled": boolean
        },
        "DomainEndpoint": "string",
        "DomainEndpointOptions": {
         "CustomEndpoint": "string",
         "CustomEndpointCertificateArn": "string",
         "CustomEndpointEnabled": boolean,
         "EnforceHTTPS": boolean,
         "TLSSecurityPolicy": "string"
        },
        "DomainEndpoints": {
         "string": "string"
        },
        "DomainName": "string",
        "EncryptionAtRestOptions": {
         "Enabled": boolean,
         "KmsKeyId": "string"
        },
        "EngineVersion": "string",
        "Id": "string",
        "LogPublishingOptions": {
         "AuditLogs": {
          "CloudWatchLogsLogGroupArn": "string",
          "Enabled": boolean
         },
         "IndexSlowLogs": {
          "CloudWatchLogsLogGroupArn": "string",
          "Enabled": boolean
         },
         "SearchSlowLogs": {
```

```
          "CloudWatchLogsLogGroupArn": "string",
          "Enabled": boolean
         }
        },
        "NodeToNodeEncryptionOptions": {
         "Enabled": boolean
        },
        "ServiceSoftwareOptions": {
         "AutomatedUpdateDate": "string",
         "Cancellable": boolean,
         "CurrentVersion": "string",
         "Description": "string",
         "NewVersion": "string",
         "OptionalDeployment": boolean,
         "UpdateAvailable": boolean,
         "UpdateStatus": "string"
        },
        "VpcOptions": {
         "SecurityGroupIds": ["string"],
         "SubnetIds": ["string"]
        }
       },
       "AwsRdsDbCluster": {
        "ActivityStreamStatus": "string",
        "AllocatedStorage": number,
        "AssociatedRoles": [{
         "RoleArn": "string",
         "Status": "string"
        }],
        "AutoMinorVersionUpgrade": boolean,
        "AvailabilityZones": ["string"],
        "BackupRetentionPeriod": integer,
        "ClusterCreateTime": "string",
        "CopyTagsToSnapshot": boolean,
        "CrossAccountClone": boolean,
        "CustomEndpoints": ["string"],
        "DatabaseName": "string",
        "DbClusterIdentifier": "string",
        "DbClusterMembers": [{
         "DbClusterParameterGroupStatus": "string",
         "DbInstanceIdentifier": "string",
         "IsClusterWriter": boolean,
         "PromotionTier": integer
        }],
```

```
        "DbClusterOptionGroupMemberships": [{
         "DbClusterOptionGroupName": "string",
         "Status": "string"
        }],
        "DbClusterParameterGroup": "string",
        "DbClusterResourceId": "string",
        "DbSubnetGroup": "string",
        "DeletionProtection": boolean,
        "DomainMemberships": [{
         "Domain": "string",
         "Fqdn": "string",
         "IamRoleName": "string",
         "Status": "string"
        }],
        "EnabledCloudwatchLogsExports": ["string"],
        "Endpoint": "string",
        "Engine": "string",
        "EngineMode": "string",
        "EngineVersion": "string",
        "HostedZoneId": "string",
        "HttpEndpointEnabled": boolean,
        "IamDatabaseAuthenticationEnabled": boolean,
        "KmsKeyId": "string",
        "MasterUsername": "string",
        "MultiAz": boolean,
        "Port": integer,
        "PreferredBackupWindow": "string",
        "PreferredMaintenanceWindow": "string",
        "ReaderEndpoint": "string",
        "ReadReplicaIdentifiers": ["string"],
        "Status": "string",
        "StorageEncrypted": boolean,
        "VpcSecurityGroups": [{
         "Status": "string",
         "VpcSecurityGroupId": "string"
        }]
       },
       "AwsRdsDbClusterSnapshot": {
        "AllocatedStorage": integer,
        "AvailabilityZones": ["string"],
        "ClusterCreateTime": "string",
        "DbClusterIdentifier": "string",
        "DbClusterSnapshotAttributes": [{
         "AttributeName": "string",
```

```
        "AttributeValues": ["string"]
       }],
       "DbClusterSnapshotIdentifier": "string",
       "Engine": "string",
       "EngineVersion": "string",
       "IamDatabaseAuthenticationEnabled": boolean,
       "KmsKeyId": "string",
       "LicenseModel": "string",
       "MasterUsername": "string",
       "PercentProgress": integer,
       "Port": integer,
       "SnapshotCreateTime": "string",
       "SnapshotType": "string",
       "Status": "string",
       "StorageEncrypted": boolean,
       "VpcId": "string"
      },
      "AwsRdsDbInstance": {
       "AllocatedStorage": number,
       "AssociatedRoles": [{
        "RoleArn": "string",
        "FeatureName": "string",
        "Status": "string"
       }],
       "AutoMinorVersionUpgrade": boolean,
       "AvailabilityZone": "string",
       "BackupRetentionPeriod": number,
       "CACertificateIdentifier": "string",
       "CharacterSetName": "string",
       "CopyTagsToSnapshot": boolean,
       "DBClusterIdentifier": "string",
       "DBInstanceClass": "string",
       "DBInstanceIdentifier": "string",
       "DbInstancePort": number,
       "DbInstanceStatus": "string",
       "DbiResourceId": "string",
       "DBName": "string",
       "DbParameterGroups": [{
        "DbParameterGroupName": "string",
        "ParameterApplyStatus": "string"
       }],
       "DbSecurityGroups": ["string"],
       "DbSubnetGroup": {
        "DbSubnetGroupArn": "string",
```

```
        "DbSubnetGroupDescription": "string",
        "DbSubnetGroupName": "string",
        "SubnetGroupStatus": "string",
        "Subnets": [{
         "SubnetAvailabilityZone": {
          "Name": "string"
         },
         "SubnetIdentifier": "string",
         "SubnetStatus": "string"
        }],
        "VpcId": "string"
       },
       "DeletionProtection": boolean,
       "Endpoint": {
        "Address": "string",
        "Port": number,
        "HostedZoneId": "string"
       },
       "DomainMemberships": [{
        "Domain": "string",
        "Fqdn": "string",
        "IamRoleName": "string",
        "Status": "string"
       }],
       "EnabledCloudwatchLogsExports": ["string"],
       "Engine": "string",
       "EngineVersion": "string",
       "EnhancedMonitoringResourceArn": "string",
       "IAMDatabaseAuthenticationEnabled": boolean,
       "InstanceCreateTime": "string",
       "Iops": number,
       "KmsKeyId": "string",
       "LatestRestorableTime": "string",
       "LicenseModel": "string",
       "ListenerEndpoint": {
        "Address": "string",
        "HostedZoneId": "string",
        "Port": number
       },
       "MasterUsername": "admin",
       "MaxAllocatedStorage": number,
       "MonitoringInterval": number,
       "MonitoringRoleArn": "string",
       "MultiAz": boolean,
```

```
        "OptionGroupMemberships": [{
         "OptionGroupName": "string",
         "Status": "string"
        }],
        "PendingModifiedValues": {
         "AllocatedStorage": number,
         "BackupRetentionPeriod": number,
         "CaCertificateIdentifier": "string",
         "DbInstanceClass": "string",
         "DbInstanceIdentifier": "string",
         "DbSubnetGroupName": "string",
         "EngineVersion": "string",
         "Iops": number,
         "LicenseModel": "string",
         "MasterUserPassword": "string",
         "MultiAZ": boolean,
         "PendingCloudWatchLogsExports": {
          "LogTypesToDisable": ["string"],
          "LogTypesToEnable": ["string"]
         },
         "Port": number,
         "ProcessorFeatures": [{
          "Name": "string",
          "Value": "string"
         }],
         "StorageType": "string"
        },
        "PerformanceInsightsEnabled": boolean,
        "PerformanceInsightsKmsKeyId": "string",
        "PerformanceInsightsRetentionPeriod": number,
        "PreferredBackupWindow": "string",
        "PreferredMaintenanceWindow": "string",
        "ProcessorFeatures": [{
         "Name": "string",
         "Value": "string"
        }],
        "PromotionTier": number,
        "PubliclyAccessible": boolean,
        "ReadReplicaDBClusterIdentifiers": ["string"],
        "ReadReplicaDBInstanceIdentifiers": ["string"],
        "ReadReplicaSourceDBInstanceIdentifier": "string",
        "SecondaryAvailabilityZone": "string",
        "StatusInfos": [{
         "Message": "string",
```

```
        "Normal": boolean,
        "Status": "string",
        "StatusType": "string"
       }],
       "StorageEncrypted": boolean,
       "TdeCredentialArn": "string",
       "Timezone": "string",
       "VpcSecurityGroups": [{
        "VpcSecurityGroupId": "string",
        "Status": "string"
       }]
      },
      "AwsRdsDbSecurityGroup": {
       "DbSecurityGroupArn": "string",
       "DbSecurityGroupDescription": "string",
       "DbSecurityGroupName": "string",
       "Ec2SecurityGroups": [{
        "Ec2SecurityGroupuId": "string",
        "Ec2SecurityGroupName": "string",
        "Ec2SecurityGroupOwnerId": "string",
        "Status": "string"
       }],
       "IpRanges": [{
        "CidrIp": "string",
        "Status": "string"
       }],
       "OwnerId": "string",
       "VpcId": "string"
      },
      "AwsRdsDbSnapshot": {
       "AllocatedStorage": integer,
       "AvailabilityZone": "string",
       "DbInstanceIdentifier": "string",
       "DbiResourceId": "string",
       "DbSnapshotIdentifier": "string",
       "Encrypted": boolean,
       "Engine": "string",
       "EngineVersion": "string",
       "IamDatabaseAuthenticationEnabled": boolean,
       "InstanceCreateTime": "string",
       "Iops": number,
       "KmsKeyId": "string",
       "LicenseModel": "string",
       "MasterUsername": "string",
```

```
        "OptionGroupName": "string",
        "PercentProgress": integer,
        "Port": integer,
        "ProcessorFeatures": [],
        "SnapshotCreateTime": "string",
        "SnapshotType": "string",
        "SourceDbSnapshotIdentifier": "string",
        "SourceRegion": "string",
        "Status": "string",
        "StorageType": "string",
        "TdeCredentialArn": "string",
        "Timezone": "string",
        "VpcId": "string"
      },
      "AwsRdsEventSubscription": {
        "CustomerAwsId": "string",
        "CustSubscriptionId": "string",
        "Enabled": boolean,
        "EventCategoriesList": ["string"],
        "EventSubscriptionArn": "string",
        "SnsTopicArn": "string",
        "SourceIdsList": ["string"],
        "SourceType": "string",
        "Status": "string",
        "SubscriptionCreationTime": "string"
      },
      "AwsRedshiftCluster": {
        "AllowVersionUpgrade": boolean,
        "AutomatedSnapshotRetentionPeriod": number,
        "AvailabilityZone": "string",
        "ClusterAvailabilityStatus": "string",
        "ClusterCreateTime": "string",
        "ClusterIdentifier": "string",
        "ClusterNodes": [{
          "NodeRole": "string",
          "PrivateIPAddress": "string",
          "PublicIPAddress": "string"
        }],
        "ClusterParameterGroups": [{
          "ClusterParameterStatusList": [{
            "ParameterApplyErrorDescription": "string",
            "ParameterApplyStatus": "string",
            "ParameterName": "string"
          }],
```

```
        "ParameterApplyStatus": "string",
        "ParameterGroupName": "string"
      }],
      "ClusterPublicKey": "string",
      "ClusterRevisionNumber": "string",
      "ClusterSecurityGroups": [{
        "ClusterSecurityGroupName": "string",
        "Status": "string"
      }],
      "ClusterSnapshotCopyStatus": {
        "DestinationRegion": "string",
        "ManualSnapshotRetentionPeriod": number,
        "RetentionPeriod": number,
        "SnapshotCopyGrantName": "string"
      },
      "ClusterStatus": "string",
      "ClusterSubnetGroupName": "string",
      "ClusterVersion": "string",
      "DBName": "string",
      "DeferredMaintenanceWindows": [{
        "DeferMaintenanceEndTime": "string",
        "DeferMaintenanceIdentifier": "string",
        "DeferMaintenanceStartTime": "string"
      }],
      "ElasticIpStatus": {
        "ElasticIp": "string",
        "Status": "string"
      },
      "ElasticResizeNumberOfNodeOptions": "string",
      "Encrypted": boolean,
      "Endpoint": {
        "Address": "string",
        "Port": number
      },
      "EnhancedVpcRouting": boolean,
      "ExpectedNextSnapshotScheduleTime": "string",
      "ExpectedNextSnapshotScheduleTimeStatus": "string",
      "HsmStatus": {
        "HsmClientCertificateIdentifier": "string",
        "HsmConfigurationIdentifier": "string",
        "Status": "string"
      },
      "IamRoles": [{
        "ApplyStatus": "string",
```

```
         "IamRoleArn": "string"
        }],
        "KmsKeyId": "string",
        "LoggingStatus":{
                    "BucketName": "string",
                    "LastFailureMessage": "string",
                    "LastFailureTime": "string",
                    "LastSuccessfulDeliveryTime": "string",
                    "LoggingEnabled": boolean,
                    "S3KeyPrefix": "string"
                },
        "MaintenanceTrackName": "string",
        "ManualSnapshotRetentionPeriod": number,
        "MasterUsername": "string",
        "NextMaintenanceWindowStartTime": "string",
        "NodeType": "string",
        "NumberOfNodes": number,
        "PendingActions": ["string"],
        "PendingModifiedValues": {
         "AutomatedSnapshotRetentionPeriod": number,
         "ClusterIdentifier": "string",
         "ClusterType": "string",
         "ClusterVersion": "string",
         "EncryptionType": "string",
         "EnhancedVpcRouting": boolean,
         "MaintenanceTrackName": "string",
         "MasterUserPassword": "string",
         "NodeType": "string",
         "NumberOfNodes": number,
         "PubliclyAccessible": "string"
        },
        "PreferredMaintenanceWindow": "string",
        "PubliclyAccessible": boolean,
        "ResizeInfo": {
         "AllowCancelResize": boolean,
         "ResizeType": "string"
        },
        "RestoreStatus": {
         "CurrentRestoreRateInMegaBytesPerSecond": number,
         "ElapsedTimeInSeconds": number,
         "EstimatedTimeToCompletionInSeconds": number,
         "ProgressInMegaBytes": number,
         "SnapshotSizeInMegaBytes": number,
         "Status": "string"
```

```
        },
        "SnapshotScheduleIdentifier": "string",
        "SnapshotScheduleState": "string",
        "VpcId": "string",
        "VpcSecurityGroups": [{
         "Status": "string",
         "VpcSecurityGroupId": "string"
        }]
       },
       "AwsRoute53HostedZone": {
        "HostedZone": {
         "Id": "string",
         "Name": "string",
         "Config": {
          "Comment": "string"
         }
        },
        "NameServers": ["string"],
        "QueryLoggingConfig": {
         "CloudWatchLogsLogGroupArn": {
          "CloudWatchLogsLogGroupArn": "string",
          "Id": "string",
          "HostedZoneId": "string"
         }
        },
        "Vpcs": [
         {
          "Id": "string",
          "Region": "string"
         }
        ]
       },
       "AwsS3AccessPoint": {
        "AccessPointArn": "string",
        "Alias": "string",
        "Bucket": "string",
        "BucketAccountId": "string",
        "Name": "string",
        "NetworkOrigin": "string",
        "PublicAccessBlockConfiguration": {
         "BlockPublicAcls": boolean,
         "BlockPublicPolicy": boolean,
         "IgnorePublicAcls": boolean,
         "RestrictPublicBuckets": boolean
```

```
        },
        "VpcConfiguration": {
         "VpcId": "string"
        }
       },
       "AwsS3AccountPublicAccessBlock": {
        "BlockPublicAcls": boolean,
        "BlockPublicPolicy": boolean,
        "IgnorePublicAcls": boolean,
        "RestrictPublicBuckets": boolean
       },
       "AwsS3Bucket": {
        "AccessControlList": "string",
        "BucketLifecycleConfiguration": {
         "Rules": [{
          "AbortIncompleteMultipartUpload": {
           "DaysAfterInitiation": number
          },
          "ExpirationDate": "string",
          "ExpirationInDays": number,
          "ExpiredObjectDeleteMarker": boolean,
          "Filter": {
           "Predicate": {
            "Operands": [{
              "Prefix": "string",
              "Type": "string"
             },
             {
              "Tag": {
               "Key": "string",
               "Value": "string"
              },
              "Type": "string"
             }
            ],
            "Type": "string"
           }
          },
          "Id": "string",
          "NoncurrentVersionExpirationInDays": number,
          "NoncurrentVersionTransitions": [{
           "Days": number,
           "StorageClass": "string"
          }],
```

```
          "Prefix": "string",
          "Status": "string",
          "Transitions": [{
           "Date": "string",
           "Days": number,
           "StorageClass": "string"
          }]
         }]
        },
        "BucketLoggingConfiguration": {
         "DestinationBucketName": "string",
         "LogFilePrefix": "string"
        },
        "BucketName": "string",
        "BucketNotificationConfiguration": {
         "Configurations": [{
          "Destination": "string",
          "Events": ["string"],
          "Filter": {
           "S3KeyFilter": {
            "FilterRules": [{
             "Name": "string",
             "Value": "string"
            }]
           }
          },
          "Type": "string"
         }]
        },
        "BucketVersioningConfiguration": {
         "IsMfaDeleteEnabled": boolean,
         "Status": "string"
        },
        "BucketWebsiteConfiguration": {
         "ErrorDocument": "string",
         "IndexDocumentSuffix": "string",
         "RedirectAllRequestsTo": {
          "HostName": "string",
          "Protocol": "string"
         },
         "RoutingRules": [{
          "Condition": {
           "HttpErrorCodeReturnedEquals": "string",
           "KeyPrefixEquals": "string"
```

```
          },
          "Redirect": {
           "HostName": "string",
           "HttpRedirectCode": "string",
           "Protocol": "string",
           "ReplaceKeyPrefixWith": "string",
           "ReplaceKeyWith": "string"
          }
         }]
        },
        "CreatedAt": "string",
        "ObjectLockConfiguration": {
         "ObjectLockEnabled": "string",
         "Rule": {
          "DefaultRetention": {
           "Days": integer,
           "Mode": "string",
           "Years": integer
          }
         }
        },
        "OwnerAccountId": "string",
        "OwnerId": "string",
        "OwnerName": "string",
        "PublicAccessBlockConfiguration": {
         "BlockPublicAcls": boolean,
         "BlockPublicPolicy": boolean,
         "IgnorePublicAcls": boolean,
         "RestrictPublicBuckets": boolean
        },
        "ServerSideEncryptionConfiguration": {
         "Rules": [{
          "ApplyServerSideEncryptionByDefault": {
           "KMSMasterKeyID": "string",
           "SSEAlgorithm": "string"
          }
         }]
        }
       },
       "AwsS3Object": {
        "ContentType": "string",
        "ETag": "string",
        "LastModified": "string",
        "ServerSideEncryption": "string",
```

```
        "SSEKMSKeyId": "string",
        "VersionId": "string"
      },
      "AwsSagemakerNotebookInstance": {
        "DirectInternetAccess": "string",
        "InstanceMetadataServiceConfiguration": {
          "MinimumInstanceMetadataServiceVersion": "string"
        },
        "InstanceType": "string",
        "LastModifiedTime": "string",
        "NetworkInterfaceId": "string",
        "NotebookInstanceArn": "string",
        "NotebookInstanceName": "string",
        "NotebookInstanceStatus": "string",
        "PlatformIdentifier": "string",
        "RoleArn": "string",
        "RootAccess": "string",
        "SecurityGroups": ["string"],
        "SubnetId": "string",
        "Url": "string",
        "VolumeSizeInGB": number
      },
      "AwsSecretsManagerSecret": {
        "Deleted": boolean,
        "Description": "string",
        "KmsKeyId": "string",
        "Name": "string",
        "RotationEnabled": boolean,
        "RotationLambdaArn": "string",
        "RotationOccurredWithinFrequency": boolean,
        "RotationRules": {
          "AutomaticallyAfterDays": integer
        }
      },
      "AwsSnsTopic": {
        "ApplicationSuccessFeedbackRoleArn": "string",
        "FirehoseFailureFeedbackRoleArn": "string",
        "FirehoseSuccessFeedbackRoleArn": "string",
        "HttpFailureFeedbackRoleArn": "string",
        "HttpSuccessFeedbackRoleArn": "string",
        "KmsMasterKeyId": "string",
        "Owner": "string",
        "SqsFailureFeedbackRoleArn": "string",
        "SqsSuccessFeedbackRoleArn": "string",
```

```
        "Subscription": {
         "Endpoint": "string",
         "Protocol": "string"
        },
        "TopicName": "string"
       },
       "AwsSqsQueue": {
        "DeadLetterTargetArn": "string",
        "KmsDataKeyReusePeriodSeconds": number,
        "KmsMasterKeyId": "string",
        "QueueName": "string"
       },
       "AwsSsmPatchCompliance": {
        "Patch": {
         "ComplianceSummary": {
          "ComplianceType": "string",
          "CompliantCriticalCount": integer,
          "CompliantHighCount": integer,
          "CompliantInformationalCount": integer,
          "CompliantLowCount": integer,
          "CompliantMediumCount": integer,
          "CompliantUnspecifiedCount": integer,
          "ExecutionType": "string",
          "NonCompliantCriticalCount": integer,
          "NonCompliantHighCount": integer,
          "NonCompliantInformationalCount": integer,
          "NonCompliantLowCount": integer,
          "NonCompliantMediumCount": integer,
          "NonCompliantUnspecifiedCount": integer,
          "OverallSeverity": "string",
          "PatchBaselineId": "string",
          "PatchGroup": "string",
          "Status": "string"
         }
        }
       },
       "AwsStepFunctionStateMachine": {
        "StateMachineArn": "string",
        "Name": "string",
        "Status": "string",
        "RoleArn": "string",
        "Type": "string",
        "LoggingConfiguration": {
         "Level": "string",
```

```
        "IncludeExecutionData": boolean
       },
       "TracingConfiguration": {
        "Enabled": boolean
       }
      },
      "AwsWafRateBasedRule": {
       "MatchPredicates": [{
        "DataId": "string",
        "Negated": boolean,
        "Type": "string"
       }],
       "MetricName": "string",
       "Name": "string",
       "RateKey": "string",
       "RateLimit": number,
       "RuleId": "string"
      },
      "AwsWafRegionalRateBasedRule": {
       "MatchPredicates": [{
        "DataId": "string",
        "Negated": boolean,
        "Type": "string"
       }],
       "MetricName": "string",
       "Name": "string",
       "RateKey": "string",
       "RateLimit": number,
       "RuleId": "string"
      },
      "AwsWafRegionalRule": {
       "MetricName": "string",
       "Name": "string",
       "RuleId": "string",
       "PredicateList": [{
           "DataId": "string",
           "Negated": boolean,
           "Type": "string"
       }]
      },
      "AwsWafRegionalRuleGroup": {
       "MetricName": "string",
       "Name": "string",
       "RuleGroupId": "string",
```

```
        "Rules": [{
         "Action": {
          "Type": "string"
         },
         "Priority": number,
         "RuleId": "string",
         "Type": "string"
        }]
       },
       "AwsWafRegionalWebAcl": {
        "DefaultAction": "string",
        "MetricName" : "string",
        "Name": "string",
        "RulesList" : [{
         "Action": {
          "Type": "string"
         },
         "Priority": number,
         "RuleId": "string",
         "Type": "string",
         "ExcludedRules": [{
          "ExclusionType": "string",
          "RuleId": "string"
         }],
         "OverrideAction": {
          "Type": "string"
         }
        }],
        "WebAclId": "string"
       },
       "AwsWafRule": {
        "MetricName": "string",
        "Name": "string",
        "PredicateList": [{
         "DataId": "string",
         "Negated": boolean,
         "Type": "string"
        }],
        "RuleId": "string"
       },
       "AwsWafRuleGroup": {
        "MetricName": "string",
        "Name": "string",
        "RuleGroupId": "string",
```

```
        "Rules": [{
         "Action": {
          "Type": "string"
         },
         "Priority": number,
         "RuleId": "string",
         "Type": "string"
        }]
       },
       "AwsWafv2RuleGroup": {
        "Arn": "string",
        "Capacity": number,
        "Description": "string",
        "Id": "string",
        "Name": "string",
        "Rules": [{
         "Action": {
         "Allow": {
          "CustomRequestHandling": {
           "InsertHeaders": [
            {
            "Name": "string",
            "Value": "string"
            },
            {
            "Name": "string",
            "Value": "string"
            }
           ]
          }
         }
         },
         "Name": "string",
         "Priority": number,
         "VisibilityConfig": {
          "CloudWatchMetricsEnabled": boolean,
          "MetricName": "string",
          "SampledRequestsEnabled": boolean
         }
        }],
        "VisibilityConfig": {
         "CloudWatchMetricsEnabled": boolean,
         "MetricName": "string",
         "SampledRequestsEnabled": boolean
```

```
        }
       },
       "AwsWafWebAcl": {
        "DefaultAction": "string",
        "Name": "string",
        "Rules": [{
         "Action": {
          "Type": "string"
         },
         "ExcludedRules": [{
          "RuleId": "string"
         }],
         "OverrideAction": {
          "Type": "string"
         },
         "Priority": number,
         "RuleId": "string",
         "Type": "string"
        }],
        "WebAclId": "string"
       },
       "AwsWafv2WebAcl": {
        "Arn": "string",
        "Capacity": number,
        "CaptchaConfig": {
         "ImmunityTimeProperty": {
          "ImmunityTime": number
         }
        },
        "DefaultAction": {
         "Block": {}
        },
        "Description": "string",
        "ManagedbyFirewallManager": boolean,
        "Name": "string",
        "Rules": [{
         "Action": {
          "RuleAction": {
           "Block": {}
          }
         },
         "Name": "string",
         "Priority": number,
         "VisibilityConfig": {
```

```
          "SampledRequestsEnabled": boolean,
          "CloudWatchMetricsEnabled": boolean,
          "MetricName": "string"
         }
        }],
        "VisibilityConfig": {
         "SampledRequestsEnabled": boolean,
         "CloudWatchMetricsEnabled": boolean,
         "MetricName": "string"
        }
       },
       "AwsXrayEncryptionConfig": {
        "KeyId": "string",
        "Status": "string",
        "Type": "string"
       },
       "Container": {
        "ContainerRuntime": "string",
        "ImageId": "string",
        "ImageName": "string",
        "LaunchedAt": "string",
        "Name": "string",
        "Privileged": boolean,
        "VolumeMounts": [{
         "Name": "string",
         "MountPath": "string"
        }]
       },
       "Other": {
        "string": "string"
       },
       "Id": "string",
       "Partition": "string",
       "Region": "string",
       "ResourceRole": "string",
       "Tags": {
        "string": "string"
       },
       "Type": "string"
      }],
      "SchemaVersion": "string",
      "Severity": {
       "Label": "string",
       "Normalized": number,
```

```
      "Original": "string"
     },
     "Sample": boolean,
     "SourceUrl": "string",
     "Threats": [{
      "FilePaths": [{
       "FileName": "string",
       "FilePath": "string",
       "Hash": "string",
       "ResourceId": "string"
      }],
      "ItemCount": number,
      "Name": "string",
      "Severity": "string"
     }],
     "ThreatIntelIndicators": [{
      "Category": "string",
      "LastObservedAt": "string",
      "Source": "string",
      "SourceUrl": "string",
      "Type": "string",
      "Value": "string"
     }],
     "Title": "string",
     "Types": ["string"],
     "UpdatedAt": "string",
     "UserDefinedFields": {
      "string": "string"
     },
     "VerificationState": "string",
     "Vulnerabilities": [{
      "CodeVulnerabilities": [{
       "Cwes": [
        "string",
        "string"
       ],
       "FilePath": {
        "EndLine": integer,
        "FileName": "string",
        "FilePath": "string",
        "StartLine": integer
       },
       "SourceArn":"string"
      }],
```

```
      "Cvss": [{
       "Adjustments": [{
        "Metric": "string",
        "Reason": "string"
       }],
       "BaseScore": number,
       "BaseVector": "string",
       "Source": "string",
       "Version": "string"
      }],
      "EpssScore": number,
      "ExploitAvailable": "string",
      "FixAvailable": "string",
      "Id": "string",
      "LastKnownExploitAt": "string",
      "ReferenceUrls": ["string"],
      "RelatedVulnerabilities": ["string"],
      "Vendor": {
       "Name": "string",
       "Url": "string",
       "VendorCreatedAt": "string",
       "VendorSeverity": "string",
       "VendorUpdatedAt": "string"
      },
      "VulnerablePackages": [{
       "Architecture": "string",
       "Epoch": "string",
       "FilePath": "string",
       "FixedInVersion": "string",
       "Name": "string",
       "PackageManager": "string",
       "Release": "string",
       "Remediation": "string",
       "SourceLayerArn": "string",
       "SourceLayerHash": "string",
       "Version": "string"
      }]
     }],
     "Workflow": {
      "Status": "string"
     },
     "WorkflowState": "string"
    }
```

```
]
```

Dampak konsolidasi pada bidang dan nilai ASFF

Security Hub menawarkan dua jenis konsolidasi:

- Tampilan kontrol terkonsolidasi (selalu aktif; tidak dapat dimatikan) - Setiap kontrol memiliki pengenal tunggal di seluruh standar. Halaman Kontrol konsol Security Hub menampilkan semua kontrol Anda di seluruh standar.
- Temuan kontrol konsolidasi (dapat diaktifkan atau dinonaktifkan) — Ketika temuan kontrol konsolidasi diaktifkan, Security Hub menghasilkan satu temuan untuk pemeriksaan keamanan bahkan ketika cek dibagikan di beberapa standar. Ini dimaksudkan untuk mengurangi kebisingan temuan. Temuan kontrol konsolidasi diaktifkan untuk Anda secara default jika Anda mengaktifkan Security Hub pada atau setelah 23 Februari 2023. Jika tidak, itu dimatikan secara default. Namun, temuan kontrol konsolidasi diaktifkan di akun anggota Security Hub hanya jika diaktifkan di akun administrator. Jika fitur dimatikan di akun administrator, itu dimatikan di akun anggota. Untuk petunjuk tentang mengaktifkan fitur ini, lihatMengaktifkan temuan kontrol terkonsolidasi.

Kedua fitur membawa perubahan untuk mengontrol bidang pencarian dan nilai diAWS Format Pencarian Keamanan (ASFF). Bagian ini merangkum perubahan tersebut.

Tampilan kontrol konsolidasi - perubahan ASFF

Fitur tampilan kontrol terkonsolidasi memperkenalkan perubahan berikut untuk mengontrol bidang pencarian dan nilai di ASFF.

Jika alur kerja Anda tidak bergantung pada nilai bidang pencarian kontrol ini, tidak diperlukan tindakan.

Jika Anda memiliki alur kerja yang bergantung pada nilai spesifik bidang pencarian kontrol ini, perbarui alur kerja Anda untuk menggunakan nilai saat ini.

Bidang ASFF	Nilai sampel sebelum tampilan kontrol konsolidasi	Nilai sampel setelah tampilan kontrol terkonsolidasi, ditambah deskripsi perubahan
Kepatuhan. SecurityControlId	Tidak berlaku (bidang baru)	EC2.2 Memperkenalkan ID kontrol tunggal di seluruh standar. `ProductFields.RuleId` masih menyediakan ID kontrol berbasis standar untuk kontrol CIS v1.2.0. `ProductFields.ControlId` masih menyediakan ID kontrol berbasis standar untuk kontrol dalam standar lain.
Kepatuhan. AssociatedStandards	Tidak berlaku (bidang baru)	[{” StandardsId “: “standar/ -praktik/ v/1.0.0"aws-foundational-security-best}] Menunjukkan standar mana kontrol diaktifkan.
ProductFields. ArchivalReasons:0/Deskripsi	Tidak berlaku (bidang baru)	“Temuan ini dalam keadaan ARCHIVED karena temuan

Bidang ASFF	Nilai sampel sebelum tampilan kontrol konsolidasi	Nilai sampel setelah tampilan kontrol terkonsolidasi, ditambah deskripsi perubahan
		kontrol konsolidasi telah diaktifkan atau dimatikan. Hal ini menyebabkan temuan di negara bagian sebelumnya diarsipkan ketika temuan baru sedang dihasilkan.” Menjelaskan mengapa Security Hub telah mengarsipkan temuan yang ada.
ProductFields. ArchivalReasons:0/ ReasonCode	Tidak berlaku (bidang baru)	“CONSOLIDATED_CONTROL_FINDINGS_UPDATE” Memberikan alasan mengapa Security Hub telah mengarsipkan temuan yang ada.
ProductFields.RecommendationUrl	https://docs.aws.amazon.com/console/securityhub/PCI.EC2.2/remediation	https://docs.aws.amazon.com/console/securityhub/EC2.2/remediation Bidang ini tidak lagi mereferensikan standar.

Bidang ASFF	Nilai sampel sebelum tampilan kontrol konsolidasi	Nilai sampel setelah tampilan kontrol terkonsolidasi, ditambah deskripsi perubahan
Remediation.Recommendation.Text	“Untuk petunjuk tentang cara memperbaiki masalah ini, lihat dokumenta si AWS Security Hub PCI DSS.”	“Untuk petunjuk tentang cara memperbaiki masalah ini, lihat dokumentasi kontrol AWS Security Hub.” Bidang ini tidak lagi mereferensikan standar.
Remediasi.Rekomendasi.Url	https://docs.aws.a mazon.com/console/ securityhub/PCI.EC 2.2/remediation	https://docs.aws.a mazon.com/console/ securityhub/EC2.2/ remediation Bidang ini tidak lagi mereferensikan standar.

Temuan kontrol konsolidasi - perubahan ASFF

Jika Anda mengaktifkan temuan kontrol konsolidasi, Anda mungkin terpengaruh oleh perubahan berikut untuk mengontrol pencarian bidang dan nilai di ASFF. Perubahan ini merupakan tambahan dari perubahan yang dijelaskan sebelumnya untuk tampilan kontrol konsolidasi.

Jika alur kerja Anda tidak bergantung pada nilai bidang pencarian kontrol ini, tidak diperlukan tindakan.

Jika Anda memiliki alur kerja yang bergantung pada nilai spesifik bidang pencarian kontrol ini, perbarui alur kerja Anda untuk menggunakan nilai saat ini.

> **Note**
>
> Respon Keamanan Otomatis pada AWS v2.0.0 mendukung temuan kontrol terkonsolidasi. Jika Anda menggunakan versi solusi ini, Anda dapat mempertahankan alur kerja saat mengaktifkan temuan kontrol konsolidasi.

Bidang ASFF	Nilai contoh sebelum mengaktif kan temuan kontrol konsolidasi	Contoh nilai setelah mengaktifkan temuan kontrol konsolidasi, dan deskripsi perubahan
GeneratorId	aws-foundational-security-best-Praktik/V/1.0.0/config.1	Kontrol keamanan/config.1 Bidang ini tidak lagi mereferen sikan standar.
Judul	PCI.config.1 harus diaktifkan AWS Config	AWS Config harus diaktifkan Bidang ini tidak lagi mereferen sikan informasi khusus standar.
Id	arn:aws:securityhub: eu-central-1:123456789012: berlangganan / pci-dss/v/3.2.1/pci.iam.5/finding/ ab6d6a26-a156-48f0-9403-1159 83e5a956	arn:aws:securityhub: eu-centra l- 1:123456789012: security-control/iam.9/finding/ab6d6a26-a156-48f0-9403-115983e5a956 Bidang ini tidak lagi mereferen sikan standar.
ProductFields.ControlId	PCI.EC2.2	Dihapus. Lihat `Complianc e.SecurityControlId` sebagai gantinya. Bidang ini dihapus demi ID kontrol agnostik standar tunggal.
ProductFields.RuleId	1.3	Dihapus. Lihat `Complianc e.SecurityControlId` sebagai gantinya.

Bidang ASFF	Nilai contoh sebelum mengaktif kan temuan kontrol konsolidasi	Contoh nilai setelah mengaktifkan temuan kontrol konsolidasi, dan deskripsi perubahan
		Bidang ini dihapus demi ID kontrol agnostik standar tunggal.
Deskripsi	Kontrol PCI DSS ini memeriksa apakah AWS Config diaktifkan di akun dan wilayah saat ini.	AWS Kontrol ini memeriksa apakah AWS Config diaktifkan di akun dan wilayah saat ini. Bidang ini tidak lagi mereferen sikan standar.

Kepelikan	“Keparahan”: {
	
	“Produk”: 90,
	
	“Label”: “KRITIS”,
	
	“Dinormalisasi”: 90,
	
	“Original”: “KRITIS”
	
	}
		“Keparahan”: {
		
		“Label”: “KRITIS”,
		
		“Dinormalisasi”: 90,
		
		“Original”: “KRITIS”
		
		}
		
		Security Hub tidak lagi menggunakan bidang Produk untuk menjelaskan tingkat keparahan temuan.

Tipe	["Pemeriksaan Perangkat Lunak dan Konfigurasi/Standar Industri dan Regulasi/PCI-DSS"]	["Pemeriksaan Perangkat Lunak dan Konfigurasi/Standar Industri dan Peraturan"] Bidang ini tidak lagi mereferen sikan standar.

Bidang ASFF	Nilai contoh sebelum mengaktif kan temuan kontrol konsolidasi	Contoh nilai setelah mengaktifkan temuan kontrol konsolidasi, dan deskripsi perubahan
Kepatuhan. RelatedRe quirements	["PCI DSS 10.5.2", “PCI DSS 11,5", “ AWS Yayasan CIS 2.5"]	["PCI DSS v3.2.1/10.5.2", “PCI DSS v3.2.1/11.5", “Tolok Ukur AWS Yayasan CIS v1.2.0/2.5"] Bidang ini menunjukkan persyarat an terkait di semua standar yang diaktifkan.
CreatedAt	2022-05-05T 08:18:13.138 Z	2022-09-25T 08:18:13.138 Z Format tetap sama, tetapi nilai diatur ulang saat Anda mengaktif kan temuan kontrol konsolidasi.
FirstObservedAt	2022-05-07T 08:18:13.138 Z	2022-09-28T 08:18:13.138 Z Format tetap sama, tetapi nilai diatur ulang saat Anda mengaktif kan temuan kontrol konsolidasi.
ProductFields.Reco mmendationUrl	https://docs.aws.amazon.com /console/securityhub/EC2.2/ remediation	Dihapus. Lihat `Remediati on.Recommendation.Url` sebagai gantinya.
ProductFields.Stan dardsArn	arn:aws:securityhub: ::standar/ - praktik/v/1.0.0 aws-foundational-s ecurity-best	Dihapus. Lihat `Complianc e.AssociatedStandards` sebagai gantinya.
ProductFields.Stan dardsControlArn	arn:aws:securityhub: us-east- 1:123456789012: control/ - praktik/v/1.0.0/config.1 aws-found ational-security-best	Dihapus. Security Hub menghasil kan satu temuan untuk pemeriksa an keamanan di seluruh standar.

Bidang ASFF	Nilai contoh sebelum mengaktif kan temuan kontrol konsolidasi	Contoh nilai setelah mengaktifkan temuan kontrol konsolidasi, dan deskripsi perubahan
ProductFields.Stan dardsGuideArn	arn:aws:securityhub: ::aturan/ /v/1.2.0 cis-aws-foundations-benchmark	Dihapus. Lihat `Complianc e.AssociatedStandards` sebagai gantinya.
ProductFields.Stan dardsGuideSubscrip tionArn	arn:aws:securityhub: us-timur-2:123456789012: berlangga nan//v/1.2.0 cis-aws-foundations-benchmark	Dihapus. Security Hub menghasil kan satu temuan untuk pemeriksa an keamanan di seluruh standar.
ProductFields.Stan dardsSubscriptionArn	arn:aws:securityhub: us-timur-1:123456789012: berlangganan/-praktik/v/1.0.0 aws-foundational-s ecurity-best	Dihapus. Security Hub menghasil kan satu temuan untuk pemeriksa an keamanan di seluruh standar.
ProductFields.aws/ securityhub/ FindingId	arn:aws:securityhub: us-east-1 : :product/aws/securityhub/ar n:aws:securityhub: us-east-1:123456789012: berlangganan/-praktik/v/1.0.0/config.1/findin g/751c2173-7372-4e12-8656-a 5210dfb1d67 aws-foundational-s ecurity-best	arn:aws:securityhub: us-east-1 : :product/aws/securityhub/ar n:aws:securityhub: us-east-1:123456789012: Security-Control/config.1/finding/75 1c2173-7372-4e12-8656-a5210 dfb1d67 Bidang ini tidak lagi mereferen sikan standar.

Nilai untuk bidang ASFF yang disediakan pelanggan setelah mengaktifkan temuan kontrol terkonsolidasi

Jika Anda mengaktifkan temuan kontrol konsolidasi, Security Hub menghasilkan satu temuan di seluruh standar dan mengarsipkan temuan asli (temuan terpisah untuk setiap standar). Untuk melihat temuan yang diarsipkan, Anda dapat mengunjungi halaman Temuan konsol Security Hub dengan filter status Rekam disetel ke ARCHIVED, atau menggunakan tindakan `GetFindings`API. Pembaruan yang Anda buat pada temuan asli di konsol Security Hub atau menggunakan

BatchUpdateFindingsAPI tidak akan disimpan dalam temuan baru (jika diperlukan, Anda dapat memulihkan data ini dengan merujuk pada temuan yang diarsipkan).

Bidang ASFF yang disediakan pelanggan	Deskripsi perubahan setelah mengaktifkan temuan kontrol konsolidasi
Kepercayaan	Reset ke status kosong.
Kekritisan	Reset ke status kosong.
Catatan	Reset ke status kosong.
RelatedFindings	Reset ke status kosong.
Kepelikan	Tingkat keparahan default temuan (cocok dengan tingkat keparahan kontrol).
Tipe	Reset ke nilai agnostik standar.
UserDefinedFields	Reset ke status kosong.
VerificationState	Reset ke status kosong.
Alur kerja	Temuan baru yang gagal memiliki nilai default`NEW`. Temuan baru yang lulus memiliki nilai default`RESOLVED`.

ID generator sebelum dan sesudah mengaktifkan temuan kontrol konsolidasi

Berikut adalah daftar perubahan ID generator untuk kontrol saat Anda mengaktifkan temuan kontrol konsolidasi. Ini berlaku untuk kontrol yang didukung Security Hub per 15 Februari 2023.

GeneratorID sebelum mengaktifkan temuan kontrol terkonsolidasi	GeneratorID setelah mengaktifkan temuan kontrol terkonsolidasi
arn:aws:securityhub: ::aturan/ /v/1.2.0/aturan/1.1 cis-aws-foundations-benchmark	kontrol keamanan/ .1 CloudWatch

GeneratorID sebelum mengaktifkan temuan kontrol terkonsolidasi	GeneratorID setelah mengaktifkan temuan kontrol terkonsolidasi
arn:aws:securityhub: ::aturan/ /v/1.2.0/aturan/1.10 cis-aws-foundations-benchmark	Kontrol keamanan/IAM.16
arn:aws:securityhub: ::aturan/ /v/1.2.0/aturan/1.11 cis-aws-foundations-benchmark	Kontrol keamanan/IAM.17
arn:aws:securityhub: ::aturan/ /v/1.2.0/aturan/1.12 cis-aws-foundations-benchmark	Kontrol keamanan/IAM.4
arn:aws:securityhub: ::aturan/ /v/1.2.0/aturan/1.13 cis-aws-foundations-benchmark	Kontrol keamanan/IAM.9
arn:aws:securityhub: ::aturan/ /v/1.2.0/aturan/1.14 cis-aws-foundations-benchmark	Kontrol keamanan/IAM.6
arn:aws:securityhub: ::aturan/ /v/1.2.0/aturan/1.16 cis-aws-foundations-benchmark	Kontrol keamanan/IAM.2
arn:aws:securityhub: ::aturan/ /v/1.2.0/aturan/1.2 cis-aws-foundations-benchmark	Kontrol keamanan/IAM.5
arn:aws:securityhub: ::aturan/ /v/1.2.0/aturan/1.20 cis-aws-foundations-benchmark	Kontrol keamanan/IAM.18
arn:aws:securityhub: ::aturan/ /v/1.2.0/aturan/1.22 cis-aws-foundations-benchmark	Kontrol keamanan/IAM.1
arn:aws:securityhub: ::aturan/ /v/1.2.0/aturan/1.3 cis-aws-foundations-benchmark	Kontrol keamanan/IAM.8
arn:aws:securityhub: ::aturan/ /v/1.2.0/aturan/1.4 cis-aws-foundations-benchmark	Kontrol keamanan/IAM.3
arn:aws:securityhub: ::aturan/ /v/1.2.0/aturan/1.5 cis-aws-foundations-benchmark	Kontrol keamanan/IAM.11

GeneratorID sebelum mengaktifkan temuan kontrol terkonsolidasi	GeneratorID setelah mengaktifkan temuan kontrol terkonsolidasi
arn:aws:securityhub: ::aturan/ /v/1.2.0/aturan/1.6 cis-aws-foundations-benchmark	Kontrol keamanan/IAM.12
arn:aws:securityhub: ::aturan/ /v/1.2.0/aturan/1.7 cis-aws-foundations-benchmark	Kontrol keamanan/IAM.13
arn:aws:securityhub: ::aturan/ /v/1.2.0/aturan/1.8 cis-aws-foundations-benchmark	Kontrol keamanan/IAM.14
arn:aws:securityhub: ::aturan/ /v/1.2.0/aturan/1.9 cis-aws-foundations-benchmark	Kontrol keamanan/IAM.15
arn:aws:securityhub: ::aturan/ /v/1.2.0/aturan/2.1 cis-aws-foundations-benchmark	kontrol keamanan/ .1 CloudTrail
arn:aws:securityhub: ::aturan/ /v/1.2.0/aturan/2.2 cis-aws-foundations-benchmark	kontrol keamanan/ .4 CloudTrail
arn:aws:securityhub: ::aturan/ /v/1.2.0/aturan/2.3 cis-aws-foundations-benchmark	kontrol keamanan/ .6 CloudTrail
arn:aws:securityhub: ::aturan/ /v/1.2.0/aturan/2.4 cis-aws-foundations-benchmark	kontrol keamanan/ .5 CloudTrail
arn:aws:securityhub: ::aturan/ /v/1.2.0/aturan/2.5 cis-aws-foundations-benchmark	Kontrol keamanan/config.1
arn:aws:securityhub: ::aturan/ /v/1.2.0/aturan/2.6 cis-aws-foundations-benchmark	kontrol keamanan/ .7 CloudTrail
arn:aws:securityhub: ::aturan/ /v/1.2.0/aturan/2.7 cis-aws-foundations-benchmark	kontrol keamanan/ .2 CloudTrail
arn:aws:securityhub: ::aturan/ /v/1.2.0/aturan/2.8 cis-aws-foundations-benchmark	Kontrol keamanan/KMS.4

GeneratorID sebelum mengaktifkan temuan kontrol terkonsolidasi	GeneratorID setelah mengaktifkan temuan kontrol terkonsolidasi
arn:aws:securityhub: ::aturan/ /v/1.2.0/aturan/2.9 cis-aws-foundations-benchmark	Kontrol keamanan/EC2.6
arn:aws:securityhub: ::aturan/ /v/1.2.0/aturan/3.1 cis-aws-foundations-benchmark	kontrol keamanan/ .2 CloudWatch
arn:aws:securityhub: ::aturan/ /v/1.2.0/aturan/3.2 cis-aws-foundations-benchmark	kontrol keamanan/ .3 CloudWatch
arn:aws:securityhub: ::aturan/ /v/1.2.0/aturan/3.3 cis-aws-foundations-benchmark	kontrol keamanan/ .1 CloudWatch
arn:aws:securityhub: ::aturan/ /v/1.2.0/aturan/3.4 cis-aws-foundations-benchmark	kontrol keamanan/ .4 CloudWatch
arn:aws:securityhub: ::aturan/ /v/1.2.0/aturan/3.5 cis-aws-foundations-benchmark	kontrol keamanan/ .5 CloudWatch
arn:aws:securityhub: ::aturan/ /v/1.2.0/aturan/3.6 cis-aws-foundations-benchmark	kontrol keamanan/ .6 CloudWatch
arn:aws:securityhub: ::aturan/ /v/1.2.0/aturan/3.7 cis-aws-foundations-benchmark	kontrol keamanan/ .7 CloudWatch
arn:aws:securityhub: ::aturan/ /v/1.2.0/aturan/3.8 cis-aws-foundations-benchmark	kontrol keamanan/ .8 CloudWatch
arn:aws:securityhub: ::aturan/ /v/1.2.0/aturan/3.9 cis-aws-foundations-benchmark	kontrol keamanan/ .9 CloudWatch
arn:aws:securityhub: ::aturan/ /v/1.2.0/aturan/3.10 cis-aws-foundations-benchmark	kontrol keamanan/ .10 CloudWatch
arn:aws:securityhub: ::aturan/ /v/1.2.0/aturan/3.11 cis-aws-foundations-benchmark	kontrol keamanan/ .11 CloudWatch

GeneratorID sebelum mengaktifkan temuan kontrol terkonsolidasi	GeneratorID setelah mengaktifkan temuan kontrol terkonsolidasi
arn:aws:securityhub: ::aturan/ /v/1.2.0/aturan/3.12 cis-aws-foundations-benchmark	kontrol keamanan/ .12 CloudWatch
arn:aws:securityhub: ::aturan/ /v/1.2.0/aturan/3.13 cis-aws-foundations-benchmark	kontrol keamanan/ .13 CloudWatch
arn:aws:securityhub: ::aturan/ /v/1.2.0/aturan/3.14 cis-aws-foundations-benchmark	kontrol keamanan/ .14 CloudWatch
arn:aws:securityhub: ::aturan/ /v/1.2.0/aturan/4.1 cis-aws-foundations-benchmark	Kontrol keamanan/EC2.13
arn:aws:securityhub: ::aturan/ /v/1.2.0/aturan/4.2 cis-aws-foundations-benchmark	Kontrol keamanan/EC2.14
arn:aws:securityhub: ::aturan/ /v/1.2.0/aturan/4.3 cis-aws-foundations-benchmark	Kontrol keamanan/EC2.2
cis-aws-foundations-benchmark/v/1.4.0/1.10	Kontrol keamanan/IAM.5
cis-aws-foundations-benchmark/v/1.4.0/1.14	Kontrol keamanan/IAM.3
cis-aws-foundations-benchmark/v/1.4.0/1.16	Kontrol keamanan/IAM.1
cis-aws-foundations-benchmark/v/1.4.0/1.17	Kontrol keamanan/IAM.18
cis-aws-foundations-benchmark/v/1.4.0/1.4	Kontrol keamanan/IAM.4
cis-aws-foundations-benchmark/v/1.4.0/1.5	Kontrol keamanan/IAM.9
cis-aws-foundations-benchmark/v/1.4.0/1.6	Kontrol keamanan/IAM.6
cis-aws-foundations-benchmark/v/1.4.0/1.7	kontrol keamanan/ .1 CloudWatch
cis-aws-foundations-benchmark/v/1.4.0/1.8	Kontrol keamanan/IAM.15
cis-aws-foundations-benchmark/v/1.4.0/1.9	Kontrol keamanan/IAM.16

GeneratorID sebelum mengaktifkan temuan kontrol terkonsolidasi	GeneratorID setelah mengaktifkan temuan kontrol terkonsolidasi
cis-aws-foundations-benchmark/v/1.4.0/2.1.2	Kontrol keamanan/S3.5
cis-aws-foundations-benchmark/v/1.4.0/2.1.5.1	Kontrol keamanan/S3.1
cis-aws-foundations-benchmark/v/1.4.0/2.1.5.2	Kontrol keamanan/S3.8
cis-aws-foundations-benchmark/v/1.4.0/2.2.1	Kontrol keamanan/EC2.7
cis-aws-foundations-benchmark/v/1.4.0/2.3.1	Kontrol keamanan/RDS.3
cis-aws-foundations-benchmark/v/1.4.0/3.1	kontrol keamanan/ .1 CloudTrail
cis-aws-foundations-benchmark/v/1.4.0/3.2	kontrol keamanan/ .4 CloudTrail
cis-aws-foundations-benchmark/v/1.4.0/3.4	kontrol keamanan/ .5 CloudTrail
cis-aws-foundations-benchmark/v/1.4.0/3.5	Kontrol keamanan/config.1
cis-aws-foundations-benchmark/v/1.4.0/3.6	Kontrol keamanan/S3.9
cis-aws-foundations-benchmark/v/1.4.0/3.7	kontrol keamanan/ .2 CloudTrail
cis-aws-foundations-benchmark/v/1.4.0/3.8	Kontrol keamanan/KMS.4
cis-aws-foundations-benchmark/v/1.4.0/3.9	Kontrol keamanan/EC2.6
cis-aws-foundations-benchmark/v/1.4.0/4.3	kontrol keamanan/ .1 CloudWatch
cis-aws-foundations-benchmark/v/1.4.0/4.4	kontrol keamanan/ .4 CloudWatch
cis-aws-foundations-benchmark/v/1.4.0/4.5	kontrol keamanan/ .5 CloudWatch
cis-aws-foundations-benchmark/v/1.4.0/4.6	kontrol keamanan/ .6 CloudWatch
cis-aws-foundations-benchmark/v/1.4.0/4.7	kontrol keamanan/ .7 CloudWatch
cis-aws-foundations-benchmark/v/1.4.0/4.8	kontrol keamanan/ .8 CloudWatch
cis-aws-foundations-benchmark/v/1.4.0/4.9	kontrol keamanan/ .9 CloudWatch

GeneratorID sebelum mengaktifkan temuan kontrol terkonsolidasi	GeneratorID setelah mengaktifkan temuan kontrol terkonsolidasi
cis-aws-foundations-benchmark/v/1.4.0/4.10	kontrol keamanan/ .10 CloudWatch
cis-aws-foundations-benchmark/v/1.4.0/4.11	kontrol keamanan/ .11 CloudWatch
cis-aws-foundations-benchmark/v/1.4.0/4.12	kontrol keamanan/ .12 CloudWatch
cis-aws-foundations-benchmark/v/1.4.0/4.13	kontrol keamanan/ .13 CloudWatch
cis-aws-foundations-benchmark/v/1.4.0/4.14	kontrol keamanan/ .14 CloudWatch
cis-aws-foundations-benchmark/v/1.4.0/5.1	Kontrol keamanan/EC2.21
cis-aws-foundations-benchmark/v/1.4.0/5.3	Kontrol keamanan/EC2.2
aws-foundational-security-best-Praktik/V/1.0.0/akunt.1	Kontrol keamanan/akun.1
aws-foundational-security-best-Praktek/V/1.0.0/ACM.1	Kontrol keamanan/ACM.1
aws-foundational-security-best-Praktik/V/1.0.0/apigateway.1	Kontrol keamanan/apigateway.1
aws-foundational-security-best-Praktik/V/1.0.0/apigateway.2	Kontrol keamanan/apigateway.2
aws-foundational-security-best-Praktik/V/1.0.0/apigateway.3	Kontrol keamanan/apigateway.3
aws-foundational-security-best-Praktik/V/1.0.0/apigateway.4	Kontrol keamanan/apigateway.4
aws-foundational-security-best-Praktik/V/1.0.0/apigateway.5	Kontrol keamanan/apigateway.5
aws-foundational-security-best-Praktik/V/1.0.0/apigateway.8	Kontrol keamanan/apigateway.8

GeneratorID sebelum mengaktifkan temuan kontrol terkonsolidasi	GeneratorID setelah mengaktifkan temuan kontrol terkonsolidasi
aws-foundational-security-best-Praktik/V/1.0.0/apigateway.9	Kontrol keamanan/apigateway.9
aws-foundational-security-best-praktik/v/1.0.0/AutoScaling .1	kontrol keamanan/ .1 AutoScaling
aws-foundational-security-best-praktik/v/1.0.0/AutoScaling .2	kontrol keamanan/ .2 AutoScaling
aws-foundational-security-best-praktik/v/1.0.0/AutoScaling .3	kontrol keamanan/ .3 AutoScaling
aws-foundational-security-best-Praktik/V/1.0.0/Autoscaling.5	Kontrol keamanan/penskalan.5
aws-foundational-security-best-praktik/v/1.0.0/AutoScaling .6	kontrol keamanan/ .6 AutoScaling
aws-foundational-security-best-praktik/v/1.0.0/AutoScaling .9	kontrol keamanan/ .9 AutoScaling
aws-foundational-security-best-praktik/v/1.0.0/CloudFront .1	kontrol keamanan/ .1 CloudFront
aws-foundational-security-best-praktik/v/1.0.0/CloudFront .3	kontrol keamanan/ .3 CloudFront
aws-foundational-security-best-praktik/v/1.0.0/CloudFront .4	kontrol keamanan/ .4 CloudFront
aws-foundational-security-best-praktik/v/1.0.0/CloudFront .5	kontrol keamanan/ .5 CloudFront
aws-foundational-security-best-praktik/v/1.0.0/CloudFront .6	kontrol keamanan/ .6 CloudFront

GeneratorID sebelum mengaktifkan temuan kontrol terkonsolidasi	GeneratorID setelah mengaktifkan temuan kontrol terkonsolidasi
aws-foundational-security-best-praktik/v/1.0.0/ CloudFront .7	kontrol keamanan/ .7 CloudFront
aws-foundational-security-best-praktik/v/1.0.0/ CloudFront .8	kontrol keamanan/ .8 CloudFront
aws-foundational-security-best-praktik/v/1.0.0/ CloudFront .9	kontrol keamanan/ .9 CloudFront
aws-foundational-security-best-praktik/v/1.0.0/ CloudFront .10	kontrol keamanan/ .10 CloudFront
aws-foundational-security-best-praktik/v/1.0.0/ CloudFront .12	kontrol keamanan/ .12 CloudFront
aws-foundational-security-best-praktik/v/1.0.0/ CloudTrail .1	kontrol keamanan/ .1 CloudTrail
aws-foundational-security-best-praktik/v/1.0.0/ CloudTrail .2	kontrol keamanan/ .2 CloudTrail
aws-foundational-security-best-praktik/v/1.0.0/ CloudTrail .4	kontrol keamanan/ .4 CloudTrail
aws-foundational-security-best-praktik/v/1.0.0/ CloudTrail .5	kontrol keamanan/ .5 CloudTrail
aws-foundational-security-best-praktik/v/1.0.0/ CodeBuild .1	kontrol keamanan/ .1 CodeBuild
aws-foundational-security-best-praktik/v/1.0.0/ CodeBuild .2	kontrol keamanan/ .2 CodeBuild
aws-foundational-security-best-praktik/v/1.0.0/ CodeBuild .3	kontrol keamanan/ .3 CodeBuild

GeneratorID sebelum mengaktifkan temuan kontrol terkonsolidasi	GeneratorID setelah mengaktifkan temuan kontrol terkonsolidasi
aws-foundational-security-best-praktik/v/1.0.0/ CodeBuild .4	kontrol keamanan/ .4 CodeBuild
aws-foundational-security-best-Praktik/V/1.0.0/ config.1	Kontrol keamanan/config.1
aws-foundational-security-best-Praktik/V/1.0.0/ dms.1	Kontrol keamanan/DMS.1
aws-foundational-security-best-Praktik/V/1.0.0/ DynamoDB.1	Kontrol keamanan/DynamoDB.1
aws-foundational-security-best-Praktik/V/1.0.0/ DynamoDB.2	Kontrol keamanan/Dynamodb.2
aws-foundational-security-best-Praktik/V/1.0.0/ DynamoDB.3	Kontrol keamanan/DynamoDB.3
aws-foundational-security-best-Praktik/V/1.0.0/ EC2.1	Kontrol keamanan/EC2.1
aws-foundational-security-best-Praktik/V/1.0.0/ EC2.3	Kontrol keamanan/EC2.3
aws-foundational-security-best-Praktik/V/1.0.0/ EC2.4	Kontrol keamanan/EC2.4
aws-foundational-security-best-Praktik/V/1.0.0/ EC2.6	Kontrol keamanan/EC2.6
aws-foundational-security-best-Praktik/V/1.0.0/ EC2.7	Kontrol keamanan/EC2.7
aws-foundational-security-best-Praktik/V/1.0.0/ EC2.8	Kontrol keamanan/EC2.8

GeneratorID sebelum mengaktifkan temuan kontrol terkonsolidasi	GeneratorID setelah mengaktifkan temuan kontrol terkonsolidasi
aws-foundational-security-best-Praktik/V/1.0.0/EC2.9	Kontrol keamanan/EC2.9
aws-foundational-security-best-Praktik/V/1.0.0/EC2.10	Kontrol keamanan/EC2.10
aws-foundational-security-best-Praktik/V/1.0.0/EC2.15	Kontrol keamanan/EC2.15
aws-foundational-security-best-Praktik/V/1.0.0/EC2.16	Kontrol keamanan/EC2.16
aws-foundational-security-best-Praktik/V/1.0.0/EC2.17	Kontrol keamanan/EC2.17
aws-foundational-security-best-Praktik/V/1.0.0/EC2.18	Kontrol keamanan/EC2.18
aws-foundational-security-best-Praktik/V/1.0.0/EC2.19	Kontrol keamanan/EC2.19
aws-foundational-security-best-Praktik/V/1.0.0/EC2.2	Kontrol keamanan/EC2.2
aws-foundational-security-best-Praktik/V/1.0.0/EC2.20	Kontrol keamanan/EC2.20
aws-foundational-security-best-Praktik/V/1.0.0/EC2.21	Kontrol keamanan/EC2.21
aws-foundational-security-best-Praktik/V/1.0.0/EC2.23	Kontrol keamanan/EC2.23
aws-foundational-security-best-Praktik/V/1.0.0/EC2.24	Kontrol keamanan/EC2.24

GeneratorID sebelum mengaktifkan temuan kontrol terkonsolidasi	GeneratorID setelah mengaktifkan temuan kontrol terkonsolidasi
aws-foundational-security-best-Praktik/V/1.0.0/EC2.25	Kontrol keamanan/EC2.25
aws-foundational-security-best-Praktik/V/1.0.0/ECR.1	Kontrol keamanan/ECR.1
aws-foundational-security-best-Praktik/V/1.0.0/ECR.2	Kontrol keamanan/ECR.2
aws-foundational-security-best-Praktik/V/1.0.0/ECR.3	Kontrol keamanan/ECR.3
aws-foundational-security-best-Praktik/V/1.0.0/ECS.1	Kontrol keamanan/ECS.1
aws-foundational-security-best-Praktik/V/1.0.0/ECS.10	Kontrol keamanan/ECS.10
aws-foundational-security-best-Praktik/V/1.0.0/ECS.12	Kontrol keamanan/ECS.12
aws-foundational-security-best-Praktik/V/1.0.0/ECS.2	Kontrol keamanan/ECS.2
aws-foundational-security-best-Praktik/V/1.0.0/ECS.3	Kontrol keamanan/ECS.3
aws-foundational-security-best-Praktek/V/1.0.0/ECS.4	Kontrol keamanan/ECS.4
aws-foundational-security-best-Praktik/V/1.0.0/ECS.5	Kontrol keamanan/ECS.5
aws-foundational-security-best-Praktik/V/1.0.0/ECS.8	Kontrol keamanan/ECS.8

GeneratorID sebelum mengaktifkan temuan kontrol terkonsolidasi	GeneratorID setelah mengaktifkan temuan kontrol terkonsolidasi
aws-foundational-security-best-Praktik/V/1.0.0/EFS.1	Kontrol keamanan/EFS.1
aws-foundational-security-best-Praktik/V/1.0.0/EFS.2	Kontrol keamanan/EFS.2
aws-foundational-security-best-Praktik/V/1.0.0/EFS.3	Kontrol keamanan/EFS.3
aws-foundational-security-best-Praktik/V/1.0.0/EFS.4	Kontrol keamanan/EFS.4
aws-foundational-security-best-Praktik/V/1.0.0/EKS.2	Kontrol keamanan/EKS.2
aws-foundational-security-best-praktik/v/1.0.0/ElasticBeanstalk .1	kontrol keamanan/ .1 ElasticBeanstalk
aws-foundational-security-best-praktik/v/1.0.0/ElasticBeanstalk .2	kontrol keamanan/ .2 ElasticBeanstalk
aws-foundational-security-best-Praktik/V/1.0.0/ELBV2.1	Kontrol keamanan/ELB.1
aws-foundational-security-best-Praktik/V/1.0.0/ELB.2	Kontrol keamanan/ELB.2
aws-foundational-security-best-Praktik/V/1.0.0/ELB.3	Kontrol keamanan/ELB.3
aws-foundational-security-best-Praktik/V/1.0.0/ELB.4	Kontrol keamanan/ELB.4
aws-foundational-security-best-Praktik/V/1.0.0/ELB.5	Kontrol keamanan/ELB.5

GeneratorID sebelum mengaktifkan temuan kontrol terkonsolidasi	GeneratorID setelah mengaktifkan temuan kontrol terkonsolidasi
aws-foundational-security-best-Praktik/V/1.0.0/ELB.6	Kontrol keamanan/ELB.6
aws-foundational-security-best-Praktik/V/1.0.0/ELB.7	Kontrol keamanan/ELB.7
aws-foundational-security-best-Praktik/V/1.0.0/ELB.8	Kontrol keamanan/ELB.8
aws-foundational-security-best-Praktik/V/1.0.0/ELB.9	Kontrol keamanan/ELB.9
aws-foundational-security-best-Praktik/V/1.0.0/ELB.10	Kontrol keamanan/ELB.10
aws-foundational-security-best-Praktik/V/1.0.0/ELB.11	Kontrol keamanan/ELB.11
aws-foundational-security-best-Praktik/V/1.0.0/ELB.12	Kontrol keamanan/ELB.12
aws-foundational-security-best-Praktik/V/1.0.0/ELB.13	Kontrol keamanan/ELB.13
aws-foundational-security-best-Praktik/V/1.0.0/ELB.14	Kontrol keamanan/ELB.14
aws-foundational-security-best-Praktik/V/1.0.0/EMR.1	Kontrol keamanan/EMR.1
aws-foundational-security-best-Praktik/V/1.0.0/ES.1	Kontrol keamanan/ES.1
aws-foundational-security-best-Praktik/V/1.0.0/es.2	Kontrol keamanan/ES.2

GeneratorID sebelum mengaktifkan temuan kontrol terkonsolidasi	GeneratorID setelah mengaktifkan temuan kontrol terkonsolidasi
aws-foundational-security-best-Praktik/V/1.0.0/ES.3	Kontrol keamanan/ES.3
aws-foundational-security-best-Praktik/V/1.0.0/es.4	Kontrol keamanan/ES.4
aws-foundational-security-best-Praktik/V/1.0.0/es.5	Kontrol keamanan/ES.5
aws-foundational-security-best-Praktik/V/1.0.0/es.6	Kontrol keamanan/ES.6
aws-foundational-security-best-Praktik/V/1.0.0/es.7	Kontrol keamanan/ES.7
aws-foundational-security-best-Praktik/V/1.0.0/es.8	Kontrol keamanan/ES.8
aws-foundational-security-best-praktik/v/1.0.0/GuardDuty .1	kontrol keamanan/ .1 GuardDuty
aws-foundational-security-best-Praktik/V/1.0.0/IAM.1	Kontrol keamanan/IAM.1
aws-foundational-security-best-Praktik/V/1.0.0/IAM.2	Kontrol keamanan/IAM.2
aws-foundational-security-best-Praktik/V/1.0.0/IAM.21	Kontrol keamanan/IAM.21
aws-foundational-security-best-Praktik/V/1.0.0/IAM.3	Kontrol keamanan/IAM.3
aws-foundational-security-best-Praktik/V/1.0.0/IAM.4	Kontrol keamanan/IAM.4

GeneratorID sebelum mengaktifkan temuan kontrol terkonsolidasi	GeneratorID setelah mengaktifkan temuan kontrol terkonsolidasi
aws-foundational-security-best-Praktik/V/1.0.0/IAM.5	Kontrol keamanan/IAM.5
aws-foundational-security-best-Praktik/V/1.0.0/IAM.6	Kontrol keamanan/IAM.6
aws-foundational-security-best-Praktik/V/1.0.0/IAM.7	Kontrol keamanan/IAM.7
aws-foundational-security-best-Praktik/V/1.0.0/IAM.8	Kontrol keamanan/IAM.8
aws-foundational-security-best-Praktik/V/1.0.0/kinesis.1	Kontrol keamanan/kinesis.1
aws-foundational-security-best-Praktek/V/1.0.0/kms.1	Kontrol keamanan/KMS.1
aws-foundational-security-best-Praktek/V/1.0.0/kms.2	Kontrol keamanan/KMS.2
aws-foundational-security-best-Praktek/V/1.0.0/kms.3	Kontrol keamanan/KMS.3
aws-foundational-security-best-Praktik/V/1.0.0/lambda.1	Kontrol keamanan/Lambda.1
aws-foundational-security-best-Praktik/V/1.0.0/lambda.2	Kontrol keamanan/Lambda.2
aws-foundational-security-best-Praktik/V/1.0.0/lambda.5	Kontrol keamanan/Lambda.5
aws-foundational-security-best-praktik/v/1.0.0/NetworkFirewall .3	kontrol keamanan/ .3 NetworkFirewall

GeneratorID sebelum mengaktifkan temuan kontrol terkonsolidasi	GeneratorID setelah mengaktifkan temuan kontrol terkonsolidasi
aws-foundational-security-best-praktik/v/1.0.0/ NetworkFirewall .4	kontrol keamanan/ .4 NetworkFirewall
aws-foundational-security-best-praktik/v/1.0.0/ NetworkFirewall .5	kontrol keamanan/ .5 NetworkFirewall
aws-foundational-security-best-praktik/v/1.0.0/ NetworkFirewall .6	kontrol keamanan/ .6 NetworkFirewall
aws-foundational-security-best-Praktik/V/1.0.0/ OpenSearch.1	Kontrol keamanan/OpenSearch.1
aws-foundational-security-best-Praktik/V/1.0.0/ OpenSearch.2	Kontrol keamanan/OpenSearch.2
aws-foundational-security-best-Praktik/V/1.0.0/ OpenSearch.3	Kontrol keamanan/OpenSearch.3
aws-foundational-security-best-Praktik/V/1.0.0/ OpenSearch.4	Kontrol keamanan/OpenSearch.4
aws-foundational-security-best-Praktik/V/1.0.0/ OpenSearch.5	Kontrol keamanan/OpenSearch.5
aws-foundational-security-best-Praktik/V/1.0.0/ OpenSearch.6	Kontrol keamanan/OpenSearch.6
aws-foundational-security-best-Praktik/V/1.0.0/ OpenSearch.7	Kontrol keamanan/OpenSearch.7
aws-foundational-security-best-Praktik/V/1.0.0/ OpenSearch.8	Kontrol keamanan/OpenSearch.8
aws-foundational-security-best-Praktik/V/1.0.0/ RDS.1	Kontrol keamanan/RDS.1

GeneratorID sebelum mengaktifkan temuan kontrol terkonsolidasi	GeneratorID setelah mengaktifkan temuan kontrol terkonsolidasi
aws-foundational-security-best-Praktik/V/1.0.0/RDS.10	Kontrol keamanan/RDS.10
aws-foundational-security-best-Praktik/V/1.0.0/RDS.11	Kontrol keamanan/RDS.11
aws-foundational-security-best-Praktik/V/1.0.0/RDS.12	Kontrol keamanan/RDS.12
aws-foundational-security-best-Praktik/V/1.0.0/RDS.13	Kontrol keamanan/RDS.13
aws-foundational-security-best-Praktik/V/1.0.0/RDS.14	Kontrol keamanan/RDS.14
aws-foundational-security-best-Praktik/V/1.0.0/RDS.15	Kontrol keamanan/RDS.15
aws-foundational-security-best-Praktik/V/1.0.0/RDS.16	Kontrol keamanan/RDS.16
aws-foundational-security-best-Praktik/V/1.0.0/RDS.17	Kontrol keamanan/RDS.17
aws-foundational-security-best-Praktik/V/1.0.0/RDS.18	Kontrol keamanan/RDS.18
aws-foundational-security-best-Praktik/V/1.0.0/RDS.19	Kontrol keamanan/RDS.19
aws-foundational-security-best-Praktik/V/1.0.0/RDS.2	Kontrol keamanan/RDS.2
aws-foundational-security-best-Praktik/V/1.0.0/RDS.20	Kontrol keamanan/RDS.20

GeneratorID sebelum mengaktifkan temuan kontrol terkonsolidasi	GeneratorID setelah mengaktifkan temuan kontrol terkonsolidasi
aws-foundational-security-best-Praktik/V/1.0.0/RDS.21	Kontrol keamanan/RDS.21
aws-foundational-security-best-Praktik/V/1.0.0/RDS.22	Kontrol keamanan/RDS.22
aws-foundational-security-best-Praktik/V/1.0.0/RDS.23	Kontrol keamanan/RDS.23
aws-foundational-security-best-Praktik/V/1.0.0/RDS.24	Kontrol keamanan/RDS.24
aws-foundational-security-best-Praktik/V/1.0.0/RDS.25	Kontrol keamanan/RDS.25
aws-foundational-security-best-Praktik/V/1.0.0/RDS.3	Kontrol keamanan/RDS.3
aws-foundational-security-best-Praktik/V/1.0.0/RDS.4	Kontrol keamanan/RDS.4
aws-foundational-security-best-Praktik/V/1.0.0/RDS.5	Kontrol keamanan/RDS.5
aws-foundational-security-best-Praktik/V/1.0.0/RDS.6	Kontrol keamanan/RDS.6
aws-foundational-security-best-Praktik/V/1.0.0/RDS.7	Kontrol keamanan/RDS.7
aws-foundational-security-best-Praktik/V/1.0.0/RDS.8	Kontrol keamanan/RDS.8
aws-foundational-security-best-Praktik/V/1.0.0/RDS.9	Kontrol keamanan/RDS.9

GeneratorID sebelum mengaktifkan temuan kontrol terkonsolidasi	GeneratorID setelah mengaktifkan temuan kontrol terkonsolidasi
aws-foundational-security-best-Praktik/V/1.0.0/Redshift.1	Kontrol keamanan/pergeseran merah.1
aws-foundational-security-best-Praktik/V/1.0.0/Redshift.2	Kontrol keamanan/pergeseran merah.2
aws-foundational-security-best-Praktik/V/1.0.0/Redshift.3	Kontrol keamanan/pergeseran merah.3
aws-foundational-security-best-Praktik/V/1.0.0/Redshift.4	Kontrol keamanan/Redshift.4
aws-foundational-security-best-Praktik/V/1.0.0/Redshift.6	Kontrol keamanan/pergeseran merah.6
aws-foundational-security-best-Praktik/V/1.0.0/Redshift.7	Kontrol keamanan/pergeseran merah.7
aws-foundational-security-best-Praktik/V/1.0.0/Redshift.8	Kontrol keamanan/pergeseran merah.8
aws-foundational-security-best-Praktik/V/1.0.0/Redshift.9	Kontrol keamanan/pergeseran merah.9
aws-foundational-security-best-Praktik/V/1.0.0/S3.1	Kontrol keamanan/S3.1
aws-foundational-security-best-Praktik/V/1.0.0/S3.12	Kontrol keamanan/S3.12
aws-foundational-security-best-Praktik/V/1.0.0/S3.13	Kontrol keamanan/S3.13
aws-foundational-security-best-Praktik/V/1.0.0/S3.2	Kontrol keamanan/S3.2

GeneratorID sebelum mengaktifkan temuan kontrol terkonsolidasi	GeneratorID setelah mengaktifkan temuan kontrol terkonsolidasi
aws-foundational-security-best-Praktik/V/1.0.0/S3.3	Kontrol keamanan/S3.3
aws-foundational-security-best-Praktik/V/1.0.0/S3.5	Kontrol keamanan/S3.5
aws-foundational-security-best-Praktik/V/1.0.0/S3.6	Kontrol keamanan/S3.6
aws-foundational-security-best-Praktik/V/1.0.0/S3.8	Kontrol keamanan/S3.8
aws-foundational-security-best-Praktik/V/1.0.0/S3.9	Kontrol keamanan/S3.9
aws-foundational-security-best-praktik/v/1.0.0/SageMaker .1	kontrol keamanan/ .1 SageMaker
aws-foundational-security-best-praktik/v/1.0.0/SageMaker .2	kontrol keamanan/ .2 SageMaker
aws-foundational-security-best-praktik/v/1.0.0/SageMaker .3	kontrol keamanan/ .3 SageMaker
aws-foundational-security-best-praktik/v/1.0.0/SecretsManager .1	kontrol keamanan/ .1 SecretsManager
aws-foundational-security-best-praktik/v/1.0.0/SecretsManager .2	kontrol keamanan/ .2 SecretsManager
aws-foundational-security-best-praktik/v/1.0.0/SecretsManager .3	kontrol keamanan/ .3 SecretsManager
aws-foundational-security-best-praktik/v/1.0.0/SecretsManager .4	kontrol keamanan/ .4 SecretsManager

GeneratorID sebelum mengaktifkan temuan kontrol terkonsolidasi	GeneratorID setelah mengaktifkan temuan kontrol terkonsolidasi
aws-foundational-security-best-Praktik/V/1.0.0/sqs.1	Kontrol keamanan/SQS.1
aws-foundational-security-best-Praktik/V/1.0.0/SSM.1	Kontrol keamanan/SSM.1
aws-foundational-security-best-Praktik/V/1.0.0/SSM.2	Kontrol keamanan/SSM.2
aws-foundational-security-best-Praktik/V/1.0.0/SSM.3	Kontrol keamanan/SSM.3
aws-foundational-security-best-Praktik/V/1.0.0/SSM.4	Kontrol keamanan/SSM.4
aws-foundational-security-best-Praktik/V/1.0.0/WAF.1	Kontrol keamanan/WAF.1
aws-foundational-security-best-Praktik/V/1.0.0/WAF.2	Kontrol keamanan/WAF.2
aws-foundational-security-best-Praktik/V/1.0.0/WAF.3	Kontrol keamanan/WAF.3
aws-foundational-security-best-Praktik/V/1.0.0/WAF.4	Kontrol keamanan/WAF.4
aws-foundational-security-best-Praktik/V/1.0.0/WAF.6	Kontrol keamanan/WAF.6
aws-foundational-security-best-Praktik/V/1.0.0/WAF.7	Kontrol keamanan/WAF.7
aws-foundational-security-best-Praktik/V/1.0.0/WAF.8	Kontrol keamanan/WAF.8

GeneratorID sebelum mengaktifkan temuan kontrol terkonsolidasi	GeneratorID setelah mengaktifkan temuan kontrol terkonsolidasi
aws-foundational-security-best-Praktik/V/1.0.0/WAF.10	Kontrol keamanan/WAF.10
PCI-DSS/V/3.2.1/PCI. AutoScaling.1	kontrol keamanan/ .1 AutoScaling
PCI-DSS/V/3.2.1/PCI. CloudTrail.1	kontrol keamanan/ .2 CloudTrail
PCI-DSS/V/3.2.1/PCI. CloudTrail.2	kontrol keamanan/ .3 CloudTrail
PCI-DSS/V/3.2.1/PCI. CloudTrail.3	kontrol keamanan/ .4 CloudTrail
PCI-DSS/V/3.2.1/PCI. CloudTrail.4	kontrol keamanan/ .5 CloudTrail
PCI-DSS/V/3.2.1/PCI. CodeBuild.1	kontrol keamanan/ .1 CodeBuild
PCI-DSS/V/3.2.1/PCI. CodeBuild.2	kontrol keamanan/ .2 CodeBuild
PCI-dss/v/3.2.1/pci.config.1	Kontrol keamanan/config.1
PCI-DSS/V/3.2.1/PCI.cw.1	kontrol keamanan/ .1 CloudWatch
PCI-DSS/V/3.2.1/PCI.dms.1	Kontrol keamanan/DMS.1
PCI-DSS/V/3.2.1/PCI.ec2.1	Kontrol keamanan/EC2.1
PCI-DSS/V/3.2.1/PCI.ec2.2	Kontrol keamanan/EC2.2
PCI-DSS/V/3.2.1/PCI.ec2.4	Kontrol keamanan/EC2.12
PCI-DSS/V/3.2.1/PCI.ec2.5	Kontrol keamanan/EC2.13
PCI-DSS/V/3.2.1/PCI.ec2.6	Kontrol keamanan/EC2.6
PCI-DSS/V/3.2.1/PCI.elbv2.1	Kontrol keamanan/ELB.1
PCI-DSS/V/3.2.1/PCI.es.1	Kontrol keamanan/ES.2
PCI-DSS/V/3.2.1/PCI.es.2	Kontrol keamanan/ES.1

GeneratorID sebelum mengaktifkan temuan kontrol terkonsolidasi	GeneratorID setelah mengaktifkan temuan kontrol terkonsolidasi
PCI-DSS/V/3.2.1/PCI. GuardDuty.1	kontrol keamanan/ .1 GuardDuty
PCI-DSS/V/3.2.1/PCI.iam.1	Kontrol keamanan/IAM.4
PCI-DSS/V/3.2.1/PCI.iam.2	Kontrol keamanan/IAM.2
PCI-DSS/V/3.2.1/PCI.iam.3	Kontrol keamanan/IAM.1
PCI-DSS/V/3.2.1/PCI.iam.4	Kontrol keamanan/IAM.6
PCI-DSS/V/3.2.1/PCI.iam.5	Kontrol keamanan/IAM.9
PCI-DSS/V/3.2.1/PCI.iam.6	Kontrol keamanan/IAM.19
PCI-DSS/V/3.2.1/PCI.iam.7	Kontrol keamanan/IAM.8
PCI-DSS/V/3.2.1/PCI.iam.8	Kontrol keamanan/IAM.10
PCI-DSS/V/3.2.1/PCI.kms.1	Kontrol keamanan/KMS.4
PCI-DSS/V/3.2.1/PCI.Lambda.1	Kontrol keamanan/Lambda.1
PCI-DSS/V/3.2.1/PCI.Lambda.2	Kontrol keamanan/Lambda.3
PCI-DSS/V/3.2.1/PCI.openSearch.1	Kontrol keamanan/OpenSearch.2
PCI-DSS/V/3.2.1/PCI.openSearch.2	Kontrol keamanan/OpenSearch.1
PCI-DSS/V/3.2.1/PCI.rds.1	Kontrol keamanan/RDS.1
PCI-DSS/V/3.2.1/PCI.rds.2	Kontrol keamanan/RDS.2
PCI-DSS/V/3.2.1/pci.redshift.1	Kontrol keamanan/pergeseran merah.1
PCI-DSS/V/3.2.1/PCI.s3.1	Kontrol keamanan/S3.3
PCI-DSS/V/3.2.1/PCI.s3.2	Kontrol keamanan/S3.2
PCI-DSS/V/3.2.1/PCI.s3.3	Kontrol keamanan/S3.7

GeneratorID sebelum mengaktifkan temuan kontrol terkonsolidasi	GeneratorID setelah mengaktifkan temuan kontrol terkonsolidasi
PCI-DSS/V/3.2.1/PCI.s3.5	Kontrol keamanan/S3.5
PCI-DSS/V/3.2.1/PCI.s3.6	Kontrol keamanan/S3.1
PCI-DSS/V/3.2.1/PCI. SageMaker.1	kontrol keamanan/ .1 SageMaker
PCI-DSS/V/3.2.1/PCI.ssm.1	Kontrol keamanan/SSM.2
PCI-DSS/V/3.2.1/PCI.ssm.2	Kontrol keamanan/SSM.3
PCI-DSS/V/3.2.1/PCI.ssm.3	Kontrol keamanan/SSM.1
service-managed-aws-control-Menara/v/1.0.0/ ACM.1	Kontrol keamanan/ACM.1
service-managed-aws-control-Menara/v/1.0.0/ apigateway.1	Kontrol keamanan/apigateway.1
service-managed-aws-control-Menara/v/1.0.0/ apigateway.2	Kontrol keamanan/apigateway.2
service-managed-aws-control-Menara/v/1.0.0/ apigateway.3	Kontrol keamanan/apigateway.3
service-managed-aws-control-Menara/v/1.0.0/ apigateway.4	Kontrol keamanan/apigateway.4
service-managed-aws-control-Menara/v/1.0.0/ apigateway.5	Kontrol keamanan/apigateway.5
service-managed-aws-control-menara/v/1.0.0/ AutoScaling .1	kontrol keamanan/ .1 AutoScaling
service-managed-aws-control-menara/v/1.0.0/ AutoScaling .2	kontrol keamanan/ .2 AutoScaling

GeneratorID sebelum mengaktifkan temuan kontrol terkonsolidasi	GeneratorID setelah mengaktifkan temuan kontrol terkonsolidasi
service-managed-aws-control-menara/v/1.0.0/ AutoScaling .3	kontrol keamanan/ .3 AutoScaling
service-managed-aws-control-menara/v/1.0.0/ AutoScaling .4	kontrol keamanan/ .4 AutoScaling
service-managed-aws-control-Menara/v/1.0.0/ AutoScaling.5	Kontrol keamanan/penskalan.5
service-managed-aws-control-menara/v/1.0.0/ AutoScaling .6	kontrol keamanan/ .6 AutoScaling
service-managed-aws-control-menara/v/1.0.0/ AutoScaling .9	kontrol keamanan/ .9 AutoScaling
service-managed-aws-control-menara/v/1.0.0/ CloudTrail .1	kontrol keamanan/ .1 CloudTrail
service-managed-aws-control-menara/v/1.0.0/ CloudTrail .2	kontrol keamanan/ .2 CloudTrail
service-managed-aws-control-menara/v/1.0.0/ CloudTrail .4	kontrol keamanan/ .4 CloudTrail
service-managed-aws-control-menara/v/1.0.0/ CloudTrail .5	kontrol keamanan/ .5 CloudTrail
service-managed-aws-control-menara/v/1.0.0/ CodeBuild .1	kontrol keamanan/ .1 CodeBuild
service-managed-aws-control-menara/v/1.0.0/ CodeBuild .2	kontrol keamanan/ .2 CodeBuild
service-managed-aws-control-menara/v/1.0.0/ CodeBuild .4	kontrol keamanan/ .4 CodeBuild

GeneratorID sebelum mengaktifkan temuan kontrol terkonsolidasi	GeneratorID setelah mengaktifkan temuan kontrol terkonsolidasi
service-managed-aws-control-menara/v/1.0.0/ CodeBuild .5	kontrol keamanan/ .5 CodeBuild
service-managed-aws-control-Menara/v/1.0.0/ dms.1	Kontrol keamanan/DMS.1
service-managed-aws-control-Menara/v/1.0.0/ DynamoDB.1	Kontrol keamanan/DynamoDB.1
service-managed-aws-control-Menara/v/1.0.0/ DynamoDB.2	Kontrol keamanan/Dynamodb.2
service-managed-aws-control-Menara/v/1.0.0/ EC2.1	Kontrol keamanan/EC2.1
service-managed-aws-control-Menara/v/1.0.0/ EC2.2	Kontrol keamanan/EC2.2
service-managed-aws-control-Menara/v/1.0.0/ EC2.3	Kontrol keamanan/EC2.3
service-managed-aws-control-Menara/v/1.0.0/ EC2.4	Kontrol keamanan/EC2.4
service-managed-aws-control-Menara/v/1.0.0/ EC2.6	Kontrol keamanan/EC2.6
service-managed-aws-control-Menara/v/1.0.0/ EC2.7	Kontrol keamanan/EC2.7
service-managed-aws-control-Menara/v/1.0.0/ EC2.8	Kontrol keamanan/EC2.8
service-managed-aws-control-Menara/v/1.0.0/ EC2.9	Kontrol keamanan/EC2.9

GeneratorID sebelum mengaktifkan temuan kontrol terkonsolidasi	GeneratorID setelah mengaktifkan temuan kontrol terkonsolidasi
service-managed-aws-control-Menara/v/1.0.0/EC2.10	Kontrol keamanan/EC2.10
service-managed-aws-control-Menara/v/1.0.0/EC2.15	Kontrol keamanan/EC2.15
service-managed-aws-control-Menara/v/1.0.0/EC2.16	Kontrol keamanan/EC2.16
service-managed-aws-control-Menara/v/1.0.0/EC2.17	Kontrol keamanan/EC2.17
service-managed-aws-control-Menara/v/1.0.0/EC2.18	Kontrol keamanan/EC2.18
service-managed-aws-control-Menara/v/1.0.0/EC2.19	Kontrol keamanan/EC2.19
service-managed-aws-control-Menara/v/1.0.0/EC2.20	Kontrol keamanan/EC2.20
service-managed-aws-control-Menara/v/1.0.0/EC2.21	Kontrol keamanan/EC2.21
service-managed-aws-control-Menara/v/1.0.0/EC2.22	Kontrol keamanan/EC2.22
service-managed-aws-control-Menara/v/1.0.0/ECR.1	Kontrol keamanan/ECR.1
service-managed-aws-control-Menara/v/1.0.0/ECR.2	Kontrol keamanan/ECR.2
service-managed-aws-control-Menara/v/1.0.0/ECR.3	Kontrol keamanan/ECR.3

GeneratorID sebelum mengaktifkan temuan kontrol terkonsolidasi	GeneratorID setelah mengaktifkan temuan kontrol terkonsolidasi
service-managed-aws-control-Menara/v/1.0.0/ECS.1	Kontrol keamanan/ECS.1
service-managed-aws-control-Menara/v/1.0.0/ECS.2	Kontrol keamanan/ECS.2
service-managed-aws-control-Menara/v/1.0.0/ECS.3	Kontrol keamanan/ECS.3
service-managed-aws-control-Menara/v/1.0.0/ECS.4	Kontrol keamanan/ECS.4
service-managed-aws-control-Menara/v/1.0.0/ECS.5	Kontrol keamanan/ECS.5
service-managed-aws-control-Menara/v/1.0.0/ECS.8	Kontrol keamanan/ECS.8
service-managed-aws-control-Menara/v/1.0.0/ECS.10	Kontrol keamanan/ECS.10
service-managed-aws-control-Menara/v/1.0.0/ECS.12	Kontrol keamanan/ECS.12
service-managed-aws-control-Menara/V/1.0.0/EFS.1	Kontrol keamanan/EFS.1
service-managed-aws-control-Menara/V/1.0.0/EFS.2	Kontrol keamanan/EFS.2
service-managed-aws-control-Menara/V/1.0.0/EFS.3	Kontrol keamanan/EFS.3
service-managed-aws-control-Menara/V/1.0.0/EFS.4	Kontrol keamanan/EFS.4

GeneratorID sebelum mengaktifkan temuan kontrol terkonsolidasi	GeneratorID setelah mengaktifkan temuan kontrol terkonsolidasi
service-managed-aws-control-Menara/v/1.0.0/eks.2	Kontrol keamanan/EKS.2
service-managed-aws-control-Menara/v/1.0.0/elb.2	Kontrol keamanan/ELB.2
service-managed-aws-control-Menara/v/1.0.0/ELB.3	Kontrol keamanan/ELB.3
service-managed-aws-control-Menara/v/1.0.0/ELB.4	Kontrol keamanan/ELB.4
service-managed-aws-control-Menara/v/1.0.0/ELB.5	Kontrol keamanan/ELB.5
service-managed-aws-control-Menara/v/1.0.0/ELB.6	Kontrol keamanan/ELB.6
service-managed-aws-control-Menara/v/1.0.0/elb.7	Kontrol keamanan/ELB.7
service-managed-aws-control-Menara/v/1.0.0/elb.8	Kontrol keamanan/ELB.8
service-managed-aws-control-Menara/v/1.0.0/elb.9	Kontrol keamanan/ELB.9
service-managed-aws-control-Menara/v/1.0.0/ELB.10	Kontrol keamanan/ELB.10
service-managed-aws-control-Menara/v/1.0.0/elb.12	Kontrol keamanan/ELB.12
service-managed-aws-control-Menara/v/1.0.0/ELB.13	Kontrol keamanan/ELB.13

GeneratorID sebelum mengaktifkan temuan kontrol terkonsolidasi	GeneratorID setelah mengaktifkan temuan kontrol terkonsolidasi
service-managed-aws-control-Menara/v/1.0.0/elb.14	Kontrol keamanan/ELB.14
service-managed-aws-control-Menara/v/1.0.0/ELBV2.1	Kontrol keamanan/ELBV2.1
service-managed-aws-control-Menara/v/1.0.0/EMR.1	Kontrol keamanan/EMR.1
service-managed-aws-control-Menara/v/1.0.0/es.1	Kontrol keamanan/ES.1
service-managed-aws-control-Menara/v/1.0.0/es.2	Kontrol keamanan/ES.2
service-managed-aws-control-Menara/v/1.0.0/es.3	Kontrol keamanan/ES.3
service-managed-aws-control-Menara/v/1.0.0/es.4	Kontrol keamanan/ES.4
service-managed-aws-control-Menara/v/1.0.0/es.5	Kontrol keamanan/ES.5
service-managed-aws-control-Menara/v/1.0.0/es.6	Kontrol keamanan/ES.6
service-managed-aws-control-Menara/v/1.0.0/es.7	Kontrol keamanan/ES.7
service-managed-aws-control-Menara/v/1.0.0/es.8	Kontrol keamanan/ES.8
service-managed-aws-control-menara/v/1.0.0/ElasticBeanstalk .1	kontrol keamanan/ .1 ElasticBeanstalk

GeneratorID sebelum mengaktifkan temuan kontrol terkonsolidasi	GeneratorID setelah mengaktifkan temuan kontrol terkonsolidasi
service-managed-aws-control-menara/v/1.0.0/ ElasticBeanstalk .2	kontrol keamanan/ .2 ElasticBeanstalk
service-managed-aws-control-menara/v/1.0.0/ GuardDuty .1	kontrol keamanan/ .1 GuardDuty
service-managed-aws-control-Menara/v/1.0.0/ iAM.1	Kontrol keamanan/IAM.1
service-managed-aws-control-Menara/v/1.0.0/ iAM.2	Kontrol keamanan/IAM.2
service-managed-aws-control-Menara/v/1.0.0/ iAM.3	Kontrol keamanan/IAM.3
service-managed-aws-control-Menara/v/1.0.0/ iAM.4	Kontrol keamanan/IAM.4
service-managed-aws-control-Menara/v/1.0.0/ iAM.5	Kontrol keamanan/IAM.5
service-managed-aws-control-Menara/v/1.0.0/ iAM.6	Kontrol keamanan/IAM.6
service-managed-aws-control-Menara/v/1.0.0/ iAM.7	Kontrol keamanan/IAM.7
service-managed-aws-control-Menara/v/1.0.0/ iAM.8	Kontrol keamanan/IAM.8
service-managed-aws-control-Menara/v/1.0.0/ iAM.21	Kontrol keamanan/IAM.21
service-managed-aws-control-Menara/v/1.0.0/kinesis.1	Kontrol keamanan/kinesis.1

GeneratorID sebelum mengaktifkan temuan kontrol terkonsolidasi	GeneratorID setelah mengaktifkan temuan kontrol terkonsolidasi
service-managed-aws-control-Menara/v/1.0.0/kms.1	Kontrol keamanan/KMS.1
service-managed-aws-control-Menara/v/1.0.0/kms.2	Kontrol keamanan/KMS.2
service-managed-aws-control-Menara/v/1.0.0/kms.3	Kontrol keamanan/KMS.3
service-managed-aws-control-Menara/v/1.0.0/lambda.1	Kontrol keamanan/Lambda.1
service-managed-aws-control-Menara/v/1.0.0/lambda.2	Kontrol keamanan/Lambda.2
service-managed-aws-control-Menara/v/1.0.0/lambda.5	Kontrol keamanan/Lambda.5
service-managed-aws-control-menara/v/1.0.0/NetworkFirewall .3	kontrol keamanan/ .3 NetworkFirewall
service-managed-aws-control-menara/v/1.0.0/NetworkFirewall .4	kontrol keamanan/ .4 NetworkFirewall
service-managed-aws-control-menara/v/1.0.0/NetworkFirewall .5	kontrol keamanan/ .5 NetworkFirewall
service-managed-aws-control-menara/v/1.0.0/NetworkFirewall .6	kontrol keamanan/ .6 NetworkFirewall
service-managed-aws-control-Menara/v/1.0.0/OpenSearch.1	Kontrol keamanan/OpenSearch.1
service-managed-aws-control-Menara/v/1.0.0/OpenSearch.2	Kontrol keamanan/OpenSearch.2

GeneratorID sebelum mengaktifkan temuan kontrol terkonsolidasi	GeneratorID setelah mengaktifkan temuan kontrol terkonsolidasi
service-managed-aws-control-Menara/v/1.0.0/OpenSearch.3	Kontrol keamanan/OpenSearch.3
service-managed-aws-control-Menara/v/1.0.0/OpenSearch.4	Kontrol keamanan/OpenSearch.4
service-managed-aws-control-Menara/v/1.0.0/OpenSearch.5	Kontrol keamanan/OpenSearch.5
service-managed-aws-control-Menara/v/1.0.0/OpenSearch.6	Kontrol keamanan/OpenSearch.6
service-managed-aws-control-Menara/v/1.0.0/OpenSearch.7	Kontrol keamanan/OpenSearch.7
service-managed-aws-control-Menara/v/1.0.0/OpenSearch.8	Kontrol keamanan/OpenSearch.8
service-managed-aws-control-Menara/V/1.0.0/RDS.1	Kontrol keamanan/RDS.1
service-managed-aws-control-Menara/V/1.0.0/RDS.2	Kontrol keamanan/RDS.2
service-managed-aws-control-Menara/V/1.0.0/RDS.3	Kontrol keamanan/RDS.3
service-managed-aws-control-Menara/V/1.0.0/RDS.4	Kontrol keamanan/RDS.4
service-managed-aws-control-Menara/V/1.0.0/RDS.5	Kontrol keamanan/RDS.5
service-managed-aws-control-Menara/v/1.0.0/RDS.6	Kontrol keamanan/RDS.6

GeneratorID sebelum mengaktifkan temuan kontrol terkonsolidasi	GeneratorID setelah mengaktifkan temuan kontrol terkonsolidasi
service-managed-aws-control-Menara/V/1.0.0/RDS.8	Kontrol keamanan/RDS.8
service-managed-aws-control-Menara/v/1.0.0/RDS.9	Kontrol keamanan/RDS.9
service-managed-aws-control-Menara/V/1.0.0/RDS.10	Kontrol keamanan/RDS.10
service-managed-aws-control-Menara/v/1.0.0/RDS.11	Kontrol keamanan/RDS.11
service-managed-aws-control-Menara/v/1.0.0/RDS.13	Kontrol keamanan/RDS.13
service-managed-aws-control-Menara/v/1.0.0/RDS.17	Kontrol keamanan/RDS.17
service-managed-aws-control-Menara/v/1.0.0/RDS.18	Kontrol keamanan/RDS.18
service-managed-aws-control-Menara/v/1.0.0/RDS.19	Kontrol keamanan/RDS.19
service-managed-aws-control-Menara/V/1.0.0/RDS.20	Kontrol keamanan/RDS.20
service-managed-aws-control-Menara/v/1.0.0/RDS.21	Kontrol keamanan/RDS.21
service-managed-aws-control-Menara/v/1.0.0/RDS.22	Kontrol keamanan/RDS.22
service-managed-aws-control-Menara/v/1.0.0/RDS.23	Kontrol keamanan/RDS.23

GeneratorID sebelum mengaktifkan temuan kontrol terkonsolidasi	GeneratorID setelah mengaktifkan temuan kontrol terkonsolidasi
service-managed-aws-control-Menara/V/1.0.0/RDS.25	Kontrol keamanan/RDS.25
service-managed-aws-control-Menara/v/1.0.0/Redshift.1	Kontrol keamanan/pergeseran merah.1
service-managed-aws-control-Menara/v/1.0.0/Redshift.2	Kontrol keamanan/pergeseran merah.2
service-managed-aws-control-Menara/v/1.0.0/Redshift.4	Kontrol keamanan/Redshift.4
service-managed-aws-control-Menara/v/1.0.0/Redshift.6	Kontrol keamanan/pergeseran merah.6
service-managed-aws-control-Menara/v/1.0.0/Redshift.7	Kontrol keamanan/pergeseran merah.7
service-managed-aws-control-Menara/v/1.0.0/Redshift.8	Kontrol keamanan/pergeseran merah.8
service-managed-aws-control-Menara/v/1.0.0/pergeseran merah.9	Kontrol keamanan/pergeseran merah.9
service-managed-aws-control-Menara/v/1.0.0/S3.1	Kontrol keamanan/S3.1
service-managed-aws-control-Menara/v/1.0.0/S3.2	Kontrol keamanan/S3.2
service-managed-aws-control-Menara/v/1.0.0/s3.3	Kontrol keamanan/S3.3
service-managed-aws-control-Menara/v/1.0.0/S3.5	Kontrol keamanan/S3.5

GeneratorID sebelum mengaktifkan temuan kontrol terkonsolidasi	GeneratorID setelah mengaktifkan temuan kontrol terkonsolidasi
service-managed-aws-control-Menara/v/1.0.0/s3.6	Kontrol keamanan/S3.6
service-managed-aws-control-Menara/v/1.0.0/s3.8	Kontrol keamanan/S3.8
service-managed-aws-control-Menara/v/1.0.0/s3.9	Kontrol keamanan/S3.9
service-managed-aws-control-Menara/v/1.0.0/s3.12	Kontrol keamanan/S3.12
service-managed-aws-control-Menara/v/1.0.0/s3.13	Kontrol keamanan/S3.13
service-managed-aws-control-menara/v/1.0.0/SageMaker .1	kontrol keamanan/ .1 SageMaker
service-managed-aws-control-menara/v/1.0.0/SecretsManager .1	kontrol keamanan/ .1 SecretsManager
service-managed-aws-control-menara/v/1.0.0/SecretsManager .2	kontrol keamanan/ .2 SecretsManager
service-managed-aws-control-menara/v/1.0.0/SecretsManager .3	kontrol keamanan/ .3 SecretsManager
service-managed-aws-control-menara/v/1.0.0/SecretsManager .4	kontrol keamanan/ .4 SecretsManager
service-managed-aws-control-Menara/v/1.0.0/sqs.1	Kontrol keamanan/SQS.1
service-managed-aws-control-Menara/V/1.0.0/SSM.1	Kontrol keamanan/SSM.1

GeneratorID sebelum mengaktifkan temuan kontrol terkonsolidasi	GeneratorID setelah mengaktifkan temuan kontrol terkonsolidasi
service-managed-aws-control-Menara/V/1.0.0/SSM.2	Kontrol keamanan/SSM.2
service-managed-aws-control-Menara/V/1.0.0/SSM.3	Kontrol keamanan/SSM.3
service-managed-aws-control-Menara/V/1.0.0/SSM.4	Kontrol keamanan/SSM.4
service-managed-aws-control-Menara/v/1.0.0/WAF.2	Kontrol keamanan/WAF.2
service-managed-aws-control-Menara/v/1.0.0/WAF.3	Kontrol keamanan/WAF.3
service-managed-aws-control-Menara/v/1.0.0/WAF.4	Kontrol keamanan/WAF.4

Bagaimana konsolidasi memengaruhi ID dan judul kontrol

Tampilan kontrol terkonsolidasi dan temuan kontrol terkonsolidasi menstandarisasi ID dan judul kontrol di seluruh standar. Istilah ID kontrol keamanan dan judul kontrol keamanan mengacu pada nilai agnostik standar ini. Tabel berikut menunjukkan pemetaan ID kontrol keamanan dan judul ke ID dan judul kontrol khusus standar. ID dan judul untuk kontrol yang termasuk dalam standar Praktik Terbaik Keamanan AWS Dasar (FSBP) tidak berubah.

Konsol Security Hub menampilkan ID kontrol keamanan agnostik standar dan judul kontrol keamanan, terlepas dari apakah temuan kontrol konsolidasi diaktifkan atau dinonaktifkan di akun Anda. Namun, temuan Security Hub berisi judul kontrol khusus standar (untuk PCI dan CIS v1.2.0) jika temuan kontrol konsolidasi dimatikan di akun Anda. Jika temuan kontrol konsolidasi dimatikan di akun Anda, temuan Security Hub berisi ID kontrol khusus standar dan ID kontrol keamanan. Untuk informasi lebih lanjut tentang bagaimana konsolidasi berdampak pada temuan kontrol, lihatTemuan kontrol sampel.

Untuk kontrol yang merupakan bagian dari Standar yang Dikelola Layanan: AWS Control Tower, awalan `CT.` dihapus dari ID kontrol dan judul dalam temuan saat temuan kontrol konsolidasi diaktifkan.

Untuk menjalankan skrip Anda sendiri di tabel ini, unduh sebagai file.csv.

Standar	ID kontrol standar dan judul	ID dan judul kontrol keamanan
CIS v1.2.0	1.1 Hindari penggunaan pengguna root	[CloudWatch.1] Filter metrik log dan alarm harus ada untuk penggunaan pengguna “root”
CIS v1.2.0	1.10 Pastikan kebijakan kata sandi IAM mencegah penggunaan kembali kata sandi	[IAM.16] Pastikan kebijakan kata sandi IAM mencegah penggunaan kembali kata sandi
CIS v1.2.0	1.11 Pastikan kebijakan kata sandi IAM kedaluwarsa kata sandi dalam waktu 90 hari atau kurang	[IAM.17] Pastikan kebijakan kata sandi IAM kedaluwarsa kata sandi dalam waktu 90 hari atau kurang
CIS v1.2.0	1.12 Pastikan tidak ada kunci akses pengguna root	[IAM.4] Kunci akses pengguna root IAM seharusnya tidak ada
CIS v1.2.0	1.13 Pastikan MFA diaktifkan untuk pengguna root	[IAM.9] MFA harus diaktifkan untuk pengguna root
CIS v1.2.0	1.14 Pastikan MFA perangkat keras diaktifkan untuk pengguna root	[IAM.6] MFA perangkat keras harus diaktifkan untuk pengguna root
CIS v1.2.0	1.16 Pastikan kebijakan IAM hanya dilampirkan pada grup atau peran	[IAM.2] Pengguna IAM seharusnya tidak memiliki kebijakan IAM yang dilampirkan
CIS v1.2.0	1.2 Pastikan otentikasi multi-fak tor (MFA) diaktifkan untuk semua pengguna IAM yang memiliki kata sandi konsol	[IAM.5] MFA harus diaktifkan untuk semua pengguna IAM yang memiliki kata sandi konsol

Standar	ID kontrol standar dan judul	ID dan judul kontrol keamanan
CIS v1.2.0	1.20 Memastikan peran dukungan telah dibuat untuk mengelola insiden dengan AWS Support	[IAM.18] Memastikan peran dukungan telah dibuat untuk mengelola insiden dengan AWS Support
CIS v1.2.0	1.22 Pastikan kebijakan IAM yang memungkinkan hak administratif “*: *” penuh tidak dibuat	[IAM.1] Kebijakan IAM seharusnya tidak mengizinkan hak administratif “*” penuh
CIS v1.2.0	1.3 Pastikan kredensil yang tidak digunakan selama 90 hari atau lebih dinonaktifkan	[IAM.8] Kredensyal pengguna IAM yang tidak digunakan harus dihapus
CIS v1.2.0	1.4 Pastikan kunci akses diputar setiap 90 hari atau kurang	[IAM.3] Kunci akses pengguna IAM harus diputar setiap 90 hari atau kurang
CIS v1.2.0	1.5 Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu huruf besar	[IAM.11] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu huruf besar
CIS v1.2.0	1.6 Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu huruf kecil	[IAM.12] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu huruf kecil
CIS v1.2.0	1.7 Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu simbol	[IAM.13] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu simbol
CIS v1.2.0	1.8 Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu nomor	[IAM.14] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu nomor
CIS v1.2.0	1.9 Pastikan kebijakan kata sandi IAM memerlukan panjang kata sandi minimum 14 atau lebih	[IAM.15] Pastikan kebijakan kata sandi IAM membutuhkan panjang kata sandi minimum 14 atau lebih

Standar	ID kontrol standar dan judul	ID dan judul kontrol keamanan
CIS v1.2.0	2.1 Pastikan CloudTrail diaktifkan di semua wilayah	[CloudTrail.1] CloudTrail harus diaktifkan dan dikonfigurasi dengan setidaknya satu jejak Multi-wilayah yang mencakup acara manajemen baca dan tulis
CIS v1.2.0	2.2 Pastikan validasi file CloudTrail log diaktifkan	[CloudTrail.4] validasi file CloudTrail log harus diaktifkan
CIS v1.2.0	2.3 Pastikan bucket S3 yang digunakan untuk menyimpan CloudTrail log tidak dapat diakses publik	[CloudTrail.6] Pastikan bucket S3 yang digunakan untuk menyimpan CloudTrail log tidak dapat diakses publik
CIS v1.2.0	2.4 Pastikan CloudTrail jalur terintegrasi dengan Log CloudWatch	[CloudTrail.5] CloudTrail jalur harus diintegrasikan dengan Amazon Logs CloudWatch
CIS v1.2.0	2.5 Pastikan AWS Config diaktifkan	[Config.1] AWS Config harus diaktifkan dan menggunakan peran terkait layanan untuk perekaman sumber daya
CIS v1.2.0	2.6 Pastikan pencatatan akses bucket S3 diaktifkan pada bucket CloudTrail S3	[CloudTrail.7] Pastikan pencatatan akses bucket S3 diaktifkan pada bucket CloudTrail S3
CIS v1.2.0	2.7 Pastikan CloudTrail log dienkripsi saat istirahat menggunakan KMS CMK	[CloudTrail.2] CloudTrail harus mengaktifkan enkripsi saat istirahat
CIS v1.2.0	2.8 Pastikan rotasi untuk CMK yang dibuat pelanggan diaktifkan	[KMS.4] rotasi AWS KMS tombol harus diaktifkan
CIS v1.2.0	2.9 Pastikan logging aliran VPC diaktifkan di semua VPC	[EC2.6] Pencatatan aliran VPC harus diaktifkan di semua VPC

Standar	ID kontrol standar dan judul	ID dan judul kontrol keamanan
CIS v1.2.0	3.1 Pastikan filter metrik log dan alarm ada untuk panggilan API yang tidak sah	[CloudWatch.2] Pastikan filter metrik log dan alarm ada untuk panggilan API yang tidak sah
CIS v1.2.0	3.10 Pastikan filter metrik log dan alarm ada untuk perubahan grup keamanan	[CloudWatch.10] Pastikan filter metrik log dan alarm ada untuk perubahan grup keamanan
CIS v1.2.0	3.11 Pastikan filter metrik log dan alarm ada untuk perubahan pada Daftar Kontrol Akses Jaringan (NACL)	[CloudWatch.11] Pastikan filter metrik log dan alarm ada untuk perubahan pada Daftar Kontrol Akses Jaringan (NACL)
CIS v1.2.0	3.12 Pastikan filter metrik log dan alarm ada untuk perubahan gateway jaringan	[CloudWatch.12] Pastikan filter metrik log dan alarm ada untuk perubahan pada gateway jaringan
CIS v1.2.0	3.13 Pastikan filter metrik log dan alarm ada untuk perubahan tabel rute	[CloudWatch.13] Pastikan filter metrik log dan alarm ada untuk perubahan tabel rute
CIS v1.2.0	3.14 Pastikan filter metrik log dan alarm ada untuk perubahan VPC	[CloudWatch.14] Pastikan filter metrik log dan alarm ada untuk perubahan VPC
CIS v1.2.0	3.2 Pastikan filter metrik log dan alarm ada untuk login Konsol Manajemen tanpa MFA	[CloudWatch.3] Pastikan filter metrik log dan alarm ada untuk login Konsol Manajemen tanpa MFA
CIS v1.2.0	3.3 Pastikan filter metrik log dan alarm ada untuk penggunaan pengguna root	[CloudWatch.1] Filter metrik log dan alarm harus ada untuk penggunaan pengguna “root”
CIS v1.2.0	3.4 Pastikan filter metrik log dan alarm ada untuk perubahan kebijakan IAM	[CloudWatch.4] Pastikan filter metrik log dan alarm ada untuk perubahan kebijakan IAM

Standar	ID kontrol standar dan judul	ID dan judul kontrol keamanan
CIS v1.2.0	3.5 Pastikan filter metrik log dan alarm ada untuk perubahan CloudTrail konfigurasi	[CloudWatch.5] Pastikan filter metrik log dan alarm ada untuk perubahan CloudTrail AWS Config urasi
CIS v1.2.0	3.6 Pastikan filter metrik log dan alarm ada untuk kegagalan AWS Management Console otentikasi	[CloudWatch.6] Pastikan filter metrik log dan alarm ada untuk kegagalan AWS Management Console otentikasi
CIS v1.2.0	3.7 Pastikan filter metrik log dan alarm ada untuk menonaktifkan atau menjadwalkan penghapusan CMK yang dibuat pelanggan	[CloudWatch.7] Pastikan filter metrik log dan alarm ada untuk menonaktifkan atau menjadwalkan penghapusan kunci yang dikelola pelanggan
CIS v1.2.0	3.8 Pastikan filter metrik log dan alarm ada untuk perubahan kebijakan bucket S3	[CloudWatch.8] Pastikan filter metrik log dan alarm ada untuk perubahan kebijakan bucket S3
CIS v1.2.0	3.9 Pastikan filter metrik log dan alarm ada untuk perubahan AWS Config konfigurasi	[CloudWatch.9] Pastikan filter metrik log dan alarm ada untuk perubahan AWS Config konfigurasi
CIS v1.2.0	4.1 Pastikan tidak ada grup keamanan yang mengizinkan masuknya dari 0.0.0.0/0 ke port 22	[EC2.13] Grup keamanan tidak boleh mengizinkan masuknya dari 0.0.0.0/0 atau: :/0 ke port 22
CIS v1.2.0	4.2 Pastikan tidak ada grup keamanan yang mengizinkan masuknya dari 0.0.0.0/0 ke port 3389	[EC2.14] Grup keamanan tidak boleh mengizinkan masuknya dari 0.0.0.0/0 atau: :/0 ke port 3389
CIS v1.2.0	4.3 Pastikan grup keamanan default dari setiap VPC membatasi semua lalu lintas	[EC2.2] Grup keamanan default VPC tidak boleh mengizinkan lalu lintas masuk atau keluar

Standar	ID kontrol standar dan judul	ID dan judul kontrol keamanan
CIS v1.4.0	1.10 Pastikan otentikasi multi-fak tor (MFA) diaktifkan untuk semua pengguna IAM yang memiliki kata sandi konsol	[IAM.5] MFA harus diaktifkan untuk semua pengguna IAM yang memiliki kata sandi konsol
CIS v1.4.0	1.14 Pastikan kunci akses diputar setiap 90 hari atau kurang	[IAM.3] Kunci akses pengguna IAM harus diputar setiap 90 hari atau kurang
CIS v1.4.0	1.16 Pastikan kebijakan IAM yang memungkinkan hak administratif “*: *” penuh tidak dilampirkan	[IAM.1] Kebijakan IAM seharusnya tidak mengizinkan hak administratif “*” penuh
CIS v1.4.0	1.17 Memastikan peran dukungan telah dibuat untuk mengelola insiden dengan AWS Support	[IAM.18] Memastikan peran dukungan telah dibuat untuk mengelola insiden dengan AWS Support
CIS v1.4.0	1.4 Pastikan tidak ada kunci akses akun pengguna root	[IAM.4] Kunci akses pengguna root IAM seharusnya tidak ada
CIS v1.4.0	1.5 Pastikan MFA diaktifkan untuk akun pengguna root	[IAM.9] MFA harus diaktifkan untuk pengguna root
CIS v1.4.0	1.6 Pastikan MFA perangkat keras diaktifkan untuk akun pengguna root	[IAM.6] MFA perangkat keras harus diaktifkan untuk pengguna root
CIS v1.4.0	1.7 Hilangkan penggunaan pengguna root untuk tugas administratif dan harian	[CloudWatch.1] Filter metrik log dan alarm harus ada untuk penggunaan pengguna “root”
CIS v1.4.0	1.8 Pastikan kebijakan kata sandi IAM membutuhkan panjang minimum 14 atau lebih	[IAM.15] Pastikan kebijakan kata sandi IAM membutuhkan panjang kata sandi minimum 14 atau lebih

Standar	ID kontrol standar dan judul	ID dan judul kontrol keamanan
CIS v1.4.0	1.9 Pastikan kebijakan kata sandi IAM mencegah penggunaan kembali kata sandi	[IAM.16] Pastikan kebijakan kata sandi IAM mencegah penggunaan kembali kata sandi
CIS v1.4.0	2.1.2 Pastikan Kebijakan Bucket S3 disetel untuk menolak permintaan HTTP	[S3.5] Bucket tujuan umum S3 harus memerlukan permintaan untuk menggunakan SSL
CIS v1.4.0	2.1.5.1 Pengaturan Akses Publik Blok S3 harus diaktifkan	[S3.1] Bucket tujuan umum S3 harus mengaktifkan pengaturan akses publik blok
CIS v1.4.0	2.1.5.2 Pengaturan Akses Publik Blok S3 harus diaktifkan pada tingkat bucket	[S3.8] Bucket tujuan umum S3 harus memblokir akses publik
CIS v1.4.0	2.2.1 Pastikan enkripsi volume EBS diaktifkan	[EC2.7] Enkripsi default EBS harus diaktifkan
CIS v1.4.0	2.3.1 Pastikan enkripsi diaktifkan untuk Instans RDS	[RDS.3] Instans RDS DB harus mengaktifkan enkripsi saat istirahat
CIS v1.4.0	3.1 Pastikan CloudTrail diaktifkan di semua wilayah	[CloudTrail.1] CloudTrail harus diaktifkan dan dikonfigurasi dengan setidaknya satu jejak Multi-wilayah yang mencakup acara manajemen baca dan tulis
CIS v1.4.0	3.2 Pastikan validasi file CloudTrail log diaktifkan	[CloudTrail.4] validasi file CloudTrail log harus diaktifkan
CIS v1.4.0	3.4 Pastikan CloudTrail jalur terintegrasi dengan Log CloudWatch	[CloudTrail.5] CloudTrail jalur harus diintegrasikan dengan Amazon Logs CloudWatch

Standar	ID kontrol standar dan judul	ID dan judul kontrol keamanan
CIS v1.4.0	3.5 Pastikan AWS Config diaktifkan di semua wilayah	[Config.1] AWS Config harus diaktifkan dan menggunakan peran terkait layanan untuk perekaman sumber daya
CIS v1.4.0	3.6 Pastikan pencatatan akses bucket S3 diaktifkan pada bucket CloudTrail S3	[CloudTrail.7] Pastikan pencatatan akses bucket S3 diaktifkan pada bucket CloudTrail S3
CIS v1.4.0	3.7 Pastikan CloudTrail log dienkripsi saat istirahat menggunakan KMS CMK	[CloudTrail.2] CloudTrail harus mengaktifkan enkripsi saat istirahat
CIS v1.4.0	3.8 Pastikan rotasi untuk CMK yang dibuat pelanggan diaktifkan	[KMS.4] rotasi AWS KMS tombol harus diaktifkan
CIS v1.4.0	3.9 Pastikan logging aliran VPC diaktifkan di semua VPC	[EC2.6] Pencatatan aliran VPC harus diaktifkan di semua VPC
CIS v1.4.0	4.4 Pastikan filter metrik log dan alarm ada untuk perubahan kebijakan IAM	[CloudWatch.4] Pastikan filter metrik log dan alarm ada untuk perubahan kebijakan IAM
CIS v1.4.0	4.5 Pastikan filter metrik log dan alarm ada untuk perubahan CloudTrail konfigurasi	[CloudWatch.5] Pastikan filter metrik log dan alarm ada untuk perubahan CloudTrail AWS Config urasi
CIS v1.4.0	4.6 Pastikan filter metrik log dan alarm ada untuk kegagalan AWS Management Console otentikasi	[CloudWatch.6] Pastikan filter metrik log dan alarm ada untuk kegagalan AWS Management Console otentikasi
CIS v1.4.0	4.7 Pastikan filter metrik log dan alarm ada untuk menonaktifkan atau menjadwalkan penghapusan CMK yang dibuat pelanggan	[CloudWatch.7] Pastikan filter metrik log dan alarm ada untuk menonaktifkan atau menjadwalkan penghapusan kunci yang dikelola pelanggan

Standar	ID kontrol standar dan judul	ID dan judul kontrol keamanan
CIS v1.4.0	4.8 Pastikan filter metrik log dan alarm ada untuk perubahan kebijakan bucket S3	[CloudWatch.8] Pastikan filter metrik log dan alarm ada untuk perubahan kebijakan bucket S3
CIS v1.4.0	4.9 Pastikan filter metrik log dan alarm ada untuk perubahan AWS Config konfigurasi	[CloudWatch.9] Pastikan filter metrik log dan alarm ada untuk perubahan AWS Config konfigurasi
CIS v1.4.0	4.10 Pastikan filter metrik log dan alarm ada untuk perubahan grup keamanan	[CloudWatch.10] Pastikan filter metrik log dan alarm ada untuk perubahan grup keamanan
CIS v1.4.0	4.11 Pastikan filter metrik log dan alarm ada untuk perubahan pada Daftar Kontrol Akses Jaringan (NACL)	[CloudWatch.11] Pastikan filter metrik log dan alarm ada untuk perubahan pada Daftar Kontrol Akses Jaringan (NACL)
CIS v1.4.0	4.12 Pastikan filter metrik log dan alarm ada untuk perubahan gateway jaringan	[CloudWatch.12] Pastikan filter metrik log dan alarm ada untuk perubahan pada gateway jaringan
CIS v1.4.0	4.13 Pastikan filter metrik log dan alarm ada untuk perubahan tabel rute	[CloudWatch.13] Pastikan filter metrik log dan alarm ada untuk perubahan tabel rute
CIS v1.4.0	4.14 Pastikan filter metrik log dan alarm ada untuk perubahan VPC	[CloudWatch.14] Pastikan filter metrik log dan alarm ada untuk perubahan VPC
CIS v1.4.0	5.1 Pastikan tidak ada ACL Jaringan yang memungkinkan masuknya dari 0.0.0.0/0 ke port administrasi server jarak jauh	[EC2.21] ACL jaringan seharusnya tidak mengizinkan masuknya dari 0.0.0.0/0 ke port 22 atau port 3389
CIS v1.4.0	5.3 Pastikan grup keamanan default dari setiap VPC membatasi semua lalu lintas	[EC2.2] Grup keamanan default VPC tidak boleh mengizinkan lalu lintas masuk atau keluar

Standar	ID kontrol standar dan judul	ID dan judul kontrol keamanan
PCI DSS v3.2.1	PCI. AutoScaling.1 Grup penskalaan otomatis yang terkait dengan penyeimbang beban harus menggunakan pemeriksaan kesehatan penyeimbang beban	[AutoScaling.1] Grup Auto Scaling yang terkait dengan penyeimbang beban harus menggunakan pemeriksaan kesehatan ELB
PCI DSS v3.2.1	PCI. CloudTrail.1 CloudTrail log harus dienkripsi saat istirahat menggunakan CMK AWS KMS	[CloudTrail.2] CloudTrail harus mengaktifkan enkripsi saat istirahat
PCI DSS v3.2.1	PCI. CloudTrail.2 CloudTrail harus diaktifkan	[CloudTrail.3] Setidaknya satu CloudTrail jejak harus diaktifkan
PCI DSS v3.2.1	PCI. CloudTrail.3 validasi file CloudTrail log harus diaktifkan	[CloudTrail.4] validasi file CloudTrail log harus diaktifkan
PCI DSS v3.2.1	PCI. CloudTrail.4 CloudTrail jalur harus diintegrasikan dengan Amazon Logs CloudWatch	[CloudTrail.5] CloudTrail jalur harus diintegrasikan dengan Amazon Logs CloudWatch
PCI DSS v3.2.1	PCI. CodeBuildURL repositori sumber Bitbucket. 1 CodeBuild GitHub atau Bitbucket harus menggunakan OAuth	[CodeBuild.1] URL repositori sumber CodeBuild Bitbucket tidak boleh berisi kredensyal sensitif
PCI DSS v3.2.1	PCI. CodeBuild.2 variabel lingkungan CodeBuild proyek tidak boleh berisi kredensil teks yang jelas	[CodeBuild.2] variabel lingkungan CodeBuild proyek tidak boleh berisi kredensil teks yang jelas
PCI DSS v3.2.1	PCI.config.1 harus diaktifkan AWS Config	[Config.1] AWS Config harus diaktifkan dan menggunakan peran terkait layanan untuk perekaman sumber daya
PCI DSS v3.2.1	PCI.CW.1 Filter metrik log dan alarm harus ada untuk penggunaan pengguna “root”	[CloudWatch.1] Filter metrik log dan alarm harus ada untuk penggunaan pengguna “root”

Standar	ID kontrol standar dan judul	ID dan judul kontrol keamanan
PCI DSS v3.2.1	Instans replikasi Layanan Migrasi Database PCI.DMS.1 tidak boleh bersifat publik	[DMS.1] Instans replikasi Layanan Migrasi Database tidak boleh bersifat publik
PCI DSS v3.2.1	Snapshot PCI.EC2.1 EBS tidak boleh dipulihkan secara publik	[EC2.1] Snapshot Amazon EBS tidak boleh dipulihkan secara publik
PCI DSS v3.2.1	Grup keamanan default PCI.EC2.2 VPC harus melarang lalu lintas masuk dan keluar	[EC2.2] Grup keamanan default VPC tidak boleh mengizinkan lalu lintas masuk atau keluar
PCI DSS v3.2.1	PCI.EC2.4 EIP EC2 yang tidak digunakan harus dihapus	[EC2.12] EIP Amazon EC2 yang tidak digunakan harus dihapus
PCI DSS v3.2.1	PCI.EC2.5 Grup keamanan tidak boleh mengizinkan masuknya dari 0.0.0.0/0 ke port 22	[EC2.13] Grup keamanan tidak boleh mengizinkan masuknya dari 0.0.0.0/0 atau: :/0 ke port 22
PCI DSS v3.2.1	Pencatatan aliran VPC PCI.EC2.6 harus diaktifkan di semua VPC	[EC2.6] Pencatatan aliran VPC harus diaktifkan di semua VPC
PCI DSS v3.2.1	PCI.elbv2.1 Application Load Balancer harus dikonfigurasi untuk mengalihkan semua permintaan HTTP ke HTTPS	[ELB.1] Application Load Balancer harus dikonfigurasi untuk mengalihkan semua permintaan HTTP ke HTTPS
PCI DSS v3.2.1	Domain PCI.ES.1 Elasticsearch harus dalam VPC	[ES.2] Domain Elasticsearch tidak boleh diakses publik
PCI DSS v3.2.1	Domain PCI.ES.2 Elasticsearch harus mengaktifkan enkripsi saat istirahat	[ES.1] Domain Elasticsearch harus mengaktifkan enkripsi saat istirahat
PCI DSS v3.2.1	PCI. GuardDuty.1 GuardDuty harus diaktifkan	[GuardDuty.1] GuardDuty harus diaktifkan

Standar	ID kontrol standar dan judul	ID dan judul kontrol keamanan
PCI DSS v3.2.1	Kunci akses pengguna root PCI.IAM.1 IAM seharusnya tidak ada	[IAM.4] Kunci akses pengguna root IAM seharusnya tidak ada
PCI DSS v3.2.1	Pengguna IAM PCI.IAM.2 tidak boleh memiliki kebijakan IAM yang dilampirkan	[IAM.2] Pengguna IAM seharusnya tidak memiliki kebijakan IAM yang dilampirkan
PCI DSS v3.2.1	Kebijakan IAM PCI.IAM.3 tidak boleh mengizinkan hak administratif “*” penuh	[IAM.1] Kebijakan IAM seharusnya tidak mengizinkan hak administratif “*” penuh
PCI DSS v3.2.1	MFA Perangkat Keras PCI.IAM.4 harus diaktifkan untuk pengguna root	[IAM.6] MFA perangkat keras harus diaktifkan untuk pengguna root
PCI DSS v3.2.1	PCI.IAM.5 MFA Virtual harus diaktifkan untuk pengguna root	[IAM.9] MFA harus diaktifkan untuk pengguna root
PCI DSS v3.2.1	MFA PCI.IAM.6 harus diaktifkan untuk semua pengguna IAM	[IAM.19] MFA harus diaktifkan untuk semua pengguna IAM
PCI DSS v3.2.1	Kredensyal pengguna IAM PCI.IAM.7 harus dinonaktifkan jika tidak digunakan dalam jumlah hari yang ditentukan sebelumnya	[IAM.8] Kredensyal pengguna IAM yang tidak digunakan harus dihapus
PCI DSS v3.2.1	Kebijakan kata sandi PCI.IAM.8 untuk pengguna IAM harus memiliki konfigurasi yang kuat	[IAM.10] Kebijakan kata sandi untuk pengguna IAM harus memiliki urasi yang kuat AWS Config
PCI DSS v3.2.1	PCI.KMS.1 Rotasi kunci master pelanggan (CMK) harus diaktifkan	[KMS.4] rotasi AWS KMS tombol harus diaktifkan
PCI DSS v3.2.1	Fungsi Lambda PCI.lambda.1 harus melarang akses publik	[Lambda.1] Kebijakan fungsi Lambda harus melarang akses publik
PCI DSS v3.2.1	PCI.lambda.2 Fungsi Lambda harus dalam VPC	[Lambda.3] Fungsi Lambda harus dalam VPC

Standar	ID kontrol standar dan judul	ID dan judul kontrol keamanan
PCI DSS v3.2.1	Domain OpenSearch PCI.openSearch.1 harus dalam VPC	[Opensearch.2] OpenSearch domain tidak boleh diakses publik
PCI DSS v3.2.1	Snapshot EBS PCI.openSearch.2 tidak boleh dipulihkan secara publik	[Opensearch.1] OpenSearch domain harus mengaktifkan enkripsi saat istirahat
PCI DSS v3.2.1	Snapshot PCI.RDS.1 RDS harus bersifat pribadi	[RDS.1] Snapshot RDS harus pribadi
PCI DSS v3.2.1	Instans PCI.RDS.2 RDS DB harus melarang akses publik	[RDS.2] Instans RDS DB harus melarang akses publik, sebagaimana ditentukan oleh urasi PubliclyAccessible AWS Config
PCI DSS v3.2.1	PCI.redshift.1 Cluster Amazon Redshift harus melarang akses publik	[Redshift.1] Cluster Amazon Redshift harus melarang akses publik
PCI DSS v3.2.1	Bucket PCI.S3.1 S3 harus melarang akses tulis publik	[S3.3] Bucket tujuan umum S3 harus memblokir akses tulis publik
PCI DSS v3.2.1	Bucket PCI.S3.2 S3 harus melarang akses baca publik	[S3.2] Bucket tujuan umum S3 harus memblokir akses baca publik
PCI DSS v3.2.1	Bucket PCI.S3.3 S3 harus mengaktifkan replikasi lintas wilayah	[S3.7] Ember tujuan umum S3 harus menggunakan replikasi lintas wilayah
PCI DSS v3.2.1	Bucket PCI.S3.5 S3 harus memerlukan permintaan untuk menggunakan Secure Socket Layer	[S3.5] Bucket tujuan umum S3 harus memerlukan permintaan untuk menggunakan SSL
PCI DSS v3.2.1	Pengaturan Akses Publik Blok PCI.S3.6 S3 harus diaktifkan	[S3.1] Bucket tujuan umum S3 harus mengaktifkan pengaturan akses publik blok

Standar	ID kontrol standar dan judul	ID dan judul kontrol keamanan
PCI DSS v3.2.1	PCI. SageMaker.1 Instans SageMaker notebook Amazon seharusnya tidak memiliki akses internet langsung	[SageMaker.1] Instans SageMaker notebook Amazon seharusnya tidak memiliki akses internet langsung
PCI DSS v3.2.1	Instans PCI.SSM.1 EC2 yang dikelola oleh Systems Manager harus memiliki status kepatuhan patch COMPLIANT setelah instalasi patch	[SSM.2] Instans Amazon EC2 yang dikelola oleh Systems Manager harus memiliki status kepatuhan patch COMPLIANT setelah instalasi patch
PCI DSS v3.2.1	Instans PCI.SSM.2 EC2 yang dikelola oleh Systems Manager harus memiliki status kepatuhan asosiasi COMPLIANT	[SSM.3] Instans Amazon EC2 yang dikelola oleh Systems Manager harus memiliki status kepatuhan asosiasi COMPLIANT
PCI DSS v3.2.1	Instans PCI.SSM.3 EC2 harus dikelola oleh AWS Systems Manager	[SSM.1] Instans Amazon EC2 harus dikelola oleh AWS Systems Manager

Memperbarui alur kerja untuk konsolidasi

Jika alur kerja Anda tidak bergantung pada format spesifik bidang pencarian kontrol apa pun, tidak diperlukan tindakan.

Jika alur kerja Anda bergantung pada format spesifik dari setiap bidang pencarian kontrol yang dicatat dalam tabel, Anda harus memperbarui alur kerja Anda. Misalnya, Jika Anda membuat aturan Amazon CloudWatch Events yang memicu tindakan untuk ID kontrol tertentu (seperti memanggil AWS Lambda fungsi jika ID kontrol sama dengan CIS 2.7), perbarui aturan untuk menggunakan CloudTrail .2, bidang untuk kontrol tersebut`Compliance.SecurityControlId`.

Jika Anda membuat wawasan khusus menggunakan salah satu bidang pencarian kontrol atau nilai yang berubah, perbarui wawasan tersebut untuk menggunakan bidang atau nilai saat ini.

Contoh ASFF

Bagian berikut berisi contoh atribut wajib dan opsional dalam AWS Security Finding Format (ASFF), serta contoh dari setiap sumber daya yang didukung ASFF.

Topik

Atribut tingkat atas yang diperlukan

Atribut tingkat atas berikut dalam AWS Security Finding Format (ASFF) diperlukan untuk semua temuan di Security Hub. Untuk informasi selengkapnya tentang atribut wajib ini, lihat AwsSecurityFindingdi Referensi AWS Security Hub API.

AwsAccountId

Akun AWS ID yang berlaku untuk temuan tersebut.

Contoh

```
"AwsAccountId": "111111111111"
```

CreatedAt

Menunjukkan kapan potensi masalah keamanan yang ditangkap oleh temuan dibuat.

Contoh

```
"CreatedAt": "2017-03-22T13:22:13.933Z"
```

> **Note**
>
> Security Hub menghapus temuan 90 hari setelah pembaruan terbaru atau 90 hari setelah tanggal pembuatan jika tidak ada pembaruan yang terjadi. Untuk menyimpan temuan selama lebih dari 90 hari, Anda dapat mengonfigurasi aturan di Amazon EventBridge yang merutekan temuan ke bucket S3 Anda.

Deskripsi

Deskripsi temuan. Bidang ini dapat berupa teks boilerplate nonspesifik atau detail yang spesifik untuk contoh temuan.

Untuk temuan kontrol yang dihasilkan Security Hub, bidang ini memberikan deskripsi kontrol.

Bidang ini tidak mereferensikan standar jika Anda mengaktifkan temuan kontrol terkonsolidasi.

Contoh

```
"Description": "This AWS control checks whether AWS Config is enabled in the current
 account and Region."
```

GeneratorId

Pengidentifikasi untuk komponen spesifik solusi (unit logika diskrit) yang menghasilkan temuan.

Untuk temuan kontrol yang dihasilkan Security Hub, bidang ini tidak mereferensikan standar jika Anda mengaktifkan temuan kontrol konsolidasi.

Contoh

```
"GeneratorId": "security-control/Config.1"
```

Id

Pengidentifikasi khusus produk untuk sebuah temuan. Untuk temuan kontrol yang dihasilkan Security Hub, bidang ini menyediakan Nama Sumber Daya Amazon (ARN) dari temuan tersebut.

Bidang ini tidak mereferensikan standar jika Anda mengaktifkan temuan kontrol terkonsolidasi.

Contoh

```
"Id": "arn:aws:securityhub:eu-central-1:123456789012:security-control/iam.9/finding/
ab6d6a26-a156-48f0-9403-115983e5a956

"
```

ProductArn

Nama Sumber Daya Amazon (ARN) yang dihasilkan oleh Security Hub yang secara unik mengidentifikasi produk temuan pihak ketiga setelah produk terdaftar di Security Hub.

Format bidang ini adalah `arn:`*`partition`*`:securityhub:`*`region`*`:`*`account-id`*`:product/`*`company-id`*`/`*`product-id`*.

- Untuk AWS layanan yang terintegrasi dengan Security Hub, `company-id` harus "`aws`“, dan `product-id` harus menjadi nama layanan AWS publik. Karena AWS produk dan layanan tidak terkait dengan akun, `account-id` bagian ARN kosong. AWS Layanan yang belum terintegrasi dengan Security Hub dianggap sebagai produk pihak ketiga.
- Untuk produk publik, `company-id` dan `product-id` harus berupa nilai ID yang ditentukan pada saat pendaftaran.
- Untuk produk pribadi, `company-id` harus ID akun. `product-id`Harus berupa kata cadangan “default” atau ID yang ditentukan pada saat pendaftaran.

Contoh

```
// Private ARN
    "ProductArn": "arn:aws:securityhub:us-east-1:111111111111:product/111111111111/
default"

// Public ARN

    "ProductArn": "arn:aws:securityhub:us-west-2::product/aws/guardduty"
    "ProductArn": "arn:aws:securityhub:us-west-2:222222222222:product/generico/secure-
pro"
```

Sumber daya

`Resources`Objek menyediakan satu set tipe data sumber daya yang menggambarkan AWS sumber daya yang mengacu pada temuan tersebut.

Contoh

```
"Resources": [
  {
    "ApplicationArn": "arn:aws:resource-groups:us-west-2:123456789012:group/
SampleApp/1234567890abcdef0",
    "ApplicationName": "SampleApp",
    "DataClassification": {
    "DetailedResultsLocation": "Path_to_Folder_Or_File",
    "Result": {
        "MimeType": "text/plain",
        "SizeClassified": 2966026,
        "AdditionalOccurrences": false,
        "Status": {
```

```
            "Code": "COMPLETE",
            "Reason": "Unsupportedfield"
        },
       "SensitiveData": [
            {
                "Category": "PERSONAL_INFORMATION",
                "Detections": [
                    {
                        "Count": 34,
                        "Type": "GE_PERSONAL_ID",
                        "Occurrences": {
                            "LineRanges": [
                                {
                                    "Start": 1,
                                    "End": 10,
                                    "StartColumn": 20
                                }
                            ],
                            "Pages": [],
                            "Records": [],
                            "Cells": []
                        }
                    },
                    {
                        "Count": 59,
                        "Type": "EMAIL_ADDRESS",
                        "Occurrences": {
                            "Pages": [
                                {
                                    "PageNumber": 1,
                                    "OffsetRange": {
                                        "Start": 1,
                                        "End": 100,
                                        "StartColumn": 10
                                     },
                                    "LineRange": {
                                        "Start": 1,
                                        "End": 100,
                                        "StartColumn": 10
                                    }
                                }
                            ]
                        }
                    },
```

```
                    {
                        "Count": 2229,
                        "Type": "URL",
                        "Occurrences": {
                           "LineRanges": [
                               {
                                   "Start": 1,
                                   "End": 13
                               }
                           ]
                        }
                    },
                    {
                        "Count": 13826,
                        "Type": "NameDetection",
                        "Occurrences": {
                            "Records": [
                                {
                                    "RecordIndex": 1,
                                    "JsonPath": "$.ssn.value"
                                }
                            ]
                        }
                    },
                    {
                        "Count": 32,
                        "Type": "AddressDetection"
                    }
                ],
                "TotalCount": 32
            }
        ],
        "CustomDataIdentifiers": {
            "Detections": [
                {
                    "Arn": "1712be25e7c7f53c731fe464f1c869b8",
                    "Name": "1712be25e7c7f53c731fe464f1c869b8",
                    "Count": 2,
                }
            ],
            "TotalCount": 2
        }
    }
},
```

```
 "Type": "AwsEc2Instance",
 "Id": "arn:aws:ec2:us-west-2:123456789012:instance/i-abcdef01234567890",
 "Partition": "aws",
 "Region": "us-west-2",
 "ResourceRole": "Target",
 "Tags": {
  "billingCode": "Lotus-1-2-3",
  "needsPatching": true
 },
 "Details": {
  "IamInstanceProfileArn": "arn:aws:iam::123456789012:role/IamInstanceProfileArn",
  "ImageId": "ami-79fd7eee",
  "IpV4Addresses": ["1.1.1.1"],
  "IpV6Addresses": ["2001:db8:1234:1a2b::123"],
  "KeyName": "testkey",
  "LaunchedAt": "2018-09-29T01:25:54Z",
  "MetadataOptions": {
   "HttpEndpoint": "enabled",
   "HttpProtocolIpv6": "enabled",
   "HttpPutResponseHopLimit": 1,
   "HttpTokens": "optional",
   "InstanceMetadataTags": "disabled"
  }
 },
  "NetworkInterfaces": [
  {
   "NetworkInterfaceId": "eni-e5aa89a3"
  }
  ],
  "SubnetId": "PublicSubnet",
  "Type": "i3.xlarge",
  "VirtualizationType": "hvm",
  "VpcId": "TestVPCIpv6"
 }

]
```

SchemaVersion

Versi skema yang diformat untuk temuan. Nilai bidang ini harus menjadi salah satu versi yang diterbitkan secara resmi yang diidentifikasi oleh AWS. Dalam rilis saat ini, versi skema AWS Security Finding Format adalah`2018-10-08`.

Contoh

```
"SchemaVersion": "2018-10-08"
```

Kepelikan

Mendefinisikan pentingnya sebuah temuan. Untuk detail tentang objek ini, lihat `Severity`di Referensi AWS Security Hub API.

`Severity`adalah objek tingkat atas dalam temuan dan bersarang di bawah objek. `FindingProviderFields`

Nilai `Severity` objek tingkat atas untuk temuan hanya boleh diperbarui oleh `BatchUpdateFindings`API.

Untuk memberikan informasi tingkat keparahan, penyedia pencarian harus memperbarui `Severity` objek di bawah `FindingProviderFields` saat membuat permintaan `BatchImportFindings`API. Jika `BatchImportFindings` permintaan untuk temuan baru hanya menyediakan `Label` atau hanya menyediakan`Normalized`, maka Security Hub secara otomatis mengisi nilai bidang lainnya. `Original`Bidang `Product` dan juga dapat dihuni.

Jika `Finding.Severity` objek tingkat atas hadir tetapi tidak `Finding.FindingProviderFields` ada, Security Hub membuat `FindingProviderFields.Severity` objek dan menyalin keseluruhan `Finding.Severity object` ke dalamnya. Ini memastikan bahwa detail asli yang disediakan penyedia dipertahankan dalam `FindingProviderFields.Severity` struktur, bahkan jika objek tingkat atas `Severity` ditimpa.

Tingkat keparahan temuan tidak mempertimbangkan kekritisan aset yang terlibat atau sumber daya yang mendasarinya. Kritikalitas didefinisikan sebagai tingkat kepentingan sumber daya yang terkait dengan temuan tersebut. Misalnya, sumber daya yang terkait dengan aplikasi kritis misi memiliki kekritisan yang lebih tinggi daripada yang terkait dengan pengujian nonproduksi. Untuk menangkap informasi tentang kekritisan sumber daya, gunakan `Criticality` bidang.

Sebaiknya gunakan panduan berikut saat menerjemahkan skor keparahan asli temuan ke nilai `Severity.Label` di ASFF.

- `INFORMATIONAL`Kategori ini dapat mencakup temuan untuk`PASSED`,`WARNING`, atau `NOT AVAILABLE` cek atau identifikasi data sensitif.
- `LOW`— Temuan yang dapat menghasilkan kompromi di masa depan. Misalnya, kategori ini mungkin mencakup kerentanan, kelemahan konfigurasi, dan kata sandi yang terbuka.

- `MEDIUM`— Temuan yang menunjukkan kompromi aktif, tetapi tidak ada indikasi bahwa musuh menyelesaikan tujuan mereka. Misalnya, kategori ini mungkin mencakup aktivitas malware, aktivitas peretasan, dan deteksi perilaku yang tidak biasa.
- `HIGH`atau `CRITICAL` — Temuan yang menunjukkan bahwa musuh menyelesaikan tujuan mereka, seperti kehilangan data aktif atau kompromi atau penolakan layanan.

Contoh

```
"Severity": {
    "Label": "CRITICAL",
    "Normalized": 90,
    "Original": "CRITICAL"
}
```

Judul

Judul temuan. Bidang ini dapat berisi teks boilerplate nonspesifik atau detail yang spesifik untuk contoh temuan ini.

Untuk temuan kontrol, bidang ini memberikan judul kontrol.

Bidang ini tidak mereferensikan standar jika Anda mengaktifkan temuan kontrol terkonsolidasi.

Contoh

```
"Title": "AWS Config should be enabled"
```

Tipe

Satu atau lebih jenis temuan dalam format *namespace*/*category*/*classifier* yang mengklasifikasikan temuan. Bidang ini tidak mereferensikan standar jika Anda mengaktifkan temuan kontrol terkonsolidasi.

`Types`seharusnya hanya diperbarui menggunakan `BatchUpdateFindings`.

Menemukan penyedia yang ingin memberikan nilai untuk `Types` harus menggunakan `Types` atribut di bawah `FindingProviderFields`.

Dalam daftar berikut, peluru tingkat atas adalah ruang nama, peluru tingkat kedua adalah kategori, dan peluru tingkat ketiga adalah pengklasifikasi. Sebaiknya penyedia pencarian menggunakan ruang nama yang ditentukan untuk membantu mengurutkan dan mengelompokkan temuan. Kategori dan

pengklasifikasi yang ditentukan juga dapat digunakan, tetapi tidak diperlukan. Hanya namespace Pemeriksaan Perangkat Lunak dan Konfigurasi yang telah menentukan pengklasifikasi.

Anda dapat menentukan jalur sebagian untuk namespace/category/classifier. Misalnya, jenis temuan berikut semuanya valid:

- TTP
- TTPS/Penghindaran Pertahanan
- TTPS/Penghindaran Pertahan/ CloudTrailStopped

Kategori taktik, teknik, dan prosedur (TTP) dalam daftar berikut selaras dengan matrixTM MITRE ATT&CK. Namespace Perilaku Tidak Biasa mencerminkan perilaku umum yang tidak biasa, seperti anomali statistik umum, dan tidak selaras dengan TTP tertentu. Namun, Anda dapat mengklasifikasikan temuan dengan tipe temuan Perilaku Tidak Biasa dan TTP.

Daftar ruang nama, kategori, dan pengklasifikasi:

- Pemeriksaan Perangkat Lunak dan Konfigurasi
  - Kerentanan
    - CVE
  - AWS Praktik Terbaik Keamanan
    - Keterjangkauan Jaringan
    - Analisis Perilaku Waktu Aktif
  - Standar Industri dan Regulasi
    - AWS Praktik Terbaik Keamanan Dasar
    - Tolok Ukur Pengerasan Host CIS
    - Tolok Ukur AWS Yayasan CIS
    - PCI-DSS
    - Kontrol Aliansi Keamanan Cloud
    - Kontrol ISO 90001
    - Kontrol ISO 27001
    - Kontrol ISO 27017
    - Kontrol ISO 27018
    - SOC 1

    - SOC 2
    - Kontrol HIPAA (AS)
    - NIST 800-53 Kontrol (AS)
    - Kontrol CSF NIST (AS)
    - Kontrol IRAP (Australia)
    - Kontrol K-ISMS (Korea)
    - Kontrol MTCS (Singapura)
    - Kontrol FISC (Jepang)
    - Kontrol Undang-Undang Nomor Saya (Jepang)
    - ENS Controls (Spanyol)
    - Kontrol Cyber Essentials Plus (Inggris)
    - Kontrol G-Cloud (Inggris)
    - Kontrol C5 (Jerman)
    - Kontrol IT-Grundschutz (Jerman)
    - Kontrol GDPR (Eropa)
    - Kontrol TISAX (Eropa)
  - Manajemen Patch
- TTP
  - Akses Awal
  - Eksekusi
  - Tetap
  - Eskalasi Hak Istimewa
  - Penghindaran Pertahanan
  - Akses Kredensi
  - Penemuan
  - Gerakan Lateral
  - Koleksi
  - Perintah dan Kontrol
- Efek
  - Eksposur Data

  - Ekfiltrasi Data
  - Penghancuran Data
  - Penolakan Layanan
  - Konsumsi Sumber Daya
- Perilaku Tidak Biasa
  - Aplikasi
  - Aliran Jaringan
  - Alamat IP
  - Pengguna
  - VM
  - Kontainer
  - Nirserver
  - Proses
  - Basis Data
  - Data
- Identifikasi Data Sensitif
  - PII
  - Kata Sandi
  - Legal
  - Keuangan
  - Keamanan
  - Bisnis

Contoh

```
"Types": [
    "Software and Configuration Checks/Vulnerabilities/CVE"
    ]
```

UpdatedAt

Menunjukkan kapan penyedia temuan terakhir memperbarui catatan temuan.

Stempel waktu ini mencerminkan waktu ketika catatan temuan terakhir atau yang terbaru diperbarui. Akibatnya, ini dapat berbeda dari `LastObservedAt` stempel waktu, yang mencerminkan kapan peristiwa atau kerentanan terakhir atau yang terbaru diamati.

Saat memperbarui catatan temuan, Anda harus memperbarui stempel waktu ini ke stempel waktu saat ini. Setelah membuat catatan temuan, `CreatedAt` dan `UpdatedAt` stempel waktu harus sama. Setelah pembaruan ke catatan temuan, nilai bidang ini harus lebih baru dari semua nilai sebelumnya yang terkandung di dalamnya.

Perhatikan bahwa `UpdatedAt` tidak dapat diperbarui dengan menggunakan operasi `BatchUpdateFindings`API. Anda hanya dapat memperbaruinya dengan menggunakan `BatchImportFindings`.

Contoh

```
"UpdatedAt": "2017-04-22T13:22:13.933Z"
```

> **Note**
>
> Security Hub menghapus temuan 90 hari setelah pembaruan terbaru atau 90 hari setelah tanggal pembuatan jika tidak ada pembaruan yang terjadi. Untuk menyimpan temuan selama lebih dari 90 hari, Anda dapat mengonfigurasi aturan di Amazon EventBridge yang merutekan temuan ke bucket S3 Anda.

Atribut tingkat atas opsional

Atribut tingkat atas ini bersifat opsional dalam AWS Security Finding Format (ASFF). Untuk informasi selengkapnya tentang atribut ini, lihat AwsSecurityFindingdi Referensi AWS Security Hub API.

Tindakan

`Action`Objek memberikan rincian tentang tindakan yang mempengaruhi atau yang diambil pada sumber daya.

Contoh

```
"Action": {
```

```
    "ActionType": "PORT_PROBE",
    "PortProbeAction": {
        "PortProbeDetails": [
            {
                "LocalPortDetails": {
                    "Port": 80,
                    "PortName": "HTTP"
                  },
                "LocalIpDetails": {
                     "IpAddressV4": "192.0.2.0"
                 },
                "RemoteIpDetails": {
                    "Country": {
                        "CountryName": "Example Country"
                    },
                    "City": {
                        "CityName": "Example City"
                    },
                   "GeoLocation": {
                       "Lon": 0,
                       "Lat": 0
                   },
                   "Organization": {
                       "AsnOrg": "ExampleASO",
                       "Org": "ExampleOrg",
                       "Isp": "ExampleISP",
                       "Asn": 64496
                   }
                }
            }
        ],
        "Blocked": false
    }
}
```

AwsAccountName

Akun AWS Nama yang digunakan untuk temuan itu.

Contoh

```
"AwsAccountName": "jane-doe-testaccount"
```

CompanyName

Nama perusahaan untuk produk yang menghasilkan temuan. Untuk temuan berbasis kontrol, perusahaan adalah. AWS

Security Hub mengisi atribut ini secara otomatis untuk setiap temuan. Anda tidak dapat memperbaruinya menggunakan `BatchImportFindings`atau `BatchUpdateFindings`. Pengecualian untuk ini adalah ketika Anda menggunakan integrasi khusus. Lihat the section called "Menggunakan integrasi produk khusus".

Saat Anda menggunakan konsol Security Hub untuk memfilter temuan berdasarkan nama perusahaan, Anda menggunakan atribut ini. Saat Anda menggunakan Security Hub API untuk memfilter temuan berdasarkan nama perusahaan, Anda menggunakan `aws/securityhub/CompanyName` atribut di bawah`ProductFields`. Security Hub tidak menyinkronkan kedua atribut tersebut.

Contoh

```
"CompanyName": "AWS"
```

Kepatuhan

`Compliance`Objek memberikan rincian temuan yang terkait dengan kontrol. Atribut ini dikembalikan untuk temuan yang dihasilkan dari kontrol Security Hub dan untuk temuan yang AWS Config dikirim ke Security Hub.

Contoh

```
"Compliance": {
    "AssociatedStandards": [
        {"StandardsId": "standards/aws-foundational-security-best-practices/v/1.0.0"},
        {"StandardsId": "standards/service-managed-aws-control-tower/v/1.0.0"},
        {"StandardsId": "standards/nist-800-53/v/5.0.0"}
    ],
    "RelatedRequirements": [
        "NIST.800-53.r5 AC-4",
        "NIST.800-53.r5 AC-4(21)",
        "NIST.800-53.r5 SC-7",
        "NIST.800-53.r5 SC-7(11)",
        "NIST.800-53.r5 SC-7(16)",
```

```
        "NIST.800-53.r5 SC-7(21)",
        "NIST.800-53.r5 SC-7(4)",
        "NIST.800-53.r5 SC-7(5)"
    ],
    "SecurityControlId": "EC2.18",
    "SecurityControlParameters":[
        {
            "Name": "authorizedTcpPorts",
            "Value": ["80", "443"]
        },
        {
            "Name": "authorizedUdpPorts",
            "Value": ["427"]
        }
    ],
    "Status": "NOT_AVAILABLE",
    "StatusReasons": [
        {
            "ReasonCode": "CONFIG_RETURNS_NOT_APPLICABLE",
            "Description": "This finding has a compliance status of NOT AVAILABLE
 because AWS Config sent Security Hub a finding with a compliance state of Not
 Applicable. The potential reasons for a Not Applicable finding from Config are that
 (1) a resource has been moved out of scope of the Config rule; (2) the Config rule has
 been deleted; (3) the resource has been deleted; or (4) the logic of the Config rule
 itself includes scenarios where Not Applicable is returned. The specific reason why
 Not Applicable is returned is not available in the Config rule evaluation."
        }
    ]
}
```

Kepercayaan

Kemungkinan bahwa temuan secara akurat mengidentifikasi perilaku atau masalah yang dimaksudkan untuk diidentifikasi.

`Confidence`seharusnya hanya diperbarui menggunakan `BatchUpdateFindings`.

Menemukan penyedia yang ingin memberikan nilai untuk `Confidence` harus menggunakan `Confidence` atribut di bawah`FindingProviderFields`. Lihat the section called “Menggunakan FindingProviderFields”.

`Confidence`dinilai berdasarkan 0-100 menggunakan skala rasio. 0 berarti kepercayaan 0 persen, dan 100 berarti kepercayaan 100 persen. Misalnya, deteksi eksfiltrasi data berdasarkan

penyimpangan statistik lalu lintas jaringan memiliki kepercayaan diri yang rendah karena eksfiltrasi aktual belum diverifikasi.

Contoh

```
"Confidence": 42
```

Kekritisan

Tingkat kepentingan yang diberikan pada sumber daya yang terkait dengan suatu temuan.

`Criticality`seharusnya hanya diperbarui dengan memanggil operasi `BatchUpdateFindings`API. Jangan perbarui objek ini dengan `BatchImportFindings`.

Menemukan penyedia yang ingin memberikan nilai untuk `Criticality` harus menggunakan `Criticality` atribut di bawah`FindingProviderFields`. Lihat the section called “Menggunakan FindingProviderFields”.

`Criticality`diberi skor pada basis 0-100, menggunakan skala rasio yang hanya mendukung bilangan bulat penuh. Skor 0 berarti bahwa sumber daya yang mendasarinya tidak memiliki kekritisan, dan skor 100 dicadangkan untuk sumber daya yang paling kritis.

Untuk setiap sumber daya, pertimbangkan hal berikut saat menetapkan`Criticality`:

- Apakah sumber daya yang terpengaruh berisi data sensitif (misalnya, bucket S3 dengan PII)?
- Apakah sumber daya yang terpengaruh memungkinkan musuh untuk memperdalam akses mereka atau memperluas kemampuan mereka untuk melakukan aktivitas berbahaya tambahan (misalnya, akun sysadmin yang disusupi)?
- Apakah sumber daya merupakan aset penting bisnis (misalnya, sistem bisnis utama yang jika dikompromikan dapat memiliki dampak pendapatan yang signifikan)?

Anda dapat menggunakan pedoman berikut:

- Sumber daya yang menggerakkan sistem mission-critical atau berisi data yang sangat sensitif dapat dinilai dalam kisaran 75-100.
- Sumber daya yang memberi daya pada sistem penting (tetapi bukan sistem kritis) atau berisi data yang cukup penting dapat dinilai dalam kisaran 25-74.
- Sumber daya yang memberi daya pada sistem yang tidak penting atau berisi data yang tidak sensitif harus dinilai dalam kisaran 0-24.

Contoh

```
"Criticality": 99
```

FindingProviderFields

`FindingProviderFields`termasuk atribut berikut:

- `Confidence`
- `Criticality`
- `RelatedFindings`
- `Severity`
- `Types`

Bidang sebelumnya bersarang di bawah `FindingProviderFields` objek, tetapi memiliki analog dengan nama yang sama dengan bidang ASFF tingkat atas. Ketika temuan baru dikirim ke Security Hub oleh penyedia pencarian, Security Hub mengisi `FindingProviderFields` objek secara otomatis jika kosong berdasarkan bidang tingkat atas yang sesuai.

Penyedia pencarian dapat memperbarui `FindingProviderFields` dengan menggunakan `BatchImportFindings`pengoperasian Security Hub API. Menemukan penyedia tidak dapat memperbarui objek ini dengan `BatchUpdateFindings`.

Untuk detail tentang cara Security Hub menangani pembaruan dari `BatchImportFindings` ke `FindingProviderFields` dan ke atribut tingkat atas yang sesuai, lihatthe section called "Menggunakan FindingProviderFields".

Pelanggan dapat memperbarui bidang tingkat atas dengan menggunakan `BatchUpdateFindings` operasi. Pelanggan tidak dapat memperbarui`FindingProviderFields`.

Contoh

```
"FindingProviderFields": {
    "Confidence": 42,
    "Criticality": 99,
    "RelatedFindings":[
      {
        "ProductArn": "arn:aws:securityhub:us-west-2::product/aws/guardduty",
```

```
        "Id": "123e4567-e89b-12d3-a456-426655440000"
      }
    ],
    "Severity": {
        "Label": "MEDIUM",
        "Original": "MEDIUM"
    },
    "Types": [ "Software and Configuration Checks/Vulnerabilities/CVE" ]
}
```

FirstObservedAt

Menunjukkan kapan potensi masalah keamanan yang ditangkap oleh temuan pertama kali diamati.

Stempel waktu ini mencerminkan waktu ketika peristiwa atau kerentanan pertama kali diamati. Akibatnya, ini dapat berbeda dari `CreatedAt` stempel waktu, yang mencerminkan waktu catatan temuan ini dibuat.

Stempel waktu ini harus tidak dapat diubah antara pembaruan catatan temuan tetapi dapat diperbarui jika stempel waktu yang lebih akurat ditentukan.

Contoh

```
"FirstObservedAt": "2017-03-22T13:22:13.933Z"
```

LastObservedAt

Menunjukkan kapan potensi masalah keamanan yang ditangkap oleh sebuah temuan baru-baru ini diamati oleh produk temuan keamanan.

Stempel waktu ini mencerminkan waktu ketika peristiwa atau kerentanan terakhir atau yang terakhir diamati. Akibatnya, ini dapat berbeda dari `UpdatedAt` stempel waktu, yang mencerminkan kapan catatan temuan ini terakhir atau yang terbaru diperbarui.

Anda dapat memberikan stempel waktu ini, tetapi tidak diperlukan pada pengamatan pertama. Jika Anda memberikan bidang ini pada pengamatan pertama, stempel waktu harus sama dengan stempel waktu. `FirstObservedAt` Anda harus memperbarui bidang ini untuk mencerminkan stempel waktu terakhir atau yang paling baru diamati setiap kali temuan diamati.

Contoh

```
"LastObservedAt": "2017-03-23T13:22:13.933Z"
```

Malware

`Malware`Objek menyediakan daftar malware yang terkait dengan temuan.

Contoh

```
"Malware": [
    {
        "Name": "Stringler",
        "Type": "COIN_MINER",
        "Path": "/usr/sbin/stringler",
        "State": "OBSERVED"
    }
]
```

Jaringan (Pensiunan)

`Network`Objek menyediakan informasi terkait jaringan tentang temuan.

Objek ini sudah pensiun. Untuk menyediakan data ini, Anda dapat memetakan data ke sumber daya di`Resources`, atau menggunakan `Action` objek.

Contoh

```
"Network": {
    "Direction": "IN",
    "OpenPortRange": {
        "Begin": 443,
        "End": 443
    },
    "Protocol": "TCP",
    "SourceIpV4": "1.2.3.4",
    "SourceIpV6": "FE80:CD00:0000:0CDE:1257:0000:211E:729C",
    "SourcePort": "42",
    "SourceDomain": "example1.com",
    "SourceMac": "00:0d:83:b1:c0:8e",
    "DestinationIpV4": "2.3.4.5",
    "DestinationIpV6": "FE80:CD00:0000:0CDE:1257:0000:211E:729C",
    "DestinationPort": "80",
    "DestinationDomain": "example2.com"
```

```
}
```

NetworkPath

`NetworkPath`Objek memberikan informasi tentang jalur jaringan yang terkait dengan temuan. Setiap entri di `NetworkPath` mewakili komponen jalur.

Contoh

```
"NetworkPath" : [
    {
        "ComponentId": "abc-01a234bc56d8901ee",
        "ComponentType": "AWS::EC2::InternetGateway",
        "Egress": {
            "Destination": {
                "Address": [ "192.0.2.0/24" ],
                "PortRanges": [
                    {
                        "Begin": 443,
                        "End": 443
                    }
                ]
            },
            "Protocol": "TCP",
            "Source": {
                "Address": ["203.0.113.0/24"]
            }
        },
        "Ingress": {
            "Destination": {
                "Address": [ "198.51.100.0/24" ],
                "PortRanges": [
                    {
                        "Begin": 443,
                        "End": 443
                    }
                 ]
            },
            "Protocol": "TCP",
            "Source": {
                "Address": [ "203.0.113.0/24" ]
            }
        }
```

```
    }
]
```

Catatan

`Note`Objek menentukan catatan yang ditentukan pengguna yang dapat Anda tambahkan ke temuan.

Penyedia temuan dapat memberikan catatan awal untuk sebuah temuan, tetapi tidak dapat menambahkan catatan setelah itu. Anda hanya dapat memperbarui catatan menggunakan `BatchUpdateFindings`.

Contoh

```
"Note": {
    "Text": "Don't forget to check under the mat.",
    "UpdatedBy": "jsmith",
    "UpdatedAt": "2018-08-31T00:15:09Z"
}
```

PatchSummary

`PatchSummary`Objek menyediakan ringkasan status kepatuhan patch untuk sebuah instance terhadap standar kepatuhan yang dipilih.

Contoh

```
"PatchSummary" : {
    "FailedCount" : 0,
    "Id" : "pb-123456789098",
    "InstalledCount" : 100,
    "InstalledOtherCount" : 1023,
    "InstalledPendingReboot" : 0,
    "InstalledRejectedCount" : 0,
    "MissingCount" : 100,
    "Operation" : "Install",
    "OperationEndTime" : "2018-09-27T23:39:31Z",
    "OperationStartTime" : "2018-09-27T23:37:31Z",
    "RebootOption" : "RebootIfNeeded"
}
```

Proses

`Process`Objek memberikan rincian terkait proses tentang temuan.

Contoh:

```
"Process": {
    "LaunchedAt": "2018-09-27T22:37:31Z",
    "Name": "syslogd",
    "ParentPid": 56789,
    "Path": "/usr/sbin/syslogd",
    "Pid": 12345,
    "TerminatedAt": "2018-09-27T23:37:31Z"
}
```

ProcessedAt

Menunjukkan kapan Security Hub menerima temuan dan mulai memprosesnya.

Ini berbeda dari `CreatedAt` dan`UpdatedAt`, yang merupakan stempel waktu yang diperlukan yang berhubungan dengan interaksi penyedia temuan dengan masalah keamanan dan temuan. Cap `ProcessedAt` waktu menunjukkan kapan Security Hub mulai memproses temuan. Temuan muncul di akun pengguna setelah pemrosesan selesai.

```
"ProcessedAt": "2023-03-23T13:22:13.933Z"
```

ProductFields

Tipe data di mana produk temuan keamanan dapat menyertakan detail spesifik solusi tambahan yang bukan merupakan bagian dari Format Pencarian AWS Keamanan yang ditentukan.

Untuk temuan yang dihasilkan oleh kontrol Security Hub, `ProductFields` sertakan informasi tentang kontrol. Lihat the section called “Menghasilkan dan memperbarui temuan kontrol”.

Bidang ini tidak boleh berisi data yang berlebihan dan tidak boleh berisi data yang bertentangan dengan bidang Format Pencarian AWS Keamanan.

Awalan `aws/` "" mewakili namespace yang dicadangkan hanya untuk AWS produk dan layanan dan tidak boleh diserahkan dengan temuan dari integrasi pihak ketiga.

Meskipun tidak diperlukan, produk harus memformat nama bidang sebagai`company-id/product-id/field-name`, di mana `company-id` dan `product-id` cocok dengan yang `ProductArn` disediakan dalam temuan.

Referensi bidang `Archival` digunakan saat Security Hub mengarsipkan temuan yang ada. Misalnya, Security Hub mengarsipkan temuan yang ada saat Anda menonaktifkan kontrol atau standar dan saat Anda mengaktifkan atau menonaktifkan temuan kontrol konsolidasi.

Bidang ini juga dapat mencakup informasi tentang standar yang mencakup kontrol yang menghasilkan temuan.

Contoh

```
"ProductFields": {
    "API", "DeleteTrail",
    "ArchivalReasons:0/Description": "The finding is in an ARCHIVED state because
 consolidated control findings has been turned on or off. This causes findings in the
 previous state to be archived when new findings are being generated.",
    "ArchivalReasons:0/ReasonCode": "CONSOLIDATED_CONTROL_FINDINGS_UPDATE",
    "aws/inspector/AssessmentTargetName": "My prod env",
    "aws/inspector/AssessmentTemplateName": "My daily CVE assessment",
    "aws/inspector/RulesPackageName": "Common Vulnerabilities and Exposures",
    "generico/secure-pro/Action.Type", "AWS_API_CALL",
    "generico/secure-pro/Count": "6",
    "Service_Name": "cloudtrail.amazonaws.com"
}
```

ProductName

Memberikan nama produk yang menghasilkan temuan. Untuk temuan berbasis kontrol, nama produknya adalah Security Hub.

Security Hub mengisi atribut ini secara otomatis untuk setiap temuan. Anda tidak dapat memperbaruinya menggunakan `BatchImportFindings`atau `BatchUpdateFindings`. Pengecualian untuk ini adalah ketika Anda menggunakan integrasi khusus. Lihat the section called “Menggunakan integrasi produk khusus”.

Saat Anda menggunakan konsol Security Hub untuk memfilter temuan berdasarkan nama produk, Anda menggunakan atribut ini.

Saat Anda menggunakan Security Hub API untuk memfilter temuan berdasarkan nama produk, Anda menggunakan `aws/securityhub/ProductName` atribut di bawah`ProductFields`.

Security Hub tidak menyinkronkan kedua atribut tersebut.

RecordState

Memberikan status catatan temuan.

Secara default, ketika awalnya dihasilkan oleh layanan, temuan dipertimbangkan`ACTIVE`.

`ARCHIVED`Negara menunjukkan bahwa temuan harus disembunyikan dari pandangan. Temuan yang diarsipkan tidak segera dihapus. Anda dapat mencari, meninjau, dan melaporkannya. Security Hub secara otomatis mengarsipkan temuan berbasis kontrol jika sumber daya terkait dihapus, sumber daya tidak ada, atau kontrol dinonaktifkan.

`RecordState`dimaksudkan untuk menemukan penyedia, dan hanya dapat diperbarui oleh `BatchImportFindings`. Anda tidak dapat memperbaruinya menggunakan `BatchUpdateFindings`.

Untuk melacak status penyelidikan Anda ke dalam sebuah temuan, gunakan `Workflow`sebagai gantinya`RecordState`.

Jika status rekaman berubah dari `ARCHIVED` ke`ACTIVE`, dan status alur kerja temuan adalah salah satu `NOTIFIED` atau`RESOLVED`, maka Security Hub secara otomatis menyetel status alur kerja ke. `NEW`

Contoh

```
"RecordState": "ACTIVE"
```

Wilayah

Menentukan Wilayah AWS dari mana temuan itu dihasilkan.

Security Hub mengisi atribut ini secara otomatis untuk setiap temuan. Anda tidak dapat memperbaruinya menggunakan `BatchImportFindings`atau `BatchUpdateFindings`.

Contoh

```
"Region": "us-west-2"
```

RelatedFindings

Memberikan daftar temuan yang terkait dengan temuan saat ini.

`RelatedFindings`seharusnya hanya diperbarui dengan operasi `BatchUpdateFindings`API. Anda tidak harus memperbarui objek ini dengan `BatchImportFindings`.

Untuk `BatchImportFindings`permintaan, penyedia pencarian harus menggunakan `RelatedFindings` objek di bawah `FindingProviderFields`.

Untuk melihat deskripsi `RelatedFindings` atribut, lihat `RelatedFinding`di Referensi AWS Security Hub API.

Contoh

```
"RelatedFindings": [
    { "ProductArn": "arn:aws:securityhub:us-west-2::product/aws/guardduty",
      "Id": "123e4567-e89b-12d3-a456-426655440000" },
    { "ProductArn": "arn:aws:securityhub:us-west-2::product/aws/guardduty",
      "Id": "AcmeNerfHerder-111111111111-x189dx7824" }
]
```

Remediasi

`Remediation`Objek memberikan informasi tentang langkah-langkah remediasi yang direkomendasikan untuk mengatasi temuan tersebut.

Contoh

```
"Remediation": {
    "Recommendation": {
        "Text": "For instructions on how to fix this issue, see the AWS Security Hub
 documentation for EC2.2.",
        "Url": "https://docs.aws.amazon.com/console/securityhub/EC2.2/remediation"
    }
}
```

Sampel

Menentukan apakah temuan adalah temuan sampel.

```
"Sample": true
```

SourceUrl

`SourceUrl`Objek menyediakan URL yang menautkan ke halaman tentang temuan saat ini dalam produk pencarian.

```
"SourceUrl": "http://sourceurl.com"
```

ThreatIntelIndicators

`ThreatIntelIndicator`Objek tersebut memberikan rincian intelijen ancaman yang terkait dengan temuan.

Contoh

```
"ThreatIntelIndicators": [
  {
    "Category": "BACKDOOR",
    "LastObservedAt": "2018-09-27T23:37:31Z",
    "Source": "Threat Intel Weekly",
    "SourceUrl": "http://threatintelweekly.org/backdoors/8888",
    "Type": "IPV4_ADDRESS",
    "Value": "8.8.8.8",
  }
]
```

Ancaman

`Threats`Objek tersebut memberikan rincian tentang ancaman yang terdeteksi oleh sebuah temuan.

Contoh

```
"Threats": [{
    "FilePaths": [{
        "FileName": "b.txt",
        "FilePath": "/tmp/b.txt",
        "Hash": "sha256",
        "ResourceId": "arn:aws:ec2:us-west-2:123456789012:volume/vol-032f3bdd89aee112f"
    }],
    "ItemCount": 3,
    "Name": "Iot.linux.mirai.vwisi",
    "Severity": "HIGH"
}]
```

UserDefinedFields

Menyediakan daftar pasangan string nama-nilai yang terkait dengan temuan. Ini adalah bidang khusus yang ditentukan pengguna yang ditambahkan ke temuan. Bidang ini dapat dihasilkan secara otomatis melalui konfigurasi spesifik Anda.

Penyedia pencarian tidak boleh menggunakan bidang ini untuk data yang dihasilkan produk. Sebagai gantinya, penyedia pencarian dapat menggunakan `ProductFields` bidang untuk data yang tidak dipetakan ke bidang Format Pencarian AWS Keamanan standar apa pun.

Bidang ini hanya dapat diperbarui menggunakan `BatchUpdateFindings`.

Contoh

```
"UserDefinedFields": {
    "reviewedByCio": "true",
    "comeBackToLater": "Check this again on Monday"
}
```

VerificationState

Memberikan kebenaran temuan. Temuan produk dapat memberikan nilai `UNKNOWN` untuk bidang ini. Produk temuan harus memberikan nilai untuk bidang ini jika ada analog yang berarti dalam sistem produk temuan. Bidang ini biasanya diisi oleh penentuan atau tindakan pengguna setelah menyelidiki temuan.

Penyedia temuan dapat memberikan nilai awal untuk atribut ini, tetapi tidak dapat memperbaruinya setelah itu. Anda hanya dapat memperbarui atribut ini dengan menggunakan `BatchUpdateFindings`.

```
"VerificationState": "Confirmed"
```

Kerentanan

`Vulnerabilities`Objek menyediakan daftar kerentanan yang terkait dengan temuan.

Contoh

```
"Vulnerabilities" : [
    {
        "CodeVulnerabilities": [{
            "Cwes": [
                "CWE-798",
                "CWE-799"
            ],
            "FilePath": {
                "EndLine": 421,
                "FileName": "package-lock.json",
```

```
                "FilePath": "package-lock.json",
                "StartLine": 420
            },
                "SourceArn":"arn:aws:lambda:us-east-1:123456789012:layer:AWS-AppConfig-
Extension:114"
        }],
        "Cvss": [
            {
                "BaseScore": 4.7,
                "BaseVector": "AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N",
                "Version": "V3"
            },
            {
                "BaseScore": 4.7,
                "BaseVector": "AV:L/AC:M/Au:N/C:C/I:N/A:N",
                "Version": "V2"
            }
        ],
        "EpssScore": 0.015,
        "ExploitAvailable": "YES",
        "FixAvailable": "YES",
        "Id": "CVE-2020-12345",
        "LastKnownExploitAt": "2020-01-16T00:01:35Z",
        "ReferenceUrls":[
           "http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-12418",
            "http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-17563"
        ],
        "RelatedVulnerabilities": ["CVE-2020-12345"],
        "Vendor": {
            "Name": "Alas",
            "Url":"https://alas.aws.amazon.com/ALAS-2020-1337.html",
            "VendorCreatedAt":"2020-01-16T00:01:43Z",
            "VendorSeverity":"Medium",
            "VendorUpdatedAt":"2020-01-16T00:01:43Z"
        },
        "VulnerablePackages": [
            {
                "Architecture": "x86_64",
                "Epoch": "1",
                "FilePath": "/tmp",
                "FixedInVersion": "0.14.0",
                "Name": "openssl",
                "PackageManager": "OS",
                "Release": "16.amzn2.0.3",
```

```
                "Remediation": "Update aws-crt to 0.14.0",
                "SourceLayerArn": "arn:aws:lambda:us-west-2:123456789012:layer:id",
                "SourceLayerHash":
 "sha256:c1962c35b63a6ff6ce7df6e042ee82371a605ca9515569edec46ff14f926f001",
                "Version": "1.0.2k"
            }
        ]
    }
]
```

Alur kerja

`Workflow`Objek tersebut memberikan informasi tentang status investigasi terhadap suatu temuan.

Bidang ini ditujukan bagi pelanggan untuk digunakan dengan alat remediasi, orkestrasi, dan tiket. Ini tidak dimaksudkan untuk menemukan penyedia.

Anda hanya dapat memperbarui `Workflow` bidang dengan `BatchUpdateFindings`. Pelanggan juga dapat memperbaruinya dari konsol. Lihat the section called “Mengatur status alur kerja temuan”.

Contoh

```
"Workflow": {
    "Status": "NEW"
}
```

WorkflowState (Pensiun)

Objek ini sudah pensiun dan telah digantikan oleh `Status` bidang `Workflow` objek.

Bidang ini menyediakan status alur kerja dari sebuah temuan. Temuan produk dapat memberikan nilai `NEW` untuk bidang ini. Produk temuan dapat memberikan nilai untuk bidang ini jika ada analog yang berarti dalam sistem produk temuan.

Contoh

```
"WorkflowState": "NEW"
```

Resources

`Resources`Objek memberikan informasi tentang sumber daya yang terlibat dalam temuan.

Ini berisi array hingga 32 objek sumber daya.

Untuk menentukan bagaimana nama sumber daya diformat, lihatAWS Sintaks Security Finding Format (ASFF).

Untuk contoh setiap objek sumber daya, pilih dari daftar berikut.

Topik

- AwsKinesis
- AwsKms
- AwsLambda
- AwsMsk
- AwsNetworkFirewall
- AwsOpenSearchService
- AwsRds
- AwsRedshift
- AwsRoute53
- AwsS3
- AwsSageMaker
- AwsSecretsManager
- AwsSns
- AwsSqs
- AwsSsm
- AwsStepFunctions
- AwsWaf
- AwsXray
- Container
- Other

Atribut sumber daya

Berikut adalah deskripsi dan contoh untuk `Resources` objek dalam AWS Security Finding Format (ASFF). Untuk informasi lebih lanjut tentang bidang ini, lihatSumber daya.

ApplicationArn

Mengidentifikasi Nama Sumber Daya Amazon (ARN) dari aplikasi yang terlibat dalam temuan.

Contoh

```
"ApplicationArn": "arn:aws:resource-groups:us-west-2:123456789012:group/
SampleApp/1234567890abcdef0"
```

ApplicationName

Mengidentifikasi nama aplikasi yang terlibat dalam temuan.

Contoh

```
"ApplicationName": "SampleApp"
```

DataClassification

DataClassificationBidang ini memberikan informasi tentang data sensitif yang terdeteksi pada sumber daya.

Contoh

```
"DataClassification": {
    "DetailedResultsLocation": "Path_to_Folder_Or_File",
    "Result": {
        "MimeType": "text/plain",
        "SizeClassified": 2966026,
        "AdditionalOccurrences": false,
        "Status": {
            "Code": "COMPLETE",
            "Reason": "Unsupportedfield"
        },
       "SensitiveData": [
            {
                "Category": "PERSONAL_INFORMATION",
                "Detections": [
                    {
                        "Count": 34,
                        "Type": "GE_PERSONAL_ID",
                        "Occurrences": {
                            "LineRanges": [
                                {
                                    "Start": 1,
                                    "End": 10,
                                    "StartColumn": 20
                                }
                            ],
                            "Pages": [],
                            "Records": [],
                            "Cells": []
                        }
```

```
                    },
                    {
                        "Count": 59,
                        "Type": "EMAIL_ADDRESS",
                        "Occurrences": {
                            "Pages": [
                                {
                                    "PageNumber": 1,
                                    "OffsetRange": {
                                        "Start": 1,
                                        "End": 100,
                                        "StartColumn": 10
                                     },
                                    "LineRange": {
                                        "Start": 1,
                                        "End": 100,
                                        "StartColumn": 10
                                    }
                                }
                            ]
                        }
                    },
                    {
                        "Count": 2229,
                        "Type": "URL",
                        "Occurrences": {
                           "LineRanges": [
                               {
                                   "Start": 1,
                                   "End": 13
                               }
                           ]
                       }
                   },
                   {
                       "Count": 13826,
                       "Type": "NameDetection",
                       "Occurrences": {
                            "Records": [
                                {
                                    "RecordIndex": 1,
                                    "JsonPath": "$.ssn.value"
                                }
                            ]
```

```
                        }
                    },
                    {
                        "Count": 32,
                        "Type": "AddressDetection"
                    }
                ],
                "TotalCount": 32
            }
        ],
        "CustomDataIdentifiers": {
            "Detections": [
                {
                    "Arn": "1712be25e7c7f53c731fe464f1c869b8",
                    "Name": "1712be25e7c7f53c731fe464f1c869b8",
                    "Count": 2,
                }
            ],
            "TotalCount": 2
        }
    }
}
```

Detail

DetailsBidang ini memberikan informasi tambahan tentang sumber daya tunggal menggunakan objek yang sesuai. Setiap sumber daya harus disediakan dalam objek sumber daya terpisah di `Resources` objek.

Perhatikan bahwa jika ukuran temuan melebihi maksimum 240 KB, maka `Details` objek dihapus dari temuan. Untuk temuan kontrol yang menggunakan AWS Config aturan, Anda dapat melihat detail sumber daya di AWS Config konsol.

Security Hub menyediakan serangkaian detail sumber daya yang tersedia untuk jenis sumber daya yang didukung. Detail ini sesuai dengan nilai `Type` objek. Gunakan jenis yang disediakan bila memungkinkan.

Misalnya, jika sumber daya adalah bucket S3, maka atur sumber daya `Type` ke `AwsS3Bucket` dan berikan detail sumber daya di `AwsS3Bucket`objek.

`Other`Objek memungkinkan Anda untuk memberikan bidang dan nilai khusus. Anda menggunakan `Other` objek dalam kasus berikut:

- Jenis sumber daya (nilai sumber dayaType) tidak memiliki objek detail yang sesuai. Untuk memberikan detail untuk sumber daya, Anda menggunakan `Other`objek.
- Objek untuk jenis sumber daya tidak menyertakan semua bidang yang ingin Anda isi. Dalam hal ini, gunakan objek detail untuk jenis sumber daya untuk mengisi bidang yang tersedia. Gunakan `Other` objek untuk mengisi bidang yang tidak ada di objek khusus tipe.
- Jenis sumber daya bukan salah satu jenis yang disediakan. Dalam hal ini, atur `Resource.Type` ke`Other`, dan gunakan `Other` objek untuk mengisi detail.

Contoh

```
"Details": {
  "AwsEc2Instance": {
    "IamInstanceProfileArn": "arn:aws:iam::123456789012:role/IamInstanceProfileArn",
    "ImageId": "ami-79fd7eee",
    "IpV4Addresses": ["1.1.1.1"],
    "IpV6Addresses": ["2001:db8:1234:1a2b::123"],
    "KeyName": "testkey",
    "LaunchedAt": "2018-09-29T01:25:54Z",
    "MetadataOptions": {
      "HttpEndpoint": "enabled",
      "HttpProtocolIpv6": "enabled",
      "HttpPutResponseHopLimit": 1,
      "HttpTokens": "optional",
      "InstanceMetadataTags": "disabled"
    },
    "NetworkInterfaces": [
    {
      "NetworkInterfaceId": "eni-e5aa89a3"
    }
    ],
    "SubnetId": "PublicSubnet",
    "Type": "i3.xlarge",
    "VirtualizationType": "hvm",
    "VpcId": "TestVPCIpv6"
  },
  "AwsS3Bucket": {
    "OwnerId": "da4d66eac431652a4d44d490a00500bded52c97d235b7b4752f9f688566fe6de",
    "OwnerName": "acmes3bucketowner"
  },
  "Other": { "LightPen": "blinky", "SerialNo": "1234abcd"}
```

```
}
```

Id

Pengidentifikasi untuk jenis sumber daya yang diberikan.

Untuk AWS sumber daya yang diidentifikasi oleh Amazon Resource Names (ARN), ini adalah ARN.

Untuk AWS sumber daya yang tidak memiliki ARN, ini adalah pengidentifikasi seperti yang didefinisikan oleh AWS layanan yang menciptakan sumber daya.

Untuk AWS non-sumber daya, ini adalah pengidentifikasi unik yang terkait dengan sumber daya.

Contoh

```
"Id": "arn:aws:s3:::example-bucket"
```

Partition

Partisi tempat sumber daya berada. Partisi adalah sekelompok Wilayah AWS. Masing-masing Akun AWS dicakup ke satu partisi.

Partisi berikut didukung:

- `aws` – Wilayah AWS
- `aws-cn`— Wilayah China
- `aws-us-gov` – AWS GovCloud (US) Region

Contoh

```
"Partition": "aws"
```

Wilayah

Kode untuk Wilayah AWS tempat sumber daya ini berada. Untuk daftar kode Wilayah, lihat Titik akhir Regional.

Contoh

```
"Region": "us-west-2"
```

ResourceRole

Mengidentifikasi peran sumber daya dalam temuan. Sumber daya adalah target aktivitas pencarian atau aktor yang melakukan aktivitas tersebut.

Contoh

```
"ResourceRole": "target"
```

Tanda

Anda dapat menambahkan tag sumber daya ke temuan yang dimasukkan ke dalam Security Hub, termasuk temuan dari produk terintegrasi Layanan AWS dan pihak ketiga. Anda dapat menandai sumber daya yang didukung oleh `GetResources` pengoperasian API AWS Resource Groups Tagging. Untuk daftar sumber daya yang didukung, lihat Layanan yang mendukung API Penandaan Resource Groups.

Menambahkan tag memberi tahu Anda tag yang dikaitkan dengan sumber daya pada saat temuan diproses. Anda dapat menyertakan `Tags` atribut hanya untuk sumber daya yang memiliki tag terkait. Jika sumber daya tidak memiliki tag terkait, jangan sertakan `Tags` atribut dalam temuan.

Dimasukkannya tag sumber daya dalam temuan menghilangkan kebutuhan untuk membangun jaringan pengayaan data atau secara manual memperkaya metadata temuan keamanan. Anda juga dapat menggunakan tag untuk mencari atau memfilter temuan dan wawasan dan membuat aturan otomatisasi.

Untuk informasi tentang pembatasan yang berlaku untuk tag, lihat Batas dan persyaratan penamaan tag.

Anda hanya dapat memberikan tag yang ada pada AWS sumber daya di bidang ini. Untuk menyediakan data yang tidak ditentukan dalam Format Pencarian AWS Keamanan, gunakan subbidang `Other` detail.

Contoh

```
"Tags": {
    "billingCode": "Lotus-1-2-3",
    "needsPatching": "true"
}
```

Tipe

Jenis sumber daya yang Anda berikan detailnya.

Bila memungkinkan, gunakan salah satu jenis sumber daya yang disediakan, seperti `AwsEc2Instance` atau`AwsS3Bucket`.

Jika jenis sumber daya tidak cocok dengan salah satu jenis sumber daya yang disediakan, setel sumber daya `Type` ke`Other`, dan gunakan subbidang `Other` detail untuk mengisi detailnya.

Nilai yang didukung tercantum di bawah Sumber Daya.

Contoh

```
"Type": "AwsS3Bucket"
```

AwsAmazonMQ

Berikut ini adalah contoh AWS Security Finding Format (ASFF) untuk `AwsAmazonMQ` sumber daya.

AwsAmazonMQBroker

`AwsAmazonMQBroker`memberikan informasi tentang broker Amazon MQ, yang merupakan lingkungan broker pesan yang berjalan di Amazon MQ.

Contoh berikut menunjukkan ASFF untuk `AwsAmazonMQBroker` objek. Untuk melihat deskripsi *`AwsAmazonMQBroker`* atribut, lihat AwsAmazonMQBroker di Referensi API.AWS Security Hub

Contoh

```
"AwsAmazonMQBroker": {
    "AutoMinorVersionUpgrade": true,
    "BrokerArn": "arn:aws:mq:us-east-1:123456789012:broker:TestBroker:b-
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "BrokerId": "b-a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "BrokerName": "TestBroker",
    "Configuration": {
        "Id": "c-a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
        "Revision": 1
    },
    "DeploymentMode": "ACTIVE_STANDBY_MULTI_AZ",
    "EncryptionOptions": {
        "UseAwsOwnedKey": true
```

```
    },
    "EngineType": "ActiveMQ",
    "EngineVersion": "5.17.2",
    "HostInstanceType": "mq.t2.micro",
    "Logs": {
        "Audit": false,
        "AuditLogGroup": "/aws/amazonmq/broker/b-a1b2c3d4-5678-90ab-cdef-EXAMPLE11111/
audit",
        "General": false,
        "GeneralLogGroup": "/aws/amazonmq/broker/b-a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111/general"
    },
    "MaintenanceWindowStartTime": {
        "DayOfWeek": "MONDAY",
        "TimeOfDay": "22:00",
        "TimeZone": "UTC"
    },
    "PubliclyAccessible": true,
    "SecurityGroups": [
        "sg-021345abcdef6789"
    ],
    "StorageType": "efs",
    "SubnetIds": [
        "subnet-1234567890abcdef0",
        "subnet-abcdef01234567890"
    ],
    "Users": [
        {
            "Username": "admin"
        }
    ]
}
```

AwsApiGateway

Berikut ini adalah contoh Format Pencarian AWS Keamanan untuk `AwsApiGateway` sumber daya.

AwsApiGatewayRestApi

`AwsApiGatewayRestApi`Objek berisi informasi tentang REST API di Amazon API Gateway versi 1.

Berikut ini adalah contoh `AwsApiGatewayRestApi` temuan dalam AWS Security Finding Format (ASFF). Untuk melihat deskripsi `AwsApiGatewayRestApi` atribut, lihat AwsApiGatewayRestApiDetailsdi Referensi AWS Security Hub API.

Contoh

```
AwsApiGatewayRestApi: {
    "Id": "exampleapi",
    "Name": "Security Hub",
    "Description": "AWS Security Hub",
    "CreatedDate": "2018-11-18T10:20:05-08:00",
    "Version": "2018-10-26",
    "BinaryMediaTypes" : ["-'*~1*'"],
    "MinimumCompressionSize": 1024,
    "ApiKeySource": "AWS_ACCOUNT_ID",
    "EndpointConfiguration": {
        "Types": [
            "REGIONAL"
        ]
    }
}
```

AwsApiGatewayStage

`AwsApiGatewayStage`Objek menyediakan informasi tentang tahap Amazon API Gateway versi 1.

Berikut ini adalah contoh `AwsApiGatewayStage` temuan dalam AWS Security Finding Format (ASFF). Untuk melihat deskripsi `AwsApiGatewayStage` atribut, lihat AwsApiGatewayStageDetailsdi Referensi AWS Security Hub API.

Contoh

```
"AwsApiGatewayStage": {
    "DeploymentId": "n7hlmf",
    "ClientCertificateId": "a1b2c3",
    "StageName": "Prod",
    "Description" : "Stage Description",
    "CacheClusterEnabled": false,
    "CacheClusterSize" : "1.6",
    "CacheClusterStatus": "NOT_AVAILABLE",
    "MethodSettings": [
        {
            "MetricsEnabled": true,
            "LoggingLevel": "INFO",
            "DataTraceEnabled": false,
            "ThrottlingBurstLimit": 100,
            "ThrottlingRateLimit": 5.0,
```

```
            "CachingEnabled": false,
            "CacheTtlInSeconds": 300,
            "CacheDataEncrypted": false,
            "RequireAuthorizationForCacheControl": true,
            "UnauthorizedCacheControlHeaderStrategy": "SUCCEED_WITH_RESPONSE_HEADER",
            "HttpMethod": "POST",
            "ResourcePath": "/echo"
        }
    ],
    "Variables": {"test": "value"},
    "DocumentationVersion": "2.0",
    "AccessLogSettings": {
        "Format": "{\"requestId\": \"$context.requestId\", \"extendedRequestId
\": \"$context.extendedRequestId\", \"ownerAccountId\": \"$context.accountId\",
 \"requestAccountId\": \"$context.identity.accountId\", \"callerPrincipal\":
 \"$context.identity.caller\", \"httpMethod\": \"$context.httpMethod\", \"resourcePath
\": \"$context.resourcePath\", \"status\": \"$context.status\", \"requestTime
\": \"$context.requestTime\", \"responseLatencyMs\": \"$context.responseLatency
\", \"errorMessage\": \"$context.error.message\", \"errorResponseType\":
 \"$context.error.responseType\", \"apiId\": \"$context.apiId\", \"awsEndpointRequestId
\": \"$context.awsEndpointRequestId\", \"domainName\": \"$context.domainName\", \"stage
\": \"$context.stage\", \"xrayTraceId\": \"$context.xrayTraceId\", \"sourceIp\":
 \"$context.identity.sourceIp\", \"user\": \"$context.identity.user\", \"userAgent
\": \"$context.identity.userAgent\", \"userArn\": \"$context.identity.userArn\",
 \"integrationLatency\": \"$context.integrationLatency\", \"integrationStatus
\": \"$context.integrationStatus\", \"authorizerIntegrationLatency\":
 \"$context.authorizer.integrationLatency\" }",
        "DestinationArn": "arn:aws:logs:us-west-2:111122223333:log-
group:SecurityHubAPIAccessLog/Prod"
    },
    "CanarySettings": {
        "PercentTraffic": 0.0,
        "DeploymentId": "ul73s8",
        "StageVariableOverrides" : [
            "String" : "String"
        ],
        "UseStageCache": false
    },
    "TracingEnabled": false,
    "CreatedDate": "2018-07-11T10:55:18-07:00",
    "LastUpdatedDate": "2020-08-26T11:51:04-07:00",
    "WebAclArn" : "arn:aws:waf-regional:us-west-2:111122223333:webacl/
cb606bd8-5b0b-4f0b-830a-dd304e48a822"
```

```
}
```

AwsApiGatewayV2Api

`AwsApiGatewayV2Api`Objek berisi informasi tentang API versi 2 di Amazon API Gateway.

Berikut ini adalah contoh `AwsApiGatewayV2Api` temuan dalam AWS Security Finding Format (ASFF). Untuk melihat deskripsi `AwsApiGatewayV2Api` atribut, lihat AwsApiGatewayV2 ApiDetails di Referensi AWS Security Hub API.

Contoh

```
"AwsApiGatewayV2Api": {
    "ApiEndpoint": "https://example.us-west-2.amazonaws.com",
    "ApiId": "a1b2c3d4",
    "ApiKeySelectionExpression": "$request.header.x-api-key",
    "CreatedDate": "2020-03-28T00:32:37Z",
   "Description": "ApiGatewayV2 Api",
   "Version": "string",
    "Name": "my-api",
    "ProtocolType": "HTTP",
    "RouteSelectionExpression": "$request.method $request.path",
   "CorsConfiguration": {
        "AllowOrigins": [ "*" ],
        "AllowCredentials": true,
        "ExposeHeaders": [ "string" ],
        "MaxAge": 3000,
        "AllowMethods": [
          "GET",
          "PUT",
          "POST",
          "DELETE",
          "HEAD"
        ],
        "AllowHeaders": [ "*" ]
    }
}
```

AwsApiGatewayV2Tahap

`AwsApiGatewayV2Stage`berisi informasi tentang tahap versi 2 untuk Amazon API Gateway.

Berikut ini adalah contoh `AwsApiGatewayV2Stage` temuan dalam AWS Security Finding Format (ASFF). Untuk melihat deskripsi `AwsApiGatewayV2Stage` atribut, lihat AwsApiGatewayV2 StageDetails di Referensi AWS Security Hub API.

Contoh

```
"AwsApiGatewayV2Stage": {
    "CreatedDate": "2020-04-08T00:36:05Z",
    "Description" : "ApiGatewayV2",
    "DefaultRouteSettings": {
        "DetailedMetricsEnabled": false,
        "LoggingLevel": "INFO",
        "DataTraceEnabled": true,
        "ThrottlingBurstLimit": 100,
        "ThrottlingRateLimit": 50
    },
    "DeploymentId": "x1zwyv",
    "LastUpdatedDate": "2020-04-08T00:36:13Z",
    "RouteSettings": {
        "DetailedMetricsEnabled": false,
        "LoggingLevel": "INFO",
        "DataTraceEnabled": true,
        "ThrottlingBurstLimit": 100,
        "ThrottlingRateLimit": 50
    },
    "StageName": "prod",
    "StageVariables": [
        "function": "my-prod-function"
    ],
    "AccessLogSettings": {
        "Format": "{\"requestId\": \"$context.requestId\", \"extendedRequestId
\": \"$context.extendedRequestId\", \"ownerAccountId\": \"$context.accountId\",
 \"requestAccountId\": \"$context.identity.accountId\", \"callerPrincipal\":
 \"$context.identity.caller\", \"httpMethod\": \"$context.httpMethod\", \"resourcePath
\": \"$context.resourcePath\", \"status\": \"$context.status\", \"requestTime
\": \"$context.requestTime\", \"responseLatencyMs\": \"$context.responseLatency
\", \"errorMessage\": \"$context.error.message\", \"errorResponseType\":
 \"$context.error.responseType\", \"apiId\": \"$context.apiId\", \"awsEndpointRequestId
\": \"$context.awsEndpointRequestId\", \"domainName\": \"$context.domainName\", \"stage
\": \"$context.stage\", \"xrayTraceId\": \"$context.xrayTraceId\", \"sourceIp\":
 \"$context.identity.sourceIp\", \"user\": \"$context.identity.user\", \"userAgent
\": \"$context.identity.userAgent\", \"userArn\": \"$context.identity.userArn\",
 \"integrationLatency\": \"$context.integrationLatency\", \"integrationStatus
```

```
\": \"$context.integrationStatus\", \"authorizerIntegrationLatency\":
 \"$context.authorizer.integrationLatency\" }",
        "DestinationArn": "arn:aws:logs:us-west-2:111122223333:log-
group:SecurityHubAPIAccessLog/Prod"
    },
    "AutoDeploy": false,
    "LastDeploymentStatusMessage": "Message",
    "ApiGatewayManaged": true,
}
```

AwsAppSync

Berikut ini adalah contoh AWS Security Finding Format (ASFF) untuk `AwsAppSync` sumber daya.

AwsAppSyncGraphQLApi

`AwsAppSyncGraphQLApi`menyediakan informasi tentang AWS AppSync GraphQL API, yang merupakan konstruksi tingkat atas untuk aplikasi Anda.

Contoh berikut menunjukkan ASFF untuk `AwsAppSyncGraphQLApi` objek. Untuk melihat deskripsi *`AwsAppSyncGraphQLApi`* atribut, lihat AwsAppSyncGraphQLAPI di Referensi API.AWS Security Hub

Contoh

```
"AwsAppSyncGraphQLApi": {
    "AdditionalAuthenticationProviders": [
    {
     "AuthenticationType": "AWS_LAMBDA",
     "LambdaAuthorizerConfig": {
      "AuthorizerResultTtlInSeconds": 300,
      "AuthorizerUri": "arn:aws:lambda:us-east-1:123456789012:function:mylambdafunc"
     }
    },
    {
     "AuthenticationType": "AWS_IAM"
    }
    ],
    "ApiId": "021345abcdef6789",
    "Arn": "arn:aws:appsync:eu-central-1:123456789012:apis/021345abcdef6789",
    "AuthenticationType": "API_KEY",
    "Id": "021345abcdef6789",
    "LogConfig": {
```

```
     "CloudWatchLogsRoleArn": "arn:aws:iam::123456789012:role/service-role/appsync-
graphqlapi-logs-eu-central-1",
     "ExcludeVerboseContent": true,
     "FieldLogLevel": "ALL"
    },
    "Name": "My AppSync App",
    "XrayEnabled": true,
}
```

AwsAthena

Berikut ini adalah contoh AWS Security Finding Format (ASFF) untuk `AwsAthena` sumber daya.

AwsAthenaWorkGroup

`AwsAthenaWorkGroup`memberikan informasi tentang workgroup Amazon Athena. Workgroup membantu Anda memisahkan pengguna, tim, aplikasi, atau beban kerja. Ini juga membantu Anda menetapkan batasan pada pemrosesan data dan melacak biaya.

Contoh berikut menunjukkan ASFF untuk `AwsAthenaWorkGroup` objek. Untuk melihat deskripsi `AwsAthenaWorkGroup` atribut, lihat AwsAthenaWorkGroupdi Referensi AWS Security Hub API.

Contoh

```
"AwsAthenaWorkGroup": {
    "Description": "My workgroup for prod workloads",
    "Name": "MyWorkgroup",
    "WorkgroupConfiguration" {
        "ResultConfiguration": {
            "EncryptionConfiguration": {
                "EncryptionOption": "SSE_KMS",
                "KmsKey": "arn:aws:kms:us-east-1:123456789012:key/a1b2c3d4-5678-90ab-
cdef-EXAMPLE11111"
            }
        }
    },
        "State": "ENABLED"
}
```

AwsAutoScaling

Berikut ini adalah contoh Format Pencarian AWS Keamanan untuk `AwsAutoScaling` sumber daya.

AwsAutoScalingAutoScalingGroup

`AwsAutoScalingAutoScalingGroup`Objek memberikan rincian tentang grup penskalaan otomatis.

Berikut ini adalah contoh `AwsAutoScalingAutoScalingGroup` temuan dalam AWS Security Finding Format (ASFF). Untuk melihat deskripsi `AwsAutoScalingAutoScalingGroup` atribut, lihat AwsAutoScalingAutoScalingGroupDetailsdi Referensi AWS Security Hub API.

Contoh

```
"AwsAutoScalingAutoScalingGroup": {
        "CreatedTime": "2017-10-17T14:47:11Z",
        "HealthCheckGracePeriod": 300,
        "HealthCheckType": "EC2",
        "LaunchConfigurationName": "mylaunchconf",
        "LoadBalancerNames": [],
        "LaunchTemplate": {
            "LaunchTemplateId": "string",
            "LaunchTemplateName": "string",
            "Version": "string"
        },
        "MixedInstancesPolicy": {
            "InstancesDistribution": {
                "OnDemandAllocationStrategy": "prioritized",
                "OnDemandBaseCapacity": number,
                "OnDemandPercentageAboveBaseCapacity": number,
                "SpotAllocationStrategy": "lowest-price",
                "SpotInstancePools": number,
                "SpotMaxPrice": "string"
            },
            "LaunchTemplate": {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateId": "string",
                    "LaunchTemplateName": "string",
                    "Version": "string"
                 },
                "CapacityRebalance": true,
                "Overrides": [
                    {
                       "InstanceType": "string",
                       "WeightedCapacity": "string"
                    }
```

```
                ]
            }
        }
    }
}
```

AwsAutoScalingLaunchConfiguration

`AwsAutoScalingLaunchConfiguration`Objek memberikan rincian tentang konfigurasi peluncuran.

Berikut ini adalah contoh `AwsAutoScalingLaunchConfiguration` temuan dalam AWS Security Finding Format (ASFF).

Untuk melihat deskripsi `AwsAutoScalingLaunchConfiguration` atribut, lihat AwsAutoScalingLaunchConfigurationDetailsdi Referensi AWS Security Hub API.

Contoh

```
AwsAutoScalingLaunchConfiguration: {
    "LaunchConfigurationName": "newtest",
    "ImageId": "ami-058a3739b02263842",
    "KeyName": "55hundredinstance",
    "SecurityGroups": [ "sg-01fce87ad6e019725" ],
    "ClassicLinkVpcSecurityGroups": [],
    "UserData": "...Base64-Encoded user data..."
    "InstanceType": "a1.metal",
    "KernelId": "",
    "RamdiskId": "ari-a51cf9cc",
    "BlockDeviceMappings": [
        {
            "DeviceName": "/dev/sdh",
            "Ebs": {
                "VolumeSize": 30,
                "VolumeType": "gp2",
                "DeleteOnTermination": false,
                "Encrypted": true,
                "SnapshotId": "snap-ffaa1e69",
                "VirtualName": "ephemeral1"
            }
        },
        {
            "DeviceName": "/dev/sdb",
```

```
            "NoDevice": true
        },
        {
            "DeviceName": "/dev/sda1",
            "Ebs": {
                "SnapshotId": "snap-02420cd3d2dea1bc0",
                "VolumeSize": 8,
                "VolumeType": "gp2",
                "DeleteOnTermination": true,
                "Encrypted": false
            }
        },
        {
            "DeviceName": "/dev/sdi",
            "Ebs": {
                "VolumeSize": 20,
                "VolumeType": "gp2",
                "DeleteOnTermination": false,
                "Encrypted": true
            }
        },
        {
            "DeviceName": "/dev/sdc",
            "NoDevice": true
        }
    ],
    "InstanceMonitoring": {
        "Enabled": false
    },
    "CreatedTime": 1620842933453,
    "EbsOptimized": false,
    "AssociatePublicIpAddress": true,
    "SpotPrice": "0.045"
}
```

AwsBackup

Berikut ini adalah contoh Format Pencarian AWS Keamanan untuk `AwsBackup` sumber daya.

AwsBackupBackupPlan

`AwsBackupBackupPlan`Objek memberikan informasi tentang rencana AWS Backup cadangan. Rencana AWS Backup cadangan adalah ekspresi kebijakan yang menentukan kapan dan bagaimana Anda ingin mencadangkan AWS sumber daya Anda.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsBackupBackupPlan` objek. Untuk melihat deskripsi `AwsBackupBackupPlan` atribut, lihat AwsBackupBackupPlandi Referensi AWS Security Hub API.

Contoh

```
"AwsBackupBackupPlan": {
    "BackupPlan": {
     "AdvancedBackupSettings": [{
      "BackupOptions": {
       "WindowsVSS":"enabled"
      },
      "ResourceType":"EC2"
     }],
     "BackupPlanName": "test",
     "BackupPlanRule": [{
      "CompletionWindowMinutes": 10080,
      "CopyActions": [{
       "DestinationBackupVaultArn": "arn:aws:backup:us-east-1:858726136373:backup-
vault:aws/efs/automatic-backup-vault",
       "Lifecycle": {
        "DeleteAfterDays": 365,
        "MoveToColdStorageAfterDays": 30
       }
      }],
      "Lifecycle": {
       "DeleteAfterDays": 35
      },
      "RuleName": "DailyBackups",
      "ScheduleExpression": "cron(0 5 ? * * *)",
      "StartWindowMinutes": 480,
      "TargetBackupVault": "Default"
      },
      {
      "CompletionWindowMinutes": 10080,
      "CopyActions": [{
       "DestinationBackupVaultArn": "arn:aws:backup:us-east-1:858726136373:backup-
vault:aws/efs/automatic-backup-vault",
       "Lifecycle": {
        "DeleteAfterDays": 365,
        "MoveToColdStorageAfterDays": 30
       }
      }],
```

```
      "Lifecycle": {
       "DeleteAfterDays": 35
      },
      "RuleName": "Monthly",
      "ScheduleExpression": "cron(0 5 1 * ? *)",
      "StartWindowMinutes": 480,
      "TargetBackupVault": "Default"
     }]
    },
    "BackupPlanArn": "arn:aws:backup:us-east-1:858726136373:backup-
plan:b6d6b896-590d-4ee1-bf29-c5ccae63f4e7",
    "BackupPlanId": "b6d6b896-590d-4ee1-bf29-c5ccae63f4e7",
    "VersionId": "ZDVjNDIzMjItYTZiNS00NzczLTg4YzctNmExMWM2NjZhY2E1"
}
```

AwsBackupBackupVault

`AwsBackupBackupVault`Objek memberikan informasi tentang brankas AWS Backup cadangan. Brankas AWS Backup cadangan adalah wadah yang menyimpan dan mengatur cadangan Anda.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsBackupBackupVault` objek. Untuk melihat deskripsi `AwsBackupBackupVault` atribut, lihat AwsBackupBackupVaultdi Referensi AWS Security Hub API.

Contoh

```
"AwsBackupBackupVault": {
    "AccessPolicy": {
     "Statement": [{
      "Action": [
       "backup:DeleteBackupVault",
       "backup:DeleteBackupVaultAccessPolicy",
       "backup:DeleteRecoveryPoint",
       "backup:StartCopyJob",
       "backup:StartRestoreJob",
       "backup:UpdateRecoveryPointLifecycle"
      ],
      "Effect": "Deny",
      "Principal": {
       "AWS": "*"
      },
      "Resource": "*"
     }],
```

```
     "Version": "2012-10-17"
    },
    "BackupVaultArn": "arn:aws:backup:us-east-1:123456789012:backup-vault:aws/efs/
automatic-backup-vault",
    "BackupVaultName": "aws/efs/automatic-backup-vault",
    "EncrytionKeyArn": "arn:aws:kms:us-east-1:444455556666:key/72ba68d4-5e43-40b0-
ba38-838bf8d06ca0",
    "Notifications": {
     "BackupVaultEvents": ["BACKUP_JOB_STARTED", "BACKUP_JOB_COMPLETED",
 "COPY_JOB_STARTED"],
     "SNSTopicArn": "arn:aws:sns:us-west-2:111122223333:MyVaultTopic"
    }
}
```

AwsBackupRecoveryPoint

`AwsBackupRecoveryPoint`Objek memberikan informasi tentang AWS Backup cadangan, juga disebut sebagai titik pemulihan. Titik AWS Backup pemulihan mewakili konten sumber daya pada waktu tertentu.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsBackupRecoveryPoint` objek. Untuk melihat deskripsi `AwsBackupBackupVault` atribut, lihat AwsBackupRecoveryPointdi Referensi AWS Security Hub API.

Contoh

```
"AwsBackupRecoveryPoint": {
    "BackupSizeInBytes": 0,
    "BackupVaultName": "aws/efs/automatic-backup-vault",
    "BackupVaultArn": "arn:aws:backup:us-east-1:111122223333:backup-vault:aws/efs/
automatic-backup-vault",
    "CalculatedLifecycle": {
     "DeleteAt": "2021-08-30T06:51:58.271Z",
     "MoveToColdStorageAt": "2020-08-10T06:51:58.271Z"
    },
    "CompletionDate": "2021-07-26T07:21:40.361Z",
    "CreatedBy": {
     "BackupPlanArn": "arn:aws:backup:us-east-1:111122223333:backup-plan:aws/
efs/73d922fb-9312-3a70-99c3-e69367f9fdad",
     "BackupPlanId": "aws/efs/73d922fb-9312-3a70-99c3-e69367f9fdad",
     "BackupPlanVersion": "ZGM4YzY5YjktMWYxNC00ZTBmLWE5MjYtZmU5OWNiZmM5ZjIz",
     "BackupRuleId": "2a600c2-42ad-4196-808e-084923ebfd25"
    },
```

```
    "CreationDate": "2021-07-26T06:51:58.271Z",
    "EncryptionKeyArn": "arn:aws:kms:us-east-1:111122223333:key/72ba68d4-5e43-40b0-
ba38-838bf8d06ca0",
    "IamRoleArn": "arn:aws:iam::111122223333:role/aws-service-role/
backup.amazonaws.com/AWSServiceRoleForBackup",
    "IsEncrypted": true,
    "LastRestoreTime": "2021-07-26T06:51:58.271Z",
    "Lifecycle": {
     "DeleteAfterDays": 35,
     "MoveToColdStorageAfterDays": 15
    },
    "RecoveryPointArn": "arn:aws:backup:us-east-1:111122223333:recovery-point:151a59e4-
f1d5-4587-a7fd-0774c6e91268",
    "ResourceArn": "arn:aws:elasticfilesystem:us-east-1:858726136373:file-system/
fs-15bd31a1",
    "ResourceType": "EFS",
    "SourceBackupVaultArn": "arn:aws:backup:us-east-1:111122223333:backup-vault:aws/
efs/automatic-backup-vault",
    "Status": "COMPLETED",
    "StatusMessage": "Failure message",
    "StorageClass": "WARM"
}
```

AwsCertificateManager

Berikut ini adalah contoh Format Pencarian AWS Keamanan untuk `AwsCertificateManager` sumber daya.

AwsCertificateManagerCertificate

`AwsCertificateManagerCertificate`Objek memberikan rincian tentang sertifikat AWS Certificate Manager (ACM).

Berikut ini adalah contoh `AwsCertificateManagerCertificate` temuan dalam AWS Security Finding Format (ASFF). Untuk melihat deskripsi `AwsCertificateManagerCertificate` atribut, lihat AwsCertificateManagerCertificateDetailsdi Referensi AWS Security Hub API.

Contoh

```
"AwsCertificateManagerCertificate": {
    "CertificateAuthorityArn": "arn:aws:acm:us-west-2:444455556666:certificate-
authority/example",
    "CreatedAt": "2019-05-24T18:12:02.000Z",
```

```
    "DomainName": "example.amazondomains.com",
    "DomainValidationOptions": [
        {
            "DomainName": "example.amazondomains.com",
            "ResourceRecord": {
                "Name": "_1bacb61828d3a1020c40a560ceed08f7.example.amazondomains.com",
                "Type": "CNAME",
                "Value": "_example.acm-validations.aws."
             },
             "ValidationDomain": "example.amazondomains.com",
             "ValidationEmails": [sample_email@sample.com],
             "ValidationMethod": "DNS",
             "ValidationStatus": "SUCCESS"
        }
    ],
    "ExtendedKeyUsages": [
        {
            "Name": "TLS_WEB_SERVER_AUTHENTICATION",
            "OId": "1.3.6.1.5.5.7.3.1"
        },
        {
            "Name": "TLS_WEB_CLIENT_AUTHENTICATION",
            "OId": "1.3.6.1.5.5.7.3.2"
        }
    ],
    "FailureReason": "",
    "ImportedAt": "2018-08-17T00:13:00.000Z",
    "InUseBy": ["arn:aws:amazondomains:us-west-2:444455556666:loadbalancer/example"],
    "IssuedAt": "2020-04-26T00:41:17.000Z",
    "Issuer": "Amazon",
    "KeyAlgorithm": "RSA-1024",
    "KeyUsages": [
        {
            "Name": "DIGITAL_SIGNATURE",
        },
        {
            "Name": "KEY_ENCIPHERMENT",
        }
    ],
    "NotAfter": "2021-05-26T12:00:00.000Z",
    "NotBefore": "2020-04-26T00:00:00.000Z",
    "Options": {
        "CertificateTransparencyLoggingPreference": "ENABLED",
    }
```

```
    "RenewalEligibility": "ELIGIBLE",
    "RenewalSummary": {
        "DomainValidationOptions": [
            {
                "DomainName": "example.amazondomains.com",
                "ResourceRecord": {
                    "Name":
 "_1bacb61828d3a1020c40a560ceed08f7.example.amazondomains.com",
                    "Type": "CNAME",
                    "Value": "_example.acm-validations.aws.com",
                },
                "ValidationDomain": "example.amazondomains.com",
                "ValidationEmails": ["sample_email@sample.com"],
                "ValidationMethod": "DNS",
                "ValidationStatus": "SUCCESS"
            }
        ],
        "RenewalStatus": "SUCCESS",
        "RenewalStatusReason": "",
        "UpdatedAt": "2020-04-26T00:41:35.000Z",
    },
    "Serial": "02:ac:86:b6:07:2f:0a:61:0e:3a:ac:fd:d9:ab:17:1a",
    "SignatureAlgorithm": "SHA256WITHRSA",
    "Status": "ISSUED",
    "Subject": "CN=example.amazondomains.com",
    "SubjectAlternativeNames": ["example.amazondomains.com"],
    "Type": "AMAZON_ISSUED"
}
```

AwsCloudFormation

Berikut ini adalah contoh Format Pencarian AWS Keamanan untuk `AwsCloudFormation` sumber daya.

AwsCloudFormationStack

`AwsCloudFormationStack`Objek memberikan rincian tentang AWS CloudFormation tumpukan yang bersarang sebagai sumber daya dalam template tingkat atas.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsCloudFormationStack` objek. Untuk melihat deskripsi `AwsCloudFormationStack` atribut, lihat AwsCloudFormationStackDetailsdi Referensi AWS Security Hub API.

Contoh


```
"AwsCloudFormationStack": {
 "Capabilities": [
  "CAPABILITY_IAM",
  "CAPABILITY_NAMED_IAM"
 ],
 "CreationTime": "2022-02-18T15:31:53.161Z",
 "Description": "AWS CloudFormation Sample",
 "DisableRollback": true,
 "DriftInformation": {
  "StackDriftStatus": "DRIFTED"
 },
 "EnableTerminationProtection": false,
 "LastUpdatedTime": "2022-02-18T15:31:53.161Z",
 "NotificationArns": [
  "arn:aws:sns:us-east-1:978084797471:sample-sns-cfn"
 ],
 "Outputs": [{
  "Description": "URL for newly created LAMP stack",
  "OutputKey": "WebsiteUrl",
  "OutputValue": "http://ec2-44-193-18-241.compute-1.amazonaws.com"
 }],
 "RoleArn": "arn:aws:iam::012345678910:role/exampleRole",
 "StackId": "arn:aws:cloudformation:us-east-1:978084797471:stack/sample-stack/
e5d9f7e0-90cf-11ec-88c6-12ac1f91724b",
 "StackName": "sample-stack",
 "StackStatus": "CREATE_COMPLETE",
 "StackStatusReason": "Success",
 "TimeoutInMinutes": 1
}
```


AwsCloudFront

Berikut ini adalah contoh Format Pencarian AWS Keamanan untuk `AwsCloudFront` sumber daya.

AwsCloudFrontDistribution

`AwsCloudFrontDistribution`Objek memberikan rincian tentang konfigurasi CloudFront distribusi Amazon.

Berikut ini adalah contoh `AwsCloudFrontDistribution` temuan dalam AWS Security Finding Format (ASFF). Untuk melihat deskripsi `AwsCloudFrontDistribution` atribut, lihat AwsCloudFrontDistributionDetailsdi Referensi AWS Security Hub API.

Contoh

```
"AwsCloudFrontDistribution": {
    "CacheBehaviors": {
        "Items": [
            {
               "ViewerProtocolPolicy": "https-only"
            }
         ]
    },
    "DefaultCacheBehavior": {
         "ViewerProtocolPolicy": "https-only"
    },
    "DefaultRootObject": "index.html",
    "DomainName": "d2wkuj2w9l34gt.cloudfront.net",
    "Etag": "E37HOT42DHPVYH",
    "LastModifiedTime": "2015-08-31T21:11:29.093Z",
    "Logging": {
         "Bucket": "myawslogbucket.s3.amazonaws.com",
         "Enabled": false,
         "IncludeCookies": false,
         "Prefix": "myawslog/"
     },
     "OriginGroups": {
          "Items": [
              {
                 "FailoverCriteria": {
                     "StatusCodes": {
                          "Items": [
                              200,
                              301,
                              404
                          ]
                          "Quantity": 3
                      }
                 }
              }
           ]
     },
```

```
     "Origins": {
           "Items": [
               {
                  "CustomOriginConfig": {
                      "HttpPort": 80,
                      "HttpsPort": 443,
                      "OriginKeepaliveTimeout": 60,
                      "OriginProtocolPolicy": "match-viewer",
                      "OriginReadTimeout": 30,
                      "OriginSslProtocols": {
                        "Items": ["SSLv3", "TLSv1"],
                        "Quantity": 2
                      }
                  }
               },
           ]
     },
                  "DomainName": "my-bucket.s3.amazonaws.com",
                  "Id": "my-origin",
                  "OriginPath": "/production",
                  "S3OriginConfig": {
                      "OriginAccessIdentity": "origin-access-identity/cloudfront/
E2YFS67H6VB6E4"
                  }
           ]
     },
     "Status": "Deployed",
     "ViewerCertificate": {
            "AcmCertificateArn": "arn:aws:acm::123456789012:AcmCertificateArn",
            "Certificate": "ASCAJRRE5XYF52TKRY5M4",
            "CertificateSource": "iam",
            "CloudFrontDefaultCertificate": true,
            "IamCertificateId": "ASCAJRRE5XYF52TKRY5M4",
            "MinimumProtocolVersion": "TLSv1.2_2021",
            "SslSupportMethod": "sni-only"
      },
      "WebAclId": "waf-1234567890"
}
```

AwsCloudTrail

Berikut ini adalah contoh Format Pencarian AWS Keamanan untuk `AwsCloudTrail` sumber daya.

AwsCloudTrailTrail

`AwsCloudTrailTrail`Objek tersebut memberikan detail tentang AWS CloudTrail jejak.

Berikut ini adalah contoh `AwsCloudTrailTrail` temuan dalam AWS Security Finding Format (ASFF). Untuk melihat deskripsi `AwsCloudTrailTrail` atribut, lihat AwsCloudTrailTrailDetailsdi Referensi AWS Security Hub API.

Contoh

```
"AwsCloudTrailTrail": {
    "CloudWatchLogsLogGroupArn": "arn:aws:logs:us-west-2:123456789012:log-
group:CloudTrail/regression:*",
    "CloudWatchLogsRoleArn": "arn:aws:iam::866482105055:role/
CloudTrail_CloudWatchLogs",
    "HasCustomEventSelectors": true,
    "HomeRegion": "us-west-2",
    "IncludeGlobalServiceEvents": true,
    "IsMultiRegionTrail": true,
    "IsOrganizationTrail": false,
    "KmsKeyId": "kmsKeyId",
    "LogFileValidationEnabled": true,
    "Name": "regression-trail",
    "S3BucketName": "cloudtrail-bucket",
    "S3KeyPrefix": "s3KeyPrefix",
    "SnsTopicArn": "arn:aws:sns:us-east-2:123456789012:MyTopic",
    "SnsTopicName": "snsTopicName",
    "TrailArn": "arn:aws:cloudtrail:us-west-2:123456789012:trail"
}
```

AwsCloudWatch

Berikut ini adalah contoh Format Pencarian AWS Keamanan untuk `AwsCloudWatch` sumber daya.

AwsCloudWatchAlarm

`AwsCloudWatchAlarm`Objek ini memberikan detail tentang CloudWatch alarm Amazon yang menonton metrik atau melakukan tindakan saat alarm berubah status.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsCloudWatchAlarm` objek. Untuk melihat deskripsi `AwsCloudWatchAlarm` atribut, lihat AwsCloudWatchAlarmDetailsdi Referensi AWS Security Hub API.

Contoh

```
"AwsCloudWatchAlarm": {
 "ActonsEnabled": true,
 "AlarmActions": [
  "arn:aws:automate:region:ec2:stop",
  "arn:aws:automate:region:ec2:terminate"
 ],
 "AlarmArn": "arn:aws:cloudwatch:us-west-2:012345678910:alarm:sampleAlarm",
 "AlarmConfigurationUpdatedTimestamp": "2022-02-18T15:31:53.161Z",
 "AlarmDescription": "Alarm Example",
 "AlarmName": "Example",
 "ComparisonOperator": "GreaterThanOrEqualToThreshold",
 "DatapointsToAlarm": 1,
 "Dimensions": [{
  "Name": "InstanceId",
  "Value": "i-1234567890abcdef0"
 }],
 "EvaluateLowSampleCountPercentile": "evaluate",
 "EvaluationPeriods": 1,
 "ExtendedStatistic": "p99.9",
 "InsufficientDataActions": [
  "arn:aws:automate:region:ec2:stop"
 ],
 "MetricName": "Sample Metric",
 "Namespace": "YourNamespace",
 "OkActions": [
  "arn:aws:swf:region:account-id:action/actions/AWS_EC2.InstanceId.Stop/1.0"
 ],
 "Period": 1,
 "Statistic": "SampleCount",
 "Threshold": 12.3,
 "ThresholdMetricId": "t1",
 "TreatMissingData": "notBreaching",
 "Unit": "Kilobytes/Second"
}
```

AwsCodeBuild

Berikut ini adalah contoh Format Pencarian AWS Keamanan untuk `AwsCodeBuild` sumber daya.

AwsCodeBuildProject

`AwsCodeBuildProject`Objek memberikan informasi tentang suatu AWS CodeBuild proyek.

Berikut ini adalah contoh `AwsCodeBuildProject` temuan dalam AWS Security Finding Format (ASFF). Untuk melihat deskripsi `AwsCodeBuildProject` atribut, lihat AwsCodeBuildProjectDetailsdi Referensi AWS Security Hub API.

Contoh

```
"AwsCodeBuildProject": {
   "Artifacts": [
      {
          "ArtifactIdentifier": "string",
          "EncryptionDisabled": boolean,
          "Location": "string",
          "Name": "string",
          "NamespaceType": "string",
          "OverrideArtifactName": boolean,
          "Packaging": "string",
          "Path": "string",
          "Type": "string"
       }
   ],
   "SecondaryArtifacts": [
      {
          "ArtifactIdentifier": "string",
          "EncryptionDisabled": boolean,
          "Location": "string",
          "Name": "string",
          "NamespaceType": "string",
          "OverrideArtifactName": boolean,
          "Packaging": "string",
          "Path": "string",
          "Type": "string"
       }
   ],
   "EncryptionKey": "string",
   "Certificate": "string",
   "Environment": {
      "Certificate": "string",
      "EnvironmentVariables": [
           {
                "Name": "string",
                "Type": "string",
                "Value": "string"
           }
```

```
      ],
   "ImagePullCredentialsType": "string",
   "PrivilegedMode": boolean,
   "RegistryCredential": {
       "Credential": "string",
       "CredentialProvider": "string"
   },
   "Type": "string"
   },
   "LogsConfig": {
        "CloudWatchLogs": {
             "GroupName": "string",
             "Status": "string",
             "StreamName": "string"
        },
        "S3Logs": {
             "EncryptionDisabled": boolean,
             "Location": "string",
             "Status": "string"
        }
   },
   "Name": "string",
   "ServiceRole": "string",
   "Source": {
        "Type": "string",
        "Location": "string",
        "GitCloneDepth": integer
   },
   "VpcConfig": {
        "VpcId": "string",
        "Subnets": ["string"],
        "SecurityGroupIds": ["string"]
   }
}
```

AwsDms

Berikut ini adalah contoh Format Pencarian AWS Keamanan untuk `AwsDms` sumber daya.

AwsDmsEndpoint

`AwsDmsEndpoint`Objek memberikan informasi tentang titik akhir AWS Database Migration Service (AWS DMS). Endpoint menyediakan koneksi, tipe penyimpanan data, dan informasi lokasi tentang penyimpanan data Anda.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsDmsEndpoint` objek. Untuk melihat deskripsi `AwsDmsEndpoint` atribut, lihat AwsDmsEndpointDetailsdi Referensi AWS Security Hub API.

Contoh

```
"AwsDmsEndpoint": {
    "CertificateArn": "arn:aws:dms:us-
east-1:123456789012:cert:EXAMPLEIGDURVZGVJQZDPWJ5A7F2YDJVSMTBWFI",
    "DatabaseName": "Test",
    "EndpointArn": "arn:aws:dms:us-
east-1:123456789012:endpoint:EXAMPLEQB3CZY33F7XV253NAJVBNPK6MJQVFVQA",
    "EndpointIdentifier": "target-db",
    "EndpointType": "TARGET",
    "EngineName": "mariadb",
    "KmsKeyId": "arn:aws:kms:us-east-1:123456789012:key/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111",
    "Port": 3306,
    "ServerName": "target-db.exampletafyu.us-east-1.rds.amazonaws.com",
    "SslMode": "verify-ca",
    "Username": "admin"
}
```

AwsDmsReplicationInstance

`AwsDmsReplicationInstance`Objek memberikan informasi tentang contoh replikasi AWS Database Migration Service (AWS DMS). DMS menggunakan contoh replikasi untuk terhubung ke penyimpanan data sumber Anda, membaca data sumber, dan memformat data untuk konsumsi oleh penyimpanan data target.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsDmsReplicationInstance` objek. Untuk melihat deskripsi `AwsDmsReplicationInstance` atribut, lihat AwsDmsReplicationInstanceDetailsdi Referensi AWS Security Hub API.

Contoh

```
"AwsDmsReplicationInstance": {
    "AllocatedStorage": 50,
    "AutoMinorVersionUpgrade": true,
    "AvailabilityZone": "us-east-1b",
    "EngineVersion": "3.5.1",
```

```
    "KmsKeyId": "arn:aws:kms:us-east-1:123456789012:key/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111",
    "MultiAZ": false,
    "PreferredMaintenanceWindow": "wed:08:08-wed:08:38",
    "PubliclyAccessible": true,
    "ReplicationInstanceClass": "dms.c5.xlarge",
    "ReplicationInstanceIdentifier": "second-replication-instance",
    "ReplicationSubnetGroup": {
        "ReplicationSubnetGroupIdentifier": "default-vpc-2344f44f"
    },
    "VpcSecurityGroups": [
        {
            "VpcSecurityGroupId": "sg-003a34e205138138b"
        }
    ]
}
```

AwsDmsReplicationTask

`AwsDmsReplicationTask`Objek memberikan informasi tentang tugas replikasi AWS Database Migration Service (AWS DMS). Tugas replikasi memindahkan sekumpulan data dari titik akhir sumber ke titik akhir target.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsDmsReplicationInstance` objek. Untuk melihat deskripsi `AwsDmsReplicationInstance` atribut, lihat AwsDmsReplicationInstancedi Referensi AWS Security Hub API.

Contoh

```
"AwsDmsReplicationTask": {
    "CdcStartPosition": "2023-08-28T14:26:22",
    "Id": "arn:aws:dms:us-
east-1:123456789012:task:YDYUOHZIXWKQSUCBMUCQCNY44SJW74VJNB5DFWQ",
    "MigrationType": "cdc",
    "ReplicationInstanceArn": "arn:aws:dms:us-
east-1:123456789012:rep:T7V6RFDP23PYQWUL26N3PF5REKML4YOUGIMYJUI",
    "ReplicationTaskIdentifier": "test-task",
    "ReplicationTaskSettings": "{\"Logging\":{\"EnableLogging\":false,
\"EnableLogContext\":false,\"LogComponents\":[{\"Severity\":\"LOGGER_SEVERITY_DEFAULT
\",\"Id\":\"TRANSFORMATION\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",
\"Id\":\"SOURCE_UNLOAD\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":
\"IO\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"TARGET_LOAD\"},
{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"PERFORMANCE\"},{\"Severity
```

\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"SOURCE_CAPTURE\"},{\"Severity\":
\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"SORTER\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT
\",\"Id\":\"REST_SERVER\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id
\":\"VALIDATOR_EXT\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":
\"TARGET_APPLY\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"TASK_MANAGER
\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"TABLES_MANAGER\"},
{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"METADATA_MANAGER\"},
{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"FILE_FACTORY\"},{\"Severity\":
\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"COMMON\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT
\",\"Id\":\"ADDONS\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"DATA_STRUCTURE
\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"COMMUNICATION\"},{\"Severity
\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"FILE_TRANSFER\"}],\"CloudWatchLogGroup
\":null,\"CloudWatchLogStream\":null},\"StreamBufferSettings\":{\"StreamBufferCount
\":3,\"CtrlStreamBufferSizeInMB\":5,\"StreamBufferSizeInMB\":8},\"ErrorBehavior
\":{\"FailOnNoTablesCaptured\":true,\"ApplyErrorUpdatePolicy\":\"LOG_ERROR\",
\"FailOnTransactionConsistencyBreached\":false,\"RecoverableErrorThrottlingMax\":1800,
\"DataErrorEscalationPolicy\":\"SUSPEND_TABLE\",\"ApplyErrorEscalationCount\":0,
\"RecoverableErrorStopRetryAfterThrottlingMax\":true,\"RecoverableErrorThrottling
\":true,\"ApplyErrorFailOnTruncationDdl\":false,\"DataTruncationErrorPolicy\":
\"LOG_ERROR\",\"ApplyErrorInsertPolicy\":\"LOG_ERROR\",\"EventErrorPolicy\":
\"IGNORE\",\"ApplyErrorEscalationPolicy\":\"LOG_ERROR\",\"RecoverableErrorCount
\":-1,\"DataErrorEscalationCount\":0,\"TableErrorEscalationPolicy\":\"STOP_TASK
\",\"RecoverableErrorInterval\":5,\"ApplyErrorDeletePolicy\":\"IGNORE_RECORD\",
\"TableErrorEscalationCount\":0,\"FullLoadIgnoreConflicts\":true,\"DataErrorPolicy
\":\"LOG_ERROR\",\"TableErrorPolicy\":\"SUSPEND_TABLE\"},\"TTSettings
\":{\"TTS3Settings\":null,\"TTRecordSettings\":null,\"EnableTT\":false},
\"FullLoadSettings\":{\"CommitRate\":10000,\"StopTaskCachedChangesApplied
\":false,\"StopTaskCachedChangesNotApplied\":false,\"MaxFullLoadSubTasks
\":8,\"TransactionConsistencyTimeout\":600,\"CreatePkAfterFullLoad\":false,
\"TargetTablePrepMode\":\"DO_NOTHING\"},\"TargetMetadata\":{\"ParallelApplyBufferSize
\":0,\"ParallelApplyQueuesPerThread\":0,\"ParallelApplyThreads\":0,\"TargetSchema
\":\"\",\"InlineLobMaxSize\":0,\"ParallelLoadQueuesPerThread\":0,\"SupportLobs
\":true,\"LobChunkSize\":64,\"TaskRecoveryTableEnabled\":false,\"ParallelLoadThreads
\":0,\"LobMaxSize\":0,\"BatchApplyEnabled\":false,\"FullLobMode\":true,
\"LimitedSizeLobMode\":false,\"LoadMaxFileSize\":0,\"ParallelLoadBufferSize\":0},
\"BeforeImageSettings\":null,\"ControlTablesSettings\":{\"historyTimeslotInMinutes
\":5,\"HistoryTimeslotInMinutes\":5,\"StatusTableEnabled\":false,
\"SuspendedTablesTableEnabled\":false,\"HistoryTableEnabled\":false,\"ControlSchema
\":\"\",\"FullLoadExceptionTableEnabled\":false},\"LoopbackPreventionSettings
\":null,\"CharacterSetSettings\":null,\"FailTaskWhenCleanTaskResourceFailed
\":false,\"ChangeProcessingTuning\":{\"StatementCacheSize\":50,\"CommitTimeout
\":1,\"BatchApplyPreserveTransaction\":true,\"BatchApplyTimeoutMin\":1,
\"BatchSplitSize\":0,\"BatchApplyTimeoutMax\":30,\"MinTransactionSize\":1000,
\"MemoryKeepTime\":60,\"BatchApplyMemoryLimit\":500,\"MemoryLimitTotal\":1024},

```
\"ChangeProcessingDdlHandlingPolicy\":{\"HandleSourceTableDropped\":true,
\"HandleSourceTableTruncated\":true,\"HandleSourceTableAltered\":true},
\"PostProcessingRules\":null}",
    "SourceEndpointArn": "arn:aws:dms:us-
east-1:123456789012:endpoint:TZPWV2VCXEGHYOKVKRNHAKJ4Q3RUXACNGFGYWRI",
    "TableMappings": "{\"rules\":[{\"rule-type\":\"selection\",\"rule-id\":
\"969761702\",\"rule-name\":\"969761702\",\"object-locator\":{\"schema-name\":\"%table
\",\"table-name\":\"%example\"},\"rule-action\":\"exclude\",\"filters\":[]}]}",
    "TargetEndpointArn": "arn:aws:dms:us-
east-1:123456789012:endpoint:ABR8LBOQB3CZY33F7XV253NAJVBNPK6MJQVFVQA"
}
```

AwsDynamoDB

Berikut ini adalah contoh Format Pencarian AWS Keamanan untuk `AwsDynamoDB` sumber daya.

AwsDynamoDbTable

`AwsDynamoDbTable`Objek memberikan rincian tentang tabel Amazon DynamoDB.

Berikut ini adalah contoh `AwsDynamoDbTable` temuan dalam AWS Security Finding Format (ASFF). Untuk melihat deskripsi `AwsDynamoDbTable` atribut, lihat AwsDynamoDbTableDetailsdi Referensi AWS Security Hub API.

Contoh

```
"AwsDynamoDbTable": {
    "AttributeDefinitions": [
        {
            "AttributeName": "attribute1",
            "AttributeType": "value 1"
        },
        {
            "AttributeName": "attribute2",
            "AttributeType": "value 2"
        },
        {
            "AttributeName": "attribute3",
            "AttributeType": "value 3"
        }
    ],
    "BillingModeSummary": {
        "BillingMode": "PAY_PER_REQUEST",
        "LastUpdateToPayPerRequestDateTime": "2019-12-03T15:23:10.323Z"
```

```
    },
    "CreationDateTime": "2019-12-03T15:23:10.248Z",
    "DeletionProtectionEnabled": true,
    "GlobalSecondaryIndexes": [
        {
            "Backfilling": false,
            "IndexArn": "arn:aws:dynamodb:us-west-2:111122223333:table/exampleTable/
index/exampleIndex",
            "IndexName": "standardsControlArnIndex",
            "IndexSizeBytes": 1862513,
            "IndexStatus": "ACTIVE",
            "ItemCount": 20,
            "KeySchema": [
                {
                    "AttributeName": "City",
                    "KeyType": "HASH"
                },
                {
                    "AttributeName": "Date",
                    "KeyType": "RANGE"
                }
            ],
            "Projection": {
                "NonKeyAttributes": ["predictorName"],
                "ProjectionType": "ALL"
            },
            "ProvisionedThroughput": {
                "LastIncreaseDateTime": "2019-03-14T13:21:00.399Z",
                "LastDecreaseDateTime": "2019-03-14T12:47:35.193Z",
                "NumberOfDecreasesToday": 0,
                "ReadCapacityUnits": 100,
                "WriteCapacityUnits": 50
            },
        }
   ],
   "GlobalTableVersion": "V1",
   "ItemCount": 2705,
   "KeySchema": [
        {
            "AttributeName": "zipcode",
            "KeyType": "HASH"
        }
    ],
```

```
    "LatestStreamArn": "arn:aws:dynamodb:us-west-2:111122223333:table/exampleTable/
stream/2019-12-03T23:23:10.248",
    "LatestStreamLabel": "2019-12-03T23:23:10.248",
    "LocalSecondaryIndexes": [
        {
            "IndexArn": "arn:aws:dynamodb:us-east-1:111122223333:table/exampleGroup/
index/exampleId",
            "IndexName": "CITY_DATE_INDEX_NAME",
            "KeySchema": [
                {
                    "AttributeName": "zipcode",
                    "KeyType": "HASH"
                }
            ],
            "Projection": {
                "NonKeyAttributes": ["predictorName"],
                "ProjectionType": "ALL"
            },
        }
    ],
    "ProvisionedThroughput": {
        "LastIncreaseDateTime": "2019-03-14T13:21:00.399Z",
        "LastDecreaseDateTime": "2019-03-14T12:47:35.193Z",
        "NumberOfDecreasesToday": 0,
        "ReadCapacityUnits": 100,
        "WriteCapacityUnits": 50
    },
    "Replicas": [
        {
            "GlobalSecondaryIndexes":[
                {
                    "IndexName": "CITY_DATE_INDEX_NAME",
                    "ProvisionedThroughputOverride": {
                        "ReadCapacityUnits": 10
                    }
                }
            ],
            "KmsMasterKeyId" : "KmsKeyId"
            "ProvisionedThroughputOverride": {
                "ReadCapacityUnits": 10
            },
            "RegionName": "regionName",
            "ReplicaStatus": "CREATING",
            "ReplicaStatusDescription": "replicaStatusDescription"
```

```
        }
    ],
    "RestoreSummary" : {
        "SourceBackupArn": "arn:aws:dynamodb:us-west-2:111122223333:table/exampleTable/
backup/backup1",
        "SourceTableArn": "arn:aws:dynamodb:us-west-2:111122223333:table/exampleTable",
        "RestoreDateTime": "2020-06-22T17:40:12.322Z",
        "RestoreInProgress": true
    },
    "SseDescription": {
        "InaccessibleEncryptionDateTime": "2018-01-26T23:50:05.000Z",
        "Status": "ENABLED",
        "SseType": "KMS",
        "KmsMasterKeyArn": "arn:aws:kms:us-east-1:111122223333:key/key1"
    },
    "StreamSpecification" : {
        "StreamEnabled": true,
        "StreamViewType": "NEW_IMAGE"
    },
    "TableId": "example-table-id-1",
    "TableName": "example-table",
    "TableSizeBytes": 1862513,
    "TableStatus": "ACTIVE"
}
```

AwsEc2

Berikut ini adalah contoh Format Pencarian AWS Keamanan untuk `AwsEc2` sumber daya.

AwsEc2ClientVpnEndpoint

`AwsEc2ClientVpnEndpoint`Objek memberikan informasi tentang AWS Client VPN titik akhir. Titik akhir Client VPN adalah sumber daya yang Anda buat dan konfigurasikan untuk mengaktifkan dan mengelola sesi VPN klien. Ini adalah titik terminasi untuk semua sesi VPN klien.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsEc2ClientVpnEndpoint` objek. Untuk melihat deskripsi `AwsEc2ClientVpnEndpoint` atribut, lihat AwsEc2 ClientVpnEndpointDetails di Referensi AWS Security Hub API.

Contoh

```
"AwsEc2ClientVpnEndpoint": {
```

```
    "AuthenticationOptions": [
        {
            "MutualAuthentication": {
                "ClientRootCertificateChainArn": "arn:aws:acm:us-
east-1:123456789012:certificate/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
            },
            "Type": "certificate-authentication"
        }
    ],
    "ClientCidrBlock": "10.0.0.0/22",
    "ClientConnectOptions": {
        "Enabled": false
    },
    "ClientLoginBannerOptions": {
        "Enabled": false
    },
    "ClientVpnEndpointId": "cvpn-endpoint-00c5d11fc4729f2a5",
    "ConnectionLogOptions": {
        "Enabled": false
    },
    "Description": "test",
    "DnsServer": ["10.0.0.0"],
    "ServerCertificateArn": "arn:aws:acm:us-east-1:123456789012:certificate/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "SecurityGroupIdSet": [
        "sg-0f7a177b82b443691"
    ],
    "SelfServicePortalUrl": "https://self-service.clientvpn.amazonaws.com/endpoints/
cvpn-endpoint-00c5d11fc4729f2a5",
    "SessionTimeoutHours": 24,
    "SplitTunnel": false,
    "TransportProtocol": "udp",
    "VpcId": "vpc-1a2b3c4d5e6f1a2b3",
    "VpnPort": 443
}
```

AwsEc2Eip

`AwsEc2Eip`Objek memberikan informasi tentang alamat IP Elastis.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsEc2Eip` objek. Untuk melihat deskripsi `AwsEc2Eip` atribut, lihat AwsEc2 EipDetails di Referensi AWS Security Hub API.

Contoh

```
"AwsEc2Eip": {
    "InstanceId": "instance1",
    "PublicIp": "192.0.2.04",
    "AllocationId": "eipalloc-example-id-1",
    "AssociationId": "eipassoc-example-id-1",
    "Domain": "vpc",
    "PublicIpv4Pool": "anycompany",
    "NetworkBorderGroup": "eu-central-1",
    "NetworkInterfaceId": "eni-example-id-1",
    "NetworkInterfaceOwnerId": "777788889999",
    "PrivateIpAddress": "192.0.2.03"
}
```

AwsEc2Instance

`AwsEc2Instance`Objek memberikan detail tentang instans Amazon EC2.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsEc2Instance` objek. Untuk melihat deskripsi `AwsEc2Instance` atribut, lihat AwsEc2 InstanceDetails di Referensi AWS Security Hub API.

Contoh

```
"AwsEc2Instance": {
    "IamInstanceProfileArn": "arn:aws:iam::123456789012:instance-profile/AdminRole",
    "ImageId": "ami-1234",
    "IpV4Addresses": [ "1.1.1.1" ],
    "IpV6Addresses": [ "2001:db8:1234:1a2b::123" ],
    "KeyName": "my_keypair",
    "LaunchedAt": "2018-05-08T16:46:19.000Z",
    "MetadataOptions": {
     "HttpEndpoint": "enabled",
     "HttpProtocolIpv6": "enabled",
     "HttpPutResponseHopLimit": 1,
     "HttpTokens": "optional",
     "InstanceMetadataTags": "disabled",
    },
    "Monitoring": {
     "State": "disabled"
    },
    "NetworkInterfaces": [
      {
         "NetworkInterfaceId": "eni-e5aa89a3"
```

```
      }
    ],
    "SubnetId": "subnet-123",
    "Type": "i3.xlarge",
    "VpcId": "vpc-123"
}
```

AwsEc2LaunchTemplate

`AwsEc2LaunchTemplate`Objek berisi detail tentang template peluncuran Amazon Elastic Compute Cloud yang menentukan informasi konfigurasi instans.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsEc2LaunchTemplate` objek. Untuk melihat deskripsi `AwsEc2LaunchTemplate` atribut, lihat AwsEc2 LaunchTemplateDetails di Referensi AWS Security Hub API.

Contoh

```
"AwsEc2LaunchTemplate": {
    "DefaultVersionNumber": "1",
    "ElasticGpuSpecifications": ["string"],
    "ElasticInferenceAccelerators": ["string"],
    "Id": "lt-0a16e9802800bdd85",
    "ImageId": "ami-0d5eff06f840b45e9",
    "LatestVersionNumber": "1",
    "LaunchTemplateData": {
     "BlockDeviceMappings": [{
      "DeviceName": "/dev/xvda",
      "Ebs": {
       "DeleteonTermination": true,
       "Encrypted": true,
       "SnapshotId": "snap-01047646ec075f543",
       "VolumeSize": 8,
       "VolumeType:" "gp2"
      }
     }],
     "MetadataOptions": {
      "HttpTokens": "enabled",
      "HttpPutResponseHopLimit" : 1
     },
     "Monitoring": {
      "Enabled": true,
     "NetworkInterfaces": [{
```

```
      "AssociatePublicIpAddress" : true,
     }],
    "LaunchTemplateName": "string",
    "LicenseSpecifications": ["string"],
    "SecurityGroupIds": ["sg-01fce87ad6e019725"],
    "SecurityGroups": ["string"],
    "TagSpecifications": ["string"]
}
```

AwsEc2NetworkAcl

`AwsEc2NetworkAcl`Objek berisi rincian tentang daftar kontrol akses jaringan Amazon EC2 (ACL).

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsEc2NetworkAcl` objek. Untuk melihat deskripsi `AwsEc2NetworkAcl` atribut, lihat AwsEc2 NetworkAclDetails di Referensi AWS Security Hub API.

Contoh

```
"AwsEc2NetworkAcl": {
    "IsDefault": false,
    "NetworkAclId": "acl-1234567890abcdef0",
    "OwnerId": "123456789012",
    "VpcId": "vpc-1234abcd",
    "Associations": [{
        "NetworkAclAssociationId": "aclassoc-abcd1234",
        "NetworkAclId": "acl-021345abcdef6789",
        "SubnetId": "subnet-abcd1234"
   }],
   "Entries": [{
        "CidrBlock": "10.24.34.0/23",
        "Egress": true,
        "IcmpTypeCode": {
            "Code": 10,
            "Type": 30
        },
        "Ipv6CidrBlock": "2001:DB8::/32",
        "PortRange": {
            "From": 20,
            "To": 40
        },
        "Protocol": "tcp",
        "RuleAction": "allow",
```

```
        "RuleNumber": 100
    }]
}
```

AwsEc2NetworkInterface

`AwsEc2NetworkInterface`Objek menyediakan informasi tentang antarmuka jaringan Amazon EC2.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsEc2NetworkInterface` objek. Untuk melihat deskripsi `AwsEc2NetworkInterface` atribut, lihat AwsEc2 NetworkInterfaceDetails di Referensi AWS Security Hub API.

Contoh

```
"AwsEc2NetworkInterface": {
    "Attachment": {
        "AttachTime": "2019-01-01T03:03:21Z",
        "AttachmentId": "eni-attach-43348162",
        "DeleteOnTermination": true,
        "DeviceIndex": 123,
        "InstanceId": "i-1234567890abcdef0",
        "InstanceOwnerId": "123456789012",
        "Status": 'ATTACHED'
    },
    "SecurityGroups": [
        {
            "GroupName": "my-security-group",
            "GroupId": "sg-903004f8"
        },
    ],
    "NetworkInterfaceId": 'eni-686ea200',
    "SourceDestCheck": false
}
```

AwsEc2RouteTable

`AwsEc2RouteTable`Objek memberikan informasi tentang tabel rute Amazon EC2.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsEc2RouteTable` objek. Untuk melihat deskripsi `AwsEc2RouteTable` atribut, lihat AwsEc2 RouteTableDetails di Referensi AWS Security Hub API.

Contoh

```
"AwsEc2RouteTable": {
    "AssociationSet": [{
     "AssociationSet": {
      "State": "associated"
        },
     "Main": true,
     "RouteTableAssociationId": "rtbassoc-08e706c45de9f7512",
     "RouteTableId": "rtb-0a59bde9cf2548e34",
    }],
    "PropogatingVgwSet": [],
    "RouteTableId": "rtb-0a59bde9cf2548e34",
    "RouteSet": [
     {
      "DestinationCidrBlock": "10.24.34.0/23",
      "GatewayId": "local",
      "Origin": "CreateRouteTable",
      "State": "active"
     },
     {
      "DestinationCidrBlock": "10.24.34.0/24",
      "GatewayId": "igw-0242c2d7d513fc5d3",
      "Origin": "CreateRoute",
      "State": "active"
     }
    ],
    "VpcId": "vpc-0c250a5c33f51d456"
}
```

AwsEc2SecurityGroup

`AwsEc2SecurityGroup`Objek tersebut menggambarkan grup keamanan Amazon EC2.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsEc2SecurityGroup` objek. Untuk melihat deskripsi `AwsEc2SecurityGroup` atribut, lihat AwsEc2 SecurityGroupDetails di Referensi AWS Security Hub API.

Contoh

```
"AwsEc2SecurityGroup": {
    "GroupName": "MySecurityGroup",
    "GroupId": "sg-903004f8",
```

```
    "OwnerId": "123456789012",
    "VpcId": "vpc-1a2b3c4d",
    "IpPermissions": [
        {
            "IpProtocol": "-1",
            "IpRanges": [],
            "UserIdGroupPairs": [
                {
                    "UserId": "123456789012",
                    "GroupId": "sg-903004f8"
                }
            ],
            "PrefixListIds": [
                {"PrefixListId": "pl-63a5400a"}
            ]
        },
        {
            "PrefixListIds": [],
            "FromPort": 22,
            "IpRanges": [
                {
                    "CidrIp": "203.0.113.0/24"
                }
            ],
            "ToPort": 22,
            "IpProtocol": "tcp",
            "UserIdGroupPairs": []
        }
    ]
}
```

AwsEc2Subnet

`AwsEc2Subnet`Objek memberikan informasi tentang subnet di Amazon EC2.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsEc2Subnet` objek. Untuk melihat deskripsi `AwsEc2Subnet` atribut, lihat AwsEc2 SubnetDetails di Referensi AWS Security Hub API.

Contoh

```
AwsEc2Subnet: {
    "AssignIpv6AddressOnCreation": false,
```

```
    "AvailabilityZone": "us-west-2c",
    "AvailabilityZoneId": "usw2-az3",
    "AvailableIpAddressCount": 8185,
    "CidrBlock": "10.0.0.0/24",
    "DefaultForAz": false,
    "MapPublicIpOnLaunch": false,
    "OwnerId": "123456789012",
    "State": "available",
    "SubnetArn": "arn:aws:ec2:us-west-2:123456789012:subnet/subnet-d5436c93",
    "SubnetId": "subnet-d5436c93",
    "VpcId": "vpc-153ade70",
    "Ipv6CidrBlockAssociationSet": [{
        "AssociationId": "subnet-cidr-assoc-EXAMPLE",
        "Ipv6CidrBlock": "2001:DB8::/32",
        "CidrBlockState": "associated"
   }]
}
```

AwsEc2TransitGateway

`AwsEc2TransitGateway`Objek ini memberikan detail tentang gateway transit Amazon EC2 yang menghubungkan cloud pribadi virtual (VPC) dan jaringan lokal Anda.

Berikut ini adalah contoh `AwsEc2TransitGateway` temuan dalam AWS Security Finding Format (ASFF). Untuk melihat deskripsi `AwsEc2TransitGateway` atribut, lihat AwsEc2 TransitGatewayDetails di Referensi AWS Security Hub API.

Contoh

```
"AwsEc2TransitGateway": {
 "AmazonSideAsn": 65000,
 "AssociationDefaultRouteTableId": "tgw-rtb-099ba47cbbea837cc",
 "AutoAcceptSharedAttachments": "disable",
 "DefaultRouteTableAssociation": "enable",
 "DefaultRouteTablePropagation": "enable",
 "Description": "sample transit gateway",
 "DnsSupport": "enable",
 "Id": "tgw-042ae6bf7a5c126c3",
 "MulticastSupport": "disable",
 "PropagationDefaultRouteTableId": "tgw-rtb-099ba47cbbea837cc",
 "TransitGatewayCidrBlocks": ["10.0.0.0/16"],
 "VpnEcmpSupport": "enable"
}
```

AwsEc2Volume

`AwsEc2Volume`Objek memberikan detail tentang volume Amazon EC2.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsEc2Volume` objek. Untuk melihat deskripsi `AwsEc2Volume` atribut, lihat AwsEc2 VolumeDetails di Referensi AWS Security Hub API.

Contoh

```
"AwsEc2Volume": {
    "Attachments": [
      {
        "AttachTime": "2017-10-17T14:47:11Z",
        "DeleteOnTermination": true,
        "InstanceId": "i-123abc456def789g",
        "Status": "attached"
      }
     ],
    "CreateTime": "2020-02-24T15:54:30Z",
    "Encrypted": true,
    "KmsKeyId": "arn:aws:kms:us-east-1:111122223333:key/wJalrXUtnFEMI/K7MDENG/
bPxRfiCYEXAMPLEKEY",
    "Size": 80,
    "SnapshotId": "",
    "Status": "available"
}
```

AwsEc2Vpc

`AwsEc2Vpc`Objek tersebut memberikan detail tentang VPC Amazon EC2.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsEc2Vpc` objek. Untuk melihat deskripsi `AwsEc2Vpc` atribut, lihat AwsEc2 VpcDetails di Referensi AWS Security Hub API.

Contoh

```
"AwsEc2Vpc": {
    "CidrBlockAssociationSet": [
        {
            "AssociationId": "vpc-cidr-assoc-0dc4c852f52abda97",
            "CidrBlock": "192.0.2.0/24",
            "CidrBlockState": "associated"
```

```
        }
    ],
    "DhcpOptionsId": "dopt-4e42ce28",
    "Ipv6CidrBlockAssociationSet": [
        {
            "AssociationId": "vpc-cidr-assoc-0dc4c852f52abda97",
            "CidrBlockState": "associated",
            "Ipv6CidrBlock": "192.0.2.0/24"
       }

    ],
    "State": "available"
}
```

AwsEc2VpcEndpointService

`AwsEc2VpcEndpointService`Objek berisi rincian tentang konfigurasi layanan untuk layanan titik akhir VPC.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsEc2VpcEndpointService` objek. Untuk melihat deskripsi `AwsEc2VpcEndpointService` atribut, lihat AwsEc2 VpcEndpointServiceDetails di Referensi AWS Security Hub API.

Contoh

```
"AwsEc2VpcEndpointService": {
    "ServiceType": [
      {
        "ServiceType": "Interface"
      }
    ],
    "ServiceId": "vpce-svc-example1",
    "ServiceName": "com.amazonaws.vpce.us-east-1.vpce-svc-example1",
    "ServiceState": "Available",
    "AvailabilityZones": [
      "us-east-1"
    ],
    "AcceptanceRequired": true,
    "ManagesVpcEndpoints": false,
    "NetworkLoadBalancerArns": [
      "arn:aws:elasticloadbalancing:us-east-1:444455556666:loadbalancer/net/my-network-
load-balancer/example1"
    ],
```

```
    "GatewayLoadBalancerArns": [],
    "BaseEndpointDnsNames": [
      "vpce-svc-04eec859668b51c34.us-east-1.vpce.amazonaws.com"
    ],
    "PrivateDnsName": "my-private-dns"
}
```

AwsEc2VpcPeeringConnection

`AwsEc2VpcPeeringConnection`Objek memberikan rincian tentang koneksi jaringan antara dua VPC.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsEc2VpcPeeringConnection` objek. Untuk melihat deskripsi `AwsEc2VpcPeeringConnection` atribut, lihat AwsEc2 VpcPeeringConnectionDetails di Referensi AWS Security Hub API.

Contoh

```
"AwsEc2VpcPeeringConnection": {
 "AccepterVpcInfo": {
  "CidrBlock": "10.0.0.0/28",
  "CidrBlockSet": [{
   "CidrBlock": "10.0.0.0/28"
  }],
  "Ipv6CidrBlockSet": [{
   "Ipv6CidrBlock": "2002::1234:abcd:ffff:c0a8:101/64"
  }],
  "OwnerId": "012345678910",
  "PeeringOptions": {
   "AllowDnsResolutionFromRemoteVpc": true,
   "AllowEgressFromLocalClassicLinkToRemoteVpc": false,
   "AllowEgressFromLocalVpcToRemoteClassicLink": true
  },
  "Region": "us-west-2",
  "VpcId": "vpc-i123456"
 },
 "ExpirationTime": "2022-02-18T15:31:53.161Z",
 "RequesterVpcInfo": {
  "CidrBlock": "192.168.0.0/28",
  "CidrBlockSet": [{
   "CidrBlock": "192.168.0.0/28"
  }],
```

```
  "Ipv6CidrBlockSet": [{
   "Ipv6CidrBlock": "2002::1234:abcd:ffff:c0a8:101/64"
  }],
  "OwnerId": "012345678910",
  "PeeringOptions": {
   "AllowDnsResolutionFromRemoteVpc": true,
   "AllowEgressFromLocalClassicLinkToRemoteVpc": false,
   "AllowEgressFromLocalVpcToRemoteClassicLink": true
  },
  "Region": "us-west-2",
  "VpcId": "vpc-i123456"
 },
 "Status": {
  "Code": "initiating-request",
  "Message": "Active"
 },
 "VpcPeeringConnectionId": "pcx-1a2b3c4d"
}
```

AwsEc2VpnConnection

`AwsEc2VpnConnection`Objek tersebut memberikan detail tentang koneksi VPN Amazon EC2.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsEc2VpnConnection` objek. Untuk melihat deskripsi `AwsEc2VpnConnection` atribut, lihat AwsEc2 VpnConnectionDetails di Referensi AWS Security Hub API.

Contoh

```
"AwsEc2VpnConnection": {
    "VpnConnectionId": "vpn-205e4f41",
    "State": "available",
    "CustomerGatewayConfiguration": "",
    "CustomerGatewayId": "cgw-5699703f",
    "Type": "ipsec.1",
    "VpnGatewayId": "vgw-2ccb2245",
    "Category": "VPN"
    "TransitGatewayId": "tgw-09b6f3a659e2b5elf",
    "VgwTelemetry": [
        {
            "OutsideIpAddress": "92.0.2.11",
            "Status": "DOWN",
            "LastStatusChange": "2016-11-11T23:09:32.000Z",
```

```
            "StatusMessage": "IPSEC IS DOWN",
            "AcceptedRouteCount": 0
        },
        {
            "OutsideIpAddress": "92.0.2.12",
            "Status": "DOWN",
            "LastStatusChange": "2016-11-11T23:10:51.000Z",
            "StatusMessage": "IPSEC IS DOWN",
            "AcceptedRouteCount": 0
        }
    ],
    "Routes": [{
        "DestinationCidrBlock": "10.24.34.0/24",
        "State": "available"
   }],
    "Options": {
        "StaticRoutesOnly": true
        "TunnelOptions": [{
            "DpdTimeoutSeconds": 30,
            "IkeVersions": ["ikev1", "ikev2"],
            "Phase1DhGroupNumbers": [14, 15, 16, 17, 18},
            "Phase1EncryptionAlgorithms": ["AES128", "AES256"],
            "Phase1IntegrityAlgorithms": ["SHA1", "SHA2-256"],
            "Phase1LifetimeSeconds": 28800,
            "Phase2DhGroupNumbers": [14, 15, 16, 17, 18],
            "Phase2EncryptionAlgorithms": ["AES128", "AES256"],
            "Phase2IntegrityAlgorithms": ["SHA1", "SHA2-256"],
            "Phase2LifetimeSeconds": 28800,
            "PreSharedKey": "RltXC3REhTw1RAdiM2s1uMfkkSDLyGJoe1QEWeGxqkQ=",
            "RekeyFuzzPercentage": 100,
            "RekeyMarginTimeSeconds": 540,
            "ReplayWindowSize": 1024,
            "TunnelInsideCidr": "10.24.34.0/23"
        }]
    }
}
```

AwsEcr

Berikut ini adalah contoh Format Pencarian AWS Keamanan untuk `AwsEcr` sumber daya.

AwsEcrContainerImage

`AwsEcrContainerImage`Objek memberikan informasi tentang gambar Amazon ECR.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsEcrContainerImage` objek. Untuk melihat deskripsi `AwsEcrContainerImage` atribut, lihat AwsEcrContainerImageDetailsdi Referensi AWS Security Hub API.

Contoh

```
"AwsEcrContainerImage": {
    "RegistryId": "123456789012",
    "RepositoryName": "repository-name",
    "Architecture": "amd64"
    "ImageDigest":
 "sha256:a568e5c7a953fbeaa2904ac83401f93e4a076972dc1bae527832f5349cd2fb10",
    "ImageTags": ["00000000-0000-0000-0000-000000000000"],
    "ImagePublishedAt": "2019-10-01T20:06:12Z"
}
```

AwsEcrRepository

`AwsEcrRepository`Objek memberikan informasi tentang repositori Amazon Elastic Container Registry.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsEcrRepository` objek. Untuk melihat deskripsi `AwsEcrRepository` atribut, lihat AwsEcrRepositoryDetailsdi Referensi AWS Security Hub API.

Contoh

```
"AwsEcrRepository": {
    "LifecyclePolicy": {
        "RegistryId": "123456789012",
    },
    "RepositoryName": "sample-repo",
    "Arn": "arn:aws:ecr:us-west-2:111122223333:repository/sample-repo",
    "ImageScanningConfiguration": {
        "ScanOnPush": true
    },
    "ImageTagMutability": "IMMUTABLE"
}
```

AwsEcs

Berikut ini adalah contoh Format Pencarian AWS Keamanan untuk `AwsEcs` sumber daya.

AwsEcsCluster

`AwsEcsCluster`Objek ini memberikan detail tentang kluster Amazon Elastic Container Service.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsEcsCluster` objek. Untuk melihat deskripsi `AwsEcsCluster` atribut, lihat AwsEcsClusterDetailsdi Referensi AWS Security Hub API.

Contoh

```
    "AwsEcsCluster": {
        "CapacityProviders": [],
        "ClusterSettings": [
            {
                "Name": "containerInsights",
                "Value": "enabled"
            }
        ],
        "Configuration": {
            "ExecuteCommandConfiguration": {
                "KmsKeyId": "kmsKeyId",
                "LogConfiguration": {
                    "CloudWatchEncryptionEnabled": true,
                    "CloudWatchLogGroupName": "cloudWatchLogGroupName",
                    "S3BucketName": "s3BucketName",
                    "S3EncryptionEnabled": true,
                    "S3KeyPrefix": "s3KeyPrefix"
                },
                "Logging": "DEFAULT"
            }
        }
        "DefaultCapacityProviderStrategy": [
            {
                "Base": 0,
                "CapacityProvider": "capacityProvider",
                "Weight": 1
            }
        ]
    }
```

AwsEcsContainer

`AwsEcsContainer`Objek berisi detail tentang wadah Amazon ECS.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsEcsContainer` objek. Untuk melihat deskripsi `AwsEcsContainer` atribut, lihat AwsEcsContainerDetailsdi Referensi AWS Security Hub API.

Contoh

```
"AwsEcsContainer": {
    "Image": "1111111/
knotejs@sha256:356131c9fef111111111111115f4ed8de5f9dce4dc3bd34bg21846588a3",
    "MountPoints": [{
        "ContainerPath": "/mnt/etc",
        "SourceVolume": "vol-03909e9"
    }],
    "Name": "knote",
    "Privileged": true
}
```

AwsEcsService

`AwsEcsService`Objek memberikan rincian tentang layanan dalam cluster Amazon ECS.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsEcsService` objek. Untuk melihat deskripsi `AwsEcsService` atribut, lihat AwsEcsServiceDetailsdi Referensi AWS Security Hub API.

Contoh

```
"AwsEcsService": {
    "CapacityProviderStrategy": [
        {
            "Base": 12,
            "CapacityProvider": "",
            "Weight": ""
        }
    ],
    "Cluster": "arn:aws:ecs:us-east-1:111122223333:cluster/example-ecs-cluster",
    "DeploymentConfiguration": {
        "DeploymentCircuitBreaker": {
            "Enable": false,
            "Rollback": false
        },
        "MaximumPercent": 200,
        "MinimumHealthyPercent": 100
```

```
    },
    "DeploymentController": "",
    "DesiredCount": 1,
    "EnableEcsManagedTags": false,
    "EnableExecuteCommand": false,
    "HealthCheckGracePeriodSeconds": 1,
    "LaunchType": "FARGATE",
    "LoadBalancers": [
        {
            "ContainerName": "",
            "ContainerPort": 23,
            "LoadBalancerName": "",
            "TargetGroupArn": ""
        }
    ],
    "Name": "sample-app-service",
    "NetworkConfiguration": {
        "AwsVpcConfiguration": {
            "Subnets": [
                "Subnet-example1",
                "Subnet-example2"
            ],
        "SecurityGroups": [
                "Sg-0ce48e9a6e5b457f5"
        ],
        "AssignPublicIp": "ENABLED"
        }
    },
    "PlacementConstraints": [
        {
            "Expression": "",
            "Type": ""
        }
    ],
    "PlacementStrategies": [
        {
            "Field": "",
            "Type": ""
        }
    ],
    "PlatformVersion": "LATEST",
    "PropagateTags": "",
    "Role": "arn:aws:iam::111122223333:role/aws-servicerole/ecs.amazonaws.com/
ServiceRoleForECS",
```

```
    "SchedulingStrategy": "REPLICA",
    "ServiceName": "sample-app-service",
    "ServiceArn": "arn:aws:ecs:us-east-1:111122223333:service/example-ecs-cluster/
sample-app-service",
    "ServiceRegistries": [
        {
            "ContainerName": "",
            "ContainerPort": 1212,
            "Port": 1221,
            "RegistryArn": ""
        }
    ],
    "TaskDefinition": "arn:aws:ecs:us-east-1:111122223333:task-definition/example-
taskdef:1"
}
```

AwsEcsTask

`AwsEcsTask`Objek memberikan detail tentang tugas Amazon ECS.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsEcsTask` objek. Untuk melihat deskripsi `AwsEcsTask` atribut, lihat AwsEcsTaskdi Referensi AWS Security Hub API.

Contoh

```
"AwsEcsTask": {
 "ClusterArn": "arn:aws:ecs:us-west-2:123456789012:task/MyCluster/1234567890123456789",
 "CreatedAt": "1557134011644",
 "Group": "service:fargate-service",
 "StartedAt": "1557134011644",
 "StartedBy": "ecs-svc/1234567890123456789",
 "TaskDefinitionArn": "arn:aws:ecs:us-west-2:123456789012:task-definition/sample-
fargate:2",
 "Version": 3,
 "Volumes": [{
  "Name": "string",
  "Host": {
   "SourcePath": "string"
  }
 }],
 "Containers": {
  "Image": "1111111/
knotejs@sha256:356131c9fef111111111111115f4ed8de5f9dce4dc3bd34bg21846588a3",
  "MountPoints": [{
```

```
   "ContainerPath": "/mnt/etc",
   "SourceVolume": "vol-03909e9"
  }],
  "Name": "knote",
  "Privileged": true
 }
}
```

AwsEcsTaskDefinition

`AwsEcsTaskDefinition`Objek berisi rincian tentang definisi tugas. Definisi tugas menjelaskan definisi kontainer dan volume tugas Amazon Elastic Container Service.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsEcsTaskDefinition` objek. Untuk melihat deskripsi `AwsEcsTaskDefinition` atribut, lihat AwsEcsTaskDefinitionDetailsdi Referensi AWS Security Hub API.

Contoh

```
    "AwsEcsTaskDefinition": {
        "ContainerDefinitions": [
            {
                "Command": ['ruby', 'hi.rb'],
                "Cpu":128,
                "Essential": true,
                "HealthCheck": {
                    "Command": ["CMD-SHELL", "curl -f http://localhost/ || exit 1"],
                    "Interval": 10,
                    "Retries": 3,
                    "StartPeriod": 5,
                    "Timeout": 20
                },
                "Image": "tongueroo/sinatra:latest",
                "Interactive": true,
                "Links": [],
                "LogConfiguration": {
                    "LogDriver": "awslogs",
                    "Options": {
                        "awslogs-group": "/ecs/sinatra-hi",
                        "awslogs-region": "ap-southeast-1",
                        "awslogs-stream-prefix": "ecs"
                    },
                    "SecretOptions": []
```

```
                },
                "MemoryReservation": 128,
                "Name": "web",
                "PortMappings": [
                    {
                        "ContainerPort": 4567,
                        "HostPort":4567,
                        "Protocol": "tcp"
                    }
                ],
                "Privileged": true,
                "StartTimeout": 10,
                "StopTimeout": 100,
            }
        ],
        "Family": "sinatra-hi",
        "NetworkMode": "host",
        "RequiresCompatibilities": ["EC2"],
        "Status": "ACTIVE",
        "TaskRoleArn": "arn:aws:iam::111122223333:role/ecsTaskExecutionRole",
    }
```

AwsEfs

Berikut ini adalah contoh Format Pencarian AWS Keamanan untuk `AwsEfs` sumber daya.

AwsEfsAccessPoint

`AwsEfsAccessPoint`Objek memberikan detail tentang file yang disimpan di Amazon Elastic File System.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsEfsAccessPoint` objek. Untuk melihat deskripsi `AwsEfsAccessPoint` atribut, lihat AwsEfsAccessPointDetailsdi Referensi AWS Security Hub API.

Contoh

```
"AwsEfsAccessPoint": {
 "AccessPointId": "fsap-05c4c0e79ba0b118a",
 "Arn": "arn:aws:elasticfilesystem:us-east-1:863155670886:access-point/
fsap-05c4c0e79ba0b118a",
 "ClientToken": "AccessPointCompliant-ASk06ZZSXsEp",
 "FileSystemId": "fs-0f8137f731cb32146",
```

```
 "PosixUser": {
  "Gid": "1000",
  "SecondaryGids": ["0", "4294967295"],
  "Uid": "1234"
 },
 "RootDirectory": {
  "CreationInfo": {
   "OwnerGid": "1000",
   "OwnerUid": "1234",
   "Permissions": "777"
  },
  "Path": "/tmp/example"
 }
}
```

AwsEks

Berikut ini adalah contoh Format Pencarian AWS Keamanan untuk `AwsEks` sumber daya.

AwsEksCluster

`AwsEksCluster`Objek tersebut memberikan detail tentang cluster Amazon EKS.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsEksCluster` objek. Untuk melihat deskripsi `AwsEksCluster` atribut, lihat AwsEksClusterDetailsdi Referensi AWS Security Hub API.

Contoh

```
{
  "AwsEksCluster": {
    "Name": "example",
    "Arn": "arn:aws:eks:us-west-2:222222222222:cluster/example",
    "CreatedAt": 1565804921.901,
    "Version": "1.12",
    "RoleArn": "arn:aws:iam::222222222222:role/example-cluster-
ServiceRole-1XWBQWYSFRE2Q",
    "ResourcesVpcConfig": {
      "EndpointPublicAccess": false,
      "SubnetIds": [
        "subnet-021345abcdef6789",
        "subnet-abcdef01234567890",
        "subnet-1234567890abcdef0"
      ],
```

```
      "SecurityGroupIds": [
        "sg-abcdef01234567890"
      ]
    },
    "Logging": {
      "ClusterLogging": [
        {
          "Types": [
            "api",
            "audit",
            "authenticator",
            "controllerManager",
            "scheduler"
          ],
          "Enabled": true
        }
      ]
    },
    "Status": "CREATING",
    "CertificateAuthorityData": {},
  }
}
```

AwsElasticBeanstalk

Berikut ini adalah contoh Format Pencarian AWS Keamanan untuk `AwsElasticBeanstalk` sumber daya.

AwsElasticBeanstalkEnvironment

`AwsElasticBeanstalkEnvironment`Objek berisi rincian tentang AWS Elastic Beanstalk lingkungan.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsElasticBeanstalkEnvironment` objek. Untuk melihat deskripsi `AwsElasticBeanstalkEnvironment` atribut, lihat AwsElasticBeanstalkEnvironmentDetailsdi Referensi AWS Security Hub API.

Contoh

```
"AwsElasticBeanstalkEnvironment": {
    "ApplicationName": "MyApplication",
    "Cname": "myexampleapp-env.devo-2.elasticbeanstalk-internal.com",
```

```
    "DateCreated": "2021-04-30T01:38:01.090Z",
    "DateUpdated": "2021-04-30T01:38:01.090Z",
    "Description": "Example description of my awesome application",
    "EndpointUrl": "eb-dv-e-p-AWSEBLoa-abcdef01234567890-021345abcdef6789.us-
east-1.elb.amazonaws.com",
    "EnvironmentArn": "arn:aws:elasticbeanstalk:us-east-1:123456789012:environment/
MyApplication/myapplication-env",
    "EnvironmentId": "e-abcd1234",
    "EnvironmentLinks": [
        {
            "EnvironmentName": "myexampleapp-env",
            "LinkName": "myapplicationLink"
        }
    ],
    "EnvironmentName": "myapplication-env",
    "OptionSettings": [
        {
            "Namespace": "aws:elasticbeanstalk:command",
            "OptionName": "BatchSize",
            "Value": "100"
        },
        {
            "Namespace": "aws:elasticbeanstalk:command",
            "OptionName": "Timeout",
            "Value": "600"
        },
        {
            "Namespace": "aws:elasticbeanstalk:command",
            "OptionName": "BatchSizeType",
            "Value": "Percentage"
        },
        {
            "Namespace": "aws:elasticbeanstalk:command",
            "OptionName": "IgnoreHealthCheck",
            "Value": "false"
        },
        {
            "Namespace": "aws:elasticbeanstalk:application",
            "OptionName": "Application Healthcheck URL",
            "Value": "TCP:80"
        }
    ],
    "PlatformArn": "arn:aws:elasticbeanstalk:us-east-1::platform/Tomcat 8 with Java 8
 running on 64bit Amazon Linux/2.7.7",
```

```
    "SolutionStackName": "64bit Amazon Linux 2017.09 v2.7.7 running Tomcat 8 Java 8",
    "Status": "Ready",
    "Tier": {
        "Name": "WebServer"
       "Type": "Standard"
       "Version": "1.0"
    },
    "VersionLabel": "Sample Application"
}
```

AwsElasticSearch

Berikut ini adalah contoh Format Pencarian AWS Keamanan untuk `AwsElasticSearch` sumber daya.

AwsElasticSearchDomain

`AwsElasticSearchDomain`Objek memberikan detail tentang domain OpenSearch Layanan Amazon.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsElasticSearchDomain` objek. Untuk melihat deskripsi `AwsElasticSearchDomain` atribut, lihat AwsElasticSearchDomainDetailsdi Referensi AWS Security Hub API.

Contoh

```
"AwsElasticSearchDomain": {
    "AccessPolicies": "string",
    "DomainStatus": {
           "DomainId": "string",
           "DomainName": "string",
           "Endpoint": "string",
           "Endpoints": {
                  "string": "string"
           }
    },
    "DomainEndpointOptions": {
           "EnforceHTTPS": boolean,
           "TLSSecurityPolicy": "string"
    },
    "ElasticsearchClusterConfig": {
           "DedicatedMasterCount": number,
           "DedicatedMasterEnabled": boolean,
```

```
            "DedicatedMasterType": "string",
            "InstanceCount": number,
            "InstanceType": "string",
            "ZoneAwarenessConfig": {
                  "AvailabilityZoneCount": number
            },
            "ZoneAwarenessEnabled": boolean
      },
      "ElasticsearchVersion": "string",
      "EncryptionAtRestOptions": {
            "Enabled": boolean,
            "KmsKeyId": "string"
      },
      "LogPublishingOptions": {
            "AuditLogs": {
                  "CloudWatchLogsLogGroupArn": "string",
                  "Enabled": boolean
            },
            "IndexSlowLogs": {
                  "CloudWatchLogsLogGroupArn": "string",
                  "Enabled": boolean
            },
            "SearchSlowLogs": {
                  "CloudWatchLogsLogGroupArn": "string",
                  "Enabled": boolean
            }
      },
      "NodeToNodeEncryptionOptions": {
            "Enabled": boolean
      },
      "ServiceSoftwareOptions": {
            "AutomatedUpdateDate": "string",
            "Cancellable": boolean,
            "CurrentVersion": "string",
            "Description": "string",
            "NewVersion": "string",
            "UpdateAvailable": boolean,
            "UpdateStatus": "string"
      },
      "VPCOptions": {
            "AvailabilityZones": [
                  "string"
            ],
            "SecurityGroupIds": [
```

```
                "string"
            ],
            "SubnetIds": [
                "string"
            ],
           "VPCId": "string"
    }
}
```

AwsElb

Berikut ini adalah contoh Format Pencarian AWS Keamanan untuk `AwsElb` sumber daya.

AwsElbLoadBalancer

`AwsElbLoadBalancer`Objek berisi rincian tentang Classic Load Balancer.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsElbLoadBalancer` objek. Untuk melihat deskripsi `AwsElbLoadBalancer` atribut, lihat AwsElbLoadBalancerDetailsdi Referensi AWS Security Hub API.

Contoh

```
"AwsElbLoadBalancer": {
    "AvailabilityZones": ["us-west-2a"],
    "BackendServerDescriptions": [
         {
            "InstancePort": 80,
            "PolicyNames": ["doc-example-policy"]
        }
    ],
    "CanonicalHostedZoneName": "Z3DZXE0EXAMPLE",
    "CanonicalHostedZoneNameID": "my-load-balancer-444455556666.us-
west-2.elb.amazonaws.com",
    "CreatedTime": "2020-08-03T19:22:44.637Z",
    "DnsName": "my-load-balancer-444455556666.us-west-2.elb.amazonaws.com",
    "HealthCheck": {
        "HealthyThreshold": 2,
        "Interval": 30,
        "Target": "HTTP:80/png",
        "Timeout": 3,
        "UnhealthyThreshold": 2
    },
    "Instances": [
```

```
        {
            "InstanceId": "i-example"
        }
    ],
    "ListenerDescriptions": [
        {
            "Listener": {
                "InstancePort": 443,
                "InstanceProtocol": "HTTPS",
                "LoadBalancerPort": 443,
                "Protocol": "HTTPS",
                "SslCertificateId": "arn:aws:iam::444455556666:server-certificate/my-
server-cert"
            },
            "PolicyNames": ["ELBSecurityPolicy-TLS-1-2-2017-01"]
        }
    ],
    "LoadBalancerAttributes": {
        "AccessLog": {
            "EmitInterval": 60,
            "Enabled": true,
            "S3BucketName": "doc-example-bucket",
            "S3BucketPrefix": "doc-example-prefix"
        },
        "ConnectionDraining": {
            "Enabled": false,
            "Timeout": 300
        },
        "ConnectionSettings": {
            "IdleTimeout": 30
        },
        "CrossZoneLoadBalancing": {
            "Enabled": true
        },
        "AdditionalAttributes": [{
            "Key": "elb.http.desyncmitigationmode",
            "Value": "strictest"
        }]

    },
    "LoadBalancerName": "example-load-balancer",
    "Policies": {
        "AppCookieStickinessPolicies": [
            {
```

```
                "CookieName": "",
                "PolicyName": ""
            }
        ],
        "LbCookieStickinessPolicies": [
            {
                "CookieExpirationPeriod": 60,
                "PolicyName": "my-example-cookie-policy"
            }
        ],
        "OtherPolicies": [
            "my-PublicKey-policy",
            "my-authentication-policy",
            "my-SSLNegotiation-policy",
            "my-ProxyProtocol-policy",
            "ELBSecurityPolicy-2015-03"
        ]
    },
    "Scheme": "internet-facing",
    "SecurityGroups": ["sg-example"],
    "SourceSecurityGroup": {
        "GroupName": "my-elb-example-group",
        "OwnerAlias": "444455556666"
    },
    "Subnets": ["subnet-example"],
    "VpcId": "vpc-a01106c2"
}
```

AwsElbv2LoadBalancer

`AwsElbv2LoadBalancer`Objek memberikan informasi tentang penyeimbang beban.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsElbv2LoadBalancer` objek. Untuk melihat deskripsi `AwsElbv2LoadBalancer` atribut, lihat AwsElbv2 LoadBalancerDetails di Referensi AWS Security Hub API.

Contoh

```
"AwsElbv2LoadBalancer": {
                        "AvailabilityZones": {
                            "SubnetId": "string",
                            "ZoneName": "string"
                        },
```

```
                    "CanonicalHostedZoneId": "string",
                    "CreatedTime": "string",
                    "DNSName": "string",
                    "IpAddressType": "string",
                    "LoadBalancerAttributes": [
                        {
                            "Key": "string",
                            "Value": "string"
                        }
                    ],
                    "Scheme": "string",
                    "SecurityGroups": [ "string" ],
                    "State": {
                        "Code": "string",
                        "Reason": "string"
                    },
                    "Type": "string",
                    "VpcId": "string"
                }
```

AwsEventBridge

Berikut ini adalah contoh Format Pencarian AWS Keamanan untuk `AwsEventBridge` sumber daya.

AwsEventSchemasRegistry

`AwsEventSchemasRegistry`Objek memberikan informasi tentang registri EventBridge skema Amazon. Skema mendefinisikan struktur peristiwa yang dikirim ke. EventBridge Registries skema adalah wadah yang mengumpulkan dan secara logis mengelompokkan skema Anda.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsEventSchemasRegistry` objek. Untuk melihat deskripsi `AwsEventSchemasRegistry` atribut, lihat AwsEventSchemasRegistrydi Referensi AWS Security Hub API.

Contoh

```
"AwsEventSchemasRegistry": {
    "Description": "This is an example event schema registry.",
    "RegistryArn": "arn:aws:schemas:us-east-1:123456789012:registry/schema-registry",
    "RegistryName": "schema-registry"
}
```

AwsEventsEndpoint

`AwsEventsEndpoint`Objek memberikan informasi tentang titik akhir EventBridge global Amazon. Titik akhir dapat meningkatkan ketersediaan aplikasi Anda dengan membuatnya toleran terhadap kesalahan regional.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsEventsEndpoint` objek. Untuk melihat deskripsi `AwsEventsEndpoint` atribut, lihat AwsEventsEndpointDetailsdi Referensi AWS Security Hub API.

Contoh

```
"AwsEventsEndpoint": {
    "Arn": "arn:aws:events:us-east-1:123456789012:endpoint/my-endpoint",
    "Description": "This is a sample endpoint.",
    "EndpointId": "04k1exajoy.veo",
    "EndpointUrl": "https://04k1exajoy.veo.endpoint.events.amazonaws.com",
    "EventBuses": [
        {
            "EventBusArn": "arn:aws:events:us-east-1:123456789012:event-bus/default"
        },
        {
            "EventBusArn": "arn:aws:events:us-east-2:123456789012:event-bus/default"
        }
    ],
    "Name": "my-endpoint",
    "ReplicationConfig": {
        "State": "ENABLED"
    },
    "RoleArn": "arn:aws:iam::123456789012:role/service-role/
Amazon_EventBridge_Invoke_Event_Bus_1258925394",
    "RoutingConfig": {
        "FailoverConfig": {
            "Primary": {
                "HealthCheck": "arn:aws:route53:::healthcheck/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111"
            },
            "Secondary": {
                "Route": "us-east-2"
            }
        }
    },
    "State": "ACTIVE"
```

```
}
```

AwsEventsEventbus

`AwsEventsEventbus`Objek memberikan informasi tentang titik akhir EventBridge global Amazon. Titik akhir dapat meningkatkan ketersediaan aplikasi Anda dengan membuatnya toleran terhadap kesalahan regional.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsEventsEventbus` objek. Untuk melihat deskripsi `AwsEventsEventbus` atribut, lihat AwsEventsEventbusDetailsdi Referensi AWS Security Hub API.

Contoh

```
"AwsEventsEventbus":
    "Arn": "arn:aws:events:us-east-1:123456789012:event-bus/my-event-bus",
    "Name": "my-event-bus",
    "Policy": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Sid\":
\"AllowAllAccountsFromOrganizationToPutEvents\",\"Effect\":\"Allow
\",\"Principal\":\"*\",\"Action\":\"events:PutEvents\",\"Resource\":
\"arn:aws:events:us-east-1:123456789012:event-bus/my-event-bus\",\"Condition
\":{\"StringEquals\":{\"aws:PrincipalOrgID\":\"o-ki7yjtkjv5\"}}},{\"Sid\":
\"AllowAccountToManageRulesTheyCreated\",\"Effect\":\"Allow\",\"Principal\":{\"AWS\":
\"arn:aws:iam::123456789012:root\"},\"Action\":[\"events:PutRule\",\"events:PutTargets
\",\"events:DeleteRule\",\"events:RemoveTargets\",\"events:DisableRule
\",\"events:EnableRule\",\"events:TagResource\",\"events:UntagResource\",
\"events:DescribeRule\",\"events:ListTargetsByRule\",\"events:ListTagsForResource\"],
\"Resource\":\"arn:aws:events:us-east-1:123456789012:rule/my-event-bus\",\"Condition\":
{\"StringEqualsIfExists\":{\"events:creatorAccount\":\"123456789012\"}}}]}"
```

AwsGuardDuty

Berikut ini adalah contoh Format Pencarian AWS Keamanan untuk `AwsGuardDuty` sumber daya.

AwsGuardDutyDetector

`AwsGuardDutyDetector`Objek tersebut memberikan informasi tentang GuardDuty detektor Amazon. Detektor adalah objek yang mewakili GuardDuty layanan. Detektor diperlukan GuardDuty untuk menjadi operasional.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsGuardDutyDetector` objek. Untuk melihat deskripsi `AwsGuardDutyDetector` atribut, lihat AwsGuardDutyDetectordi Referensi AWS Security Hub API.

Contoh

```
"AwsGuardDutyDetector": {
    "FindingPublishingFrequency": "SIX_HOURS",
    "ServiceRole": "arn:aws:iam::123456789012:role/aws-service-role/
guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty",
    "Status": "ENABLED",
    "DataSources": {
        "CloudTrail": {
            "Status": "ENABLED"
        },
        "DnsLogs": {
            "Status": "ENABLED"
        },
        "FlowLogs": {
            "Status": "ENABLED"
        },
        "S3Logs": {
             "Status": "ENABLED"
         },
         "Kubernetes": {
             "AuditLogs": {
                "Status": "ENABLED"
             }
         },
         "MalwareProtection": {
             "ScanEc2InstanceWithFindings": {
                "EbsVolumes": {
                    "Status": "ENABLED"
                 }
             },
            "ServiceRole": "arn:aws:iam::123456789012:role/aws-service-role/malware-
protection.guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDutyMalwareProtection"
         }
    }
}
```

AwsIam

Berikut ini adalah contoh Format Pencarian AWS Keamanan untuk `AwsIam` sumber daya.

AwsIamAccessKey

`AwsIamAccessKey`Objek berisi rincian tentang kunci akses IAM yang terkait dengan temuan.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsIamAccessKey` objek. Untuk melihat deskripsi `AwsIamAccessKey` atribut, lihat AwsIamAccessKeyDetailsdi Referensi AWS Security Hub API.

Contoh

```
"AwsIamAccessKey": {
                        "AccessKeyId": "string",
                        "AccountId": "string",
                        "CreatedAt": "string",
                        "PrincipalId": "string",
                        "PrincipalName": "string",
                        "PrincipalType": "string",
                        "SessionContext": {
                            "Attributes": {
                                "CreationDate": "string",
                                "MfaAuthenticated": boolean
                            },
                            "SessionIssuer": {
                                "AccountId": "string",
                                "Arn": "string",
                                "PrincipalId": "string",
                                "Type": "string",
                                "UserName": "string"
                            }
                        },
                        "Status": "string"
                    }
```

AwsIamGroup

`AwsIamGroup`Objek berisi rincian tentang grup IAM.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsIamGroup` objek. Untuk melihat deskripsi `AwsIamGroup` atribut, lihat AwsIamGroupDetailsdi Referensi AWS Security Hub API.

Contoh

```
"AwsIamGroup": {
    "AttachedManagedPolicies": [
        {
            "PolicyArn": "arn:aws:iam::aws:policy/ExampleManagedAccess",
            "PolicyName": "ExampleManagedAccess",
        }
    ],
    "CreateDate": "2020-04-28T14:08:37.000Z",
    "GroupId": "AGPA4TPS3VLP7QEXAMPLE",
    "GroupName": "Example_User_Group",
    "GroupPolicyList": [
        {
            "PolicyName": "ExampleGroupPolicy"
        }
    ],
    "Path": "/"
}
```

AwsIamPolicy

`AwsIamPolicy`Objek mewakili kebijakan izin IAM.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsIamPolicy` objek. Untuk melihat deskripsi `AwsIamPolicy` atribut, lihat AwsIamPolicyDetailsdi Referensi AWS Security Hub API.

Contoh

```
"AwsIamPolicy": {
    "AttachmentCount": 1,
    "CreateDate": "2017-09-14T08:17:29.000Z",
    "DefaultVersionId": "v1",
    "Description": "Example IAM policy",
    "IsAttachable": true,
    "Path": "/",
    "PermissionsBoundaryUsageCount": 5,
    "PolicyId": "ANPAJ2UCCR6DPCEXAMPLE",
```

```
    "PolicyName": "EXAMPLE-MANAGED-POLICY",
    "PolicyVersionList": [
        {
            "VersionId": "v1",
            "IsDefaultVersion": true,
            "CreateDate": "2017-09-14T08:17:29.000Z"
        }
    ],
    "UpdateDate": "2017-09-14T08:17:29.000Z"
}
```

AwsIamRole

`AwsIamRole`Objek berisi informasi tentang peran IAM, termasuk semua kebijakan peran.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsIamRole` objek. Untuk melihat deskripsi `AwsIamRole` atribut, lihat AwsIamRoleDetailsdi Referensi AWS Security Hub API.

Contoh

```
"AwsIamRole": {
    "AssumeRolePolicyDocument": "{'Version': '2012-10-17','Statement': [{'Effect':
 'Allow','Action': 'sts:AssumeRole'}]}",
    "AttachedManagedPolicies": [
        {
            "PolicyArn": "arn:aws:iam::aws:policy/ExamplePolicy1",
            "PolicyName": "Example policy 1"
        },
        {
            "PolicyArn": "arn:aws:iam::444455556666:policy/ExamplePolicy2",
            "PolicyName": "Example policy 2"
        }
        ],
        "CreateDate": "2020-03-14T07:19:14.000Z",
        "InstanceProfileList": [
            {
                "Arn": "arn:aws:iam::333333333333:ExampleProfile",
                "CreateDate": "2020-03-11T00:02:27Z",
                "InstanceProfileId": "AIPAIXEU4NUHUPEXAMPLE",
                "InstanceProfileName": "ExampleInstanceProfile",
                "Path": "/",
                "Roles": [
                    {
```

```
                    "Arn": "arn:aws:iam::444455556666:role/example-role",
                     "AssumeRolePolicyDocument": "",
                     "CreateDate": "2020-03-11T00:02:27Z",
                     "Path": "/",
                     "RoleId": "AROAJ52OTH4H7LEXAMPLE",
                     "RoleName": "example-role",
                }
            ]
        }
    ],
    "MaxSessionDuration": 3600,
    "Path": "/",
    "PermissionsBoundary": {
        "PermissionsBoundaryArn": "arn:aws:iam::aws:policy/AdministratorAccess",
        "PermissionsBoundaryType": "PermissionsBoundaryPolicy"
    },
    "RoleId": "AROA4TPS3VLEXAMPLE",
    "RoleName": "BONESBootstrapHydra-OverbridgeOpsFunctionsLambda",
    "RolePolicyList": [
        {
            "PolicyName": "Example role policy"
        }
    ]
}
```

AwsIamUser

`AwsIamUser`Objek memberikan informasi tentang pengguna.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsIamUser` objek. Untuk melihat deskripsi `AwsIamUser` atribut, lihat AwsIamUserDetailsdi Referensi AWS Security Hub API.

Contoh

```
"AwsIamUser": {
    "AttachedManagedPolicies": [
        {
            "PolicyName": "ExamplePolicy",
            "PolicyArn": "arn:aws:iam::aws:policy/ExampleAccess"
        }
    ],
    "CreateDate": "2018-01-26T23:50:05.000Z",
    "GroupList": [],
```

```
    "Path": "/",
    "PermissionsBoundary" : {
        "PermissionsBoundaryArn" : "arn:aws:iam::aws:policy/AdministratorAccess",
        "PermissionsBoundaryType" : "PermissionsBoundaryPolicy"
    },
    "UserId": "AIDACKCEVSQ6C2EXAMPLE",
    "UserName": "ExampleUser",
    "UserPolicyList": [
        {
            "PolicyName": "InstancePolicy"
        }
    ]
}
```

AwsKinesis

Berikut ini adalah contoh Format Pencarian AWS Keamanan untuk `AwsKinesis` sumber daya.

AwsKinesisStream

`AwsKinesisStream`Objek ini memberikan detail tentang Amazon Kinesis Data Streams.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsKinesisStream` objek. Untuk melihat deskripsi `AwsKinesisStream` atribut, lihat AwsKinesisStreamDetailsdi Referensi AWS Security Hub API.

Contoh

```
"AwsKinesisStream": {
 "Name": "test-vir-kinesis-stream",
 "Arn": "arn:aws:kinesis:us-east-1:293279581038:stream/test-vir-kinesis-stream",
 "RetentionPeriodHours": 24,
 "ShardCount": 2,
 "StreamEncryption": {
  "EncryptionType": "KMS",
  "KeyId": "arn:aws:kms:us-east-1:293279581038:key/849cf029-4143-4c59-91f8-
ea76007247eb"
 }
}
```

AwsKms

Berikut ini adalah contoh Format Pencarian AWS Keamanan untuk `AwsKms` sumber daya.

AwsKmsKey

`AwsKmsKey`Objek memberikan rincian tentang file AWS KMS key.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsKmsKey` objek. Untuk melihat deskripsi `AwsKmsKey` atribut, lihat AwsKmsKeyDetailsdi Referensi AWS Security Hub API.

Contoh

```
"AwsKmsKey": {
                        "AWSAccountId": "string",
                        "CreationDate": "string",
                        "Description": "string",
                        "KeyId": "string",
                        "KeyManager": "string",
                        "KeyRotationStatus": boolean,
                        "KeyState": "string",
                        "Origin": "string"
                    }
```

AwsLambda

Berikut ini adalah contoh Format Pencarian AWS Keamanan untuk `AwsLambda` sumber daya.

AwsLambdaFunction

`AwsLambdaFunction`Objek memberikan rincian tentang konfigurasi fungsi Lambda.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsLambdaFunction` objek. Untuk melihat deskripsi `AwsLambdaFunction` atribut, lihat AwsLambdaFunctionDetailsdi Referensi AWS Security Hub API.

Contoh

```
"AwsLambdaFunction": {
    "Architectures": [
        "x86_64"
    ],
    "Code": {
        "S3Bucket": "DOC-EXAMPLE-BUCKET",
        "S3Key": "samplekey",
```

```
        "S3ObjectVersion": "2",
        "ZipFile": "myzip.zip"
    },
    "CodeSha256": "1111111111111abcdef",
    "DeadLetterConfig": {
        "TargetArn": "arn:aws:lambda:us-east-2:123456789012:queue:myqueue:2"
    },
    "Environment": {
        "Variables": {
            "Stage": "foobar"
         },
        "Error": {
            "ErrorCode": "Sample-error-code",
            "Message": "Caller principal is a manager."
         }
     },
    "FunctionName": "CheckOut",
    "Handler": "main.py:lambda_handler",
    "KmsKeyArn": "arn:aws:kms:us-west-2:123456789012:key/mykey",
    "LastModified": "2001-09-11T09:00:00Z",
    "Layers": {
        "Arn": "arn:aws:lambda:us-east-2:123456789012:layer:my-layer:3",
        "CodeSize": 169
    },
    "PackageType": "Zip",
    "RevisionId": "23",
    "Role": "arn:aws:iam::123456789012:role/Accounting-Role",
    "Runtime": "go1.7",
    "Timeout": 15,
    "TracingConfig": {
        "Mode": "Active"
    },
    "Version": "$LATEST$",
    "VpcConfig": {
        "SecurityGroupIds": ["sg-085912345678492fb", "sg-08591234567bdgdc"],
         "SubnetIds": ["subnet-071f712345678e7c8", "subnet-07fd123456788a036"]
    },
    "MasterArn": "arn:aws:lambda:us-east-2:123456789012:\$LATEST",
    "MemorySize": 2048
}
```

AwsLambdaLayerVersion

`AwsLambdaLayerVersion`Objek memberikan rincian tentang versi lapisan Lambda.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsLambdaLayerVersion` objek. Untuk melihat deskripsi `AwsLambdaLayerVersion` atribut, lihat AwsLambdaLayerVersionDetailsdi Referensi AWS Security Hub API.

Contoh

```
"AwsLambdaLayerVersion": {
    "Version": 2,
    "CompatibleRuntimes": [
        "java8"
    ],
    "CreatedDate": "2019-10-09T22:02:00.274+0000"
}
```

AwsMsk

Berikut ini adalah contoh Format Pencarian AWS Keamanan untuk `AwsMsk` sumber daya.

AwsMskCluster

`AwsMskCluster`Objek tersebut memberikan informasi tentang cluster Amazon Managed Streaming for Apache Kafka (Amazon MSK).

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsMskCluster` objek. Untuk melihat deskripsi `AwsMskCluster` atribut, lihat AwsMskClusterDetailsdi Referensi AWS Security Hub API.

Contoh

```
"AwsMskCluster": {
        "ClusterInfo": {
            "ClientAuthentication": {
                "Sasl": {
                    "Scram": {
                        "Enabled": true
                    },
                    "Iam": {
                        "Enabled": true
                    }
                },
                "Tls": {
```

```
                    "CertificateAuthorityArnList": [],
                    "Enabled": false
                },
                "Unauthenticated": {
                    "Enabled": false
                }
            },
            "ClusterName": "my-cluster",
            "CurrentVersion": "K2PWKAKR8XB7XF",
            "EncryptionInfo": {
                "EncryptionAtRest": {
                    "DataVolumeKMSKeyId": "arn:aws:kms:us-east-1:123456789012:key/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
                },
                "EncryptionInTransit": {
                    "ClientBroker": "TLS",
                    "InCluster": true
                }
            },
            "EnhancedMonitoring": "PER_TOPIC_PER_BROKER",
            "NumberOfBrokerNodes": 3
        }
}
```

AwsNetworkFirewall

Berikut ini adalah contoh Format Pencarian AWS Keamanan untuk `AwsNetworkFirewall` sumber daya.

AwsNetworkFirewallFirewall

`AwsNetworkFirewallFirewall`Objek berisi rincian tentang AWS Network Firewall firewall.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsNetworkFirewallFirewall` objek. Untuk melihat deskripsi `AwsNetworkFirewallFirewall` atribut, lihat AwsNetworkFirewallFirewallDetailsdi Referensi AWS Security Hub API.

Contoh

```
"AwsNetworkFirewallFirewall": {
    "DeleteProtection": false,
```

```
    "FirewallArn": "arn:aws:network-firewall:us-east-1:024665936331:firewall/
testfirewall",
    "FirewallPolicyArn": "arn:aws:network-firewall:us-east-1:444455556666:firewall-
policy/InitialFirewall",
    "FirewallId": "dea7d8e9-ae38-4a8a-b022-672a830a99fa",
    "FirewallName": "testfirewall",
    "FirewallPolicyChangeProtection": false,
    "SubnetChangeProtection": false,
    "SubnetMappings": [
        {
            "SubnetId": "subnet-0183481095e588cdc"
        },
        {
            "SubnetId": "subnet-01f518fad1b1c90b0"
        }
    ],
    "VpcId": "vpc-40e83c38"
}
```

AwsNetworkFirewallFirewallPolicy

`AwsNetworkFirewallFirewallPolicy`Objek memberikan rincian tentang kebijakan firewall. Kebijakan firewall mendefinisikan perilaku firewall jaringan.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsNetworkFirewallFirewallPolicy` objek. Untuk melihat deskripsi `AwsNetworkFirewallFirewallPolicy` atribut, lihat AwsNetworkFirewallFirewallPolicyDetailsdi Referensi AWS Security Hub API.

Contoh

```
"AwsNetworkFirewallFirewallPolicy": {
   "FirewallPolicy": {
    "StatefulRuleGroupReferences": [
        {
            "ResourceArn": "arn:aws:network-firewall:us-east-1:444455556666:stateful-
rulegroup/PatchesOnly"
        }
    ],
    "StatelessDefaultActions": [ "aws:forward_to_sfe" ],
    "StatelessFragmentDefaultActions": [ "aws:forward_to_sfe" ],
    "StatelessRuleGroupReferences": [
       {
```

```
          "Priority": 1,
          "ResourceArn": "arn:aws:network-firewall:us-east-1:444455556666:stateless-
rulegroup/Stateless-1"
       }
     ]
   },
   "FirewallPolicyArn": "arn:aws:network-firewall:us-east-1:444455556666:firewall-
policy/InitialFirewall",
   "FirewallPolicyId": "9ceeda22-6050-4048-a0ca-50ce47f0cc65",
   "FirewallPolicyName": "InitialFirewall",
   "Description": "Initial firewall"
}
```

AwsNetworkFirewallRuleGroup

`AwsNetworkFirewallRuleGroup`Objek memberikan rincian tentang kelompok AWS Network Firewall aturan. Kelompok aturan digunakan untuk memeriksa dan mengontrol lalu lintas jaringan. Kelompok aturan stateless berlaku untuk paket individu. Kelompok aturan stateful berlaku untuk paket dalam konteks arus lalu lintas mereka.

Grup aturan direferensikan dalam kebijakan firewall.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsNetworkFirewallRuleGroup` objek. Untuk melihat deskripsi `AwsNetworkFirewallRuleGroup` atribut, lihat AwsNetworkFirewallRuleGroupDetailsdi Referensi AWS Security Hub API.

Contoh - kelompok aturan tanpa kewarganegaraan

```
"AwsNetworkFirewallRuleGroup": {
    "Capacity": 600,
    "RuleGroupArn": "arn:aws:network-firewall:us-east-1:444455556666:stateless-
rulegroup/Stateless-1",
    "RuleGroupId": "fb13c4df-b6da-4c1e-91ec-84b7a5487493",
    "RuleGroupName": "Stateless-1"
    "Description": "Example of a stateless rule group",
    "Type": "STATELESS",
    "RuleGroup": {
        "RulesSource": {
            "StatelessRulesAndCustomActions": {
                "CustomActions": [],
                "StatelessRules": [
                    {
```

```
                        "Priority": 1,
                        "RuleDefinition": {
                            "Actions": [
                                "aws:pass"
                            ],
                            "MatchAttributes": {
                                "DestinationPorts": [
                                    {
                                        "FromPort": 443,
                                        "ToPort": 443
                                    }
                                ],
                                "Destinations": [
                                    {
                                        "AddressDefinition": "192.0.2.0/24"
                                    }
                                ],
                                "Protocols": [
                                           6
                                ],
                                "SourcePorts": [
                                    {
                                        "FromPort": 0,
                                        "ToPort": 65535
                                    }
                                ],
                                "Sources": [
                                    {
                                         "AddressDefinition": "198.51.100.0/24"
                                    }
                                ]
                            }
                        }
                    }
                ]
            }
        }
    }
}
```

Contoh - kelompok aturan stateful

```
"AwsNetworkFirewallRuleGroup": {
```

```
    "Capacity": 100,
    "RuleGroupArn": "arn:aws:network-firewall:us-east-1:444455556666:stateful-
rulegroup/tupletest",
    "RuleGroupId": "38b71c12-da80-4643-a6c5-03337f8933e0",
    "RuleGroupName": "ExampleRuleGroup",
    "Description": "Example of a stateful rule group",
    "Type": "STATEFUL",
    "RuleGroup": {
        "RuleSource": {
            "StatefulRules": [
                {
                    "Action": "PASS",
                    "Header": {
                        "Destination": "Any",
                        "DestinationPort": "443",
                        "Direction": "ANY",
                        "Protocol": "TCP",
                        "Source": "Any",
                        "SourcePort": "Any"
                    },
                    "RuleOptions": [
                        {
                           "Keyword": "sid:1"
                        }
                    ]
                }
            ]
         }
    }
}
```

Berikut ini adalah daftar contoh nilai yang valid untuk `AwsNetworkFirewallRuleGroup` atribut:

- `Action`

  Nilai yang valid: `PASS | DROP | ALERT`

- `Protocol`

  Nilai yang valid: `IP TCP | UDP | ICMP | HTTP | FTP | TLS | SMB | DNS | DCERPC | SSH | SMTP | IMAP | MSN | KRB5 | IKEV2 | TFTP | NTP | DHCP`

- `Flags`

Nilai yang valid: `FIN SYN | RST | PSH | ACK | URG | ECE | CWR`

- `Masks`

  Nilai yang valid: `FIN SYN | RST | PSH | ACK | URG | ECE | CWR`

AwsOpenSearchService

Berikut ini adalah contoh Format Pencarian AWS Keamanan untuk `AwsOpenSearchService` sumber daya.

AwsOpenSearchServiceDomain

`AwsOpenSearchServiceDomain`Objek berisi informasi tentang domain OpenSearch Layanan Amazon.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsOpenSearchServiceDomain` objek. Untuk melihat deskripsi `AwsOpenSearchServiceDomain` atribut, lihat AwsOpenSearchServiceDomainDetailsdi Referensi AWS Security Hub API.

Contoh

```
"AwsOpenSearchServiceDomain": {
    "AccessPolicies": "IAM_Id",
    "AdvancedSecurityOptions": {
        "Enabled": true,
        "InternalUserDatabaseEnabled": true,
        "MasterUserOptions": {
            "MasterUserArn": "arn:aws:iam::123456789012:user/third-master-use",
            "MasterUserName": "third-master-use",
            "MasterUserPassword": "some-password"
        }
    },
    "Arn": "arn:aws:Opensearch:us-east-1:111122223333:somedomain",
    "ClusterConfig": {
        "InstanceType": "c5.large.search",
        "InstanceCount": 1,
        "DedicatedMasterEnabled": true,
        "ZoneAwarenessEnabled": false,
        "ZoneAwarenessConfig": {
            "AvailabilityZoneCount": 2
```

```
        },
        "DedicatedMasterType": "c5.large.search",
        "DedicatedMasterCount": 3,
        "WarmEnabled": true,
        "WarmCount": 3,
        "WarmType": "ultrawarm1.large.search"
    },
    "DomainEndpoint": "https://es-2021-06-23t17-04-qowmgghud5vofgb5e4wmi.eu-
central-1.es.amazonaws.com",
    "DomainEndpointOptions": {
        "EnforceHTTPS": false,
        "TLSSecurityPolicy": "Policy-Min-TLS-1-0-2019-07",
        "CustomEndpointCertificateArn": "arn:aws:acm:us-
east-1:111122223333:certificate/bda1bff1-79c0-49d0-abe6-50a15a7477d4",
        "CustomEndpointEnabled": true,
        "CustomEndpoint": "example.com"
    },
    "DomainEndpoints": {
        "vpc": "vpc-endpoint-h2dsd34efgyghrtguk5gt6j2foh4.us-east-1.es.amazonaws.com"
    },
    "DomainName": "my-domain",
    "EncryptionAtRestOptions": {
        "Enabled": false,
        "KmsKeyId": "1a2a3a4-1a2a-3a4a-5a6a-1a2a3a4a5a6a"
    },
    "EngineVersion": "7.1",
    "Id": "123456789012",
    "LogPublishingOptions": {
        "IndexSlowLogs": {
            "CloudWatchLogsLogGroupArn": "arn:aws:logs:us-east-1:111122223333:log-
group:/aws/aes/domains/es-index-slow-logs",
            "Enabled": true
        },
        "SearchSlowLogs": {
            "CloudWatchLogsLogGroupArn": "arn:aws:logs:us-east-1:111122223333:log-
group:/aws/aes/domains/es-slow-logs",
            "Enabled": true
        },
        "AuditLogs": {
            "CloudWatchLogsLogGroupArn": "arn:aws:logs:us-east-1:111122223333:log-
group:/aws/aes/domains/es-slow-logs",
            "Enabled": true
        }
    },
```

```
    "NodeToNodeEncryptionOptions": {
        "Enabled": true
    },
    "ServiceSoftwareOptions": {
        "AutomatedUpdateDate": "2022-04-28T14:08:37.000Z",
        "Cancellable": false,
        "CurrentVersion": "R20210331",
        "Description": "There is no software update available for this domain.",
        "NewVersion": "OpenSearch_1.0",
        "UpdateAvailable": false,
        "UpdateStatus": "COMPLETED",
        "OptionalDeployment": false
    },
    "VpcOptions": {
        "SecurityGroupIds": [
            "sg-2a3a4a5a"
        ],
        "SubnetIds": [
            "subnet-1a2a3a4a"
        ],
    }
}
```

AwsRds

Berikut ini adalah contoh Format Pencarian AWS Keamanan untuk `AwsRds` sumber daya.

AwsRdsDbCluster

`AwsRdsDbCluster`Objek memberikan rincian tentang cluster database Amazon RDS.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsRdsDbCluster` objek. Untuk melihat deskripsi `AwsRdsDbCluster` atribut, lihat AwsRdsDbClusterDetailsdi Referensi AWS Security Hub API.

Contoh

```
"AwsRdsDbCluster": {
    "ActivityStreamStatus": "stopped",
    "AllocatedStorage": 1,
    "AssociatedRoles": [
        {
        "RoleArn": "arn:aws:iam::777788889999:role/aws-service-role/rds.amazonaws.com/
AWSServiceRoleForRDS",
```

```
        "Status": "PENDING"
        }
    ],
    "AutoMinorVersionUpgrade": true,
    "AvailabilityZones": [
        "us-east-1a",
        "us-east-1c",
        "us-east-1e"
    ],
    "BackupRetentionPeriod": 1,
    "ClusterCreateTime": "2020-06-22T17:40:12.322Z",
    "CopyTagsToSnapshot": true,
    "CrossAccountClone": false,
    "CustomEndpoints": [],
    "DatabaseName": "Sample name",
    "DbClusterIdentifier": "database-3",
    "DbClusterMembers": [
        {
        "DbClusterParameterGroupStatus": "in-sync",
        "DbInstanceIdentifier": "database-3-instance-1",
        "IsClusterWriter": true,
        "PromotionTier": 1,
        }
    ],
    "DbClusterOptionGroupMemberships": [],
    "DbClusterParameterGroup": "cluster-parameter-group",
    "DbClusterResourceId": "cluster-example",
    "DbSubnetGroup": "subnet-group",
    "DeletionProtection": false,
    "DomainMemberships": [],
    "Status": "modifying",
    "EnabledCloudwatchLogsExports": [
        "audit",
        "error",
        "general",
        "slowquery"
    ],
    "Endpoint": "database-3.cluster-example.us-east-1.rds.amazonaws.com",
    "Engine": "aurora-mysql",
    "EngineMode": "provisioned",
    "EngineVersion": "5.7.mysql_aurora.2.03.4",
    "HostedZoneId": "ZONE1",
    "HttpEndpointEnabled": false,
    "IamDatabaseAuthenticationEnabled": false,
```

```
    "KmsKeyId": "arn:aws:kms:us-east-1:777788889999:key/key1",
    "MasterUsername": "admin",
    "MultiAz": false,
    "Port": 3306,
    "PreferredBackupWindow": "04:52-05:22",
    "PreferredMaintenanceWindow": "sun:09:32-sun:10:02",
    "ReaderEndpoint": "database-3.cluster-ro-example.us-east-1.rds.amazonaws.com",
    "ReadReplicaIdentifiers": [],
    "Status": "Modifying",
    "StorageEncrypted": true,
    "VpcSecurityGroups": [
        {
            "Status": "active",
            "VpcSecurityGroupId": "sg-example-1"
        }
    ],
}
```

AwsRdsDbClusterSnapshot

`AwsRdsDbClusterSnapshot`Objek berisi informasi tentang snapshot cluster Amazon RDS DB.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsRdsDbClusterSnapshot` objek. Untuk melihat deskripsi `AwsRdsDbClusterSnapshot` atribut, lihat AwsRdsDbClusterSnapshotDetailsdi Referensi AWS Security Hub API.

Contoh

```
"AwsRdsDbClusterSnaphot": {
    "AllocatedStorage": 0,
    "AvailabilityZones": [
        "us-east-1a",
        "us-east-1d",
        "us-east-1e"
    ],
    "ClusterCreateTime": "2020-06-12T13:23:15.577Z",
    "DbClusterIdentifier": "database-2",
    "DbClusterSnapshotAttributes": [{
        "AttributeName": "restore",
        "AttributeValues": ["123456789012"]
    }],
    "DbClusterSnapshotIdentifier": "rds:database-2-2020-06-23-03-52",
    "Engine": "aurora",
```

```
    "EngineVersion": "5.6.10a",
    "IamDatabaseAuthenticationEnabled": false,
    "KmsKeyId": "arn:aws:kms:us-east-1:777788889999:key/key1",
    "LicenseModel": "aurora",
    "MasterUsername": "admin",
    "PercentProgress": 100,
    "Port": 0,
    "SnapshotCreateTime": "2020-06-22T17:40:12.322Z",
    "SnapshotType": "automated",
    "Status": "available",
    "StorageEncrypted": true,
    "VpcId": "vpc-faf7e380"
}
```

AwsRdsDbInstance

`AwsRdsDbInstance`Objek memberikan detail tentang instans Amazon RDS DB.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsRdsDbInstance` objek. Untuk melihat deskripsi `AwsRdsDbInstance` atribut, lihat AwsRdsDbInstanceDetailsdi Referensi AWS Security Hub API.

Contoh

```
"AwsRdsDbInstance": {
    "AllocatedStorage": 20,
    "AssociatedRoles": [],
    "AutoMinorVersionUpgrade": true,
    "AvailabilityZone": "us-east-1d",
    "BackupRetentionPeriod": 7,
    "CaCertificateIdentifier": "certificate1",
    "CharacterSetName": "",
    "CopyTagsToSnapshot": true,
    "DbClusterIdentifier": "",
    "DbInstanceArn": "arn:aws:rds:us-east-1:111122223333:db:database-1",
    "DbInstanceClass": "db.t2.micro",
    "DbInstanceIdentifier": "database-1",
    "DbInstancePort": 0,
    "DbInstanceStatus": "available",
    "DbiResourceId": "db-EXAMPLE123",
    "DbName": "",
    "DbParameterGroups": [
        {
```

```
            "DbParameterGroupName": "default.mysql5.7",
            "ParameterApplyStatus": "in-sync"
        }
    ],
    "DbSecurityGroups": [],


    "DbSubnetGroup": {
        "DbSubnetGroupName": "my-group-123abc",
        "DbSubnetGroupDescription": "My subnet group",
        "VpcId": "vpc-example1",
        "SubnetGroupStatus": "Complete",
        "Subnets": [
            {
                "SubnetIdentifier": "subnet-123abc",
                "SubnetAvailabilityZone": {
                    "Name": "us-east-1d"
                },
                "SubnetStatus": "Active"
            },
            {
                "SubnetIdentifier": "subnet-456def",
                "SubnetAvailabilityZone": {
                    "Name": "us-east-1c"
                },
                "SubnetStatus": "Active"
            }
      ],
        "DbSubnetGroupArn": ""
    },
    "DeletionProtection": false,
    "DomainMemberships": [],
    "EnabledCloudWatchLogsExports": [],
    "Endpoint": {
        "address": "database-1.example.us-east-1.rds.amazonaws.com",
        "port": 3306,
        "hostedZoneId": "ZONEID1"
    },
    "Engine": "mysql",
    "EngineVersion": "5.7.22",
    "EnhancedMonitoringResourceArn": "arn:aws:logs:us-east-1:111122223333:log-
group:Example:log-stream:db-EXAMPLE1",
    "IamDatabaseAuthenticationEnabled": false,
    "InstanceCreateTime": "2020-06-22T17:40:12.322Z",
```

```
    "Iops": "",
    "KmsKeyId": "",
    "LatestRestorableTime": "2020-06-24T05:50:00.000Z",
    "LicenseModel": "general-public-license",
    "ListenerEndpoint": "",
    "MasterUsername": "admin",
    "MaxAllocatedStorage": 1000,
    "MonitoringInterval": 60,
    "MonitoringRoleArn": "arn:aws:iam::111122223333:role/rds-monitoring-role",
    "MultiAz": false,
    "OptionGroupMemberships": [
        {
            "OptionGroupName": "default:mysql-5-7",
            "Status": "in-sync"
        }
    ],
    "PreferredBackupWindow": "03:57-04:27",
    "PreferredMaintenanceWindow": "thu:10:13-thu:10:43",
    "PendingModifiedValues": {
        "DbInstanceClass": "",
        "AllocatedStorage": "",
        "MasterUserPassword": "",
        "Port": "",
        "BackupRetentionPeriod": "",
        "MultiAZ": "",
        "EngineVersion": "",
        "LicenseModel": "",
        "Iops": "",
        "DbInstanceIdentifier": "",
        "StorageType": "",
        "CaCertificateIdentifier": "",
        "DbSubnetGroupName": "",
        "PendingCloudWatchLogsExports": "",
        "ProcessorFeatures": []
    },
    "PerformanceInsightsEnabled": false,
    "PerformanceInsightsKmsKeyId": "",
    "PerformanceInsightsRetentionPeriod": "",
    "ProcessorFeatures": [],
    "PromotionTier": "",
    "PubliclyAccessible": false,
    "ReadReplicaDBClusterIdentifiers": [],
    "ReadReplicaDBInstanceIdentifiers": [],
    "ReadReplicaSourceDBInstanceIdentifier": "",
```

```
    "SecondaryAvailabilityZone": "",
    "StatusInfos": [],
    "StorageEncrypted": false,
    "StorageType": "gp2",
    "TdeCredentialArn": "",
    "Timezone": "",
    "VpcSecurityGroups": [
        {
            "VpcSecurityGroupId": "sg-example1",
            "Status": "active"
        }
    ]
}
```

AwsRdsDbSecurityGroup

`AwsRdsDbSecurityGroup`Objek berisi informasi tentang Amazon Relational Database Service

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsRdsDbSecurityGroup` objek. Untuk melihat deskripsi `AwsRdsDbSecurityGroup` atribut, lihat AwsRdsDbSecurityGroupDetailsdi Referensi AWS Security Hub API.

Contoh

```
"AwsRdsDbSecurityGroup": {
    "DbSecurityGroupArn": "arn:aws:rds:us-west-1:111122223333:secgrp:default",
    "DbSecurityGroupDescription": "default",
    "DbSecurityGroupName": "mysecgroup",
    "Ec2SecurityGroups": [
        {
          "Ec2SecurityGroupuId": "myec2group",
          "Ec2SecurityGroupName": "default",
          "Ec2SecurityGroupOwnerId": "987654321021",
          "Status": "authorizing"
        }
    ],
    "IpRanges": [
        {
          "Cidrip": "0.0.0.0/0",
          "Status": "authorizing"
        }
    ],
    "OwnerId": "123456789012",
```

```
    "VpcId": "vpc-1234567f"
}
```

AwsRdsDbSnapshot

`AwsRdsDbSnapshot`Objek berisi detail tentang snapshot cluster Amazon RDS DB.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsRdsDbSnapshot` objek. Untuk melihat deskripsi `AwsRdsDbSnapshot` atribut, lihat AwsRdsDbSnapshotDetailsdi Referensi AWS Security Hub API.

Contoh

```
"AwsRdsDbSnapshot": {
    "DbSnapshotIdentifier": "rds:database-1-2020-06-22-17-41",
    "DbInstanceIdentifier": "database-1",
    "SnapshotCreateTime": "2020-06-22T17:41:29.967Z",
    "Engine": "mysql",
    "AllocatedStorage": 20,
    "Status": "available",
    "Port": 3306,
    "AvailabilityZone": "us-east-1d",
    "VpcId": "vpc-example1",
    "InstanceCreateTime": "2020-06-22T17:40:12.322Z",
    "MasterUsername": "admin",
    "EngineVersion": "5.7.22",
    "LicenseModel": "general-public-license",
    "SnapshotType": "automated",
    "Iops": null,
    "OptionGroupName": "default:mysql-5-7",
    "PercentProgress": 100,
    "SourceRegion": null,
    "SourceDbSnapshotIdentifier": "",
    "StorageType": "gp2",
    "TdeCredentialArn": "",
    "Encrypted": false,
    "KmsKeyId": "",
    "Timezone": "",
    "IamDatabaseAuthenticationEnabled": false,
    "ProcessorFeatures": [],
    "DbiResourceId": "db-resourceexample1"
}
```

AwsRdsEventSubscription

`AwsRdsEventSubscription`Berisi rincian tentang langganan pemberitahuan acara RDS. Langganan memungkinkan RDS untuk memposting acara ke topik SNS.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsRdsEventSubscription` objek. Untuk melihat deskripsi `AwsRdsEventSubscription` atribut, lihat AwsRdsEventSubscriptionDetailsdi Referensi AWS Security Hub API.

Contoh

```
"AwsRdsEventSubscription": {
    "CustSubscriptionId": "myawsuser-secgrp",
    "CustomerAwsId": "111111111111",
    "Enabled": true,
    "EventCategoriesList": [
        "configuration change",
        "failure"
    ],
    "EventSubscriptionArn": "arn:aws:rds:us-east-1:111111111111:es:my-instance-events",
    "SnsTopicArn": "arn:aws:sns:us-east-1:111111111111:myawsuser-RDS",
    "SourceIdsList": [
        "si-sample",
        "mysqldb-rr"
    ],
    "SourceType": "db-security-group",
    "Status": "creating",
    "SubscriptionCreationTime": "2021-06-27T01:38:01.090Z"
}
```

AwsRedshift

Berikut ini adalah contoh Format Pencarian AWS Keamanan untuk `AwsRedshift` sumber daya.

AwsRedshiftCluster

`AwsRedshiftCluster`Objek berisi detail tentang cluster Amazon Redshift.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsRedshiftCluster` objek. Untuk melihat deskripsi `AwsRedshiftCluster` atribut, lihat AwsRedshiftClusterDetailsdi Referensi AWS Security Hub API.

Contoh


```
"AwsRedshiftCluster": {
    "AllowVersionUpgrade": true,
    "AutomatedSnapshotRetentionPeriod": 1,
    "AvailabilityZone": "us-west-2d",
    "ClusterAvailabilityStatus": "Unavailable",
    "ClusterCreateTime": "2020-08-03T19:22:44.637Z",
    "ClusterIdentifier": "redshift-cluster-1",
    "ClusterNodes": [
        {
            "NodeRole": "LEADER",
            "PrivateIPAddress": "192.0.2.108",
            "PublicIPAddress": "198.51.100.29"
        },
        {
            "NodeRole": "COMPUTE-0",
            "PrivateIPAddress": "192.0.2.22",
            "PublicIPAddress": "198.51.100.63"
        },
        {
             "NodeRole": "COMPUTE-1",
             "PrivateIPAddress": "192.0.2.224",
             "PublicIPAddress": "198.51.100.226"
        }
        ],
    "ClusterParameterGroups": [
        {
            "ClusterParameterStatusList": [
                {
                    "ParameterName": "max_concurrency_scaling_clusters",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
                {
                    "ParameterName": "enable_user_activity_logging",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
                {
                    "ParameterName": "auto_analyze",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
```

```
                {
                    "ParameterName": "query_group",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
                {
                    "ParameterName": "datestyle",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
                {
                    "ParameterName": "extra_float_digits",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
                {
                    "ParameterName": "search_path",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
                {
                    "ParameterName": "statement_timeout",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
                {
                    "ParameterName": "wlm_json_configuration",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
                {
                    "ParameterName": "require_ssl",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
                {
                    "ParameterName": "use_fips_ssl",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                }
            ],
            "ParameterApplyStatus": "in-sync",
            "ParameterGroupName": "temp"
        }
```

```
    ],
    "ClusterPublicKey": "JalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY Amazon-Redshift",
    "ClusterRevisionNumber": 17498,
    "ClusterSecurityGroups": [
        {
            "ClusterSecurityGroupName": "default",
            "Status": "active"
        }
    ],
    "ClusterSnapshotCopyStatus": {
        "DestinationRegion": "us-west-2",
        "ManualSnapshotRetentionPeriod": -1,
        "RetentionPeriod": 1,
        "SnapshotCopyGrantName": "snapshotCopyGrantName"
    },
    "ClusterStatus": "available",
    "ClusterSubnetGroupName": "default",
    "ClusterVersion": "1.0",
    "DBName": "dev",
    "DeferredMaintenanceWindows": [
        {
            "DeferMaintenanceEndTime": "2020-10-07T20:34:01.000Z",
            "DeferMaintenanceIdentifier": "deferMaintenanceIdentifier",
            "DeferMaintenanceStartTime": "2020-09-07T20:34:01.000Z"
        }
     ],
    "ElasticIpStatus": {
        "ElasticIp": "203.0.113.29",
        "Status": "active"
    },
    "ElasticResizeNumberOfNodeOptions": "4",
    "Encrypted": false,
    "Endpoint": {
        "Address": "redshift-cluster-1.example.us-west-2.redshift.amazonaws.com",
        "Port": 5439
    },
    "EnhancedVpcRouting": false,
    "ExpectedNextSnapshotScheduleTime": "2020-10-13T20:34:01.000Z",
    "ExpectedNextSnapshotScheduleTimeStatus": "OnTrack",
    "HsmStatus": {
        "HsmClientCertificateIdentifier": "hsmClientCertificateIdentifier",
        "HsmConfigurationIdentifier": "hsmConfigurationIdentifier",
        "Status": "applying"
    },
```

```
    "IamRoles": [
        {
             "ApplyStatus": "in-sync",
             "IamRoleArn": "arn:aws:iam::111122223333:role/RedshiftCopyUnload"
        }
    ],
    "KmsKeyId": "kmsKeyId",
    "LoggingStatus": {
        "BucketName": "test-bucket",
        "LastFailureMessage": "test message",
        "LastFailureTime": "2020-08-09T13:00:00.000Z",
        "LastSuccessfulDeliveryTime": "2020-08-08T13:00:00.000Z",
        "LoggingEnabled": true,
        "S3KeyPrefix": "/"
    },
    "MaintenanceTrackName": "current",
    "ManualSnapshotRetentionPeriod": -1,
    "MasterUsername": "awsuser",
    "NextMaintenanceWindowStartTime": "2020-08-09T13:00:00.000Z",
    "NodeType": "dc2.large",
    "NumberOfNodes": 2,
    "PendingActions": [],
    "PendingModifiedValues": {
        "AutomatedSnapshotRetentionPeriod": 0,
        "ClusterIdentifier": "clusterIdentifier",
        "ClusterType": "clusterType",
        "ClusterVersion": "clusterVersion",
        "EncryptionType": "None",
        "EnhancedVpcRouting": false,
        "MaintenanceTrackName": "maintenanceTrackName",
        "MasterUserPassword": "masterUserPassword",
        "NodeType": "dc2.large",
        "NumberOfNodes": 1,
        "PubliclyAccessible": true
    },
    "PreferredMaintenanceWindow": "sun:13:00-sun:13:30",
    "PubliclyAccessible": true,
    "ResizeInfo": {
        "AllowCancelResize": true,
        "ResizeType": "ClassicResize"
    },
    "RestoreStatus": {
        "CurrentRestoreRateInMegaBytesPerSecond": 15,
        "ElapsedTimeInSeconds": 120,
```

```
        "EstimatedTimeToCompletionInSeconds": 100,
        "ProgressInMegaBytes": 10,
        "SnapshotSizeInMegaBytes": 1500,
        "Status": "restoring"
    },
    "SnapshotScheduleIdentifier": "snapshotScheduleIdentifier",
    "SnapshotScheduleState": "ACTIVE",
     "VpcId": "vpc-example",
    "VpcSecurityGroups": [
        {
            "Status": "active",
            "VpcSecurityGroupId": "sg-example"
        }
    ]
}
```

AwsRoute53

Berikut ini adalah contoh Format Pencarian AWS Keamanan untuk `AwsRoute53` sumber daya.

AwsRoute53HostedZone

`AwsRoute53HostedZone`Objek memberikan informasi tentang zona yang dihosting Amazon Route 53, termasuk empat server nama yang ditetapkan ke zona yang dihosting. Zona yang dihosting mewakili kumpulan catatan yang dapat dikelola bersama, milik nama domain induk tunggal.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsRoute53HostedZone` objek. Untuk melihat deskripsi `AwsRoute53HostedZone` atribut, lihat AwsRoute53 HostedZoneDetails di Referensi AWS Security Hub API.

Contoh

```
"AwsRoute53HostedZone": {
    "HostedZone": {
        "Id": "Z06419652JEMGO9TA2XKL",
        "Name": "asff.testing",
        "Config": {
            "Comment": "This is an example comment."
        }
    },
    "NameServers": [
        "ns-470.awsdns-32.net",
        "ns-1220.awsdns-12.org",
```

```
        "ns-205.awsdns-13.com",
        "ns-1960.awsdns-51.co.uk"
    ],
    "QueryLoggingConfig": {
        "CloudWatchLogsLogGroupArn": {
            "CloudWatchLogsLogGroupArn": "arn:aws:logs:us-east-1:123456789012:log-
group:asfftesting:*",
            "Id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
            "HostedZoneId": "Z00932193AF5H180PPNZD"
        }
    },
    "Vpcs": [
        {
            "Id": "vpc-05d7c6e36bc03ea76",
            "Region": "us-east-1"
        }
    ]
}
```

AwsS3

Berikut ini adalah contoh Format Pencarian AWS Keamanan untuk `AwsS3` sumber daya.

AwsS3AccessPoint

`AwsS3AccessPoint`memberikan informasi tentang jalur akses Amazon S3. Titik akses S3 diberi nama titik akhir jaringan yang dilampirkan ke bucket S3 yang dapat Anda gunakan untuk melakukan operasi objek S3.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsS3AccessPoint` objek. Untuk melihat deskripsi *`AwsS3AccessPoint`* atribut, lihat AWSS3 AccessPointDetails di Referensi API.AWS Security Hub

Contoh

```
"AwsS3AccessPoint": {
        "AccessPointArn": "arn:aws:s3:us-east-1:123456789012:accesspoint/asff-access-
point",
        "Alias": "asff-access-point-hrzrlukc5m36ft7okagglf3gmwluquse1b-s3alias",
        "Bucket": "DOC-EXAMPLE-BUCKET1",
        "BucketAccountId": "123456789012",
        "Name": "asff-access-point",
        "NetworkOrigin": "VPC",
```

```
        "PublicAccessBlockConfiguration": {
            "BlockPublicAcls": true,
            "BlockPublicPolicy": true,
            "IgnorePublicAcls": true,
            "RestrictPublicBuckets": true
        },
        "VpcConfiguration": {
            "VpcId": "vpc-1a2b3c4d5e6f1a2b3"
        }
}
```

AwsS3AccountPublicAccessBlock

`AwsS3AccountPublicAccessBlock`memberikan informasi tentang konfigurasi Blok Akses Publik Amazon S3 untuk akun.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsS3AccountPublicAccessBlock` objek. Untuk melihat deskripsi *`AwsS3AccountPublicAccessBlock`* atribut, lihat AWSS3 AccountPublicAccessBlockDetails di Referensi API.AWS Security Hub

Contoh

```
"AwsS3AccountPublicAccessBlock": {
    "BlockPublicAcls": true,
    "BlockPublicPolicy": true,
    "IgnorePublicAcls": false,
    "RestrictPublicBuckets": true
}
```

AwsS3Bucket

`AwsS3Bucket`Objek tersebut memberikan detail tentang bucket Amazon S3.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsS3Bucket` objek. Untuk melihat deskripsi *`AwsS3Bucket`* atribut, lihat AWSS3 BucketDetails di Referensi API.AWS Security Hub

Contoh

```
"AwsS3Bucket": {
    "AccessControlList": "{\"grantSet\":null,\"grantList\":[{\"grantee\":{\"id\":
\"4df55416215956920d9d056aa8b99803a294ea221222bb668b55a8c6bca81094\",\"displayName
```

```
\":null},\"permission\":\"FullControl\"},{\"grantee\":\"AllUsers\",\"permission\":
\"ReadAcp\"},{\"grantee\":\"AuthenticatedUsers\",\"permission\":\"ReadAcp\"}",,
    "BucketLifecycleConfiguration": {
       "Rules": [
           {
               "AbortIncompleteMultipartUpload": {
                   "DaysAfterInitiation": 5
               },
               "ExpirationDate": "2021-11-10T00:00:00.000Z",
               "ExpirationInDays": 365,
               "ExpiredObjectDeleteMarker": false,
               "Filter": {
                   "Predicate": {
                       "Operands": [
                           {
                               "Prefix": "tmp/",
                               "Type": "LifecyclePrefixPredicate"
                           },
                           {
                               "Tag": {
                                   "Key": "ArchiveAge",
                                   "Value": "9m"
                               },
                               "Type": "LifecycleTagPredicate"
                           }
                       ],
                       "Type": "LifecycleAndOperator"
                   }
               },
               "ID": "Move rotated logs to Glacier",
               "NoncurrentVersionExpirationInDays": -1,
               "NoncurrentVersionTransitions": [
                   {
                       "Days": 2,
                       "StorageClass": "GLACIER"
                   }
               ],
               "Prefix": "rotated/",
               "Status": "Enabled",
               "Transitions": [
                   {
                       "Date": "2020-11-10T00:00:00.000Z",
                       "Days": 100,
                       "StorageClass": "GLACIER"
```

```
                }
            ]
        }
    ]
},
"BucketLoggingConfiguration": {
 "DestinationBucketName": "s3serversideloggingbucket-858726136312",
 "LogFilePrefix": "buckettestreadwrite23435/"
},
"BucketName": "DOC-EXAMPLE-BUCKET1",
"BucketNotificationConfiguration": {
 "Configurations": [{
  "Destination": "arn:aws:lambda:us-east-1:123456789012:function:s3_public_write",
  "Events": [
   "s3:ObjectCreated:Put"
  ],
  "Filter": {
   "S3KeyFilter": {
    "FilterRules": [
    {
     "Name": "AffS3BucketNotificationConfigurationS3KeyFilterRuleName.PREFIX",
     "Value": "pre"
    },
    {
     "Name": "AffS3BucketNotificationConfigurationS3KeyFilterRuleName.SUFFIX",
     "Value": "suf"
    },
    ]
   }
  },
  "Type": "LambdaConfiguration"
 }]
},
"BucketVersioningConfiguration": {
 "IsMfaDeleteEnabled": true,
 "Status": "Off"
},
"BucketWebsiteConfiguration": {
 "ErrorDocument": "error.html",
 "IndexDocumentSuffix": "index.html",
 "RedirectAllRequestsTo": {
  "HostName": "example.com",
  "Protocol": "http"
 },
```

```
     "RoutingRules": [{
      "Condition": {
       "HttpErrorCodeReturnedEquals": "Redirected",
       "KeyPrefixEquals": "index"
         },
      "Redirect": {
       "HostName": "example.com",
       "HttpRedirectCode": "401",
       "Protocol": "HTTP",
       "ReplaceKeyPrefixWith": "string",
       "ReplaceKeyWith": "string"
      }
     }]
    },
    "CreatedAt": "2007-11-30T01:46:56.000Z",
    "ObjectLockConfiguration": {
     "ObjectLockEnabled": "Enabled",
     "Rule": {
      "DefaultRetention": {
       "Days": null,
       "Mode": "GOVERNANCE",
       "Years": 12
      },
     },
    },
    "OwnerId": "AIDACKCEVSQ6C2EXAMPLE",
    "OwnerName": "s3bucketowner",
    "PublicAccessBlockConfiguration": {
        "BlockPublicAcls": true,
        "BlockPublicPolicy": true,
        "IgnorePublicAcls": true,
        "RestrictPublicBuckets": true,
    },
    "ServerSideEncryptionConfiguration": {
        "Rules": [
            {
                "ApplyServerSideEncryptionByDefault": {
                    "SSEAlgorithm": "AES256",
                    "KMSMasterKeyID": "12345678-abcd-abcd-abcd-123456789012"
                }
            }
        ]
     }
```

```
}
```

AwsS3Object

`AwsS3Object`Objek memberikan informasi tentang objek Amazon S3.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsS3Object` objek. Untuk melihat deskripsi *`AwsS3Object`* atribut, lihat AWSS3 ObjectDetails di Referensi API.AWS Security Hub

Contoh

```
"AwsS3Object": {
    "ContentType": "text/html",
    "ETag": "\"30a6ec7e1a9ad79c203d05a589c8b400\"",
    "LastModified": "2012-04-23T18:25:43.511Z",
    "ServerSideEncryption": "aws:kms",
    "SSEKMSKeyId": "arn:aws:kms:us-west-2:123456789012:key/4dff8393-e225-4793-
a9a0-608ec069e5a7",
    "VersionId": "ws31OurgOOjH_HHllIxPE35P.MELYaYh"
}
```

AwsSageMaker

Berikut ini adalah contoh Format Pencarian AWS Keamanan untuk `AwsSageMaker` sumber daya.

AwsSageMakerNotebookInstance

`AwsSageMakerNotebookInstance`Objek menyediakan informasi tentang instance SageMaker notebook Amazon, yang merupakan instance komputasi pembelajaran mesin yang menjalankan Aplikasi Notebook Jupyter.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsSageMakerNotebookInstance` objek. Untuk melihat deskripsi `AwsSageMakerNotebookInstance` atribut, lihat AwsSageMakerNotebookInstanceDetailsdi Referensi AWS Security Hub API.

Contoh

```
"AwsSageMakerNotebookInstance": {
    "DirectInternetAccess": "Disabled",
    "InstanceMetadataServiceConfiguration": {
     "MinimumInstanceMetadataServiceVersion": "1",
```

```
    },
    "InstanceType": "ml.t2.medium",
    "LastModifiedTime": "2022-09-09 22:48:32.012000+00:00",
    "NetworkInterfaceId": "eni-06c09ac2541a1bed3",
    "NotebookInstanceArn": "arn:aws:sagemaker:us-east-1:001098605940:notebook-instance/
sagemakernotebookinstancerootaccessdisabledcomplia-8myjcyofzixm",
    "NotebookInstanceName":
 "SagemakerNotebookInstanceRootAccessDisabledComplia-8MYjcyofZiXm",
    "NotebookInstanceStatus": "InService",
    "PlatformIdentifier": "notebook-al1-v1",
    "RoleArn": "arn:aws:iam::001098605940:role/sechub-SageMaker-1-scenar-
SageMakerCustomExecution-1R0X32HGC38IW",
    "RootAccess": "Disabled",
    "SecurityGroups": [
     "sg-06b347359ab068745"
    ],
    "SubnetId": "subnet-02c0deea5fa64578e",
    "Url":
 "sagemakernotebookinstancerootaccessdisabledcomplia-8myjcyofzixm.notebook.us-
east-1.sagemaker.aws",
    "VolumeSizeInGB": 5
}
```

AwsSecretsManager

Berikut ini adalah contoh Format Pencarian AWS Keamanan untuk `AwsSecretsManager` sumber daya.

AwsSecretsManagerSecret

`AwsSecretsManagerSecret`Objek memberikan rincian tentang rahasia Secrets Manager.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsSecretsManagerSecret` objek. Untuk melihat deskripsi `AwsSecretsManagerSecret` atribut, lihat AwsSecretsManagerSecretDetailsdi Referensi AWS Security Hub API.

Contoh

```
"AwsSecretsManagerSecret": {
    "RotationRules": {
        "AutomaticallyAfterDays": 30
    },
    "RotationOccurredWithinFrequency": true,
```

```
    "KmsKeyId": "kmsKeyId",
    "RotationEnabled": true,
    "RotationLambdaArn": "arn:aws:lambda:us-
west-2:777788889999:function:MyTestRotationLambda",
    "Deleted": false,
    "Name": "MyTestDatabaseSecret",
    "Description": "My test database secret"
}
```

AwsSns

Berikut ini adalah contoh Format Pencarian AWS Keamanan untuk `AwsSns` sumber daya.

AwsSnsTopic

`AwsSnsTopic`Objek berisi rincian tentang topik Amazon Simple Notification Service.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsSnsTopic` objek. Untuk melihat deskripsi `AwsSnsTopic` atribut, lihat AwsSnsTopicDetailsdi Referensi AWS Security Hub API.

Contoh

```
"AwsSnsTopic": {
    "ApplicationSuccessFeedbackRoleArn": "arn:aws:iam::123456789012:role/
ApplicationSuccessFeedbackRoleArn",
    "FirehoseFailureFeedbackRoleArn": "arn:aws:iam::123456789012:role/
FirehoseFailureFeedbackRoleArn",
    "FirehoseSuccessFeedbackRoleArn": "arn:aws:iam::123456789012:role/
FirehoseSuccessFeedbackRoleArn",
    "HttpFailureFeedbackRoleArn": "arn:aws:iam::123456789012:role/
HttpFailureFeedbackRoleArn",
    "HttpSuccessFeedbackRoleArn": "arn:aws:iam::123456789012:role/
HttpSuccessFeedbackRoleArn",
    "KmsMasterKeyId": "alias/ExampleAlias",
    "Owner": "123456789012",
    "SqsFailureFeedbackRoleArn": "arn:aws:iam::123456789012:role/
SqsFailureFeedbackRoleArn",
    "SqsSuccessFeedbackRoleArn": "arn:aws:iam::123456789012:role/
SqsSuccessFeedbackRoleArn",
    "Subscription": {
         "Endpoint": "http://sampleendpoint.com",
         "Protocol": "http"
    },
```

```
    "TopicName": "SampleTopic"
}
```

AwsSqs

Berikut ini adalah contoh Format Pencarian AWS Keamanan untuk `AwsSqs` sumber daya.

AwsSqsQueue

`AwsSqsQueue`Objek berisi informasi tentang antrian Amazon Simple Queue Service.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsSqsQueue` objek. Untuk melihat deskripsi `AwsSqsQueue` atribut, lihat AwsSqsQueueDetailsdi Referensi AWS Security Hub API.

Contoh

```
"AwsSqsQueue": {
    "DeadLetterTargetArn": "arn:aws:sqs:us-west-2:123456789012:queue/target",
    "KmsDataKeyReusePeriodSeconds": 60,,
    "KmsMasterKeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
    "QueueName": "sample-queue"
}
```

AwsSsm

Berikut ini adalah contoh Format Pencarian AWS Keamanan untuk `AwsSsm` sumber daya.

AwsSsmPatchCompliance

`AwsSsmPatchCompliance`Objek memberikan informasi tentang status patch pada instance berdasarkan baseline patch yang digunakan untuk menambal instance.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsSsmPatchCompliance` objek. Untuk melihat deskripsi `AwsSsmPatchCompliance` atribut, lihat AwsSsmPatchComplianceDetailsdi Referensi AWS Security Hub API.

Contoh

```
"AwsSsmPatchCompliance": {
    "Patch": {
        "ComplianceSummary": {
            "ComplianceType": "Patch",
```

```
            "CompliantCriticalCount": 0,
            "CompliantHighCount": 0,
            "CompliantInformationalCount": 0,
            "CompliantLowCount": 0,
            "CompliantMediumCount": 0,
            "CompliantUnspecifiedCount": 461,
            "ExecutionType": "Command",
            "NonCompliantCriticalCount": 0,
            "NonCompliantHighCount": 0,
            "NonCompliantInformationalCount": 0,
            "NonCompliantLowCount": 0,
            "NonCompliantMediumCount": 0,
            "NonCompliantUnspecifiedCount": 0,
            "OverallSeverity": "UNSPECIFIED",
            "PatchBaselineId": "pb-0c5b2769ef7cbe587",
            "PatchGroup": "ExamplePatchGroup",
            "Status": "COMPLIANT"
        }
    }
}
```

AwsStepFunctions

Berikut ini adalah contoh Format Pencarian AWS Keamanan untuk `AwsStepFunctions` sumber daya.

AwsStepFunctionStateMachine

`AwsStepFunctionStateMachine`Objek memberikan informasi tentang mesin AWS Step Functions negara, yang merupakan alur kerja yang terdiri dari serangkaian langkah yang digerakkan oleh peristiwa.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsStepFunctionStateMachine` objek. Untuk melihat deskripsi `AwsStepFunctionStateMachine` atribut, lihat AwsStepFunctionStateMachinedi Referensi AWS Security Hub API.

Contoh

```
"AwsStepFunctionStateMachine": {
    "StateMachineArn": "arn:aws:states:us-
east-1:123456789012:stateMachine:StepFunctionsLogDisableNonCompliantResource-
fQLujTeXvwsb",
```

```
    "Name": "StepFunctionsLogDisableNonCompliantResource-fQLujTeXvwsb",
    "Status": "ACTIVE",
    "RoleArn": "arn:aws:iam::123456789012:role/teststepfunc-
StatesExecutionRole-1PNM71RVO1UKT",
    "Type": "STANDARD",
    "LoggingConfiguration": {
        "Level": "OFF",
        "IncludeExecutionData": false
    },
    "TracingConfiguration": {
        "Enabled": false
    }
}
```

AwsWaf

Berikut ini adalah contoh Format Pencarian AWS Keamanan untuk `AwsWaf` sumber daya.

AwsWafRateBasedRule

`AwsWafRateBasedRule`Objek berisi rincian tentang aturan AWS WAF berbasis tarif untuk sumber daya global. Aturan AWS WAF berbasis tarif menyediakan pengaturan untuk menunjukkan kapan harus mengizinkan, memblokir, atau menghitung permintaan. Aturan berbasis tarif mencakup jumlah permintaan yang tiba selama periode waktu tertentu.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsWafRateBasedRule` objek. Untuk melihat deskripsi `AwsWafRateBasedRule` atribut, lihat AwsWafRateBasedRuleDetailsdi Referensi AWS Security Hub API.

Contoh

```
"AwsWafRateBasedRule":{
    "MatchPredicates" : [{
        "DataId" : "391b7a7e-5f00-40d2-b114-3f27ceacbbb0",
        "Negated" : "True",
        "Type" : "IPMatch" ,
    }],
    "MetricName" : "MetricName",
    "Name" : "Test",
    "RateKey" : "IP",
    "RateLimit" : 235000,
    "RuleId" : "5dfb4085-f103-4ec6-b39a-d4a0dae5f47f"
```

```
}
```

AwsWafRegionalRateBasedRule

`AwsWafRegionalRateBasedRule`Objek berisi rincian tentang aturan berbasis tarif untuk sumber daya Regional. Aturan berbasis tarif menyediakan pengaturan untuk menunjukkan kapan harus mengizinkan, memblokir, atau menghitung permintaan. Aturan berbasis tarif mencakup jumlah permintaan yang tiba selama periode waktu tertentu.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsWafRegionalRateBasedRule` objek. Untuk melihat deskripsi `AwsWafRegionalRateBasedRule` atribut, lihat AwsWafRegionalRateBasedRuleDetailsdi Referensi AWS Security Hub API.

Contoh

```
"AwsWafRegionalRateBasedRule":{
    "MatchPredicates" : [{
        "DataId" : "391b7a7e-5f00-40d2-b114-3f27ceacbbb0",
        "Negated" : "True",
        "Type" : "IPMatch" ,
    }],
    "MetricName" : "MetricName",
    "Name" : "Test",
    "RateKey" : "IP",
    "RateLimit" : 235000,
    "RuleId" : "5dfb4085-f103-4ec6-b39a-d4a0dae5f47f"
}
```

AwsWafRegionalRule

`AwsWafRegionalRule`Objek memberikan rincian tentang aturan AWS WAF Regional. Aturan ini mengidentifikasi permintaan web yang ingin Anda izinkan, blokir, atau hitung.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsWafRegionalRule` objek. Untuk melihat deskripsi `AwsWafRegionalRule` atribut, lihat AwsWafRegionalRuleDetailsdi Referensi AWS Security Hub API.

Contoh

```
"AwsWafRegionalRule": {
```

```
    "MetricName": "SampleWAF_Rule__Metric_1",
    "Name": "bb-waf-regional-rule-not-empty-conditions-compliant",
    "RuleId": "8f651760-24fa-40a6-a9ed-4b60f1de95fe",
    "PredicateList": [{
        "DataId": "127d9346-e607-4e93-9286-c1296fb5445a",
        "Negated": false,
        "Type": "GeoMatch"
    }]
}
```

AwsWafRegionalRuleGroup

`AwsWafRegionalRuleGroup`Objek memberikan rincian tentang kelompok aturan AWS WAF Regional. Grup aturan adalah kumpulan aturan standar yang Anda tambahkan ke daftar kontrol akses web (web ACL).

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsWafRegionalRuleGroup` objek. Untuk melihat deskripsi `AwsWafRegionalRuleGroup` atribut, lihat AwsWafRegionalRuleGroupDetailsdi Referensi AWS Security Hub API.

Contoh

```
"AwsWafRegionalRuleGroup": {
    "MetricName": "SampleWAF_Metric_1",
    "Name": "bb-WAFClassicRuleGroupWithRuleCompliant",
    "RuleGroupId": "2012ca6d-e66d-4d9b-b766-bfb03ad77cfb",
    "Rules": [{
        "Action": {
            "Type": "ALLOW"
        }
    }],
        "Priority": 1,
        "RuleId": "cdd225da-32cf-4773-8dc5-3bca3ed9c19c",
        "Type": "REGULAR"
}
```

AwsWafRegionalWebAcl

`AwsWafRegionalWebAcl`memberikan rincian tentang daftar kontrol akses web AWS WAF Regional (web ACL). ACL web berisi aturan yang mengidentifikasi permintaan yang ingin Anda izinkan, blokir, atau hitung.

Berikut ini adalah contoh `AwsWafRegionalWebAcl` temuan dalam AWS Security Finding Format (ASFF). Untuk melihat deskripsi `AwsApiGatewayV2Stage` atribut, lihat AwsWafRegionalWebAclDetailsdi Referensi AWS Security Hub API.

Contoh

```
"AwsWafRegionalWebAcl": {
    "DefaultAction": "ALLOW",
    "MetricName" : "web-regional-webacl-metric-1",
    "Name": "WebACL_123",
    "RulesList": [
        {
            "Action": {
                "Type": "Block"
            },
            "Priority": 3,
            "RuleId": "24445857-852b-4d47-bd9c-61f05e4d223c",
            "Type": "REGULAR",
            "ExcludedRules": [
                {
                    "ExclusionType": "Exclusion",
                    "RuleId": "Rule_id_1"
                }
            ],
            "OverrideAction": {
                "Type": "OVERRIDE"
            }
        }
    ],
    "WebAclId": "443c76f4-2e72-4c89-a2ee-389d501c1f67"
}
```

AwsWafRule

`AwsWafRule`memberikan informasi tentang AWS WAF aturan. AWS WAF Aturan mengidentifikasi permintaan web yang ingin Anda izinkan, blokir, atau hitung.

Berikut ini adalah contoh `AwsWafRule` temuan dalam AWS Security Finding Format (ASFF). Untuk melihat deskripsi `AwsApiGatewayV2Stage` atribut, lihat AwsWafRuleDetailsdi Referensi AWS Security Hub API.

Contoh

```
"AwsWafRule": {
    "MetricName": "AwsWafRule_Metric_1",
    "Name": "AwsWafRule_Name_1",
    "PredicateList": [{
        "DataId": "cdd225da-32cf-4773-1dc2-3bca3ed9c19c",
        "Negated": false,
        "Type": "GeoMatch"
    }],
    "RuleId": "8f651760-24fa-40a6-a9ed-4b60f1de953e"
}
```

AwsWafRuleGroup

`AwsWafRuleGroup`memberikan informasi tentang kelompok AWS WAF aturan. Grup AWS WAF aturan adalah kumpulan aturan yang telah ditentukan sebelumnya yang Anda tambahkan ke daftar kontrol akses web (web ACL).

Berikut ini adalah contoh `AwsWafRuleGroup` temuan dalam AWS Security Finding Format (ASFF). Untuk melihat deskripsi `AwsApiGatewayV2Stage` atribut, lihat AwsWafRuleGroupDetailsdi Referensi AWS Security Hub API.

Contoh

```
"AwsWafRuleGroup": {
    "MetricName": "SampleWAF_Metric_1",
    "Name": "bb-WAFRuleGroupWithRuleCompliant",
    "RuleGroupId": "2012ca6d-e66d-4d9b-b766-bfb03ad77cfb",
    "Rules": [{
        "Action": {
            "Type": "ALLOW",
        },
        "Priority": 1,
        "RuleId": "cdd225da-32cf-4773-8dc5-3bca3ed9c19c",
        "Type": "REGULAR"
    }]
}
```

AwsWafv2RuleGroup

`AwsWafv2RuleGroup`Objek memberikan rincian tentang grup aturan AWS WAF V2.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsWafv2RuleGroup` objek. Untuk melihat deskripsi `AwsWafv2RuleGroup` atribut, lihat AwsWafv2 RuleGroupDetails di Referensi AWS Security Hub API.

Contoh

```
"AwsWafv2RuleGroup": {
    "Arn": "arn:aws:wafv2:us-east-1:123456789012:global/rulegroup/wafv2rulegroupasff/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "Capacity": 1000,
    "Description": "Resource for ASFF",
    "Id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "Name": "wafv2rulegroupasff",
    "Rules": [{
     "Action": {
     "Allow": {
      "CustomRequestHandling": {
       "InsertHeaders": [
        {
        "Name": "AllowActionHeader1Name",
        "Value": "AllowActionHeader1Value"
        },
        {
        "Name": "AllowActionHeader2Name",
        "Value": "AllowActionHeader2Value"
        }
       ]
      }
     },
     "Name": "RuleOne",
     "Priority": 1,
     "VisibilityConfig": {
      "CloudWatchMetricsEnabled": true,
      "MetricName": "rulegroupasff",
      "SampledRequestsEnabled": false
     }
    }],
    "VisibilityConfig": {
     "CloudWatchMetricsEnabled": true,
     "MetricName": "rulegroupasff",
     "SampledRequestsEnabled": false
    }
}
```

AwsWafWebAcl

`AwsWafWebAcl`Objek memberikan rincian tentang ACL AWS WAF web.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsWafWebAcl` objek. Untuk melihat deskripsi `AwsWafWebAcl` atribut, lihat AwsWafWebAclDetailsdi Referensi AWS Security Hub API.

Contoh

```
"AwsWafWebAcl": {
    "DefaultAction": "ALLOW",
    "Name": "MyWafAcl",
    "Rules": [
        {
            "Action": {
                "Type": "ALLOW"
            },
            "ExcludedRules": [
                {
                    "RuleId": "5432a230-0113-5b83-bbb2-89375c5bfa98"
                }
            ],
            "OverrideAction": {
                "Type": "NONE"
            },
            "Priority": 1,
            "RuleId": "5432a230-0113-5b83-bbb2-89375c5bfa98",
            "Type": "REGULAR"
        }
    ],
    "WebAclId": "waf-1234567890"
}
```

AwsWafv2WebAcl

`AwsWafv2WebAcl`Objek memberikan rincian tentang ACL web AWS WAF V2.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsWafv2WebAcl` objek. Untuk melihat deskripsi `AwsWafv2WebAcl` atribut, lihat AwsWafv2 WebAclDetails di Referensi AWS Security Hub API.

Contoh

```
"AwsWafv2WebAcl": {
    "Arn": "arn:aws:wafv2:us-east-1:123456789012:regional/webacl/WebACL-RoaD4QexqSxG/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "Capacity": 1326,
    "CaptchaConfig": {
     "ImmunityTimeProperty": {
      "ImmunityTime": 500
     }
    },
    "DefaultAction": {
     "Block": {}
    },
    "Description": "Web ACL for JsonBody testing",
    "ManagedbyFirewallManager": false,
    "Name": "WebACL-RoaD4QexqSxG",
    "Rules": [{
     "Action": {
      "RuleAction": {
       "Block": {}
      }
     },
     "Name": "TestJsonBodyRule",
     "Priority": 1,
     "VisibilityConfig": {
      "SampledRequestsEnabled": true,
      "CloudWatchMetricsEnabled": true,
      "MetricName": "JsonBodyMatchMetric"
     }
    }],
    "VisibilityConfig": {
     "SampledRequestsEnabled": true,
     "CloudWatchMetricsEnabled": true,
     "MetricName": "TestingJsonBodyMetric"
    }
}
```

AwsXray

Berikut ini adalah contoh Format Pencarian AWS Keamanan untuk `AwsXray` sumber daya.

AwsXrayEncryptionConfig

`AwsXrayEncryptionConfig`Objek berisi informasi tentang konfigurasi enkripsi untuk AWS X-Ray.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsXrayEncryptionConfig` objek. Untuk melihat deskripsi `AwsXrayEncryptionConfig` atribut, lihat AwsXrayEncryptionConfigDetailsdi Referensi AWS Security Hub API.

Contoh

```
"AwsXRayEncryptionConfig":{
    "KeyId": "arn:aws:kms:us-east-2:222222222222:key/example-key",
    "Status": "UPDATING",
    "Type":"KMS"
}
```

Container

Detail kontainer yang terkait dengan temuan.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `Container` objek. Untuk melihat deskripsi `Container` atribut, lihat ContainerDetailsdi Referensi AWS Security Hub API.

Contoh

```
"Container": {
    "ContainerRuntime": "docker",
    "ImageId": "image12",
    "ImageName": "1111111/
knotejs@sha256:372131c9fef111111111111115f4ed3ea5f9dce4dc3bd34ce21846588a3",
    "LaunchedAt": "2018-09-29T01:25:54Z",
    "Name": "knote",
    "Privileged": true,
    "VolumeMounts": [{
        "Name": "vol-03909e9",
        "MountPath": "/mnt/etc"
    }]
}
```

Other

`Other`Objek memungkinkan Anda untuk memberikan bidang dan nilai khusus. Anda menggunakan `Other` objek dalam kasus berikut.

- Jenis sumber daya tidak memiliki `Details` objek yang sesuai. Untuk memberikan detail untuk sumber daya, Anda menggunakan `Other` objek.

- `Details`Objek untuk tipe sumber daya tidak menyertakan semua atribut yang ingin Anda isi. Dalam hal ini, gunakan `Details` objek untuk jenis sumber daya untuk mengisi atribut yang tersedia. Gunakan `Other` objek untuk mengisi atribut yang tidak ada dalam objek tipe-spesifik.
- Jenis sumber daya bukan salah satu jenis yang disediakan. Dalam hal ini, Anda mengatur `Resource.Type` ke`Other`, dan menggunakan `Other` objek untuk mengisi rincian.

Jenis: Peta hingga 50 pasangan nilai kunci

Setiap pasangan kunci-nilai harus memenuhi persyaratan berikut.

- Kunci harus berisi kurang dari 128 karakter.
- Nilai harus mengandung kurang dari 1.024 karakter.

Wawasan di AWS Security Hub

Wawasan AWS Security Hub adalah kumpulan temuan terkait. Ini mengidentifikasi area keamanan yang membutuhkan perhatian dan intervensi. Misalnya, wawasan mungkin menunjukkan instans EC2 yang merupakan subjek temuan yang mendeteksi praktik keamanan yang buruk. Wawasan menyatukan temuan dari seluruh penyedia pencarian.

Setiap wawasan didefinisikan oleh grup berdasarkan pernyataan dan filter opsional. Kelompok berdasarkan pernyataan menunjukkan bagaimana mengelompokkan temuan yang cocok, dan mengidentifikasi jenis item yang diterapkan wawasan tersebut. Misalnya, jika wawasan dikelompokkan berdasarkan pengidentifikasi sumber daya, maka wawasan menghasilkan daftar pengidentifikasi sumber daya. Filter opsional mengidentifikasi temuan yang cocok untuk wawasan. Misalnya, Anda mungkin ingin hanya melihat temuan dari penyedia atau temuan tertentu yang terkait dengan jenis sumber daya tertentu.

Security Hub menawarkan beberapa wawasan terkelola bawaan. Anda tidak dapat mengubah atau menghapus wawasan terkelola.

Untuk melacak masalah keamanan yang unik untuk AWS lingkungan dan penggunaan Anda, Anda dapat membuat wawasan khusus.

Wawasan hanya mengembalikan hasil jika Anda telah mengaktifkan integrasi atau standar yang menghasilkan temuan yang cocok. Misalnya, wawasan terkelola 29. Sumber daya teratas berdasarkan jumlah pemeriksaan CIS yang gagal hanya mengembalikan hasil jika Anda mengaktifkan standar CIS AWS Foundations.

Topik

Melihat dan memfilter daftar wawasan

Halaman Wawasan menampilkan daftar wawasan yang tersedia.

Secara default, daftar menampilkan wawasan terkelola dan kustom. Untuk memfilter daftar wawasan berdasarkan jenis wawasan, pilih jenis wawasan dari menu tarik-turun yang berada di sebelah bidang filter.

- Untuk menampilkan semua wawasan yang tersedia, pilih Semua wawasan. Ini adalah pilihan default.
- Untuk hanya menampilkan wawasan terkelola, pilih wawasan terkelola Security Hub.
- Untuk hanya menampilkan wawasan khusus, pilih Wawasan khusus.

Anda juga dapat memfilter daftar wawasan berdasarkan teks dalam nama wawasan.

Di bidang filter, ketik teks yang akan digunakan untuk memfilter daftar. Filter tidak peka huruf besar/kecil. Filter mencari wawasan yang berisi teks di mana saja dalam nama wawasan.

Melihat dan mengambil tindakan atas hasil dan temuan wawasan

Untuk setiap wawasan, AWS Security Hub pertama-tama menentukan temuan yang cocok dengan kriteria filter, dan kemudian menggunakan atribut pengelompokan untuk mengelompokkan temuan yang cocok.

Dari halaman konsol Insights, Anda dapat melihat dan mengambil tindakan atas hasil dan temuan.

Jika Anda mengaktifkan agregasi lintas wilayah, maka di Wilayah agregasi, hasil untuk wawasan terkelola mencakup temuan dari Wilayah agregasi dan Wilayah tertaut. Untuk hasil wawasan khusus, jika wawasan tidak difilter menurut Wilayah, maka hasilnya mencakup temuan dari Wilayah agregasi dan Wilayah terkait.

Di Wilayah lain, hasil wawasan hanya untuk Wilayah tersebut.

Untuk informasi tentang cara mengonfigurasi agregasi lintas wilayah, lihat. Agregasi Lintas Wilayah

Melihat dan mengambil tindakan pada hasil wawasan (konsol)

Hasil wawasan terdiri dari daftar hasil yang dikelompokkan untuk wawasan. Misalnya, jika wawasan dikelompokkan berdasarkan pengidentifikasi sumber daya, maka hasil wawasan adalah daftar pengidentifikasi sumber daya. Setiap item dalam daftar hasil menunjukkan jumlah temuan yang cocok untuk item tersebut.

Perhatikan bahwa jika temuan dikelompokkan berdasarkan pengidentifikasi sumber daya atau jenis sumber daya, maka hasilnya mencakup semua sumber daya dalam temuan yang cocok. Ini termasuk

sumber daya yang memiliki tipe berbeda dari jenis sumber daya yang ditentukan dalam kriteria filter. Misalnya, wawasan mengidentifikasi temuan yang terkait dengan ember S3. Jika temuan yang cocok berisi sumber daya bucket S3 dan sumber daya kunci akses IAM, maka hasil wawasan akan mencantumkan kedua sumber daya tersebut.

Daftar hasil diurutkan dari sebagian besar hingga temuan pencocokan paling sedikit.

Security Hub hanya dapat menampilkan 100 hasil. Jika ada lebih dari 100 nilai pengelompokan, Anda hanya melihat 100 yang pertama.

Selain daftar hasil, hasil wawasan menampilkan serangkaian bagan yang merangkum jumlah temuan yang cocok untuk atribut berikut.

- Label keparahan — Jumlah temuan untuk setiap label keparahan
- Akun AWS ID — Lima ID akun teratas untuk temuan yang cocok
- Jenis sumber daya - Lima jenis sumber daya teratas untuk temuan yang cocok
- ID Sumber Daya — Lima ID sumber daya teratas untuk temuan yang cocok
- Nama produk - Lima penyedia temuan teratas untuk temuan yang cocok

Jika Anda telah mengonfigurasi tindakan kustom, maka Anda dapat mengirim hasil yang dipilih ke tindakan kustom. Tindakan harus dikaitkan dengan CloudWatch aturan untuk jenis `Security Hub Insight Results` acara. Lihat the section called “Respon dan remediasi otomatis”.

Jika Anda belum mengonfigurasi tindakan khusus, maka menu Tindakan dinonaktifkan.

Untuk menampilkan dan mengambil tindakan pada daftar hasil wawasan

1. Buka konsol AWS Security Hub di https://console.aws.amazon.com/securityhub/.
2. Pada panel navigasi, silakan pilih Wawasan.
3. Untuk menampilkan daftar hasil insight, pilih nama insight.
4. Pilih kotak centang untuk setiap hasil untuk dikirim ke tindakan kustom.
5. Dari menu Tindakan, pilih tindakan kustom.

Melihat hasil wawasan (Security Hub API, AWS CLI)

Untuk melihat hasil insight, Anda dapat menggunakan panggilan API atau file AWS Command Line Interface.

Untuk melihat hasil wawasan (Security Hub API, AWS CLI)

- Security Hub API — Gunakan `GetInsightResults`operasi. Untuk mengidentifikasi wawasan untuk mengembalikan hasil, Anda memerlukan wawasan ARN. Untuk mendapatkan wawasan ARN untuk wawasan khusus, gunakan operasi. `GetInsights`
- AWS CLI— Pada baris perintah, jalankan `get-insight-results`perintah.

```
aws securityhub get-insight-results --insight-arn <insight ARN>
```

Contoh:

```
aws securityhub get-insight-results --insight-arn "arn:aws:securityhub:us-
west-1:123456789012:insight/123456789012/custom/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

Melihat temuan untuk hasil wawasan (konsol)

Dari daftar hasil wawasan, Anda dapat menampilkan daftar temuan untuk setiap hasil.

Untuk menampilkan dan mengambil tindakan atas temuan wawasan

1. Buka konsol AWS Security Hub di https://console.aws.amazon.com/securityhub/.
2. Pada panel navigasi, silakan pilih Wawasan.
3. Untuk menampilkan daftar hasil insight, pilih nama insight.
4. Untuk menampilkan daftar temuan untuk hasil wawasan, pilih item dari daftar hasil.

Daftar temuan menunjukkan temuan aktif untuk hasil wawasan yang dipilih yang memiliki status alur kerja `NEW` atau`NOTIFIED`.

Dari daftar temuan, Anda dapat melakukan tindakan berikut.

- Ubah filter dan pengelompokan untuk daftar
- Lihat detail untuk temuan individu
- Perbarui status alur kerja temuan
- Kirim temuan ke tindakan khusus

Wawasan terkelola

AWSSecurity Hub menyediakan beberapa wawasan terkelola.

Anda tidak dapat mengedit atau menghapus wawasan terkelola Security Hub. Anda dapat melihat dan mengambil tindakan atas hasil dan temuan wawasan. Anda juga dapat menggunakan wawasan terkelola sebagai dasar untuk wawasan kustom baru.

Seperti semua wawasan, wawasan terkelola hanya mengembalikan hasil jika Anda telah mengaktifkan integrasi produk atau standar keamanan yang dapat menghasilkan temuan yang cocok.

Untuk wawasan yang dikelompokkan berdasarkan pengidentifikasi sumber daya, hasilnya mencakup pengidentifikasi semua sumber daya dalam temuan yang cocok. Ini termasuk sumber daya yang memiliki tipe berbeda dari jenis sumber daya dalam kriteria filter. Misalnya, insight 2 mengidentifikasi temuan yang terkait dengan bucket Amazon S3. Jika temuan yang cocok berisi sumber daya bucket S3 dan sumber daya kunci akses IAM, maka hasil insight menyertakan kedua resource tersebut.

Security Hub menawarkan wawasan terkelola berikut:

1. AWSsumber daya dengan temuan terbanyak

   ARN: `arn:aws:securityhub:::insight/securityhub/default/1`

   Dikelompokkan berdasarkan: Pengidentifikasi sumber daya

   Menemukan filter:

   - Record state adalah `ACTIVE`
   - Status alur kerja adalah `NEW` atau `NOTIFIED`

2. Bucket S3 dengan izin tulis atau baca publik

   ARN: `arn:aws:securityhub:::insight/securityhub/default/10`

   Dikelompokkan berdasarkan: Pengidentifikasi sumber daya

   Menemukan filter:

   - Jenis dimulai dengan `Effects/Data Exposure`
   - Jenis sumber daya adalah `AwsS3Bucket`

- Record state adalah `ACTIVE`
- Status alur kerja adalah `NEW` atau `NOTIFIED`

3. AMI yang menghasilkan temuan terbanyak

   ARN: `arn:aws:securityhub:::insight/securityhub/default/3`

   Dikelompokkan berdasarkan: ID gambar instans EC2

   Menemukan filter:

   - Jenis sumber daya adalah `AwsEc2Instance`
   - Record state adalah `ACTIVE`
   - Status alur kerja adalah `NEW` atau `NOTIFIED`

4. Contoh EC2 yang terlibat dalam Taktik, Teknik, dan Prosedur (TTP) yang dikenal

   ARN: `arn:aws:securityhub:::insight/securityhub/default/14`

   Dikelompokkan berdasarkan: ID Sumber Daya

   Menemukan filter:

   - Jenis dimulai dengan `TTPs`
   - Jenis sumber daya adalah `AwsEc2Instance`
   - Record state adalah `ACTIVE`
   - Status alur kerja adalah `NEW` atau `NOTIFIED`

5. AWSkepala sekolah dengan aktivitas kunci akses yang mencurigakan

   ARN: `arn:aws:securityhub:::insight/securityhub/default/9`

   Dikelompokkan berdasarkan: Nama utama kunci akses IAM

   Menemukan filter:

   - Jenis sumber daya adalah `AwsIamAccessKey`
   - Record state adalah `ACTIVE`
   - Status alur kerja adalah `NEW` atau `NOTIFIED`

6. AWScontoh sumber daya yang tidak memenuhi standar keamanan/praktik terbaik

   ARN: `arn:aws:securityhub:::insight/securityhub/default/6`

Dikelompokkan berdasarkan: ID Sumber Daya

Menemukan filter:

- Tipe adalah `Software and Configuration Checks/Industry and Regulatory Standards/AWS Security Best Practices`
- Record state adalah `ACTIVE`
- Status alur kerja adalah `NEW` atau `NOTIFIED`

7. AWSsumber daya yang terkait dengan eksfiltrasi data potensial

   ARN: `arn:aws:securityhub:::insight/securityhub/default/7`

   Dikelompokkan berdasarkan:: Resource ID

   Menemukan filter:

   - Jenis dimulai dengan Efek/Eksfiltrasi Data/
   - Record state adalah `ACTIVE`
   - Status alur kerja adalah `NEW` atau `NOTIFIED`

8. AWSsumber daya yang terkait dengan konsumsi sumber daya yang tidak sah

   ARN: `arn:aws:securityhub:::insight/securityhub/default/8`

   Dikelompokkan berdasarkan: ID Sumber Daya

   Menemukan filter:

   - Jenis dimulai dengan `Effects/Resource Consumption`
   - Record state adalah `ACTIVE`
   - Status alur kerja adalah `NEW` atau `NOTIFIED`

9. Bucket S3 yang tidak memenuhi standar keamanan/praktik terbaik

   ARN: `arn:aws:securityhub:::insight/securityhub/default/11`

   Dikelompokkan berdasarkan: ID Sumber Daya

   Menemukan filter:

   - Jenis sumber daya adalah `AwsS3Bucket`

- Tipe adalah `Software and Configuration Checks/Industry and Regulatory Standards/AWS Security Best Practices`
- Record state adalah `ACTIVE`
- Status alur kerja adalah `NEW` atau `NOTIFIED`

10. Bucket S3 dengan data sensitif

    ARN: `arn:aws:securityhub:::insight/securityhub/default/12`

    Dikelompokkan berdasarkan: ID Sumber Daya

    Menemukan filter:

    - Jenis sumber daya adalah `AwsS3Bucket`
    - Jenis dimulai dengan `Sensitive Data Identifications/`
    - Record state adalah `ACTIVE`
    - Status alur kerja adalah `NEW` atau `NOTIFIED`

11. Kredensil yang mungkin bocor

    ARN: `arn:aws:securityhub:::insight/securityhub/default/13`

    Dikelompokkan berdasarkan: ID Sumber Daya

    Menemukan filter:

    - Jenis dimulai dengan `Sensitive Data Identifications/Passwords/`
    - Record state adalah `ACTIVE`
    - Status alur kerja adalah `NEW` atau `NOTIFIED`

12. Instans EC2 yang memiliki patch keamanan yang hilang untuk kerentanan penting

    ARN: `arn:aws:securityhub:::insight/securityhub/default/16`

    Dikelompokkan berdasarkan: ID Sumber Daya

    Menemukan filter:

    - Jenis dimulai dengan `Software and Configuration Checks/Vulnerabilities/CVE`
    - Jenis sumber daya adalah `AwsEc2Instance`
    - Record state adalah `ACTIVE`
    - Status alur kerja adalah `NEW` atau `NOTIFIED`

13. Instans EC2 dengan perilaku umum yang tidak biasa

    ARN: `arn:aws:securityhub:::insight/securityhub/default/17`

    Dikelompokkan berdasarkan: ID Sumber Daya

    Menemukan filter:

    - Jenis dimulai dengan `Unusual Behaviors`
    - Jenis sumber daya adalah `AwsEc2Instance`
    - Record state adalah `ACTIVE`
    - Status alur kerja adalah `NEW` atau `NOTIFIED`
14. Instans EC2 yang memiliki port yang dapat diakses dari Internet

    ARN: `arn:aws:securityhub:::insight/securityhub/default/18`

    Dikelompokkan berdasarkan: ID Sumber Daya

    Menemukan filter:

    - Jenis dimulai dengan `Software and Configuration Checks/AWS Security Best Practices/Network Reachability`
    - Jenis sumber daya adalah `AwsEc2Instance`
    - Record state adalah `ACTIVE`
    - Status alur kerja adalah `NEW` atau `NOTIFIED`
15. Instans EC2 yang tidak memenuhi standar keamanan/praktik terbaik

    ARN: `arn:aws:securityhub:::insight/securityhub/default/19`

    Dikelompokkan berdasarkan: ID Sumber Daya

    Menemukan filter:

    - Jenis dimulai dengan salah satu dari berikut ini:
      - `Software and Configuration Checks/Industry and Regulatory Standards/`
      - `Software and Configuration Checks/AWS Security Best Practices`
    - Jenis sumber daya adalah `AwsEc2Instance`
    - Record state adalah `ACTIVE`
    - Status alur kerja adalah `NEW` atau `NOTIFIED`

16. Instans EC2 yang terbuka untuk Internet

    ARN: `arn:aws:securityhub:::insight/securityhub/default/21`

    Dikelompokkan berdasarkan: ID Sumber Daya

    Menemukan filter:

    - Jenis dimulai dengan `Software and Configuration Checks/AWS Security Best Practices/Network Reachability`
    - Jenis sumber daya adalah `AwsEc2Instance`
    - Record state adalah `ACTIVE`
    - Status alur kerja adalah `NEW` atau `NOTIFIED`
17. Instans EC2 yang terkait dengan pengintaian musuh

    ARN: `arn:aws:securityhub:::insight/securityhub/default/22`

    Dikelompokkan berdasarkan: ID Sumber Daya

    Menemukan filter:

    - Jenis dimulai dengan TTPS/Discovery/Recon
    - Jenis sumber daya adalah `AwsEc2Instance`
    - Record state adalah `ACTIVE`
    - Status alur kerja adalah `NEW` atau `NOTIFIED`
18. AWSsumber daya yang terkait dengan malware

    ARN: `arn:aws:securityhub:::insight/securityhub/default/23`

    Dikelompokkan berdasarkan: ID Sumber Daya

    Menemukan filter:

    - Jenis dimulai dengan salah satu dari berikut ini:
      - `Effects/Data Exfiltration/Trojan`
      - `TTPs/Initial Access/Trojan`
      - `TTPs/Command and Control/Backdoor`
      - `TTPs/Command and Control/Trojan`
      - `Software and Configuration Checks/Backdoor`

    - `Unusual Behaviors/VM/Backdoor`
  - Record state adalah `ACTIVE`
  - Status alur kerja adalah `NEW` atau `NOTIFIED`

19. AWSsumber daya yang terkait dengan masalah cryptocurrency

    ARN: `arn:aws:securityhub:::insight/securityhub/default/24`

    Dikelompokkan berdasarkan: ID Sumber Daya

    Menemukan filter:

  - Jenis dimulai dengan salah satu dari berikut ini:
    - `Effects/Resource Consumption/Cryptocurrency`
    - `TTPs/Command and Control/CryptoCurrency`
  - Record state adalah `ACTIVE`
  - Status alur kerja adalah `NEW` atau `NOTIFIED`

20. AWSsumber daya dengan upaya akses yang tidak sah

    ARN: `arn:aws:securityhub:::insight/securityhub/default/25`

    Dikelompokkan berdasarkan: ID Sumber Daya

    Menemukan filter:

  - Jenis dimulai dengan salah satu dari berikut ini:
    - `TTPs/Command and Control/UnauthorizedAccess`
    - `TTPs/Initial Access/UnauthorizedAccess`
    - `Effects/Data Exfiltration/UnauthorizedAccess`
    - `Unusual Behaviors/User/UnauthorizedAccess`
    - `Effects/Resource Consumption/UnauthorizedAccess`
  - Record state adalah `ACTIVE`
  - Status alur kerja adalah `NEW` atau `NOTIFIED`

21. Indikator Ancaman Intel dengan hit terbanyak dalam seminggu terakhir

    ARN: `arn:aws:securityhub:::insight/securityhub/default/26`

    Menemukan filter:

- Dibuat dalam 7 hari terakhir

22. Akun teratas berdasarkan jumlah temuan

    ARN: `arn:aws:securityhub:::insight/securityhub/default/27`

    Dikelompokkan berdasarkan: ID Akun AWS

    Menemukan filter:

    - Record state adalah `ACTIVE`
    - Status alur kerja adalah `NEW` atau `NOTIFIED`

23. Produk teratas berdasarkan jumlah temuan

    ARN: `arn:aws:securityhub:::insight/securityhub/default/28`

    Dikelompokkan berdasarkan: Nama produk

    Menemukan filter:

    - Record state adalah `ACTIVE`
    - Status alur kerja adalah `NEW` atau `NOTIFIED`

24. Keparahan berdasarkan jumlah temuan

    ARN: `arn:aws:securityhub:::insight/securityhub/default/29`

    Dikelompokkan berdasarkan: Label keparahan

    Menemukan filter:

    - Record state adalah `ACTIVE`
    - Status alur kerja adalah `NEW` atau `NOTIFIED`

25. Ember S3 teratas berdasarkan jumlah temuan

    ARN: `arn:aws:securityhub:::insight/securityhub/default/30`

    Dikelompokkan berdasarkan: ID Sumber Daya

    Menemukan filter:

    - Jenis sumber daya adalah `AwsS3Bucket`
    - Record state adalah `ACTIVE`
    - Status alur kerja adalah `NEW` atau `NOTIFIED`

26. Instans EC2 teratas berdasarkan jumlah temuan

    ARN: `arn:aws:securityhub:::insight/securityhub/default/31`

    Dikelompokkan berdasarkan: ID Sumber Daya

    Menemukan filter:

    - Jenis sumber daya adalah `AwsEc2Instance`
    - Record state adalah `ACTIVE`
    - Status alur kerja adalah `NEW` atau `NOTIFIED`
27. AMI teratas berdasarkan jumlah temuan

    ARN: `arn:aws:securityhub:::insight/securityhub/default/32`

    Dikelompokkan berdasarkan: ID gambar instans EC2

    Menemukan filter:

    - Jenis sumber daya adalah `AwsEc2Instance`
    - Record state adalah `ACTIVE`
    - Status alur kerja adalah `NEW` atau `NOTIFIED`
28. Pengguna IAM teratas berdasarkan jumlah temuan

    ARN: `arn:aws:securityhub:::insight/securityhub/default/33`

    Dikelompokkan berdasarkan: ID kunci akses IAM

    Menemukan filter:

    - Jenis sumber daya adalah `AwsIamAccessKey`
    - Record state adalah `ACTIVE`
    - Status alur kerja adalah `NEW` atau `NOTIFIED`
29. Sumber daya teratas berdasarkan jumlah pemeriksaan CIS yang gagal

    ARN: `arn:aws:securityhub:::insight/securityhub/default/34`

    Dikelompokkan berdasarkan: ID Sumber Daya

    Menemukan filter:

- Generator ID dimulai dengan `arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule`
- Diperbarui di hari terakhir
- Status kepatuhan adalah `FAILED`
- Record state adalah `ACTIVE`
- Status alur kerja adalah `NEW` atau `NOTIFIED`

30. Integrasi teratas berdasarkan jumlah temuan

    ARN: `arn:aws:securityhub:::insight/securityhub/default/35`

    Dikelompokkan berdasarkan: Produk ARN

    Menemukan filter:

    - Record state adalah `ACTIVE`
    - Status alur kerja adalah `NEW` atau `NOTIFIED`

31. Sumber daya dengan pemeriksaan keamanan paling gagal

    ARN: `arn:aws:securityhub:::insight/securityhub/default/36`

    Dikelompokkan berdasarkan: ID Sumber Daya

    Menemukan filter:

    - Diperbarui di hari terakhir
    - Status kepatuhan adalah `FAILED`
    - Record state adalah `ACTIVE`
    - Status alur kerja adalah `NEW` atau `NOTIFIED`

32. Pengguna IAM dengan aktivitas mencurigakan

    ARN: `arn:aws:securityhub:::insight/securityhub/default/37`

    Dikelompokkan berdasarkan: Pengguna IAM

    Menemukan filter:

    - Jenis sumber daya adalah `AwsIamUser`
    - Record state adalah `ACTIVE`
    - Status alur kerja adalah `NEW` atau `NOTIFIED`

33. Sumber daya dengan AWS Health temuan terbanyak

    ARN: `arn:aws:securityhub:::insight/securityhub/default/38`

    Dikelompokkan berdasarkan: ID Sumber Daya

    Menemukan filter:

    - `ProductName` sama `Health`
34. Sumber daya dengan AWS Config temuan terbanyak

    ARN: `arn:aws:securityhub:::insight/securityhub/default/39`

    Dikelompokkan berdasarkan: ID Sumber Daya

    Menemukan filter:

    - `ProductName` sama `Config`
35. Aplikasi dengan temuan terbanyak

    ARN: `arn:aws:securityhub:::insight/securityhub/default/40`

    Dikelompokkan berdasarkan: ResourceApplicationArn

    Menemukan filter:

    - `RecordState` sama `ACTIVE`
    - `Workflow.Status` sama `NEW` atau `NOTIFIED`

Wawasan khusus

SelainAWSWawasan terkelola Hub Keamanan, Anda dapat membuat wawasan khusus di Hub Keamanan untuk melacak masalah yang spesifik untuk lingkungan Anda. Wawasan khusus menyediakan cara untuk melacak subset masalah yang dikuratori.

Berikut adalah beberapa contoh wawasan khusus yang mungkin berguna untuk disiapkan:

- Jika Anda memiliki akun administrator, Anda dapat menyiapkan wawasan khusus untuk melacak temuan kritis dan tingkat keparahan tinggi yang memengaruhi akun anggota.
- Jika Anda mengandalkan spesifikterpaduAWSlayanan, Anda dapat mengatur wawasan khusus untuk melacak temuan kritis dan tingkat keparahan tinggi dari layanan tersebut.

- Jika Anda mengandalkanintegrasi pihak ketiga, Anda dapat mengatur wawasan khusus untuk melacak temuan kritis dan tingkat keparahan tinggi dari produk terintegrasi itu.

Anda dapat membuat wawasan khusus yang benar-benar baru, atau mulai dari wawasan kustom atau terkelola yang ada.

Setiap wawasan dikonfigurasi dengan opsi berikut.

- Atribut pengelompokan- Atribut pengelompokan menentukan item mana yang ditampilkan dalam daftar hasil wawasan. Misalnya, jika atribut pengelompokanNama produk, maka hasil wawasan menampilkan jumlah temuan yang terkait dengan masing-masing penyedia temuan.
- Filter opsional- Filter mempersempit temuan yang cocok untuk wawasan.

  Saat menanyakan temuan Anda, Security Hub menerapkan logika Boolean AND ke kumpulan filter. Dengan kata lain, temuan hanya cocok jika cocok dengan semua filter yang disediakan. Misalnya, jika filter adalah “Nama produkGuardDuty“dan “Jenis sumber daya adalah`AwsS3Bucket`,” maka temuan yang cocok harus sesuai dengan kedua kriteria ini.

  Namun, Security Hub menerapkan logika Boolean OR ke filter yang menggunakan atribut yang sama tetapi nilai yang berbeda. Misalnya, jika filter adalah “Nama produkGuardDuty“dan” Nama produk adalah Amazon Inspector,” maka temuan cocok jika dihasilkan oleh baikGuardDutyatau Inspektur Amazon.

Perhatikan bahwa jika Anda menggunakan pengidentifikasi sumber daya atau jenis sumber daya sebagai atribut pengelompokan, maka hasil wawasan mencakup semua sumber daya yang ada dalam temuan yang cocok. Daftar ini tidak terbatas pada sumber daya yang cocok dengan filter jenis sumber daya. Misalnya, wawasan mengidentifikasi temuan yang terkait dengan bucket S3, dan mengelompokkan temuan tersebut berdasarkan pengidentifikasi sumber daya. Temuan yang cocok berisi sumber daya bucket S3 dan sumber daya kunci akses IAM. Hasil wawasan mencakup kedua sumber daya.

Membuat wawasan khusus (konsol)

Dari konsol, Anda dapat membuat wawasan yang sama sekali baru.

Untuk membuat wawasan khusus

1. BukaAWSKeamanan Hub konsol dihttps://console.aws.amazon.com/securityhub/.

2. Di panel navigasi, pilih Insights (Wawasan).
3. PilihBuat wawasan.
4. Untuk memilih atribut pengelompokan untuk wawasan:

    a. Pilih kotak pencarian untuk menampilkan opsi filter.
    b. PilihKelompok oleh.
    c. Pilih atribut yang akan digunakan untuk mengelompokkan temuan yang terkait dengan wawasan ini.
    d. Pilih Apply (Terapkan).
5. (Opsional) Pilih filter tambahan apa pun yang akan digunakan untuk wawasan ini. Untuk setiap filter, tentukan kriteria filter, lalu pilihTerapkan.
6. PilihBuat wawasan.
7. Masukkan sebuahNama wawasan, lalu pilihBuat wawasan.

Membuat wawasan khusus (terprogram)

Pilih metode yang Anda inginkan, dan ikuti langkah-langkah untuk membuat wawasan khusus secara terprogram di Hub Keamanan. Anda dapat menentukan filter untuk mempersempit koleksi temuan dalam wawasan ke subset tertentu.

Tab berikut menyertakan petunjuk dalam beberapa bahasa untuk membuat wawasan khusus. Untuk dukungan dalam bahasa tambahan, lihatAlat untuk MembangunAWS.

Security Hub API

1. Jalankan`CreateInsight`operasi.
2. Mengisi`Name`parameter dengan nama untuk wawasan kustom Anda.
3. Mengisi`Filters`parameter untuk menentukan temuan untuk memasukkan dalam wawasan.
4. Mengisi`GroupByAttribute`parameter untuk menentukan atribut yang digunakan untuk kelompok temuan yang termasuk dalam wawasan.
5. Opsional, mengisi`SortCriteria`parameter untuk mengurutkan temuan dengan bidang tertentu.

Jika Anda telah mengaktifkanagregasi lintas wilayahdan memanggil API ini dari Wilayah agregasi, wawasan berlaku untuk pencocokan temuan dalam agregasi dan Wilayah terkait.

AWS CLI

1. Pada baris perintah, jalankan`create-insight`perintah.
2. Mengisi`name`parameter dengan nama untuk wawasan kustom Anda.
3. Mengisi`filters`parameter untuk menentukan temuan untuk memasukkan dalam wawasan.
4. Mengisi`group-by-attribute`parameter untuk menentukan atribut yang digunakan untuk kelompok temuan yang termasuk dalam wawasan.

Jika Anda telah mengaktifkanagregasi lintas wilayahdan jalankan perintah ini dari Wilayah agregasi, wawasan berlaku untuk pencocokan temuan dari agregasi dan Wilayah terkait.

```
aws securityhub create-insight --name <insight name> --filters <filter values> --
group-by-attribute <attribute name>
```

Contoh

```
aws securityhub create-insight --name "Critical role findings" --filters
 '{"ResourceType": [{ "Comparison": "EQUALS", "Value": "AwsIamRole"}],
 "SeverityLabel": [{"Comparison": "EQUALS", "Value": "CRITICAL"}]}' --group-by-
attribute "ResourceId"
```

PowerShell

1. Gunakan`New-SHUBInsight`cmdlet.
2. Mengisi`Name`parameter dengan nama untuk wawasan kustom Anda.
3. Mengisi`Filter`parameter untuk menentukan temuan untuk memasukkan dalam wawasan.
4. Mengisi`GroupByAttribute`parameter untuk menentukan atribut yang digunakan untuk kelompok temuan yang termasuk dalam wawasan.

Jika Anda telah mengaktifkanagregasi lintas wilayahdan menggunakan cmdlet ini dari Wilayah agregasi, wawasan berlaku untuk pencocokan temuan dari agregasi dan Wilayah terkait.

Contoh

```
$Filter = @{
    AwsAccountId = [Amazon.SecurityHub.Model.StringFilter]@{
        Comparison = "EQUALS"
        Value = "XXX"
```

```
    }
    ComplianceStatus = [Amazon.SecurityHub.Model.StringFilter]@{
        Comparison = "EQUALS"
        Value = 'FAILED'
    }
}
New-SHUBInsight -Filter $Filter -Name TestInsight -GroupByAttribute ResourceId
```

Memodifikasi wawasan kustom (konsol)

Anda dapat memodifikasi wawasan kustom yang ada untuk mengubah nilai pengelompokan dan filter. Setelah melakukan perubahan, Anda dapat menyimpan pembaruan ke wawasan asli, atau menyimpan versi yang diperbarui sebagai wawasan baru.

Untuk memodifikasi wawasan

1. BukaAWSKeamanan Hub konsol dihttps://console.aws.amazon.com/securityhub/.
2. Di panel navigasi, pilih Insights (Wawasan).
3. Pilih wawasan khusus untuk dimodifikasi.
4. Edit konfigurasi wawasan sesuai kebutuhan.
   - Untuk mengubah atribut yang digunakan untuk mengelompokkan temuan dalam wawasan:
     a. Untuk menghapus pengelompokan yang ada, pilihXdi sampingKelompok olehpengaturan.
     b. Pilih kotak pencarian.
     c. Pilih atribut yang akan digunakan untuk pengelompokan.
     d. Pilih Apply (Terapkan).
   - Untuk menghapus filter dari wawasan, pilih yang dilingkariXdi samping filter.
   - Untuk menambahkan filter ke wawasan:
     a. Pilih kotak pencarian.
     b. Pilih atribut dan nilai yang akan digunakan sebagai filter.
     c. Pilih Apply (Terapkan).
5. Saat Anda menyelesaikan pembaruan, pilihSimpan wawasan.
6. Saat diminta, lakukan salah satu hal berikut:
   - Untuk memperbarui wawasan yang ada untuk mencerminkan perubahan Anda, pilihMemperbarui***<Insight_Name>***dan kemudian pilihSimpan wawasan.

- Untuk membuat wawasan baru dengan pembaruan, pilihSimpan wawasan baru. Masukkan sebuahNama wawasan, lalu pilihSimpan wawasan.

Memodifikasi wawasan khusus (terprogram)

Untuk memodifikasi wawasan khusus, pilih metode pilihan Anda, dan ikuti instruksinya.

Security Hub API

1. Jalankan`UpdateInsight`operasi.
2. Untuk mengidentifikasi wawasan kustom, berikan Amazon Resource Name (ARN) wawasan. Untuk mendapatkan ARN wawasan kustom, jalankan`GetInsights`operasi.
3. Perbarui`Name`,`Filters`, dan`GroupByAttribute`parameter yang diperlukan.

AWS CLI

1. Pada baris perintah, jalankan`update-insight`perintah.
2. Untuk mengidentifikasi wawasan kustom, berikan Amazon Resource Name (ARN) wawasan. Untuk mendapatkan ARN wawasan kustom, jalankan`get-insights`perintah.
3. Perbarui`name`,`filters`, dan`group-by-attribute`parameter yang diperlukan.

```
aws securityhub update-insight --insight-arn <insight ARN> [--name <new name>] [--
filters <new filters>] [--group-by-attribute <new grouping attribute>]
```

Contoh

```
aws securityhub update-insight --insight-arn "arn:aws:securityhub:us-
west-1:123456789012:insight/123456789012/custom/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111" --filters '{"ResourceType": [{ "Comparison": "EQUALS", "Value":
 "AwsIamRole"}], "SeverityLabel": [{"Comparison": "EQUALS", "Value": "HIGH"}]}' --
name "High severity role findings"
```

PowerShell

1. Gunakan`Update-SHUBInsight`cmdlet.
2. Untuk mengidentifikasi wawasan kustom, berikan Amazon Resource Name (ARN) wawasan. Untuk mendapatkan ARN wawasan kustom, gunakan`Get-SHUBInsight`cmdlet.

3. PerbaruiName,Filter, danGroupByAttributeparameter yang diperlukan.

Contoh

```
$Filter = @{
    ResourceType = [Amazon.SecurityHub.Model.StringFilter]@{
        Comparison = "EQUALS"
        Value = "AwsIamRole"
    }
    SeverityLabel = [Amazon.SecurityHub.Model.StringFilter]@{
        Comparison = "EQUALS"
        Value = "HIGH"
    }
}

Update-SHUBInsight -InsightArn "arn:aws:securityhub:us-
west-1:123456789012:insight/123456789012/custom/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111" -Filter $Filter -Name "High severity role findings"
```

Membuat wawasan kustom baru dari wawasan terkelola (konsol)

Anda tidak dapat menyimpan perubahan atau menghapus wawasan terkelola. Anda dapat menggunakan wawasan terkelola sebagai dasar untuk wawasan kustom baru.

Untuk membuat wawasan kustom baru dari wawasan terkelola

1. BukaAWSKeamanan Hub konsol dihttps://console.aws.amazon.com/securityhub/.
2. Di panel navigasi, pilih Insights (Wawasan).
3. Pilih wawasan yang dikelola untuk dikerjakan.
4. Edit konfigurasi wawasan sesuai kebutuhan.
   - Untuk mengubah atribut yang digunakan untuk mengelompokkan temuan dalam wawasan:
     a. Untuk menghapus pengelompokan yang ada, pilihXdi sampingKelompok olehpengaturan.
     b. Pilih kotak pencarian.
     c. Pilih atribut yang akan digunakan untuk pengelompokan.
     d. Pilih Apply (Terapkan).
   - Untuk menghapus filter dari wawasan, pilih yang dilingkariXdi samping filter.

- Untuk menambahkan filter ke wawasan:
  a. Pilih kotak pencarian.
  b. Pilih atribut dan nilai yang akan digunakan sebagai filter.
  c. Pilih Apply (Terapkan).

5. Ketika pembaruan Anda selesai, pilihBuat wawasan.
6. Saat diminta, masukkanNama wawasan, lalu pilihBuat wawasan.

Menghapus wawasan kustom (konsol)

Bila Anda tidak lagi menginginkan wawasan khusus, Anda dapat menghapusnya. Anda tidak dapat menghapus wawasan terkelola.

Menghapus wawasan kustom

1. BukaAWSKonsol Hub Keamanan dihttps://console.aws.amazon.com/securityhub/.
2. Di panel navigasi, pilih Insights (Wawasan).
3. Temukan wawasan khusus untuk dihapus.
4. Untuk wawasan itu, pilih ikon opsi lainnya (tiga titik di pojok kanan atas kartu).
5. Pilih Delete (Hapus).

Menghapus wawasan kustom (programmatic)

Untuk menghapus wawasan kustom, pilih metode yang Anda inginkan, dan ikuti instruksi.

Security Hub API

1. Jalankan`DeleteInsight`operasi.
2. Untuk mengidentifikasi wawasan kustom untuk dihapus, berikan ARN wawasan. Untuk mendapatkan ARN wawasan kustom, jalankan`GetInsights`operasi.

AWS CLI

1. Pada baris perintah, jalankan`delete-insight`perintah.
2. Untuk mengidentifikasi wawasan kustom, berikan wawasan ARN. Untuk mendapatkan ARN wawasan kustom, jalankan`get-insights`perintah.

```
aws securityhub delete-insight --insight-arn <insight ARN>
```

Contoh

```
aws securityhub delete-insight --insight-arn "arn:aws:securityhub:us-
west-1:123456789012:insight/123456789012/custom/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111"
```

PowerShell

1. Gunakan`Remove-SHUBInsight`cmdlet.
2. Untuk mengidentifikasi wawasan kustom, berikan wawasan ARN. Untuk mendapatkan ARN wawasan kustom, gunakan`Get-SHUBInsight`cmdlet.

Contoh

```
-InsightArn "arn:aws:securityhub:us-west-1:123456789012:insight/123456789012/custom/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

Otomatisasi

Otomatisasi Security Hub dapat membantu Anda dengan cepat memodifikasi dan memulihkan temuan berdasarkan spesifikasi Anda.

Security Hub saat ini mendukung dua jenis otomatisasi:

- Aturan otomatisasi — Secara otomatis memperbarui dan menekan temuan dalam waktu dekat berdasarkan kriteria yang Anda tentukan.
- Respons dan remediasi otomatis — Buat EventBridge aturan khusus yang menentukan tindakan otomatis yang harus diambil terhadap temuan dan wawasan tertentu.

Aturan otomatisasi berlaku sebelum EventBridge aturan. Artinya, aturan otomatisasi dipicu dan memperbarui temuan sebelum dikirim ke EventBridge. EventBridge aturan kemudian berlaku untuk temuan yang diperbarui.

Saat menyiapkan otomatisasi untuk kontrol keamanan, sebaiknya filter berdasarkan ID kontrol daripada judul atau deskripsi. Sementara Security Hub terkadang memperbarui judul dan deskripsi kontrol, ID kontrol tetap sama.

Topik

Aturan otomatisasi

Aturan otomatisasi dapat digunakan untuk memperbarui temuan secara otomatis di Security Hub. Saat temuan dicerna, Security Hub dapat menerapkan berbagai tindakan aturan, seperti menekan temuan, mengubah tingkat keparahannya, dan menambahkan catatan pada temuan. Tindakan aturan tersebut berlaku ketika temuan cocok dengan kriteria yang Anda tentukan, seperti sumber daya atau ID akun mana yang terkait dengan temuan tersebut atau judulnya.

Contoh kasus penggunaan untuk aturan otomatisasi meliputi:

- Meningkatkan keparahan temuan `CRITICAL` jika ID sumber daya temuan mengacu pada sumber daya bisnis yang penting.

- Meningkatkan keparahan temuan dari `HIGH` `CRITICAL` jika temuan tersebut memengaruhi sumber daya dalam akun produksi tertentu.
- Menetapkan temuan spesifik yang memiliki tingkat keparahan status `INFORMATIONAL` `SUPPRESSED` alur kerja.

Aturan otomatisasi dapat digunakan untuk memperbarui bidang pencarian pilihan di AWS Security Finding Format (ASFF). Aturan berlaku untuk temuan baru dan temuan terbaru.

Anda dapat membuat aturan kustom dari awal, atau menggunakan templat aturan yang disediakan oleh Security Hub. Jika Anda menggunakan template aturan, Anda dapat memodifikasinya sesuai kebutuhan untuk kasus penggunaan Anda.

Cara kerja aturan otomatisasi

Administrator Security Hub dapat membuat aturan otomatisasi dengan menentukan kriteria aturan. Jika temuan cocok dengan kriteria yang ditentukan, Security Hub menerapkan tindakan aturan padanya. Untuk informasi selengkapnya tentang kriteria dan tindakan yang tersedia, lihatKriteria aturan dan tindakan aturan yang tersedia.

Hanya akun administrator Security Hub yang dapat membuat, menghapus, mengedit, dan melihat aturan otomatisasi. Aturan yang dibuat administrator berlaku untuk temuan di akun administrator dan semua akun anggota. Dengan memberikan ID akun anggota sebagai kriteria aturan, administrator Security Hub juga dapat menggunakan aturan otomatisasi untuk memperbarui temuan atau mengambil tindakan terhadap temuan di akun anggota tertentu.

Aturan otomatisasi hanya berlaku Wilayah AWS di tempat pembuatannya. Untuk menerapkan aturan di beberapa Wilayah, administrator yang didelegasikan harus membuat aturan di setiap Wilayah. Ini dapat dilakukan melalui konsol Security Hub, Security Hub API, atau AWS CloudFormation. Anda juga dapat menggunakan skrip penyebaran Multi-wilayah.

Untuk mendapatkan riwayat tentang bagaimana aturan otomatisasi telah mengubah temuan Anda, lihatMeninjau riwayat penemuan.

> **Important**
>
> Aturan otomatisasi berlaku untuk temuan baru dan terbaru yang dihasilkan atau diserap oleh Security Hub setelah Anda membuat aturan. Security Hub memperbarui temuan kontrol setiap 12-24 jam atau ketika sumber daya terkait berubah status. Untuk informasi selengkapnya, lihat Jadwal untuk menjalankan pemeriksaan keamanan. Aturan

otomatisasi mengevaluasi bidang temuan asli yang disediakan penyedia. Aturan tidak dipicu saat Anda memperbarui bidang pencarian setelah pembuatan aturan melalui BatchUpdateFindingsoperasi.

Security Hub saat ini mendukung maksimal 100 aturan otomatisasi untuk akun administrator.

Urutan aturan

Saat membuat aturan otomatisasi, Anda menetapkan setiap aturan pesanan. Ini menentukan urutan di mana Security Hub menerapkan aturan otomatisasi Anda, dan menjadi penting ketika beberapa aturan terkait dengan bidang temuan atau pencarian yang sama.

Ketika beberapa tindakan aturan berhubungan dengan bidang temuan atau pencarian yang sama, aturan dengan nilai numerik tertinggi untuk urutan aturan berlaku terakhir dan memiliki efek akhir.

Saat Anda membuat aturan di konsol Security Hub, Security Hub secara otomatis menetapkan urutan aturan berdasarkan urutan pembuatan aturan. Aturan yang paling baru dibuat memiliki nilai numerik terendah untuk urutan aturan dan oleh karena itu berlaku terlebih dahulu. Security Hub menerapkan aturan berikutnya dalam urutan menaik.

Saat Anda membuat aturan melalui Security Hub API atau AWS CLI, Security Hub menerapkan aturan dengan nilai numerik terendah untuk `RuleOrder` pertama. Ini kemudian menerapkan aturan selanjutnya dalam urutan menaik. Jika beberapa temuan memiliki hal yang sama`RuleOrder`, Security Hub menerapkan aturan dengan nilai sebelumnya untuk `UpdatedAt` bidang terlebih dahulu (yaitu, aturan yang terakhir diedit berlaku terakhir).

Anda dapat mengubah urutan aturan kapan saja.

Contoh urutan aturan:

Aturan A (urutan aturan adalah**1**):

- Kriteria Aturan A
  - `ProductName` = `Security Hub`
  - `Resources.Type`adalah `S3 Bucket`
  - `Compliance.Status` = `FAILED`
  - `RecordState`adalah `NEW`
  - `Workflow.Status` = `ACTIVE`

- Aturan A tindakan
  - Perbarui `Confidence` ke `95`
  - Perbarui `Severity` ke `CRITICAL`

Aturan B (urutan aturan adalah**2**):

- Kriteria aturan B
  - `AwsAccountId` = `123456789012`
- Tindakan aturan B
  - Perbarui `Severity` ke `INFORMATIONAL`

Aturan Tindakan diterapkan terlebih dahulu pada temuan Security Hub yang cocok dengan kriteria Aturan A. Selanjutnya, tindakan Aturan B berlaku untuk temuan Security Hub dengan ID akun yang ditentukan. Dalam contoh ini, karena Aturan B berlaku terakhir, nilai akhir `Severity` dalam temuan dari ID akun yang ditentukan adalah`INFORMATIONAL`. Berdasarkan tindakan Aturan A, nilai akhir dari temuan `Confidence` yang cocok adalah`95`.

Kriteria aturan dan tindakan aturan yang tersedia

Bidang ASFF berikut saat ini didukung sebagai kriteria untuk aturan otomatisasi.

Bidang ASFF	Filter	Jenis bidang
`AwsAccountId`	`CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS`	String
`AwsAccountName`	`CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS`	String
`CompanyName`	`CONTAINS, EQUALS, PREFIX, NOT_CONTAINS,`	String

Bidang ASFF	Filter	Jenis bidang
	NOT_EQUALS, PREFIX_NOT_EQUALS	
ComplianceAssociatedStandardsId	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
ComplianceSecurityControlId	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
ComplianceStatus	Is, Is Not	Pilih: [FAILED,NOT_AVAILABLE ,PASSED,WARNING]
Confidence	Eq (equal-to), Gte (greater-than-equal), Lte (less-than-equal)	Jumlah
CreatedAt	Start, End, DateRange	Tanggal (diformat sebagai 2022-12-01T 21:47:39.269 Z)
Criticality	Eq (equal-to), Gte (greater-than-equal), Lte (less-than-equal)	Jumlah
Description	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
FirstObservedAt	Start, End, DateRange	Tanggal (diformat sebagai 2022-12-01T 21:47:39.269 Z)

Bidang ASFF	Filter	Jenis bidang
GeneratorId	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
Id	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
LastObservedAt	Start, End, DateRange	Tanggal (diformat sebagai 2022-12-01T 21:47:39.269 Z)
NoteText	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
NoteUpdatedAt	Start, End, DateRange	Tanggal (diformat sebagai 2022-12-01T 21:47:39.269 Z)
NoteUpdatedBy	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
ProductArn	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
ProductName	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String

Bidang ASFF	Filter	Jenis bidang
RecordState	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
RelatedFindingsId	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
RelatedFindingsProductArn	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
ResourceApplicationArn	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
ResourceApplicationName	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
ResourceDetailsOther	CONTAINS, EQUALS, NOT_CONTAINS, NOT_EQUALS	Peta
ResourceId	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String

Bidang ASFF	Filter	Jenis bidang
ResourcePartition	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
ResourceRegion	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
ResourceTags	CONTAINS, EQUALS, NOT_CONTAINS, NOT_EQUALS	Peta
ResourceType	Is, Is Not	Pilih (lihat Sumber yang didukung oleh ASFF)
SeverityLabel	Is, Is Not	Pilih: [CRITICAL,HIGH,MEDIUM,LOW,INFORMATIONAL]
SourceUrl	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
Title	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
Type	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String

Bidang ASFF	Filter	Jenis bidang
UpdatedAt	Start, End, DateRange	Tanggal (diformat sebagai 2022-12-01T 21:47:39.269 Z)
UserDefinedFields	CONTAINS, EQUALS, NOT_CONTAINS, NOT_EQUALS	Peta
VerificationState	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
WorkflowStatus	Is, Is Not	Pilih: [NEW,NOTIFIED,RESOLVED,SUPPRESSED]

Bidang ASFF berikut saat ini didukung sebagai tindakan untuk aturan otomatisasi:

- Confidence
- Criticality
- Note
- RelatedFindings
- Severity
- Types
- UserDefinedFields
- VerificationState
- Workflow

Untuk informasi selengkapnya tentang bidang ASFF tertentu, lihat sintaks AWS Security Finding Format (ASFF) dan contoh ASFF.

> **Tip**
>
> Jika Anda ingin Security Hub berhenti menghasilkan temuan untuk kontrol tertentu, sebaiknya nonaktifkan kontrol alih-alih menggunakan aturan otomatisasi. Saat Anda menonaktifkan kontrol, Security Hub berhenti menjalankan pemeriksaan keamanan di dalamnya dan berhenti menghasilkan temuan untuk itu, sehingga Anda tidak akan dikenakan biaya untuk kontrol tersebut. Sebaiknya gunakan aturan otomatisasi untuk mengubah nilai bidang ASFF tertentu untuk temuan yang sesuai dengan kriteria yang ditentukan. Untuk informasi selengkapnya tentang menonaktifkan kontrol, lihat. Mengaktifkan dan menonaktifkan kontrol di semua standar

Membuat aturan otomatisasi

Anda dapat membuat aturan kustom dari awal atau menggunakan templat aturan Security Hub yang telah diisi sebelumnya.

Anda hanya dapat membuat satu aturan otomatisasi pada satu waktu. Untuk membuat beberapa aturan otomatisasi, ikuti prosedur konsol beberapa kali, atau panggil API atau perintah beberapa kali dengan parameter yang Anda inginkan.

Anda harus membuat aturan otomatisasi di setiap Wilayah dan akun di mana Anda ingin aturan tersebut diterapkan pada temuan.

Saat Anda membuat aturan otomatisasi di konsol Security Hub, Security Hub menampilkan pratinjau temuan yang diterapkan aturan Anda. Pratinjau saat ini tidak didukung jika kriteria aturan Anda menyertakan filter CONTAINS atau NOT_CONTAINS. Anda dapat memilih filter ini untuk jenis bidang peta dan string.

> **Important**
>
> AWS merekomendasikan agar Anda tidak menyertakan informasi identitas pribadi, rahasia, atau sensitif dalam nama aturan, deskripsi, atau bidang lainnya.

Membuat aturan dari template (hanya konsol)

Saat ini, hanya konsol Security Hub yang mendukung template aturan. Template ini mencerminkan kasus penggunaan umum untuk aturan otomatisasi dan dapat membantu Anda memulai dengan

fitur tersebut. Selesaikan langkah-langkah berikut untuk membuat aturan otomatisasi dari templat di konsol.

Console

1. Buka AWS Security Hub konsol di https://console.aws.amazon.com/securityhub/.

   Masuk ke akun administrator Security Hub.
2. Di panel navigasi, pilih Otomatisasi.
3. Pilih Buat aturan. Untuk Jenis Aturan, pilih Buat aturan dari templat.
4. Pilih template aturan dari menu drop-down.
5. (Opsional) Jika perlu untuk kasus penggunaan Anda, ubah bagian Aturan, Kriteria, dan Tindakan Otomatis. Anda harus menentukan setidaknya satu kriteria aturan dan satu tindakan aturan.

   Jika didukung untuk kriteria yang Anda pilih, konsol akan menampilkan pratinjau temuan yang sesuai dengan kriteria Anda.
6. Untuk status Aturan, pilih apakah Anda ingin aturan Diaktifkan atau Dinonaktifkan setelah dibuat.
7. (Opsional) Perluas bagian Pengaturan tambahan. Pilih Abaikan aturan berikutnya untuk temuan yang cocok dengan kriteria ini jika Anda ingin aturan ini menjadi aturan terakhir yang diterapkan pada temuan yang cocok dengan kriteria aturan.
8. (Opsional) Untuk Tag, tambahkan tag sebagai pasangan nilai kunci untuk membantu Anda mengidentifikasi aturan dengan mudah.
9. Pilih Buat aturan.

Membuat aturan khusus

Pilih metode pilihan Anda, dan selesaikan langkah-langkah berikut untuk membuat aturan otomatisasi kustom.

Console

1. Buka AWS Security Hub konsol di https://console.aws.amazon.com/securityhub/.

   Masuk ke akun administrator Security Hub.
2. Di panel navigasi, pilih Otomatisasi.

3. Pilih Buat aturan. Untuk Jenis Aturan, pilih Buat aturan kustom.
4. Di bagian Aturan, berikan nama aturan unik dan deskripsi untuk aturan Anda.
5. Untuk Kriteria, gunakan menu drop-down Kunci, Operator, dan Nilai untuk menentukan kriteria aturan Anda. Anda harus menentukan setidaknya satu kriteria aturan.

   Jika didukung untuk kriteria yang Anda pilih, konsol akan menampilkan pratinjau temuan yang sesuai dengan kriteria Anda.
6. Untuk tindakan Otomatis, gunakan menu tarik-turun untuk menentukan bidang pencarian mana yang akan diperbarui saat temuan cocok dengan kriteria aturan Anda. Anda harus menentukan setidaknya satu tindakan aturan.
7. Untuk status Aturan, pilih apakah Anda ingin aturan Diaktifkan atau Dinonaktifkan setelah dibuat.
8. (Opsional) Perluas bagian Pengaturan tambahan. Pilih Abaikan aturan berikutnya untuk temuan yang cocok dengan kriteria ini jika Anda ingin aturan ini menjadi aturan terakhir yang diterapkan pada temuan yang cocok dengan kriteria aturan.
9. (Opsional) Untuk Tag, tambahkan tag sebagai pasangan nilai kunci untuk membantu Anda mengidentifikasi aturan dengan mudah.
10. Pilih Buat aturan.

API

1. Jalankan `CreateAutomationRule`dari akun administrator Security Hub. API ini membuat aturan dengan Amazon Resource Name (ARN) tertentu.
2. Sediakan nama dan deskripsi untuk aturan.
3. Tetapkan `IsTerminal` parameter ke `true` jika Anda ingin aturan ini menjadi aturan terakhir yang diterapkan pada temuan yang cocok dengan kriteria aturan.
4. Untuk `RuleOrder` parameter, berikan urutan aturan. Security Hub menerapkan aturan dengan nilai numerik yang lebih rendah untuk parameter ini terlebih dahulu.
5. Untuk `RuleStatus` parameter, tentukan apakah Anda ingin Security Hub mengaktifkan dan mulai menerapkan aturan ke temuan setelah pembuatan. Jika tidak ada nilai yang ditentukan, nilai defaultnya adalah `ENABLED`. Nilai `DISABLED` berarti bahwa aturan dijeda setelah penciptaan.
6. Untuk `Criteria` parameter, berikan kriteria yang ingin digunakan Security Hub untuk memfilter temuan Anda. Tindakan aturan akan berlaku untuk temuan yang sesuai dengan

kriteria. Untuk daftar kriteria yang didukung, lihatKriteria aturan dan tindakan aturan yang tersedia.

7. Untuk `Actions` parameternya, berikan tindakan yang ingin dilakukan Security Hub saat ada kecocokan antara temuan dan kriteria yang ditentukan. Untuk daftar tindakan yang didukung, lihatKriteria aturan dan tindakan aturan yang tersedia.

Contoh permintaan API:

```
{
    "Actions": [{
        "Type": "FINDING_FIELDS_UPDATE",
        "FindingFieldsUpdate": {
            "Workflow": {
                "Status": "SUPPRESSED"
            },
            "Note": {
                "Text": "Known issue that is not a risk.",
                "UpdatedBy": "sechub-automation"
            }
        }
    }],
    "Criteria": {
        "ProductName": [{
            "Value": "Security Hub",
            "Comparison": "EQUALS"
        }],
        "ComplianceStatus": [{
            "Value": "FAILED",
            "Comparison": "EQUALS"
        }],
        "RecordState": [{
            "Value": "ACTIVE",
            "Comparison": "EQUALS"
        }],
        "WorkflowStatus": [{
            "Value": "NEW",
            "Comparison": "EQUALS"
        }],
        "GeneratorId": [{
            "Value": "aws-foundational-security-best-practices/v/1.0.0/IAM.1",
            "Comparison": "EQUALS"
        }]
```

```
    },
    "Description": "Sample rule description",
    "IsTerminal": false,
    "RuleName": "sample-rule-name",
    "RuleOrder": 1,
    "RuleStatus": "ENABLED",
}
```

AWS CLI

1. Jalankan `create-automation-rule`perintah dari akun administrator Security Hub. Perintah ini membuat aturan dengan Nama Sumber Daya Amazon (ARN) tertentu.
2. Sediakan nama dan deskripsi untuk aturan.
3. Sertakan `is-terminal` parameter jika Anda ingin aturan ini menjadi aturan terakhir yang diterapkan pada temuan yang cocok dengan kriteria aturan. Jika tidak, sertakan `no-is-terminal` parameternya.
4. Untuk `rule-order` parameter, berikan urutan aturan. Security Hub menerapkan aturan dengan nilai numerik yang lebih rendah untuk parameter ini terlebih dahulu.
5. Untuk `rule-status` parameter, tentukan apakah Anda ingin Security Hub mengaktifkan dan mulai menerapkan aturan ke temuan setelah pembuatan. Jika tidak ada nilai yang ditentukan, nilai defaultnya adalah `ENABLED`. Nilai `DISABLED` berarti bahwa aturan dijeda setelah penciptaan.
6. Untuk `criteria` parameter, berikan kriteria yang ingin digunakan Security Hub untuk memfilter temuan Anda. Tindakan aturan akan berlaku untuk temuan yang sesuai dengan kriteria. Untuk daftar kriteria yang didukung, lihatKriteria aturan dan tindakan aturan yang tersedia.
7. Untuk `actions` parameternya, berikan tindakan yang ingin dilakukan Security Hub saat ada kecocokan antara temuan dan kriteria yang ditentukan. Untuk daftar tindakan yang didukung, lihatKriteria aturan dan tindakan aturan yang tersedia.

Contoh perintah:

```
aws securityhub create-automation-rule \
--actions '[{
 "Type": "FINDING_FIELDS_UPDATE",
 "FindingFieldsUpdate": {
 "Severity": {
 "Label": "HIGH"
```

```
 },
 "Note": {
 "Text": "Known issue that is a risk. Updated by automation rules",
 "UpdatedBy": "sechub-automation"
 }
 }
 }]' \
--criteria '{
 "SeverityLabel": [{
 "Value": "INFORMATIONAL",
 "Comparison": "EQUALS"
 }]
 }' \
--description "A sample rule" \
--no-is-terminal \
--rule-name "sample rule" \
--rule-order 1 \
--rule-status "ENABLED" \
--region us-east-1
```

Melihat aturan otomatisasi

Pilih metode pilihan Anda, dan ikuti langkah-langkah untuk melihat aturan otomatisasi Anda dan detail setiap aturan.

Console

1. Buka AWS Security Hub konsol di https://console.aws.amazon.com/securityhub/.

   Masuk ke akun administrator Security Hub.
2. Di panel navigasi, pilih Otomatisasi.
3. Pilih nama aturan. Atau, pilih aturan.
4. Pilih Tindakan dan Tampilan.

API

1. Untuk melihat aturan otomatisasi akun Anda, jalankan `ListAutomationRules`dari akun administrator Security Hub. API ini mengembalikan aturan ARN dan metadata lainnya untuk aturan Anda. Tidak ada parameter input yang diperlukan untuk API ini, tetapi Anda dapat

secara opsional menyediakan `MaxResults` untuk membatasi jumlah hasil dan `NextToken` sebagai parameter pagination. Nilai awal `NextToken` harus`NULL`.

Contoh permintaan API:

```
{
 "MaxResults": 50,
 "NextToken": "cVpdnSampleTokenYcXgTockBW44c"
}
```

2. Untuk detail aturan tambahan, termasuk kriteria dan tindakan untuk aturan, jalankan `BatchGetAutomationRules`dari akun administrator Security Hub.

   Contoh permintaan API:

```
{
    "AutomationRulesArns": [
      "arn:aws:securityhub:us-east-1:123456789012:automation-
rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
      "arn:aws:securityhub:us-east-1:123456789012:automation-
rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
      "arn:aws:securityhub:us-east-1:123456789012:automation-
rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE33333",
      "arn:aws:securityhub:us-east-1:123456789012:automation-
rule/a1b2c3d4-5678-90ab-cdef-EXAMPLEaaaaa"
    ]
}
```

AWS CLI

1. Untuk melihat aturan otomatisasi akun Anda, jalankan `list-automation-rules`perintah dari akun administrator Security Hub. Perintah ini mengembalikan aturan ARN dan metadata lainnya untuk aturan Anda. Tidak ada parameter input yang diperlukan untuk perintah ini, tetapi Anda dapat secara opsional menyediakan `max-results` untuk membatasi jumlah hasil dan `next-token` sebagai parameter pagination.

   Contoh perintah:

```
aws securityhub list-automation-rules  \
--max-results 5 \
```

```
--next-token cVpdnSampleTokenYcXgTockBW44c \
--region us-east-1
```

2. Untuk detail aturan tambahan, termasuk kriteria dan tindakan untuk aturan, jalankan batch-get-automation-rulesperintah dari akun administrator Security Hub.

   Contoh perintah:

```
aws securityhub batch-get-automation-rules \
--automation-rules-arns '["arn:aws:securityhub:us-
east-1:123456789012:automation-rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
 "arn:aws:securityhub:us-east-1:123456789012:automation-rule/a1b2c3d4-5678-90ab-
cdef-EXAMPLE22222"]' \
--region us-east-1
```

Mengedit aturan otomatisasi

Saat Anda mengedit aturan otomatisasi, perubahan tersebut berlaku untuk temuan baru dan terbaru yang dihasilkan atau diserap oleh Security Hub setelah aturan diedit.

Pilih metode pilihan Anda, dan ikuti langkah-langkah untuk mengedit konten aturan otomatisasi. Anda dapat mengedit satu atau beberapa aturan dengan satu permintaan. Untuk petunjuk tentang urutan aturan pengeditan, lihatUrutan aturan pengeditan.

Console

1. Buka AWS Security Hub konsol di https://console.aws.amazon.com/securityhub/.

   Masuk ke akun administrator Security Hub.
2. Di panel navigasi, pilih Otomatisasi.
3. Pilih aturan yang ingin Anda edit. Pilih Tindakan dan Edit.
4. Ubah aturan sesuai keinginan, dan pilih Simpan perubahan.

API

1. Jalankan BatchUpdateAutomationRulesdari akun administrator Security Hub.
2. Untuk `RuleArn` parameternya, berikan ARN dari aturan yang ingin Anda edit.

3. Berikan nilai baru untuk parameter yang ingin Anda edit. Anda dapat mengedit parameter apa pun kecualiRuleArn.

Contoh permintaan API:

```
{
    "UpdateAutomationRulesRequestItems": [
        {
            "RuleArn": "arn:aws:securityhub:us-east-1:123456789012:automation-
rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
            "RuleOrder": 15,
            "RuleStatus": "Enabled"
        },
        {
            "RuleArn": "arn:aws:securityhub:us-east-1:123456789012:automation-
rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
            "RuleStatus": "Disabled"
        }
    ]
}
```

AWS CLI

1. Jalankan batch-update-automation-rulesperintah dari akun administrator Security Hub.
2. Untuk RuleArn parameternya, berikan ARN dari aturan yang ingin Anda edit.
3. Berikan nilai baru untuk parameter yang ingin Anda edit. Anda dapat mengedit parameter apa pun kecualiRuleArn.

Contoh perintah:

```
aws securityhub batch-update-automation-rules \
--update-automation-rules-request-items '[
    {
      "Actions": [{
        "Type": "FINDING_FIELDS_UPDATE",
        "FindingFieldsUpdate": {
          "Note": {
            "Text": "Known issue that is a risk",
            "UpdatedBy": "sechub-automation"
```

```
          },
          "Workflow": {
            "Status": "NEW"
          }
        }
      }],
      "Criteria": {
        "SeverityLabel": [{
         "Value": "LOW",
         "Comparison": "EQUALS"
        }]
      },
      "RuleArn": "arn:aws:securityhub:us-east-1:123456789012:automation-
rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
      "RuleOrder": 14,
      "RuleStatus": "DISABLED",
    }
  ]' \
--region us-east-1
```

Urutan aturan pengeditan

Dalam beberapa kasus, Anda mungkin ingin mempertahankan kriteria aturan dan tindakan apa adanya, tetapi mengubah urutan di mana Security Hub menerapkan aturan otomatisasi. Pilih metode pilihan Anda, dan ikuti langkah-langkah untuk mengedit urutan aturan.

Console

1. Buka AWS Security Hub konsol di https://console.aws.amazon.com/securityhub/.

   Masuk ke akun administrator Security Hub.
2. Di panel navigasi, pilih Otomatisasi.
3. Pilih aturan yang urutannya ingin Anda ubah. Pilih Edit prioritas.
4. Pilih Pindah ke atas untuk meningkatkan prioritas aturan dengan satu unit. Pilih Pindah ke bawah untuk mengurangi prioritas aturan sebanyak satu unit. Pilih Pindah ke atas untuk menetapkan aturan urutan 1 (ini memberikan aturan lebih diutamakan daripada aturan lain yang ada).

> **Note**
>
> Saat Anda membuat aturan di konsol Security Hub, Security Hub secara otomatis menetapkan urutan aturan berdasarkan urutan pembuatan aturan. Aturan yang paling baru dibuat memiliki nilai numerik terendah untuk urutan aturan dan oleh karena itu berlaku terlebih dahulu.

API

1. Jalankan `BatchUpdateAutomationRules`dari akun administrator Security Hub.
2. Untuk `RuleArn` parameternya, berikan ARN dari aturan yang urutannya ingin Anda edit.
3. Ubah nilai `RuleOrder` bidang.

> **Note**
>
> Jika beberapa aturan memiliki hal yang sama`RuleOrder`, Security Hub menerapkan aturan dengan nilai sebelumnya untuk `UpdatedAt` bidang terlebih dahulu (yaitu, aturan yang terakhir diedit berlaku terakhir).

AWS CLI

1. Jalankan `batch-update-automation-rules`perintah dari akun administrator Security Hub.
2. Untuk `RuleArn` parameternya, berikan ARN dari aturan yang urutannya ingin Anda edit.
3. Ubah nilai `RuleOrder` bidang.

> **Note**
>
> Jika beberapa aturan memiliki hal yang sama`RuleOrder`, Security Hub menerapkan aturan dengan nilai sebelumnya untuk `UpdatedAt` bidang terlebih dahulu (yaitu, aturan yang terakhir diedit berlaku terakhir).

Menghapus aturan otomatisasi

Saat Anda menghapus aturan otomatisasi, Security Hub menghapusnya dari akun Anda dan tidak lagi menerapkan aturan tersebut pada temuan.

Pilih metode pilihan Anda, dan ikuti langkah-langkah untuk menghapus aturan otomatisasi. Anda dapat menghapus satu atau beberapa aturan dalam satu permintaan.

> **Tip**
>
> Sebagai alternatif untuk penghapusan, Anda dapat menonaktifkan aturan. Ini mempertahankan aturan untuk penggunaan di masa mendatang, tetapi Security Hub tidak akan menerapkan aturan tersebut ke temuan yang cocok sampai Anda mengaktifkannya.

Console

1. Buka AWS Security Hub konsol di https://console.aws.amazon.com/securityhub/.

   Masuk ke akun administrator Security Hub.
2. Di panel navigasi, pilih Otomatisasi.
3. Pilih aturan yang ingin Anda hapus. Pilih Tindakan dan Hapus (untuk mempertahankan aturan, tetapi nonaktifkan sementara, pilih Nonaktifkan).
4. Konfirmasikan pilihan Anda, dan pilih Hapus.

API

1. Jalankan `BatchDeleteAutomationRules`dari akun administrator Security Hub.
2. Untuk `AutomationRulesArns` parameter, berikan ARN dari aturan yang ingin Anda hapus (untuk mempertahankan aturan, tetapi nonaktifkan sementara, sediakan `DISABLED` `RuleStatus` parameternya).

Contoh permintaan API:

```
{
    "AutomationRulesArns": [
        "arn:aws:securityhub:us-east-1:123456789012:automation-
rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
```

```
        "arn:aws:securityhub:us-east-1:123456789012:automation-
rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
        "arn:aws:securityhub:us-east-1:123456789012:automation-
rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE33333",
        "arn:aws:securityhub:us-east-1:123456789012:automation-
rule/a1b2c3d4-5678-90ab-cdef-EXAMPLEaaaaa"
    ]
}
```

AWS CLI

1. Jalankan batch-delete-automation-rulesperintah dari akun administrator Security Hub.
2. Untuk `automation-rules-arns` parameter, berikan ARN dari aturan yang ingin Anda hapus (untuk mempertahankan aturan, tetapi nonaktifkan sementara, sediakan `DISABLED` `RuleStatus` parameternya).

Contoh perintah:

```
aws securityhub batch-delete-automation-rules \
--automation-rules-arns '["arn:aws:securityhub:us-east-1:123456789012:automation-
rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"]' \
--region us-east-1
```

Contoh aturan otomatisasi

Bagian ini mencakup beberapa contoh aturan otomatisasi untuk kasus penggunaan umum. Contoh ini sesuai dengan templat aturan di konsol Security Hub.

Tingkatkan tingkat keparahan menjadi Kritis saat sumber daya tertentu seperti bucket S3 berisiko

Dalam contoh ini, kriteria aturan dicocokkan ketika `ResourceId` dalam temuan adalah bucket Amazon Simple Storage Service (Amazon S3) tertentu. Tindakan aturannya adalah mengubah tingkat keparahan temuan yang cocok menjadi`CRITICAL`. Anda dapat memodifikasi template ini untuk diterapkan ke sumber daya lain.

Contoh permintaan API:

```
{
    "IsTerminal": true,
    "RuleName": "Elevate severity of findings that relate to important resources",
    "RuleOrder": 1,
    "RuleStatus": "ENABLED",
    "Description": "Elevate finding severity to CRITICAL when specific resource such as
 an S3 bucket is at risk",
    "Criteria": {
        "ProductName": [{
            "Value": "Security Hub",
            "Comparison": "EQUALS"
        }],
        "ComplianceStatus": [{
            "Value": "FAILED",
            "Comparison": "EQUALS"
        }],
        "RecordState": [{
            "Value": "ACTIVE",
            "Comparison": "EQUALS"
        }],
        "WorkflowStatus": [{
            "Value": "NEW",
            "Comparison": "EQUALS"
        }],
        "ResourceId": [{
            "Value": "arn:aws:s3:::examplebucket/developers/design_info.doc",
            "Comparison": "EQUALS"
        }]
    },
    "Actions": [{
        "Type": "FINDING_FIELDS_UPDATE",
        "FindingFieldsUpdate": {
            "Severity": {
                "Label": "CRITICAL"
            },
            "Note": {
                "Text": "This is a critical resource. Please review ASAP.",
                "UpdatedBy": "sechub-automation"
            }
        }
    }]
}
```

Contoh perintah CLI:

```
aws securityhub create-automation-rule \
--is-terminal \
--rule-name "Elevate severity of findings that relate to important resources" \
--rule-order 1 \
--rule-status "ENABLED" \

--description "Elevate finding severity to CRITICAL when specific resource such as an
 S3 bucket is at risk" \
--criteria '{
"ProductName": [{
"Value": "Security Hub",
"Comparison": "EQUALS"
}],
"ComplianceStatus": [{
"Value": "FAILED",
"Comparison": "EQUALS"
}],
"RecordState": [{
"Value": "ACTIVE",
"Comparison": "EQUALS"
}],
"WorkflowStatus": [{
"Value": "NEW",
"Comparison": "EQUALS"
}],
"ResourceId": [{
"Value": "arn:aws:s3:::examplebucket/developers/design_info.doc",
"Comparison": "EQUALS"
}]
}' \
--actions '[{
"Type": "FINDING_FIELDS_UPDATE",
"FindingFieldsUpdate": {
"Severity": {
"Label": "CRITICAL"
},
"Note": {
"Text": "This is a critical resource. Please review ASAP.",
"UpdatedBy": "sechub-automation"
}
}
```

```
}]' \
--region us-east-1
```

Meningkatkan keparahan temuan yang berhubungan dengan sumber daya dalam akun produksi

Dalam contoh ini, kriteria aturan dicocokkan ketika temuan `HIGH` tingkat keparahan dihasilkan di akun produksi tertentu. Tindakan aturannya adalah mengubah tingkat keparahan temuan yang cocok menjadi`CRITICAL`.

Contoh permintaan API:

```
{
    "IsTerminal": false,
    "RuleName": "Elevate severity for production accounts",
    "RuleOrder": 1,
    "RuleStatus": "ENABLED",
    "Description": "Elevate finding severity from HIGH to CRITICAL for findings that
 relate to resources in specific production accounts",
    "Criteria": {
        "ProductName": [{
            "Value": "Security Hub",
            "Comparison": "EQUALS"
        }],
        "ComplianceStatus": [{
            "Value": "FAILED",
            "Comparison": "EQUALS"
        }],
        "RecordState": [{
            "Value": "ACTIVE",
            "Comparison": "EQUALS"
        }],
        "WorkflowStatus": [{
            "Value": "NEW",
            "Comparison": "EQUALS"
        }],
        "SeverityLabel": [{
            "Value": "HIGH",
            "Comparison": "EQUALS"
        }],
        "AwsAccountId": [
        {
            "Value": "111122223333",
```

```
            "Comparison": "EQUALS"
        },
        {
            "Value": "123456789012",
            "Comparison": "EQUALS"
        }]
    },
    "Actions": [{
        "Type": "FINDING_FIELDS_UPDATE",
        "FindingFieldsUpdate": {
            "Severity": {
                "Label": "CRITICAL"
            },
            "Note": {
                "Text": "A resource in production accounts is at risk. Please review
 ASAP.",
                "UpdatedBy": "sechub-automation"
            }
        }
    }]
}
```

Contoh perintah CLI:

```
aws securityhub create-automation-rule \
--no-is-terminal \
--rule-name "Elevate severity of findings that relate to resources in production
 accounts" \
--rule-order 1 \
--rule-status "ENABLED" \
--description "Elevate finding severity from HIGH to CRITICAL for findings that relate
 to resources in specific production accounts" \
--criteria '{
"ProductName": [{
"Value": "Security Hub",
"Comparison": "EQUALS"
}],
"ComplianceStatus": [{
"Value": "FAILED",
"Comparison": "EQUALS"
}],
"RecordState": [{
```

```
"Value": "ACTIVE",
"Comparison": "EQUALS"
}],
"SeverityLabel": [{
"Value": "HIGH",
"Comparison": "EQUALS"
}],
"AwsAccountId": [
{
"Value": "111122223333",
"Comparison": "EQUALS"
},
{
"Value": "123456789012",
"Comparison": "EQUALS"
}]
}' \
--actions '[{
"Type": "FINDING_FIELDS_UPDATE",
"FindingFieldsUpdate": {
"Severity": {
"Label": "CRITICAL"
},
"Note": {
"Text": "A resource in production accounts is at risk. Please review ASAP.",
"UpdatedBy": "sechub-automation"
}
}
}]' \
--region us-east-1
```

Menekan temuan informasi

Dalam contoh ini, kriteria aturan dicocokkan untuk temuan `INFORMATIONAL` tingkat keparahan yang dikirim ke Security Hub dari Amazon GuardDuty. Tindakan aturannya adalah mengubah status alur kerja dari temuan yang cocok menjadi. `SUPPRESSED`

Contoh permintaan API:

```
{
    "IsTerminal": false,
    "RuleName": "Suppress informational findings",
    "RuleOrder": 1,
```

```
    "RuleStatus": "ENABLED",
    "Description": "Suppress GuardDuty findings with INFORMATIONAL severity",
    "Criteria": {
        "ProductName": [{
            "Value": "GuardDuty",
            "Comparison": "EQUALS"
        }],
        "RecordState": [{
            "Value": "ACTIVE",
            "Comparison": "EQUALS"
        }],
        "WorkflowStatus": [{
            "Value": "NEW",
            "Comparison": "EQUALS"
        }],
        "SeverityLabel": [{
            "Value": "INFORMATIONAL",
            "Comparison": "EQUALS"
        }]
    },
    "Actions": [{
        "Type": "FINDING_FIELDS_UPDATE",
        "FindingFieldsUpdate": {
            "Workflow": {
                "Status": "SUPPRESSED"
            },
            "Note": {
                "Text": "Automatically suppress GuardDuty findings with INFORMATIONAL
 severity",
                "UpdatedBy": "sechub-automation"
            }
        }
    }]
}
```

Contoh perintah CLI:

```
aws securityhub create-automation-rule \
--no-is-terminal \
--rule-name "Suppress informational findings" \
--rule-order 1 \
--rule-status "ENABLED" \
```

```
--description "Suppress GuardDuty findings with INFORMATIONAL severity" \
--criteria '{
"ProductName": [{
"Value": "GuardDuty",
"Comparison": "EQUALS"
}],
"ComplianceStatus": [{
"Value": "FAILED",
"Comparison": "EQUALS"
}],
"RecordState": [{
"Value": "ACTIVE",
"Comparison": "EQUALS"
}],
"WorkflowStatus": [{
"Value": "NEW",
"Comparison": "EQUALS"
}],
"SeverityLabel": [{
"Value": "INFORMATIONAL",
"Comparison": "EQUALS"
}]
}' \
--actions '[{
"Type": "FINDING_FIELDS_UPDATE",
"FindingFieldsUpdate": {
"Workflow": {
"Status": "SUPPRESSED"
},
"Note": {
"Text": "Automatically suppress GuardDuty findings with INFORMATIONAL severity",
"UpdatedBy": "sechub-automation"
}
}
}]' \
--region us-east-1
```

Respon dan remediasi otomatis

Dengan Amazon EventBridge, Anda dapat mengotomatiskan AWS layanan Anda untuk merespons secara otomatis peristiwa sistem seperti masalah ketersediaan aplikasi atau perubahan sumber daya. Acara dari AWS layanan dikirimkan ke EventBridge dalam waktu hampir real time dan secara

terjamin. Anda dapat menulis aturan sederhana untuk menunjukkan acara mana yang Anda minati dan tindakan otomatis apa yang harus diambil ketika suatu acara cocok dengan aturan. Tindakan yang dapat dipicu secara otomatis meliputi hal-hal berikut:

- Mengambil fungsi AWS Lambda
- Memanggil perintah Amazon EC2 run
- Mengirim peristiwa ke Amazon Kinesis Data Streams
- Mengaktifkan mesin keadaan AWS Step Functions
- Memberi tahu topik Amazon SNS atau antrean Amazon SQS
- Mengirim temuan ke tiket pihak ketiga, obrolan, SIEM, atau alat manajemen dan respons insiden

Security Hub secara otomatis mengirimkan semua temuan baru dan semua pembaruan temuan yang ada ke EventBridge sebagai EventBridge peristiwa. Anda juga dapat membuat tindakan kustom yang memungkinkan Anda mengirim temuan dan hasil wawasan yang dipilih EventBridge.

Anda kemudian mengonfigurasi EventBridge aturan untuk merespons setiap jenis acara.

Untuk informasi selengkapnya tentang penggunaan EventBridge, lihat Panduan EventBridge Pengguna Amazon.

> **Note**
>
> Sebagai praktik terbaik, pastikan bahwa izin yang diberikan kepada pengguna Anda untuk mengakses EventBridge menggunakan kebijakan IAM dengan hak istimewa paling sedikit yang hanya memberikan izin yang diperlukan.
> Untuk informasi selengkapnya, lihat Identitas dan manajemen akses di Amazon EventBridge.

Satu set templat untuk respons dan remediasi otomatis lintas akun juga tersedia di AWS Solusi. Template memanfaatkan aturan EventBridge acara dan fungsi Lambda. Anda menerapkan solusi menggunakan AWS CloudFormation danAWS Systems Manager. Solusinya dapat membuat respons dan tindakan remediasi yang sepenuhnya otomatis. Ini juga dapat menggunakan tindakan kustom Security Hub untuk membuat respons dan tindakan remediasi yang dipicu pengguna. Untuk detail tentang cara mengonfigurasi dan menggunakan solusi, lihat halaman AWS Solusi Respons Keamanan Otomatis.

Topik

Jenis integrasi Security Hub dengan EventBridge

Security Hub menggunakan jenis EventBridge acara berikut untuk mendukung jenis integrasi berikut EventBridge.

Di EventBridge dasbor untuk Security Hub, Semua Acara mencakup semua jenis acara ini.

Semua temuan (Security Hub Findings - Imported)

Security Hub secara otomatis mengirimkan semua temuan baru dan semua pembaruan temuan yang ada ke EventBridge sebagai Security Hub Findings - Importedperistiwa. Setiap Security Hub Findings - Importedperistiwa berisi satu temuan.

Setiap `BatchUpdateFindings`permintaan `BatchImportFindings`dan memicu suatu Security Hub Findings - Importedperistiwa.

Untuk akun administrator, feed acara EventBridge termasuk peristiwa untuk temuan dari akun mereka dan dari akun anggota mereka.

Di Wilayah agregasi, umpan acara mencakup peristiwa untuk temuan dari Wilayah agregasi dan Wilayah terkait. Temuan Lintas Wilayah dimasukkan dalam umpan acara dalam waktu dekat. Untuk informasi tentang cara mengonfigurasi agregasi pencarian, lihatAgregasi Lintas Wilayah.

Anda dapat menentukan aturan EventBridge yang secara otomatis merutekan temuan ke bucket Amazon S3, alur kerja remediasi, atau alat pihak ketiga. Aturan dapat mencakup filter yang hanya menerapkan aturan jika temuan memiliki nilai atribut tertentu.

Anda menggunakan metode ini untuk secara otomatis mengirim semua temuan, atau semua temuan yang memiliki karakteristik spesifik, ke alur kerja respons atau remediasi.

Lihat the section called “Mengkonfigurasi aturan untuk temuan yang dikirim secara otomatis”.

Temuan untuk tindakan kustom (Security Hub Findings - Custom Action)

Security Hub juga mengirimkan temuan yang terkait dengan tindakan kustom ke EventBridge as Security Hub Findings - Custom Actionevents.

Ini berguna bagi analis yang bekerja dengan konsol Security Hub yang ingin mengirim temuan tertentu, atau serangkaian kecil temuan, ke alur kerja respons atau remediasi. Anda dapat memilih tindakan kustom hingga 20 temuan sekaligus. Setiap temuan dikirim EventBridge sebagai EventBridge acara terpisah.

Saat membuat tindakan kustom, Anda menetapkannya ID tindakan kustom. Anda dapat menggunakan ID ini untuk membuat EventBridge aturan yang mengambil tindakan tertentu setelah menerima temuan yang terkait dengan ID tindakan kustom tersebut.

Lihat the section called “Mengkonfigurasi dan menggunakan tindakan kustom”.

Misalnya, Anda dapat membuat tindakan kustom di Security Hub yang dipanggil`send_to_ticketing`. Kemudian EventBridge, Anda membuat aturan yang dipicu saat EventBridge menerima temuan yang menyertakan ID tindakan `send_to_ticketing` kustom. Aturannya mencakup logika untuk mengirim temuan ke sistem tiket Anda. Anda kemudian dapat memilih temuan dalam Security Hub dan menggunakan tindakan kustom di Security Hub untuk mengirim temuan secara manual ke sistem tiket Anda.

Untuk contoh cara mengirim temuan Security Hub EventBridge untuk diproses lebih lanjut, lihat Cara Mengintegrasikan Tindakan AWS Security Hub Kustom dengan PagerDuty dan Cara Mengaktifkan Tindakan Kustom AWS Security Hub di Blog Jaringan AWS Mitra (APN).

Hasil wawasan untuk tindakan kustom (Security Hub Insight Results)

Anda juga dapat menggunakan tindakan kustom untuk mengirim kumpulan hasil wawasan ke EventBridge sebagai Security Hub Insight Resultsperistiwa. Hasil wawasan adalah sumber daya yang cocok dengan wawasan. Perhatikan bahwa ketika Anda mengirim hasil wawasan ke EventBridge, Anda tidak mengirimkan temuan ke EventBridge. Anda hanya mengirimkan pengenal sumber daya yang terkait dengan hasil wawasan. Anda dapat mengirim hingga 100 pengidentifikasi sumber daya sekaligus.

Mirip dengan tindakan kustom untuk temuan, pertama-tama Anda membuat tindakan kustom di Security Hub, lalu membuat aturan di EventBridge.

Lihat the section called “Mengkonfigurasi dan menggunakan tindakan kustom”.

Misalnya, Anda melihat hasil wawasan tertentu yang menarik yang ingin Anda bagikan dengan rekan kerja. Dalam hal ini, Anda dapat menggunakan tindakan khusus untuk mengirimkan hasil wawasan tersebut ke kolega melalui sistem obrolan atau tiket.

EventBridge format acara untuk Security Hub

Jenis Security Hub Findings - ImportedSecurity Findings - Custom Action,, dan Security Hub Insight Resultsacara menggunakan format acara berikut.

Format acara adalah format yang digunakan saat Security Hub mengirimkan acara ke EventBridge.

Security Hub Findings - Imported

Security Hub Findings - Importedperistiwa yang dikirim dari Security Hub untuk EventBridge menggunakan format berikut.

```
{
   "version":"0",
   "id":"CWE-event-id",
   "detail-type":"Security Hub Findings - Imported",
   "source":"aws.securityhub",
   "account":"111122223333",
   "time":"2019-04-11T21:52:17Z",
   "region":"us-west-2",
   "resources":[
      "arn:aws:securityhub:us-west-2::product/aws/macie/arn:aws:macie:us-
west-2:111122223333:integtest/trigger/6294d71b927c41cbab915159a8f326a3/alert/
f2893b211841"
   ],
   "detail":{
      "findings": [{
         <finding content>
       }]
   }
}
```

*<finding content>*adalah konten, dalam format JSON, dari temuan yang dikirim oleh acara. Setiap peristiwa mengirimkan satu temuan.

Untuk daftar lengkap menemukan atribut, lihatAWS Format Pencarian Keamanan (ASFF).

Untuk informasi tentang cara mengonfigurasi EventBridge aturan yang dipicu oleh peristiwa ini, lihatthe section called “Mengkonfigurasi aturan untuk temuan yang dikirim secara otomatis”.

Security Hub Findings - Custom Action

Security Hub Findings - Custom Actionperistiwa yang dikirim dari Security Hub untuk EventBridge menggunakan format berikut. Setiap temuan dikirim dalam acara terpisah.

```
{
  "version": "0",
  "id": "1a1111a1-b22b-3c33-444d-5555e5ee5555",
  "detail-type": "Security Hub Findings - Custom Action",
  "source": "aws.securityhub",
  "account": "111122223333",
  "time": "2019-04-11T18:43:48Z",
  "region": "us-west-1",
  "resources": [
    "arn:aws:securityhub:us-west-1:111122223333:action/custom/custom-action-name"
  ],
  "detail": {
    "actionName":"custom-action-name",
    "actionDescription": "description of the action",
    "findings": [
      {
        <finding content>
      }
    ]
  }
}
```

*<finding content>*adalah konten, dalam format JSON, dari temuan yang dikirim oleh acara. Setiap peristiwa mengirimkan satu temuan.

Untuk daftar lengkap menemukan atribut, lihatAWS Format Pencarian Keamanan (ASFF).

Untuk informasi tentang cara mengonfigurasi EventBridge aturan yang dipicu oleh peristiwa ini, lihatthe section called “Mengkonfigurasi dan menggunakan tindakan kustom”.

Security Hub Insight Results

Security Hub Insight Resultsperistiwa yang dikirim dari Security Hub untuk EventBridge menggunakan format berikut.

```
{
  "version": "0",
  "id": "1a1111a1-b22b-3c33-444d-5555e5ee5555",
  "detail-type": "Security Hub Insight Results",
  "source": "aws.securityhub",
  "account": "111122223333",
  "time": "2017-12-22T18:43:48Z",
  "region": "us-west-1",
  "resources": [
      "arn:aws:securityhub:us-west-1:111122223333::product/aws/macie:us-
west-1:222233334444:test/trigger/1ec9cf700ef6be062b19584e0b7d84ec/alert/f2893b211841"
  ],
  "detail": {
    "actionName":"name of the action",
    "actionDescription":"description of the action",
    "insightArn":"ARN of the insight",
    "insightName":"Name of the insight",
    "resultType":"ResourceAwsIamAccessKeyUserName",
    "number of results":"number of results, max of 100",
    "insightResults": [
        {"result 1": 5},
        {"result 2": 6}
    ]
  }
}
```

Untuk informasi tentang cara membuat EventBridge aturan yang dipicu oleh peristiwa ini, lihatthe section called “Mengkonfigurasi dan menggunakan tindakan kustom”.

Mengkonfigurasi EventBridge aturan untuk temuan yang dikirim secara otomatis

Anda dapat membuat aturan EventBridge yang mendefinisikan tindakan yang harus diambil saat Security Hub Findings - Importedacara diterima. Security Hub Findings - Importedperistiwa dipicu oleh pembaruan dari keduanya `BatchImportFindings`dan `BatchUpdateFindings`.

Setiap aturan berisi pola peristiwa, yang mengidentifikasi peristiwa yang memicu aturan. Pola acara selalu berisi sumber peristiwa (`aws.securityhub`) dan jenis acara (Temuan Security Hub - Imported). Pola peristiwa juga dapat menentukan filter untuk mengidentifikasi temuan yang berlaku aturan tersebut.

Aturan tersebut kemudian mengidentifikasi target aturan. Targetnya adalah tindakan yang harus diambil saat EventBridge menerima Temuan Security Hub - Acara yang diimpor dan temuannya cocok dengan filter.

Instruksi yang diberikan di sini menggunakan EventBridge konsol. Saat Anda menggunakan konsol, EventBridge secara otomatis membuat kebijakan berbasis sumber daya yang diperlukan yang memungkinkan EventBridge untuk menulis ke Log. CloudWatch

Anda juga dapat menggunakan operasi `PutRule`API EventBridge API. Namun, jika Anda menggunakan EventBridge API, Anda harus membuat kebijakan berbasis sumber daya. Untuk detail tentang kebijakan yang diperlukan, lihat Izin CloudWatch log di Panduan EventBridge Pengguna Amazon.

Format pola acara

Format pola acara untuk Temuan Security Hub - Peristiwa yang diimpor adalah sebagai berikut:

```
{
  "source": [
    "aws.securityhub"
  ],
  "detail-type": [
    "Security Hub Findings - Imported"
  ],
  "detail": {
    "findings": {
      <attribute filter values>
    }
  }
}
```

- `source`mengidentifikasi Security Hub sebagai layanan yang menghasilkan acara.
- `detail-type`mengidentifikasi jenis acara.
- `detail`bersifat opsional dan memberikan nilai filter untuk pola acara. Jika pola peristiwa tidak mengandung `detail` bidang, maka semua temuan memicu aturan.

Anda dapat memfilter temuan berdasarkan atribut temuan apa pun. Untuk setiap atribut, Anda menyediakan array dipisahkan koma dari satu atau lebih nilai.

```
"<attribute name>": [ "<value1>", "<value2>"]
```

Jika Anda memberikan lebih dari satu nilai untuk atribut, maka nilai-nilai tersebut digabungkan oleh`OR`. Temuan cocok dengan filter untuk atribut individual jika temuan memiliki salah satu nilai yang terdaftar. Misalnya, jika Anda memberikan keduanya `INFORMATIONAL` dan `LOW` sebagai nilai untuk`Severity.Label`, maka temuan tersebut cocok jika memiliki label keparahan salah satu `INFORMATIONAL` atau`LOW`.

Atribut bergabung dengan`AND`. Temuan cocok jika cocok dengan kriteria filter untuk semua atribut yang disediakan.

Ketika Anda memberikan nilai atribut, itu harus mencerminkan lokasi atribut tersebut dalam struktur AWS Security Finding Format (ASFF).

> **Tip**
>
> Saat memfilter temuan kontrol, sebaiknya gunakan bidang `SecurityControlId` atau `SecurityControlArn` ASFF sebagai filter, bukan `Title` atau. `Description` Bidang yang terakhir dapat berubah sesekali, sedangkan ID kontrol dan ARN adalah pengidentifikasi statis.

Dalam contoh berikut, pola peristiwa memberikan nilai filter untuk `ProductArn` dan`Severity.Label`, sehingga temuan cocok jika dihasilkan oleh Amazon Inspector dan memiliki label keparahan salah satu atau`INFORMATIONAL`. `LOW`

```
{
    "source": [
        "aws.securityhub"
     ],
    "detail-type": [
        "Security Hub Findings - Imported"
    ],
    "detail": {
        "findings": {
            "ProductArn": ["arn:aws:securityhub:us-east-1::product/aws/inspector"],
            "Severity": {
                "Label": ["INFORMATIONAL", "LOW"]
            }
        }
```

```
    }
}
```

Membuat aturan acara

Anda dapat menggunakan pola peristiwa yang telah ditentukan atau pola acara khusus untuk membuat aturan di EventBridge. Jika Anda memilih pola yang telah ditentukan, EventBridge secara otomatis mengisi dan. `source` `detail-type` EventBridge juga menyediakan bidang untuk menentukan nilai filter untuk atribut temuan berikut:

- `AwsAccountId`
- `Compliance.Status`
- `Criticality`
- `ProductArn`
- `RecordState`
- `ResourceId`
- `ResourceType`
- `Severity.Label`
- `Types`
- `Workflow.Status`

Untuk membuat EventBridge aturan

1. Buka EventBridge konsol Amazon di https://console.aws.amazon.com/events/.
2. Dengan menggunakan nilai berikut, buat EventBridge aturan yang memantau penemuan peristiwa:

   - Untuk Tipe aturan, pilih Aturan dengan pola peristiwa.
   - Pilih cara membangun pola acara.

Untuk membangun pola acara dengan...	Lakukan ini...	
Template	Di bagian Pola acara, pilih opsi berikut:	

Untuk membangun pola acara dengan...	Lakukan ini...	
	• Untuk Sumber peristiwa, pilih Layanan AWS. • Untuk AWSlayanan, pilih Security Hub. • Untuk jenis Acara, pilih Temuan Security Hub - Imported. • (Opsional) Untuk membuat aturan lebih spesifik, tambahkan nilai filter. Misalnya, untuk membatasi aturan pada temuan dengan status rekaman aktif, untuk status Rekaman Khusus, pilih Aktif.	

Untuk membangun pola acara dengan...	Lakukan ini...	
Pola acara khusus (Gunakan pola kustom jika Anda ingin memfilter temuan berdasarkan atribut yang tidak muncul di EventBridge konsol.)	• Di bagian Pola acara, pilih Pola kustom (editor JSON), lalu tempelkan pola acara berikut ke area teks: `{ "source": [ "aws.securityhub" ], "detail-type": [ "Security Hub Findings - Imported" ], "detail": { "findings": { "<attribute name>": [ "<value1>", "<value2>" ] } } }` • Perbarui pola acara untuk menyertakan atribut dan nilai atribut yang ingin Anda gunakan sebagai filter. Misalnya, untuk menerapkan aturan pada temuan yang memiliki status verifikasi `TRUE_POSITIVE` ,	

Untuk membangun pola acara dengan...	Lakukan ini...	
	gunakan contoh pola berikut: `{ "source": [ "aws.securityhub" ], "detail-type": [ "Security Hub Findings - Imported" ], "detail": { "findings": { "VerificationState": ["TRUE_POSITIVE"] } } }`	

- Untuk jenis Target, pilih AWSlayanan, dan untuk Pilih target, pilih target seperti topik atau AWS Lambda fungsi Amazon SNS. Target terpicu saat peristiwa diterima yang sesuai dengan pola peristiwa yang ditentukan dalam aturan.

Untuk detail tentang membuat aturan, lihat Membuat EventBridge aturan Amazon yang bereaksi terhadap peristiwa di Panduan EventBridge Pengguna Amazon.

Menggunakan tindakan khusus untuk mengirim temuan dan hasil wawasan ke EventBridge

Untuk menggunakan tindakan kustom Security Hub untuk mengirim temuan atau hasil wawasan EventBridge, Anda terlebih dahulu membuat tindakan kustom di Security Hub. Kemudian, tentukan aturan EventBridge yang berlaku untuk tindakan kustom Anda.

Anda dapat membuat hingga 50 tindakan kustom.

Jika Anda mengaktifkan agregasi lintas wilayah, dan mengelola temuan dari Wilayah agregasi, buat tindakan kustom di Wilayah agregasi.

Aturan dalam EventBridge menggunakan ARN dari tindakan kustom.

Membuat tindakan kustom (konsol)

Saat membuat tindakan kustom, Anda menentukan nama, deskripsi, dan pengenal unik.

Untuk membuat tindakan kustom di Security Hub (konsol)

1. Buka AWS Security Hub konsol di https://console.aws.amazon.com/securityhub/.
2. Di panel navigasi, pilih Pengaturan dan kemudian pilih Tindakan kustom.
3. Pilih Buat tindakan kustom.
4. Berikan Nama, Deskripsi, dan ID tindakan Kustom untuk tindakan tersebut.

   Nama harus kurang dari 20 karakter.

   ID tindakan kustom harus unik untuk setiap AWS akun.
5. Pilih Buat tindakan kustom.
6. Catat ARN tindakan Kustom. Anda perlu menggunakan ARN saat membuat aturan untuk dikaitkan dengan tindakan ini di. EventBridge

Membuat tindakan kustom (Security Hub API,AWS CLI)

Untuk membuat tindakan kustom, Anda dapat menggunakan panggilan API atauAWS Command Line Interface.

Untuk membuat tindakan kustom (Security Hub API,AWS CLI)

- Security Hub API — Gunakan `CreateActionTarget`operasi. Saat membuat tindakan kustom, Anda memberikan nama, deskripsi, dan pengenal tindakan kustom.
- AWS CLI— Pada baris perintah, jalankan `create-action-target`perintah.

```
create-action-target --name <customActionName> --
description <customActionDescription> --id <customActionidentifier>
```

Contoh

```
aws securityhub create-action-target --name "Send to remediation" --description
 "Action to send the finding for remediation tracking" --id "Remediation"
```

Mendefinisikan aturan di EventBridge

Untuk memproses tindakan kustom, Anda harus membuat aturan yang sesuai di EventBridge. Definisi aturan mencakup ARN dari tindakan kustom.

Pola acara untuk Temuan Security Hub - peristiwa Tindakan Kustom memiliki format berikut:

```
{
  "source": [
    "aws.securityhub"
  ],
  "detail-type": [
    "Security Hub Findings - Custom Action"
  ],
  "resources": [ "<custom action ARN>" ]
}
```

Pola acara untuk acara Hasil Wawasan Security Hub memiliki format berikut:

```
{
  "source": [
    "aws.securityhub"
  ],
  "detail-type": [
    "Security Hub Insight Results"
  ],
  "resources": [ "<custom action ARN>" ]
}
```

Dalam kedua pola, *<custom action ARN>* adalah ARN dari tindakan khusus. Anda dapat mengonfigurasi aturan yang berlaku untuk lebih dari satu tindakan kustom.

Instruksi yang diberikan di sini adalah untuk EventBridge konsol. Saat Anda menggunakan konsol, EventBridge secara otomatis membuat kebijakan berbasis sumber daya yang diperlukan yang memungkinkan EventBridge untuk menulis ke Log. CloudWatch

Anda juga dapat menggunakan operasi `PutRule`API EventBridge API. Namun, jika Anda menggunakan EventBridge API, Anda harus membuat kebijakan berbasis sumber daya. Untuk detail tentang kebijakan yang diperlukan, lihat Izin CloudWatch log di Panduan EventBridge Pengguna Amazon.

Untuk mendefinisikan aturan di EventBridge

1. Buka EventBridge konsol Amazon di https://console.aws.amazon.com/events/.
2. Di panel navigasi, pilih Aturan.
3. Pilih Buat aturan.
4. Masukkan nama dan deskripsi untuk aturan.
5. Untuk bus acara, pilih bus acara yang ingin Anda kaitkan dengan aturan ini. Jika Anda ingin aturan ini cocok dengan peristiwa yang berasal dari akun Anda, pilih default. Saat layanan AWS di akun Anda menghasilkan kejadian, layanan tersebut akan selalu masuk ke bus kejadian default akun Anda.
6. Untuk Tipe aturan, pilih Aturan dengan pola peristiwa.
7. Pilih Selanjutnya.
8. Untuk sumber Acara, pilih AWSacara.
9. Untuk pola Acara, pilih Formulir pola acara.
10. Untuk Sumber peristiwa, pilih Layanan AWS.
11. Untuk AWSlayanan, pilih Security Hub.
12. Untuk Jenis peristiwa, lakukan salah satu hal berikut:
    - Untuk membuat aturan yang akan diterapkan saat Anda mengirim temuan ke tindakan kustom, pilih Temuan Security Hub - Tindakan Kustom.
    - Untuk membuat aturan yang akan diterapkan saat Anda mengirim hasil wawasan ke tindakan kustom, pilih Hasil Wawasan Security Hub.
13. Pilih ARN tindakan khusus khusus, tambahkan ARN tindakan kustom.

    Jika aturan berlaku untuk beberapa tindakan kustom, pilih Tambah untuk menambahkan lebih banyak ARN tindakan kustom.
14. Pilih Berikutnya.
15. Di bawah Pilih target, pilih dan konfigurasikan target yang akan dipanggil saat aturan ini cocok.
16. Pilih Berikutnya.

17. (Opsional) Masukkan satu atau lebih tanda untuk aturan. Untuk informasi selengkapnya, lihat EventBridge tag Amazon di Panduan EventBridge Pengguna Amazon.
18. Pilih Berikutnya.
19. Tinjau detail aturan dan pilih Buat aturan.

    Saat Anda melakukan tindakan kustom pada hasil temuan atau wawasan di akun Anda, peristiwa akan dihasilkan EventBridge.

Memilih tindakan khusus untuk temuan dan hasil wawasan

Setelah membuat tindakan dan EventBridge aturan kustom Security Hub, Anda dapat mengirimkan hasil temuan dan wawasan EventBridge untuk pengelolaan dan pemrosesan lebih lanjut.

Acara dikirim ke EventBridge hanya di akun di mana mereka dilihat. Jika Anda melihat temuan menggunakan akun administrator, acara dikirim ke EventBridge akun administrator.

Agar panggilan AWS API efektif, implementasi kode target harus beralih peran ke akun anggota. Ini juga berarti bahwa peran yang Anda alihkan harus diterapkan ke setiap anggota di mana tindakan diperlukan.

Untuk mengirim temuan ke EventBridge

1. Buka AWS Security Hub konsol di https://console.aws.amazon.com/securityhub/.
2. Menampilkan daftar temuan:
   - Dari Temuan, Anda dapat melihat temuan dari semua integrasi dan kontrol produk yang diaktifkan.
   - Dari standar Keamanan, Anda dapat menavigasi ke daftar temuan yang dihasilkan dari kontrol yang dipilih. Lihat the section called “Melihat detail untuk kontrol”.
   - Dari Integrasi, Anda dapat menavigasi ke daftar temuan yang dihasilkan oleh integrasi yang diaktifkan. Lihat the section called “Melihat temuan dari integrasi”.
   - Dari Wawasan, Anda dapat menavigasi ke daftar temuan untuk hasil wawasan. Lihat the section called “Melihat hasil dan temuan wawasan”.
3. Pilih temuan yang akan dikirim EventBridge. Anda dapat memilih hingga 20 temuan sekaligus.
4. Dari Tindakan, pilih tindakan kustom yang selaras dengan EventBridge aturan yang akan diterapkan.

Security Hub mengirimkan temuan Security Hub terpisah - peristiwa Tindakan Kustom untuk setiap temuan.

Untuk mengirimkan hasil wawasan ke EventBridge

1. Buka AWS Security Hub konsol di https://console.aws.amazon.com/securityhub/.
2. Pada panel navigasi, silakan pilih Wawasan.
3. Pada halaman Insights, pilih insight yang menyertakan hasil yang akan dikirimkan EventBridge.
4. Pilih hasil wawasan yang akan dikirim EventBridge. Anda dapat memilih hingga 20 hasil sekaligus.
5. Dari Tindakan, pilih tindakan kustom yang selaras dengan EventBridge aturan yang akan diterapkan.

Integrasi produk di AWS Security Hub

AWSSecurity Hub dapat mengumpulkan data pencarian keamanan dari beberapa AWS layanan dan dari solusi keamanan AWS Partner Network (APN) yang didukung. Agregasi ini memberikan pandangan komprehensif tentang keamanan dan kepatuhan di seluruh AWS lingkungan Anda.

Anda juga dapat mengirim temuan yang dihasilkan dari produk keamanan khusus Anda sendiri.

> **Important**
>
> Dari integrasi produk yang didukung AWS dan mitra, Security Hub hanya menerima dan mengkonsolidasikan temuan yang dihasilkan setelah Anda mengaktifkan Security Hub. Akun AWS
> Layanan tidak secara surut menerima dan mengkonsolidasikan temuan keamanan yang dihasilkan sebelum Anda mengaktifkan Security Hub.

Untuk detail tentang cara Security Hub mengenakan biaya untuk temuan yang tertelan, lihat harga Security Hub.

Topik

Mengelola integrasi produk

Halaman Integrasi di AWS Management Console menyediakan akses ke semua integrasi produk yang tersedia AWS dan pihak ketiga. AWS Security Hub API juga menyediakan operasi untuk memungkinkan Anda mengelola integrasi.

> **Note**
>
> Beberapa integrasi tidak tersedia di semua Wilayah. Jika integrasi tidak didukung di Wilayah saat ini, itu tidak tercantum di halaman Integrasi.

Lihat juga the section called “Integrasi yang didukung di China (Beijing) dan China (Ningxia)” dan the section called “Integrasi yang didukung di AWS GovCloud (AS-Timur) dan AWS GovCloud (AS-Barat)”.

Melihat dan memfilter daftar integrasi (konsol)

Dari halaman Integrasi, Anda dapat melihat dan memfilter daftar integrasi.

Untuk melihat daftar integrasi

1. Buka konsol AWS Security Hub di https://console.aws.amazon.com/securityhub/.
2. Di panel navigasi Security Hub, pilih Integrasi.

Pada halaman Integrasi, integrasi dengan AWS layanan lain terdaftar terlebih dahulu, diikuti oleh integrasi dengan produk pihak ketiga.

Untuk setiap integrasi, halaman Integrasi menyediakan informasi berikut.

- Nama perusahaan
- Nama produk
- Deskripsi integrasi
- Kategori yang diterapkan integrasi
- Cara mengaktifkan integrasi
- Status integrasi saat ini

Anda dapat memfilter daftar dengan memasukkan teks dari bidang berikut.

- Nama perusahaan
- Nama produk
- Deskripsi integrasi
- Kategori

Melihat informasi tentang integrasi produk (Security Hub API, AWS CLI)

Untuk melihat informasi tentang integrasi produk, Anda dapat menggunakan panggilan API atau. AWS Command Line Interface Anda dapat menampilkan informasi tentang semua integrasi produk, atau informasi tentang integrasi produk yang telah Anda aktifkan.

Untuk melihat informasi tentang semua integrasi produk yang tersedia (Security Hub API, AWS CLI)

- Security Hub API — Gunakan `DescribeProducts`operasi. Untuk mengidentifikasi integrasi produk tertentu untuk kembali, gunakan `ProductArn` parameter untuk menyediakan integrasi ARN.
- AWS CLI— Pada baris perintah, jalankan `describe-products`perintah. Untuk mengidentifikasi integrasi produk tertentu untuk kembali, berikan ARN integrasi.

```
aws securityhub describe-products --product-arn "<integrationARN>"
```

Contoh

```
aws securityhub describe-products --product-arn "arn:aws:securityhub:us-
east-1::product/3coresec/3coresec"
```

Untuk melihat informasi tentang integrasi produk yang telah Anda aktifkan (Security Hub API, AWS CLI)

- Security Hub API — Gunakan `ListEnabledProductsForImport`operasi.
- AWS CLI— Pada baris perintah, jalankan `list-enabled-products-for-import`perintah.

```
aws securityhub list-enabled-products-for-import
```

Mengaktifkan integrasi

Pada halaman Integrasi, setiap integrasi menyediakan langkah-langkah yang diperlukan untuk mengaktifkan integrasi.

Untuk sebagian besar integrasi dengan AWS layanan lain, satu-satunya langkah yang diperlukan adalah mengaktifkan layanan lainnya. Informasi integrasi mencakup tautan ke halaman beranda

layanan. Saat Anda mengaktifkan layanan lain, izin tingkat sumber daya yang memungkinkan Security Hub menerima temuan dari layanan akan dibuat dan diterapkan secara otomatis.

Untuk integrasi produk pihak ketiga, Anda mungkin perlu membeli integrasi dari AWS Marketplace, dan kemudian mengkonfigurasi integrasi. Informasi integrasi menyediakan tautan untuk melakukan tugas-tugas tersebut.

Jika lebih dari satu versi produk tersedia AWS Marketplace, pilih versi untuk berlangganan dan kemudian pilih Lanjutkan Berlangganan. Misalnya, beberapa produk menawarkan versi standar dan AWS GovCloud (US) versi.

Saat Anda mengaktifkan integrasi produk, kebijakan sumber daya secara otomatis dilampirkan ke langganan produk tersebut. Kebijakan sumber daya ini menentukan izin yang dibutuhkan Security Hub untuk menerima temuan dari produk tersebut.

Menonaktifkan dan mengaktifkan aliran temuan dari integrasi (konsol)

Pada halaman Integrasi, untuk integrasi yang mengirimkan temuan, informasi Status menunjukkan apakah Anda saat ini menerima temuan.

Untuk berhenti menerima temuan, pilih Berhenti menerima temuan.

Untuk melanjutkan menerima temuan, pilih Terima temuan.

Menonaktifkan alur temuan dari integrasi (Security Hub API,) AWS CLI

Untuk menonaktifkan alur temuan dari integrasi, Anda dapat menggunakan panggilan API atau AWS Command Line Interface.

Untuk menonaktifkan alur temuan dari integrasi (Security Hub API, AWS CLI)

- Security Hub API — Gunakan `DisableImportFindingsForProduct`operasi. Untuk mengidentifikasi integrasi yang akan dinonaktifkan, Anda memerlukan ARN langganan Anda. Untuk mendapatkan ARN berlangganan untuk integrasi Anda yang diaktifkan, gunakan operasi. `ListEnabledProductsForImport`
- AWS CLI— Pada baris perintah, jalankan `disable-import-findings-for-product`perintah.

  ```
  aws securityhub disable-import-findings-for-product --product-subscription-
  arn <subscription ARN>
  ```

  Contoh

```
aws securityhub disable-import-findings-for-product --product-subscription-arn
 "arn:aws:securityhub:us-west-1:123456789012:product-subscription/crowdstrike/
crowdstrike-falcon"
```

Mengaktifkan aliran temuan dari integrasi (Security Hub API, AWS CLI)

Untuk mengaktifkan alur temuan dari integrasi, Anda dapat menggunakan panggilan API atau panggilan AWS Command Line Interface.

Untuk mengaktifkan aliran temuan dari integrasi (Security Hub API, AWS CLI)

- Security Hub API — Gunakan `EnableImportFindingsForProduct`operasi. Untuk mengaktifkan Security Hub menerima temuan dari integrasi, Anda memerlukan ARN produk. Untuk mendapatkan ARN untuk integrasi yang tersedia, gunakan operasi. `DescribeProducts`
- AWS CLI: Pada baris perintah, jalankan `enable-import-findings-for-product`perintah.

  ```
  aws securityhub enable-import-findings-for-product --product-arn <integration ARN>
  ```

  Contoh

  ```
  aws securityhub enable-import-findings-for product --product-arn
   "arn:aws:securityhub:us-east-1:123456789333:product/crowdstrike/crowdstrike-falcon"
  ```

Melihat temuan dari integrasi

Untuk integrasi yang Anda terima temuannya (Status Menerima temuan), untuk melihat daftar temuan, pilih Lihat temuan.

Daftar temuan menunjukkan temuan aktif untuk integrasi yang dipilih yang memiliki status alur kerja `NEW` atau`NOTIFIED`.

Jika Anda mengaktifkan agregasi lintas wilayah, maka di Wilayah agregasi, daftar tersebut mencakup temuan dari Wilayah agregasi dan dari Wilayah tertaut tempat integrasi diaktifkan. Security Hub tidak secara otomatis mengaktifkan integrasi berdasarkan konfigurasi agregasi lintas wilayah.

Di Wilayah lain, daftar temuan untuk integrasi hanya berisi temuan dari Wilayah saat ini.

Untuk informasi tentang cara mengonfigurasi agregasi lintas wilayah, lihat. Agregasi Lintas Wilayah

Dari daftar temuan, Anda dapat melakukan tindakan berikut.

- Ubah filter dan pengelompokan untuk daftar
- Lihat detail untuk temuan individu
- Perbarui status alur kerja temuan
- Kirim temuan ke tindakan khusus

Layanan AWS Integrasi dengan AWS Security Hub

AWS Security Hub mendukung integrasi dengan beberapa lainnya Layanan AWS.

> **Note**
>
> Beberapa integrasi hanya tersedia di pilih Wilayah AWS.
> Jika integrasi tidak didukung di Wilayah tertentu, integrasi tidak tercantum di halaman Integrasi konsol Security Hub.
> Untuk informasi selengkapnya, lihat Integrasi yang didukung di China (Beijing) dan China (Ningxia) dan Integrasi yang didukung di AWS GovCloud (AS-Timur) dan AWS GovCloud (AS-Barat).

Kecuali ditunjukkan di bawah ini, Layanan AWS integrasi yang mengirim temuan ke Security Hub diaktifkan secara otomatis setelah Anda mengaktifkan Security Hub. Integrasi yang menerima temuan Security Hub mungkin memerlukan langkah tambahan untuk aktivasi. Tinjau informasi tentang setiap integrasi untuk mempelajari lebih lanjut.

Ikhtisar integrasi AWS layanan dengan Security Hub

Berikut adalah ikhtisar AWS layanan yang mengirimkan temuan ke Security Hub atau menerima temuan dari Security Hub.

AWS Layanan terintegrasi	Arahan	
AWS Config	Mengirim temuan	
AWS Firewall Manager	Mengirim temuan	

AWS Layanan terintegrasi	Arahan
Amazon GuardDuty	Mengirim temuan
AWS Health	Mengirim temuan
AWS Identity and Access Management Access Analyzer	Mengirim temuan
Amazon Inspector	Mengirim temuan
AWS IoT Device Defender	Mengirim temuan
Amazon Macie	Mengirim temuan
AWS Systems Manager Manajer Patch	Mengirim temuan
AWS Audit Manager	Menerima temuan
AWS Chatbot	Menerima temuan
Detektif Amazon	Menerima temuan
Danau Keamanan Amazon	Menerima temuan
AWS Systems Manager Explorer dan OpsCenter	Menerima dan memperbarui temuan
AWS Trusted Advisor	Menerima temuan

AWS layanan yang mengirimkan temuan ke Security Hub

AWS Layanan berikut terintegrasi dengan Security Hub dengan mengirimkan temuan ke Security Hub. Security Hub mengubah temuan menjadi AWS Security Finding Format.

AWS Config (Mengirim temuan)

AWS Config adalah layanan yang memungkinkan Anda menilai, mengaudit, dan mengevaluasi konfigurasi AWS sumber daya Anda. AWS Config terus memantau dan merekam konfigurasi AWS

sumber daya Anda dan memungkinkan Anda untuk mengotomatiskan evaluasi konfigurasi yang direkam terhadap konfigurasi yang diinginkan.

Dengan menggunakan integrasi dengan AWS Config, Anda dapat melihat hasil evaluasi aturan AWS Config terkelola dan kustom sebagai temuan di Security Hub. Temuan ini dapat dilihat bersama temuan Security Hub lainnya, memberikan gambaran menyeluruh tentang postur keamanan Anda.

AWS Config menggunakan Amazon EventBridge untuk mengirim evaluasi AWS Config aturan ke Security Hub. Security Hub mengubah evaluasi aturan menjadi temuan yang mengikuti Format Pencarian AWS Keamanan. Security Hub kemudian memperkaya temuan dengan upaya terbaik dengan mendapatkan informasi lebih lanjut tentang sumber daya yang terkena dampak, seperti Nama Sumber Daya Amazon (ARN) dan tanggal pembuatan. Tag sumber daya dalam evaluasi AWS Config aturan tidak disertakan dalam temuan Security Hub.

Untuk informasi selengkapnya tentang integrasi ini, lihat bagian berikut.

Cara AWS Config mengirim temuan ke Security Hub

Semua temuan di Security Hub menggunakan format JSON standar ASFF. ASFF mencakup rincian tentang asal temuan, sumber daya yang terpengaruh, dan status temuan saat ini. AWS Config mengirimkan evaluasi aturan terkelola dan kustom ke Security Hub melalui EventBridge. Security Hub mengubah evaluasi aturan menjadi temuan yang mengikuti ASFF dan memperkaya temuan berdasarkan upaya terbaik.

Jenis temuan yang AWS Config dikirim ke Security Hub

Setelah integrasi diaktifkan, AWS Config kirimkan evaluasi semua aturan AWS Config terkelola dan aturan khusus ke Security Hub. Hanya evaluasi dari AWS Config aturan terkait layanan, seperti yang digunakan untuk menjalankan pemeriksaan pada kontrol keamanan, yang dikecualikan.

Mengirim AWS Config temuan ke Security Hub

Ketika integrasi diaktifkan, Security Hub akan secara otomatis menetapkan izin yang diperlukan untuk menerima temuan dari. AWS Config Security Hub menggunakan izin service-to-service tingkat yang memberi Anda cara aman untuk mengaktifkan integrasi ini dan mengimpor temuan dari AWS Config melalui Amazon EventBridge.

Latensi untuk mengirim temuan

Saat AWS Config membuat temuan baru, Anda biasanya dapat melihat temuan di Security Hub dalam waktu lima menit.

Mencoba kembali saat Security Hub tidak tersedia

AWS Config mengirimkan temuan ke Security Hub dengan upaya terbaik melalui EventBridge. Jika acara tidak berhasil dikirim ke Security Hub, EventBridge coba ulang pengiriman hingga 24 jam atau 185 kali, mana yang lebih dulu.

Memperbarui AWS Config temuan yang ada di Security Hub

Setelah AWS Config mengirim temuan ke Security Hub, ia dapat mengirim pembaruan ke temuan yang sama ke Security Hub untuk mencerminkan pengamatan tambahan dari aktivitas temuan. Pembaruan hanya dikirim untuk `ComplianceChangeNotification` acara. Jika tidak terjadi perubahan kepatuhan, pembaruan tidak akan dikirim ke Security Hub. Security Hub menghapus temuan 90 hari setelah pembaruan terbaru atau 90 hari setelah pembuatan jika tidak ada pembaruan yang terjadi.

Security Hub tidak mengarsipkan temuan yang dikirim dari AWS Config meskipun Anda menghapus sumber daya terkait.

Daerah di mana AWS Config temuan ada

AWS Config Temuan ini terjadi secara regional. AWS Config mengirimkan temuan ke Security Hub di Wilayah atau Wilayah yang sama di mana temuan terjadi.

Melihat AWS Config temuan di Security Hub

Untuk melihat AWS Config temuan Anda, pilih Temuan dari panel navigasi Security Hub. Untuk memfilter temuan agar hanya menampilkan AWS Config temuan, pilih Nama produk di drop-down bilah pencarian. Masukkan Config, dan pilih Apply.

Menafsirkan AWS Config menemukan nama di Security Hub

Security Hub mengubah evaluasi AWS Config aturan menjadi temuan yang mengikuti. AWS Format Pencarian Keamanan (ASFF) AWS Config evaluasi aturan menggunakan pola peristiwa yang berbeda dibandingkan dengan ASFF. Tabel berikut memetakan bidang evaluasi AWS Config aturan dengan rekan ASFF mereka seperti yang muncul di Security Hub.

Jenis temuan evaluasi aturan Config	Tipe temuan ASFF	Nilai hardcode
detail. awsAccountId	AwsAccountId	

Jenis temuan evaluasi aturan Config	Tipe temuan ASFF	Nilai hardcode
detail. newEvaluationResult. resultRecordedTime	CreatedAt	
detail. newEvaluationResult. resultRecordedTime	UpdatedAt	
	ProductArn	<partition><region >“arn ::securityhub:: :product/ aws/config”
	ProductName	“Config”
	CompanyName	"AWS"
	Wilayah	“eu-sentral-1"
configRuleArn	GeneratorId, ProductFields	
detail. ConfigRuleARN/mene mukan/hash	Id	
detail. configRuleName	Judul, ProductFields	
detail. configRuleName	Deskripsi	“Temuan ini dibuat untuk perubahan kepatuhan sumber daya untuk aturan konfigura si:`${detail.ConfigRul eName}` ”
Item Konfigurasi “ARN” atau Security Hub menghitung ARN	Sumber Daya [i] .id	
detail.ResourceType	Sumber Daya [i] .Type	"AwsS3Bucket"
	Sumber Daya [i] .Partisi	"aws"
	Sumber Daya [i] .Region	“eu-sentral-1"

Jenis temuan evaluasi aturan Config	Tipe temuan ASFF	Nilai hardcode
Item Konfigurasi “konfigurasi”	Sumber Daya [i] .Detail	
	SchemaVersion	“2018-10-08"
	Keparahan. Label	Lihat “Menafsirkan Label Keparahan” di bawah ini
	Tipe	["Pemeriksaan Perangkat Lunak dan Konfigurasi"]
detail. newEvaluationResult.ComplianceType	Kepatuhan.Status	“GAGAL”, “NOT_AVAILABLE”, “LULUS”, atau “PERINGATAN”
	Alur kerja.Status	“DISELESAIKAN” jika AWS Config temuan dihasilkan dengan Compliance.Status dari “LULUS,” atau jika Compliance.Status berubah dari “GAGAL” menjadi “LULUS.” Jika tidak, Workflow. Status akan menjadi “BARU.” Anda dapat mengubah nilai ini dengan operasi BatchUpdateFindingsAPI.

Menafsirkan label keparahan

Semua temuan dari evaluasi AWS Config aturan memiliki label keparahan default MEDIUM di ASFF. Anda dapat memperbarui label keparahan temuan dengan operasi `BatchUpdateFindings`API.

Temuan khas dari AWS Config

Security Hub mengubah evaluasi AWS Config aturan menjadi temuan yang mengikuti ASFF. Berikut ini adalah contoh temuan khas dari AWS Config dalam ASFF.

> **Note**
>
> Jika deskripsi lebih dari 1024 karakter, itu akan dipotong menjadi 1024 karakter dan akan mengatakan “(terpotong)” di akhir.


```
{
 "SchemaVersion": "2018-10-08",
 "Id": "arn:aws:config:eu-central-1:123456789012:config-rule/config-rule-mburzq/
finding/45g070df80cb50b68fa6a43594kc6fda1e517932",
 "ProductArn": "arn:aws:securityhub:eu-central-1::product/aws/config",
 "ProductName": "Config",
 "CompanyName": "AWS",
 "Region": "eu-central-1",
 "GeneratorId": "arn:aws:config:eu-central-1:123456789012:config-rule/config-rule-
mburzq",
 "AwsAccountId": "123456789012",
 "Types": [
  "Software and Configuration Checks"
 ],
 "CreatedAt": "2022-04-15T05:00:37.181Z",
 "UpdatedAt": "2022-04-19T21:20:15.056Z",
 "Severity": {
  "Label": "MEDIUM",
  "Normalized": 40
 },
 "Title": "s3-bucket-level-public-access-prohibited-config-integration-demo",
 "Description": "This finding is created for a resource compliance change for config
 rule: s3-bucket-level-public-access-prohibited-config-integration-demo",
 "ProductFields": {
  "aws/securityhub/ProductName": "Config",
  "aws/securityhub/CompanyName": "AWS",
  "aws/securityhub/FindingId": "arn:aws:securityhub:eu-central-1::product/aws/
config/arn:aws:config:eu-central-1:123456789012:config-rule/config-rule-mburzq/
finding/46f070df80cd50b68fa6a43594dc5fda1e517902",
  "aws/config/ConfigRuleArn": "arn:aws:config:eu-central-1:123456789012:config-rule/
config-rule-mburzq",
  "aws/config/ConfigRuleName": "s3-bucket-level-public-access-prohibited-config-
integration-demo",
  "aws/config/ConfigComplianceType": "NON_COMPLIANT"
 },
 "Resources": [{
```

```
  "Type": "AwsS3Bucket",
  "Id": "arn:aws:s3:::config-integration-demo-bucket",
  "Partition": "aws",
  "Region": "eu-central-1",
  "Details": {
   "AwsS3Bucket": {
    "OwnerId": "4edbba300f1caa608fba2aad2c8fcfe30c32ca32777f64451eec4fb2a0f10d8c",
    "CreatedAt": "2022-04-15T04:32:53.000Z"
   }
  }
 }],
 "Compliance": {
  "Status": "FAILED"
 },
 "WorkflowState": "NEW",
 "Workflow": {
  "Status": "NEW"
 },
 "RecordState": "ACTIVE",
 "FindingProviderFields": {
  "Severity": {
   "Label": "MEDIUM"
  },
  "Types": [
   "Software and Configuration Checks"
  ]
 }
}
```


Mengaktifkan dan mengonfigurasi integrasi

Setelah Anda mengaktifkan Security Hub, integrasi ini diaktifkan secara otomatis. AWS Config segera mulai mengirim temuan ke Security Hub.

Menghentikan publikasi temuan ke Security Hub

Untuk menghentikan pengiriman temuan ke Security Hub, Anda dapat menggunakan konsol Security Hub, Security Hub API, atau AWS CLI.

Lihat Menonaktifkan dan mengaktifkan aliran temuan dari integrasi (konsol) atau Menonaktifkan alur temuan dari integrasi (Security Hub API,) AWS CLI.

AWS Firewall Manager (Mengirim temuan)

Firewall Manager mengirimkan temuan ke Security Hub ketika kebijakan firewall aplikasi web (WAF) untuk sumber daya atau aturan daftar kontrol akses web (web ACL) tidak sesuai. Firewall Manager juga mengirimkan temuan ketika AWS Shield Advanced tidak melindungi sumber daya, atau ketika serangan diidentifikasi.

Setelah Anda mengaktifkan Security Hub, integrasi ini diaktifkan secara otomatis. Firewall Manager segera mulai mengirim temuan ke Security Hub.

Untuk mempelajari lebih lanjut tentang integrasi, lihat halaman Integrasi di konsol Security Hub.

Untuk mempelajari lebih lanjut tentang Firewall Manager, lihat Panduan AWS WAF Pengembang.

Amazon GuardDuty (Mengirim temuan)

GuardDuty mengirimkan semua temuan yang dihasilkannya ke Security Hub.

Temuan baru GuardDuty dikirim ke Security Hub dalam waktu lima menit. Pembaruan temuan dikirim berdasarkan pengaturan temuan yang diperbarui untuk Amazon EventBridge dalam GuardDuty pengaturan.

Saat Anda menghasilkan temuan GuardDuty sampel menggunakan halaman GuardDuty Pengaturan, Security Hub menerima temuan sampel dan menghilangkan awalan `[Sample]` dalam jenis temuan. Misalnya, tipe pencarian sampel GuardDuty `[SAMPLE] Recon:IAMUser/ResourcePermissions` ditampilkan seperti `Recon:IAMUser/ResourcePermissions` di Security Hub.

Setelah Anda mengaktifkan Security Hub, integrasi ini diaktifkan secara otomatis. GuardDuty segera mulai mengirim temuan ke Security Hub.

Untuk informasi selengkapnya tentang GuardDuty integrasi, lihat Integrasi dengan AWS Security Hub di Panduan GuardDuty Pengguna Amazon.

AWS Health (Mengirim temuan)

AWS Health memberikan visibilitas berkelanjutan ke kinerja sumber daya Anda dan ketersediaan AWS layanan dan akun Anda. Anda dapat menggunakan AWS Health peristiwa untuk mempelajari bagaimana perubahan layanan dan sumber daya dapat memengaruhi aplikasi yang berjalan AWS.

Integrasi dengan AWS Health tidak menggunakan`BatchImportFindings`. Sebagai gantinya, AWS Health gunakan pesan service-to-service acara untuk mengirim temuan ke Security Hub.

Untuk informasi selengkapnya tentang integrasi, lihat bagian berikut.

Cara AWS Health mengirim temuan ke Security Hub

Di 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 memfilter daftar temuan dan melihat detail untuk temuan. Lihat Mengelola dan meninjau detail dan riwayat penemuan. Anda juga dapat melacak status penyelidikan ke temuan. Lihat Mengambil tindakan atas temuan di AWS Security Hub.

Semua temuan di Security Hub menggunakan format JSON standar yang disebut. AWS Format Pencarian Keamanan (ASFF) ASFF mencakup rincian tentang sumber masalah, sumber daya yang terpengaruh, dan status temuan saat ini.

AWS Health adalah salah satu AWS layanan yang mengirimkan temuan ke Security Hub.

Jenis temuan yang AWS Health dikirim ke Security Hub

Setelah integrasi diaktifkan, AWS Health kirimkan semua temuan terkait keamanan yang dihasilkannya ke Security Hub. Temuan dikirim ke Security Hub menggunakan fileAWS Format Pencarian Keamanan (ASFF). Temuan terkait keamanan didefinisikan sebagai berikut:

- Temuan apa pun yang terkait dengan layanan AWS keamanan
- Temuan apa pun dengan kata-kata`security`,`abuse`, atau `certificate` di AWS Health TypeCode
- Temuan apa pun di mana AWS Health layanan tersebut berada `risk` atau `abuse`

Mengirim AWS Health temuan ke Security Hub

Ketika Anda memilih untuk menerima temuan dari AWS Health, Security Hub akan secara otomatis menetapkan izin yang diperlukan untuk menerima temuan dari. AWS Health Security Hub menggunakan izin service-to-service tingkat yang memberi Anda cara yang aman dan mudah untuk mengaktifkan integrasi ini dan mengimpor temuan dari AWS Health melalui Amazon EventBridge atas nama Anda. Memilih Terima Temuan memberikan izin Security Hub untuk mengkonsumsi temuan dari AWS Health.

Latensi untuk mengirim temuan

Saat AWS Health membuat temuan baru, biasanya dikirim ke Security Hub dalam waktu lima menit.

Mencoba kembali saat Security Hub tidak tersedia

AWS Health mengirimkan temuan ke Security Hub dengan upaya terbaik melalui EventBridge. Jika acara tidak berhasil dikirim ke Security Hub, EventBridge coba lagi mengirim acara selama 24 jam.

Memperbarui temuan yang ada di Security Hub

Setelah AWS Health mengirim temuan ke Security Hub, ia dapat mengirim pembaruan ke temuan yang sama untuk mencerminkan pengamatan tambahan dari aktivitas temuan ke Security Hub.

Daerah di mana temuan ada

Untuk acara global, AWS Health kirimkan temuan ke Security Hub di us-east-1 AWS (partisi), cn-northwest-1 (partisi China), dan -1 (partisi). gov-us-west GovCloud AWS Health mengirimkan peristiwa khusus Wilayah ke Security Hub di Wilayah atau Wilayah yang sama tempat kejadian terjadi.

Melihat AWS Health temuan di Security Hub

Untuk melihat AWS Health temuan Anda di Security Hub, pilih Temuan dari panel navigasi. Untuk memfilter temuan agar hanya menampilkan AWS Health temuan, pilih Kesehatan dari bidang Nama produk.

Menafsirkan AWS Health menemukan nama di Security Hub

AWS Health mengirimkan temuan ke Security Hub menggunakan fileAWS Format Pencarian Keamanan (ASFF). AWS Health temuan menggunakan pola peristiwa yang berbeda dibandingkan dengan format ASFF Security Hub. Tabel di bawah ini merinci semua bidang AWS Health temuan dengan rekan ASFF mereka saat muncul di Security Hub.

Jenis temuan Kesehatan	Tipe temuan ASFF	Nilai hardcode
akun	AwsAccountId	
detail.starttime	CreatedAt	

Jenis temuan Kesehatan	Tipe temuan ASFF	Nilai hardcode
Detail.eventDescription.LatestDescription	Deskripsi	
detail. eventTypeCode	GeneratorId	
detail.eventARN (termasuk akun) + hash dari detail.startTime	Id	
<region>“arn:aws:securityhub:: :product/aws/health”	ProductArn	
akun atau resourceID	Sumber Daya [i] .id	
	Sumber Daya [i] .Type	“Lainnya”
	SchemaVersion	“2018-10-08"
	Keparahan. Label	Lihat “Menafsirkan Label Keparahan” di bawah ini
“AWS Health -” detail. eventTypeCode	Judul	
-	Tipe	["Pemeriksaan Perangkat Lunak dan Konfigurasi"]
event.time	UpdatedAt	
URL acara di konsol Health	SourceUrl	

Menafsirkan label keparahan

Label keparahan dalam temuan ASFF ditentukan menggunakan logika berikut:

- Keparahan KRITIS jika:
  - `service`Bidang dalam AWS Health temuan memiliki nilai `Risk`

- `typeCode`Bidang dalam AWS Health temuan memiliki nilai `AWS_S3_OPEN_ACCESS_BUCKET_NOTIFICATION`
- `typeCode`Bidang dalam AWS Health temuan memiliki nilai `AWS_SHIELD_INTERNET_TRAFFIC_LIMITATIONS_PLACED_IN_RESPONSE_TO_DDOS_ATTACK`
- `typeCode`Bidang dalam AWS Health temuan memiliki nilai `AWS_SHIELD_IS_RESPONDING_TO_A_DDOS_ATTACK_AGAINST_YOUR_AWS_RESOURCES`

Tingkat keparahan TINGGI jika:

- `service`Bidang dalam AWS Health temuan memiliki nilai `Abuse`
- `typeCode`Bidang dalam AWS Health temuan berisi nilai `SECURITY_NOTIFICATION`
- `typeCode`Bidang dalam AWS Health temuan berisi nilai `ABUSE_DETECTION`

Tingkat keparahan MEDIUM jika:

- `service`Bidang dalam temuan ini adalah salah satu dari yang berikut:`ACM`,`ARTIFACT`,`AUDITMANAGER`,`BACKUP`,`CLOUDENDURE`,`CLOUDHSM`,`CLOUDTRAIL`,`CLOUDWATCH` `WAF`
- Bidang TypeCode dalam AWS Health temuan berisi nilai `CERTIFICATE`
- Bidang TypeCode dalam AWS Health temuan berisi nilai `END_OF_SUPPORT`

Temuan khas dari AWS Health

AWS Health mengirimkan temuan ke Security Hub menggunakan fileAWS Format Pencarian Keamanan (ASFF). Berikut ini adalah contoh temuan khas dari AWS Health.

> **Note**
>
> Jika deskripsi lebih dari 1024 karakter, itu akan dipotong menjadi 1024 karakter dan akan mengatakan (terpotong) di akhir.

```
{
            "SchemaVersion": "2018-10-08",
            "Id": "arn:aws:health:us-east-1:123456789012:event/SES/
AWS_SES_CMF_PENDING_TO_SUCCESS/
AWS_SES_CMF_PENDING_TO_SUCCESS_303388638044_33fe2115-8dad-40ce-
b533-78e29f49de96/101F7FBAEFC663977DA09CFF56A29236602834D2D361E6A8CA5140BFB3A69B30",
            "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/health",
```

```
            "GeneratorId": "AWS_SES_CMF_PENDING_TO_SUCCESS",
            "AwsAccountId": "123456789012",
            "Types": [
                "Software and Configuration Checks"
            ],
            "CreatedAt": "2022-01-07T16:34:04.000Z",
            "UpdatedAt": "2022-01-07T19:17:43.000Z",
            "Severity": {
                "Label": "MEDIUM",
                "Normalized": 40
            },
            "Title": "AWS Health - AWS_SES_CMF_PENDING_TO_SUCCESS",
            "Description": "Congratulations! Amazon SES has successfully detected the
 MX record required to use 4557227d-9257-4e49-8d5b-18a99ced4be9.cmf.pinpoint.sysmon-
iad.adzel.com as a custom MAIL FROM domain for verified identity cmf.pinpoint.sysmon-
iad.adzel.com in AWS Region US East (N. Virginia).\\n\\nYou can now use this MAIL
 FROM domain with cmf.pinpoint.sysmon-iad.adzel.com and any other verified identity
 that is configured to use it. For information about how to configure a verified
 identity to use a custom MAIL FROM domain, see http://docs.aws.amazon.com/ses/latest/
DeveloperGuide/mail-from-set.html .\\n\\nPlease note that this email only applies to
 AWS Region US East (N. Virginia).",
            "SourceUrl": "https://phd.aws.amazon.com/phd/home#/event-log?
eventID=arn:aws:health:us-east-1::event/SES/AWS_SES_CMF_PENDING_TO_SUCCESS/
AWS_SES_CMF_PENDING_TO_SUCCESS_303388638044_33fe2115-8dad-40ce-b533-78e29f49de96",
            "ProductFields": {
                "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/
aws/health/arn:aws:health:us-east-1::event/SES/AWS_SES_CMF_PENDING_TO_SUCCESS/
AWS_SES_CMF_PENDING_TO_SUCCESS_303388638044_33fe2115-8dad-40ce-b533-78e29f49de96",
                "aws/securityhub/ProductName": "Health",
                "aws/securityhub/CompanyName": "AWS"
            },
            "Resources": [
                {
                    "Type": "Other",
                    "Id": "4557227d-9257-4e49-8d5b-18a99ced4be9.cmf.pinpoint.sysmon-
iad.adzel.com"
                }
            ],
            "WorkflowState": "NEW",
            "Workflow": {
                "Status": "NEW"
            },
            "RecordState": "ACTIVE",
            "FindingProviderFields": {
```

```
                "Severity": {
                    "Label": "MEDIUM"
                },
                "Types": [
                    "Software and Configuration Checks"
                ]
            }
        }
    ]
}
```

Mengaktifkan dan mengonfigurasi integrasi

Setelah Anda mengaktifkan Security Hub, integrasi ini diaktifkan secara otomatis. AWS Health segera mulai mengirim temuan ke Security Hub.

Menghentikan publikasi temuan ke Security Hub

Untuk menghentikan pengiriman temuan ke Security Hub, Anda dapat menggunakan konsol Security Hub, Security Hub API, atau AWS CLI.

Lihat Menonaktifkan dan mengaktifkan aliran temuan dari integrasi (konsol) atau Menonaktifkan alur temuan dari integrasi (Security Hub API,) AWS CLI.

AWS Identity and Access Management Access Analyzer (Mengirim temuan)

Dengan IAM Access Analyzer, semua temuan dikirim ke Security Hub.

IAM Access Analyzer menggunakan penalaran berbasis logika untuk menganalisis kebijakan berbasis sumber daya yang diterapkan pada sumber daya yang didukung di akun Anda. IAM Access Analyzer menghasilkan temuan ketika mendeteksi pernyataan kebijakan yang memungkinkan prinsipal eksternal mengakses sumber daya di akun Anda.

Di IAM Access Analyzer, hanya akun administrator yang dapat melihat temuan untuk penganalisis yang berlaku untuk organisasi. Untuk penganalisis organisasi, bidang `AwsAccountId` ASFF mencerminkan ID akun administrator. Di bawah`ProductFields`, `ResourceOwnerAccount` bidang menunjukkan akun di mana temuan itu ditemukan. Jika Anda mengaktifkan penganalisis satu per satu untuk setiap akun, Security Hub menghasilkan beberapa temuan, satu yang mengidentifikasi ID akun administrator dan satu yang mengidentifikasi ID akun sumber daya.

Untuk informasi selengkapnya, lihat Integrasi dengan AWS Security Hub di Panduan Pengguna IAM.

Amazon Inspector (Mengirim temuan)

Amazon Inspector adalah layanan manajemen kerentanan yang terus memindai beban kerja Anda AWS untuk mencari kerentanan. Amazon Inspector secara otomatis menemukan dan memindai instans Amazon EC2 dan gambar kontainer yang berada di Amazon Elastic Container Registry. Pemindaian mencari kerentanan perangkat lunak dan eksposur jaringan yang tidak diinginkan.

Setelah Anda mengaktifkan Security Hub, integrasi ini diaktifkan secara otomatis. Amazon Inspector segera mulai mengirim semua temuan yang dihasilkannya ke Security Hub.

Untuk informasi selengkapnya tentang integrasi, lihat Integrasi dengan AWS Security Hub di Panduan Pengguna Amazon Inspector.

Security Hub juga dapat menerima temuan dari Amazon Inspector Classic. Amazon Inspector Classic mengirimkan temuan ke Security Hub yang dihasilkan melalui proses penilaian untuk semua paket aturan yang didukung.

Untuk informasi selengkapnya tentang integrasi, lihat Integrasi dengan AWS Security Hub di Panduan Pengguna Amazon Inspector Classic.

Temuan untuk Amazon Inspector dan Amazon Inspector Classic menggunakan produk yang sama ARN. Temuan Amazon Inspector memiliki entri berikut di: `ProductFields`

```
"aws/inspector/ProductVersion": "2",
```

AWS IoT Device Defender (Mengirim temuan)

AWS IoT Device Defender adalah layanan keamanan yang mengaudit konfigurasi perangkat IoT Anda, memantau perangkat yang terhubung untuk mendeteksi perilaku abnormal, dan membantu mengurangi risiko keamanan.

Setelah mengaktifkan keduanya AWS IoT Device Defender dan Security Hub, kunjungi halaman Integrasi konsol Security Hub, dan pilih Terima temuan untuk Audit, Deteksi, atau keduanya. AWS IoT Device Defender Audit dan Deteksi mulai mengirimkan semua temuan ke Security Hub.

AWS IoT Device Defender Audit mengirimkan ringkasan cek ke Security Hub, yang berisi informasi umum untuk jenis pemeriksaan audit tertentu dan tugas audit. AWS IoT Device Defender Deteksi mengirimkan temuan pelanggaran untuk pembelajaran mesin (ML), statistik, dan perilaku statis ke Security Hub. Audit juga mengirimkan pembaruan pencarian ke Security Hub.

Untuk informasi selengkapnya tentang integrasi ini, lihat Integrasi dengan AWS Security Hub di Panduan AWS IoT Pengembang.

Amazon Macie (Mengirim temuan)

Temuan dari Macie dapat menunjukkan bahwa ada potensi pelanggaran kebijakan atau bahwa data sensitif, seperti informasi identitas pribadi (PII), hadir dalam data yang disimpan organisasi Anda di Amazon S3.

Setelah Anda mengaktifkan Security Hub, Macie secara otomatis mulai mengirim temuan kebijakan ke Security Hub. Anda dapat mengonfigurasi integrasi untuk juga mengirim temuan data sensitif ke Security Hub.

Di Security Hub, jenis temuan untuk kebijakan atau temuan data sensitif diubah menjadi nilai yang kompatibel dengan ASFF. Misalnya, jenis `Policy:IAMUser/S3BucketPublic` temuan di Macie ditampilkan seperti `Effects/Data Exposure/Policy:IAMUser-S3BucketPublic` di Security Hub.

Macie juga mengirimkan temuan sampel yang dihasilkan ke Security Hub. Untuk temuan sampel, nama sumber daya yang terpengaruh adalah `macie-sample-finding-bucket` dan nilai untuk `Sample` bidang tersebut adalah`true`.

Untuk informasi selengkapnya, lihat Integrasi Amazon Macie dengan AWS Security Hub di Panduan Pengguna Amazon Macie.

AWS Systems Manager Patch Manager (Mengirim temuan)

AWS Systems Manager Patch Manager mengirimkan temuan ke Security Hub ketika instance dalam armada pelanggan tidak sesuai dengan standar kepatuhan patch mereka.

Patch Manager mengotomatiskan proses menambal instance terkelola dengan jenis pembaruan terkait keamanan dan jenis pembaruan lainnya.

Setelah Anda mengaktifkan Security Hub, integrasi ini diaktifkan secara otomatis. Systems Manager Patch Manager segera mulai mengirim temuan ke Security Hub.

Untuk informasi selengkapnya tentang menggunakan Patch Manager, lihat AWS Systems Manager Patch Manager di Panduan AWS Systems Manager Pengguna.

AWS layanan yang menerima temuan dari Security Hub

AWS Layanan berikut terintegrasi dengan Security Hub dan menerima temuan dari Security Hub. Jika dicatat, layanan terintegrasi juga dapat memperbarui temuan. Dalam hal ini, menemukan pembaruan yang Anda buat dalam layanan terintegrasi juga akan tercermin dalam Security Hub.

AWS Audit Manager (Menerima temuan)

AWS Audit Manager menerima temuan dari Security Hub. Temuan ini membantu pengguna Audit Manager untuk mempersiapkan audit.

Untuk mempelajari Audit Manager selengkapnya, lihat Panduan Pengguna AWS Audit Manager. AWS Pemeriksaan Security Hub yang didukung dengan AWS Audit Manager mencantumkan kontrol tempat Security Hub mengirimkan temuannya ke Audit Manager.

AWS Chatbot (Menerima temuan)

AWS Chatbot adalah agen interaktif yang membantu Anda memantau dan berinteraksi dengan AWS sumber daya Anda di saluran Slack dan ruang obrolan Amazon Chime.

AWS Chatbot menerima temuan dari Security Hub.

Untuk mempelajari lebih lanjut tentang AWS Chatbot integrasi dengan Security Hub, lihat ikhtisar integrasi Security Hub di Panduan AWS Chatbot Administrator.

Detektif Amazon (Menerima temuan)

Detective secara otomatis mengumpulkan data log dari AWS sumber daya Anda dan menggunakan pembelajaran mesin, analisis statistik, dan teori grafik untuk membantu Anda memvisualisasikan dan melakukan penyelidikan keamanan yang lebih cepat dan lebih efisien.

Integrasi Security Hub dengan Detective memungkinkan Anda untuk beralih dari temuan GuardDuty Amazon di Security Hub ke Detective. Anda kemudian dapat menggunakan alat Detektif dan visualisasi untuk menyelidikinya. Integrasi tidak memerlukan konfigurasi tambahan di Security Hub atau Detective.

Untuk temuan yang diterima dari yang lain Layanan AWS, panel rincian temuan di konsol Security Hub mencakup sub-bagian Investigasi di Detektif. Subbagian itu berisi tautan ke Detektif di mana Anda dapat menyelidiki lebih lanjut masalah keamanan yang ditandai oleh temuan tersebut. Anda

juga dapat membuat grafik perilaku di Detective berdasarkan temuan Security Hub untuk melakukan penyelidikan yang lebih efektif. Untuk informasi selengkapnya, lihat temuan AWS keamanan di Panduan Administrasi Detektif Amazon.

Jika agregasi lintas wilayah diaktifkan, maka ketika Anda berputar dari Wilayah agregasi, Detektif terbuka di Wilayah tempat temuan itu berasal.

Jika tautan tidak berfungsi, maka untuk saran pemecahan masalah, lihat Memecahkan masalah pivot.

Danau Keamanan Amazon (Menerima temuan)

Security Lake adalah layanan danau data keamanan yang dikelola sepenuhnya. Anda dapat menggunakan Security Lake untuk secara otomatis memusatkan data keamanan dari sumber cloud, lokal, dan kustom ke dalam data lake yang disimpan di akun Anda. Pelanggan dapat menggunakan data dari Security Lake untuk kasus penggunaan investigasi dan analitik.

Untuk mengaktifkan integrasi ini, Anda harus mengaktifkan kedua layanan dan menambahkan Security Hub sebagai sumber di konsol Security Lake, Security Lake API, atau AWS CLI. Setelah Anda menyelesaikan langkah-langkah ini, Security Hub mulai mengirim semua temuan ke Security Lake.

Security Lake secara otomatis menormalkan temuan Security Hub dan mengubahnya menjadi skema open-source standar yang disebut Open Cybersecurity Schema Framework (OCSF). Di Security Lake, Anda dapat menambahkan satu atau lebih pelanggan untuk mengkonsumsi temuan Security Hub.

Untuk informasi selengkapnya tentang integrasi ini, termasuk petunjuk tentang menambahkan Security Hub sebagai sumber dan membuat pelanggan, lihat Integrasi dengan AWS Security Hub di Panduan Pengguna Amazon Security Lake.

AWS Systems Manager Explorer dan OpsCenter (Menerima dan memperbarui temuan)

AWS Systems Manager Jelajahi dan OpsCenter terima temuan dari Security Hub, dan perbarui temuan tersebut di Security Hub.

Explorer memberi Anda dasbor yang dapat disesuaikan, memberikan wawasan dan analisis utama tentang kesehatan operasional dan kinerja lingkungan Anda. AWS

OpsCenter memberi Anda lokasi pusat untuk melihat, menyelidiki, dan menyelesaikan item pekerjaan operasional.

Untuk informasi selengkapnya tentang Explorer dan OpsCenter, lihat Manajemen operasi di Panduan AWS Systems Manager Pengguna.

AWS Trusted Advisor (Menerima temuan)

Trusted Advisor mengacu pada praktik terbaik yang dipelajari dari melayani ratusan ribu AWS pelanggan. Trusted Advisor memeriksa AWS lingkungan Anda, dan kemudian membuat rekomendasi ketika ada peluang untuk menghemat uang, meningkatkan ketersediaan dan kinerja sistem, atau membantu menutup kesenjangan keamanan.

Saat Anda mengaktifkan keduanya Trusted Advisor dan Security Hub, integrasi diperbarui secara otomatis.

Security Hub mengirimkan hasil pemeriksaan Praktik Terbaik Keamanan AWS Dasar ke Trusted Advisor.

Untuk informasi selengkapnya tentang integrasi Security Hub Trusted Advisor, lihat Melihat kontrol AWS Security Hub AWS Trusted Advisor di Panduan Pengguna AWS Support.

Integrasi produk mitra pihak ketiga yang tersedia

AWS Security Hub terintegrasi dengan beberapa produk mitra pihak ketiga. Integrasi dapat melakukan satu atau lebih tindakan berikut:

- Kirim temuan yang dihasilkannya ke Security Hub.
- Menerima temuan dari Security Hub.
- Perbarui temuan di Security Hub.

Semua integrasi yang mengirimkan temuan ke Security Hub memiliki Nama Sumber Daya Amazon (ARN).

> **Note**
>
> Beberapa integrasi hanya tersedia di pilih Wilayah AWS.
> Halaman Integrasi konsol Security Hub mencantumkan semua integrasi yang didukung untuk Wilayah saat ini.

Untuk informasi selengkapnya, lihat Integrasi yang didukung di China (Beijing) dan China (Ningxia) dan Integrasi yang didukung di AWS GovCloud (AS-Timur) dan AWS GovCloud (AS-Barat).

Jika Anda memiliki solusi keamanan dan tertarik untuk menjadi mitra Security Hub, email <securityhub-partners@amazon.com>. Untuk informasi selengkapnya, lihat Panduan Integrasi Mitra AWS Security Hub.

Ikhtisar integrasi pihak ketiga dengan Security Hub

Berikut ikhtisar integrasi pihak ketiga yang mengirimkan temuan ke Security Hub atau menerima temuan dari Security Hub.

Integrasi	Arahan	ARN (jika ada)
3CORESec – 3CORESec NTA	Mengirim temuan	`arn:aws:securityhub: <REGION>::product/3coresec/3coresec`
Alert Logic – SIEMless Threat Management	Mengirim temuan	`arn:aws:securityhub: <REGION>:733251395267:product/alertlogic/althreatmanagement`
Aqua Security – Aqua Cloud Native Security Platform	Mengirim temuan	`arn:aws:securityhub: <REGION>::product/aquasecurity/aquasecurity`
Aqua Security – Kube-bench	Mengirim temuan	`arn:aws:securityhub: <REGION>::product/aqua-security/kube-bench`
Armor – Armor Anywhere	Mengirim temuan	`arn:aws:securityhub: <REGION>:67970361`

Integrasi	Arahan	ARN (jika ada)
		5338:product/armor defense/armoranywh ere
AttackIQ – AttackIQ	Mengirim temuan	arn:aws:securityhu b: *<REGION>*::product /attackiq/attackiq- platform
Barracuda Networks – Cloud Security Guardian	Mengirim temuan	arn:aws:securityhu b: *<REGION>*:15178405 5945:product/barra cuda/cloudsecurity guardian
BigID – BigID Enterprise	Mengirim temuan	arn:aws:securityhu b: *<REGION>*::product /bigid/bigid-enter prise
Blue Hexagon – Blue Hexagon forAWS	Mengirim temuan	arn:aws:securityhu b: *<REGION>*::product /blue-hexagon/blue- hexagon-for-aws
Capitis Solutions – C2VS	Mengirim temuan	arn:aws:securityhu b: *<REGION>*::product/ capitis/c2vs
Check Point – CloudGuard IaaS	Mengirim temuan	arn:aws:securityhu b: *<REGION>*:75824556 3457:product/check point/cloudguard-i aas

Integrasi	Arahan	ARN (jika ada)
Check Point – CloudGuard Posture Management	Mengirim temuan	`arn:aws:securityhub: <REGION>:634729597623:product/checkpoint/dome9-arc`
Claroty – xDome	Mengirim temuan	`arn:aws:securityhub: <REGION>::product/claroty/xdome`
Cloud Storage Security—Antivirus for Amazon S3	Mengirim temuan	`arn:aws:securityhub: <REGION>::product/cloud-storage-security/antivirus-for-amazon-s3`
Contrast Security	Mengirim temuan	`arn:aws:securityhub: <REGION>::product/contrast-security/security-assess`
CrowdStrike – CrowdStrike Falcon	Mengirim temuan	`arn:aws:securityhub: <REGION>:517716713836:product/crowdstrike/crowdstrike-falcon`
CyberArk – Privileged Threat Analytics	Mengirim temuan	`arn:aws:securityhub: <REGION>:749430749651:product/cyberark/cyberark-pta`
Data Theorem – Data Theorem	Mengirim temuan	`arn:aws:securityhub: <REGION>::product/data-theorem/api-cloud-web-secure`

Integrasi	Arahan	ARN (jika ada)
Drata	Mengirim temuan	`arn:aws:securityhub: <REGION>::product/drata/drata-integration`
Forcepoint – Forcepoint CASB	Mengirim temuan	`arn:aws:securityhub: <REGION>:365761988620:product/forcepoint/forcepoint-casb`
Forcepoint – Forcepoint Cloud Security Gateway	Mengirim temuan	`arn:aws:securityhub: <REGION>::product/forcepoint/forcepoint-cloud-security-gateway`
Forcepoint – Forcepoint DLP	Mengirim temuan	`arn:aws:securityhub: <REGION>:365761988620:product/forcepoint/forcepoint-dlp`
Forcepoint – Forcepoint NGFW	Mengirim temuan	`arn:aws:securityhub: <REGION>:365761988620:product/forcepoint/forcepoint-ngfw`
Fugue – Fugue	Mengirim temuan	`arn:aws:securityhub: <REGION>::product/fugue/fugue`

Integrasi	Arahan	ARN (jika ada)
Guardicore – Centra 4.0	Mengirim temuan	`arn:aws:securityhub: <REGION>::product/guardicore/guardicore`
HackerOne – Vulnerability Intelligence	Mengirim temuan	`arn:aws:securityhub: <REGION>::product/hackerone/vulnerability-intelligence`
JFrog – Xray	Mengirim temuan	`arn:aws:securityhub: <REGION>::product/jfrog/jfrog-xray`
Juniper Networks – vSRX Next Generation Firewall	Mengirim temuan	`arn:aws:securityhub: <REGION>::product/juniper-networks/vsrx-next-generation-firewall`
k9 Security – Access Analyzer	Mengirim temuan	`arn:aws:securityhub: <REGION>::product/k9-security/access-analyzer`
Lacework – Lacework	Mengirim temuan	`arn:aws:securityhub: <REGION>::product/lacework/lacework`
McAfee – MVISION Cloud Native Application Protection Platform (CNAPP)	Mengirim temuan	`arn:aws:securityhub: <REGION>::product/mcafee-skyhigh/mcafee-mvision-cloud-aws`

Integrasi	Arahan	ARN (jika ada)
NETSCOUT – NETSCOUT Cyber Investigator	Mengirim temuan	`arn:aws:securityhub:us-east-1::product/netscout/netscout-cyber-investigator`
Palo Alto Networks – Prisma Cloud Compute	Mengirim temuan	`arn:aws:securityhub: <REGION>:496947949261:product/twistlock/twistlock-enterprise`
Palo Alto Networks – Prisma Cloud Enterprise	Mengirim temuan	`arn:aws:securityhub: <REGION>:188619942792:product/paloaltonetworks/redlock`
Plerion – Cloud Security Platform	Mengirim temuan	`arn:aws:securityhub: <REGION>::product/plerion/cloud-security-platform`
Prowler – Prowler	Mengirim temuan	`arn:aws:securityhub: <REGION>::product/prowler/prowler`
Qualys – Vulnerability Management	Mengirim temuan	`arn:aws:securityhub: <REGION>:805950163170:product/qualys/qualys-vm`
Rapid7 – InsightVM	Mengirim temuan	`arn:aws:securityhub: <REGION>:336818582268:product/rapid7/insightvm`

Integrasi	Arahan	ARN (jika ada)
SecureCloudDB – SecureCloudDB	Mengirim temuan	`arn:aws:securityhub: <REGION>::product/securecloudb/securecloudb`
SentinelOne – SentinelOne	Mengirim temuan	`arn:aws:securityhub: <REGION>::product/sentinelone/endpoint-protection`
Snyk	Mengirim temuan	`arn:aws:securityhub: <region>::product/snyk/snyk`
Sonrai Security – Sonrai Dig	Mengirim temuan	`arn:aws:securityhub: <REGION>::product/sonrai-security/sonrai-dig`
Sophos – Server Protection	Mengirim temuan	`arn:aws:securityhub: <REGION>:062897671886:product/sophos/sophos-server-protection`
StackRox – StackRox Kubernetes Security	Mengirim temuan	`arn:aws:securityhub: <REGION>::product/stackrox/kubernetes-security`
Sumo Logic – Machine Data Analytics	Mengirim temuan	`arn:aws:securityhub: <REGION>:956882708938:product/sumologicinc/sumologic-mda`

Integrasi	Arahan	ARN (jika ada)
Symantec – Cloud Workload Protection	Mengirim temuan	`arn:aws:securityhub: <REGION>:754237914691:product/symantec-corp/symantec-cwp`
Tenable – Tenable.io	Mengirim temuan	`arn:aws:securityhub: <REGION>:422820575223:product/tenable/tenable-io`
Trend Micro – Cloud One	Mengirim temuan	`arn:aws:securityhub: <REGION>::product/trend-micro/cloud-one`
Vectra – Cognito Detect	Mengirim temuan	`arn:aws:securityhub: <REGION>:978576646331:product/vectra-ai/cognito-detect`
Wiz	Mengirim temuan	`arn:aws:securityhub: <REGION>::product/wiz-security/wiz-security`
Atlassian - Jira Service Management	Menerima dan memperbarui temuan	Tidak berlaku
Atlassian - Jira Service Management Cloud	Menerima dan memperbarui temuan	Tidak berlaku
Atlassian – Opsgenie	Menerima temuan	Tidak berlaku
Fortinet – FortiCNP	Menerima temuan	Tidak berlaku
IBM – QRadar	Menerima temuan	Tidak berlaku

Integrasi	Arahan	ARN (jika ada)
Logz.io Cloud SIEM	Menerima temuan	Tidak berlaku
MetricStream	Menerima temuan	Tidak berlaku
MicroFocus – MicroFocus Arcsight	Menerima temuan	Tidak berlaku
New Relic Vulnerability Management	Menerima temuan	Tidak berlaku
PagerDuty – PagerDuty	Menerima temuan	Tidak berlaku
Palo Alto Networks – Cortex XSOAR	Menerima temuan	Tidak berlaku
Palo Alto Networks – VM-Series	Menerima temuan	Tidak berlaku
Rackspace Technology – Cloud Native Security	Menerima temuan	Tidak berlaku
Rapid7 – InsightConnect	Menerima temuan	Tidak berlaku
RSA – RSA Archer	Menerima temuan	Tidak berlaku
ServiceNow – ITSM	Menerima dan memperbarui temuan	Tidak berlaku
Slack – Slack	Menerima temuan	Tidak berlaku
Splunk – Splunk Enterprise	Menerima temuan	Tidak berlaku
Splunk – Splunk Phantom	Menerima temuan	Tidak berlaku
ThreatModeler	Menerima temuan	Tidak berlaku
Trellix – Trellix Helix	Menerima temuan	Tidak berlaku

Integrasi	Arahan	ARN (jika ada)
Caveonix – Caveonix Cloud	Mengirim dan menerima temuan	`arn:aws:securityhub: <REGION>::product/caveonix/caveonix-cloud`
Cloud Custodian – Cloud Custodian	Mengirim dan menerima temuan	`arn:aws:securityhub: <REGION>::product/cloud-custodian/cloud-custodian`
DisruptOps, Inc. – DisruptOPS	Mengirim dan menerima temuan	`arn:aws:securityhub: <REGION>::product/disruptops-inc/disruptops`
Kion	Mengirim dan menerima temuan	`arn:aws:securityhub: <REGION>::product/cloudtamerio/cloudtamerio`
Turbot – Turbot	Mengirim dan menerima temuan	`arn:aws:securityhub: <REGION>:453761072151:product/turbot/turbot`

Integrasi pihak ketiga yang mengirimkan temuan ke Security Hub

Integrasi produk mitra pihak ketiga berikut mengirimkan temuan ke Security Hub. Security Hub mengubah temuan menjadi AWS Security Finding Format.

3CORESec – 3CORESec NTA

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>::product/3coresec/3coresec`

3CORESecmenyediakan layanan deteksi terkelola untuk lokal dan AWS sistem. Integrasi mereka dengan Security Hub memungkinkan visibilitas ke dalam ancaman seperti malware, eskalasi hak istimewa, pergerakan lateral, dan segmentasi jaringan yang tidak tepat.

Tautan produk

Dokumentasi mitra

Alert Logic – SIEMless Threat Management

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>:733251395267:product/alertlogic/althreatmanagement`

Dapatkan tingkat cakupan yang tepat: kerentanan dan visibilitas aset, deteksi ancaman dan manajemen insiden AWS WAF, dan opsi analis SOC yang ditetapkan.

Tautan produk

Dokumentasi mitra

Aqua Security – Aqua Cloud Native Security Platform

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>::product/aquasecurity/aquasecurity`

Aqua Cloud Native Security Platform (CSP)menyediakan keamanan siklus hidup penuh untuk aplikasi berbasis container dan tanpa server, dari pipeline CI/CD hingga lingkungan produksi runtime.

Tautan produk

Dokumentasi mitra

Aqua Security – Kube-bench

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>::product/aqua-security/kube-bench`

Kube-benchadalah alat open-source yang menjalankan Center for Internet Security (CIS) Kubernetes Benchmark terhadap lingkungan Anda.

Tautan produk

Dokumentasi mitra

Armor – Armor Anywhere

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>:679703615338:product/armordefense/armoranywhere`

Armor Anywherememberikan keamanan dan kepatuhan terkelola untuk AWS.

Tautan produk

Dokumentasi mitra

AttackIQ – AttackIQ

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>::product/attackiq/attackiq-platform`

AttackIQ Platformmengemulasi perilaku permusuhan nyata yang selaras dengan MITRE ATT&CK Framework untuk membantu memvalidasi dan meningkatkan postur keamanan Anda secara keseluruhan.

Tautan produk

Dokumentasi mitra

Barracuda Networks – Cloud Security Guardian

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>:151784055945:product/barracuda/cloudsecurityguardian`

Barracuda Cloud Security Sentrymembantu organisasi tetap aman saat membangun aplikasi di, dan memindahkan beban kerja ke, cloud publik.

AWS Tautan Marketplace

Tautan produk

BigID – BigID Enterprise

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>::product/bigid/bigid-enterprise`

BigID Enterprise Privacy Management PlatformIni membantu perusahaan mengelola dan melindungi data sensitif (PII) di semua sistem mereka.

Tautan produk

Dokumentasi mitra

Blue Hexagon— Blue Hexagon untuk AWS

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>::product/blue-hexagon/blue-hexagon-for-aws`

Blue Hexagonadalah platform deteksi ancaman waktu nyata. Ini menggunakan prinsip pembelajaran mendalam untuk mendeteksi ancaman yang diketahui dan tidak diketahui, termasuk malware dan anomali jaringan.

AWS Tautan Marketplace

Dokumentasi mitra

Capitis Solutions – C2VS

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>::product/capitis/c2vs`

C2VSadalah solusi kepatuhan yang dapat disesuaikan yang dirancang untuk secara otomatis mengidentifikasi kesalahan konfigurasi spesifik aplikasi Anda dan akar penyebabnya.

Tautan produk

Dokumentasi mitra

Check Point – CloudGuard IaaS

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>:758245563457:product/checkpoint/cloudguard-iaas`

Check Point CloudGuarddengan mudah memperluas keamanan pencegahan ancaman yang komprehensif untuk AWS sekaligus melindungi aset di cloud.

Tautan produk

Dokumentasi mitra

Check Point – CloudGuard Posture Management

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>:634729597623:product/checkpoint/dome9-arc`

Platform SaaS yang memberikan keamanan jaringan cloud yang dapat diverifikasi, perlindungan IAM tingkat lanjut, dan kepatuhan dan tata kelola yang komprehensif.

Tautan produk

Dokumentasi mitra

Claroty – xDome

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>::product/claroty/xdome`

Claroty xDomemembantu organisasi mengamankan sistem siber-fisik mereka di seluruh Extended Internet of Things (XioT) dalam lingkungan industri (OT), perawatan kesehatan (IoMT), dan perusahaan (IoT).

Tautan produk

Dokumentasi mitra

Cloud Storage Security— Antivirus for Amazon S3

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>::product/cloud-storage-security/antivirus-for-amazon-s3`

Cloud Storage Securitymenyediakan pemindaian anti-malware dan antivirus asli cloud untuk objek Amazon S3.

Antivirus for Amazon S3 menawarkan pemindaian objek dan file waktu nyata dan terjadwal di Amazon S3 untuk malware dan ancaman. Ini memberikan visibilitas dan remediasi untuk masalah dan file yang terinfeksi.

Tautan produk

Dokumentasi mitra

Contrast Security – Contrast Assess

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>::product/contrast-security/security-assess`

Contrast Security Contrast Assessadalah alat IAST yang menawarkan deteksi kerentanan waktu nyata di aplikasi web, API, dan layanan mikro. Contrast Assessterintegrasi dengan Security Hub untuk membantu memberikan visibilitas dan respons terpusat untuk semua beban kerja Anda.

Tautan produk

Dokumentasi mitra

CrowdStrike – CrowdStrike Falcon

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>:517716713836:product/crowdstrike/crowdstrike-falcon`

Sensor CrowdStrike Falcon tunggal yang ringan menyatukan antivirus generasi berikutnya, deteksi dan respons titik akhir, dan perburuan terkelola 24/7 melalui cloud.

Tautan produk

Dokumentasi mitra

CyberArk – Privileged Threat Analytics

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>:749430749651:product/cyberark/cyberark-pta`

Privileged Threat Analyticsmengumpulkan, mendeteksi, memperingatkan, dan menanggapi aktivitas berisiko tinggi dan perilaku akun istimewa untuk menahan serangan yang sedang berlangsung.

Tautan produk

Dokumentasi mitra

Data Theorem – Data Theorem

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>::product/data-theorem/api-cloud-web-secure`

Data Theoremterus memindai aplikasi web, API, dan sumber daya cloud untuk mencari kelemahan keamanan dan celah privasi data untuk mencegah pelanggaran AppSec data.

Tautan produk

Dokumentasi mitra

Drata

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>::product/drata/drata-integration`

Drataadalah platform otomatisasi kepatuhan yang membantu Anda mencapai dan mempertahankan kepatuhan dengan berbagai kerangka kerja, seperti SOC2, ISO, dan GDPR. Integrasi antara Drata dan Security Hub membantu Anda memusatkan temuan keamanan di satu lokasi.

AWS Tautan Marketplace

Dokumentasi mitra

Forcepoint – Forcepoint CASB

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>:365761988620:product/forcepoint/forcepoint-casb`

Forcepoint CASBmemungkinkan Anda menemukan penggunaan aplikasi cloud, menganalisis risiko, dan menegakkan kontrol yang sesuai untuk SaaS dan aplikasi khusus.

Tautan produk

Dokumentasi mitra

Forcepoint – Forcepoint Cloud Security Gateway

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>::product/forcepoint/forcepoint-cloud-security-gateway`

Forcepoint Cloud Security Gatewayadalah layanan keamanan cloud konvergen yang menyediakan visibilitas, kontrol, dan perlindungan ancaman bagi pengguna dan data, di mana pun mereka berada.

Tautan produk

Dokumentasi mitra

Forcepoint – Forcepoint DLP

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>:365761988620:product/forcepoint/forcepoint-dlp`

Forcepoint DLPmengatasi risiko yang berpusat pada manusia dengan visibilitas dan kontrol di mana pun orang-orang Anda bekerja dan di mana pun data Anda berada.

Tautan produk

Dokumentasi mitra

Forcepoint – Forcepoint NGFW

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>:365761988620:product/forcepoint/forcepoint-ngfw`

Forcepoint NGFWmemungkinkan Anda menghubungkan AWS lingkungan Anda ke jaringan perusahaan Anda dengan skalabilitas, perlindungan, dan wawasan yang diperlukan untuk mengelola jaringan Anda dan menanggapi ancaman.

Tautan produk

Dokumentasi mitra

Fugue – Fugue

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>::product/fugue/fugue`

Fugueadalah platform cloud-native tanpa agen dan dapat diskalakan yang mengotomatiskan validasi berkelanjutan infrastructure-as-code dan lingkungan runtime cloud menggunakan kebijakan yang sama.

Tautan produk

Dokumentasi mitra

Guardicore – Centra 4.0

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>::product/guardicore/guardicore`

Guardicore Centramenyediakan visualisasi aliran, segmentasi mikro, dan deteksi pelanggaran untuk beban kerja di pusat data dan cloud modern.

Tautan produk

Dokumentasi mitra

HackerOne – Vulnerability Intelligence

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>::product/hackerone/vulnerability-intelligence`

HackerOnePlatform ini bermitra dengan komunitas peretas global untuk mengungkap masalah keamanan yang paling relevan. Vulnerability Intelligencememungkinkan organisasi Anda melampaui pemindaian otomatis. Ini berbagi kerentanan yang telah divalidasi oleh peretas HackerOne etis dan memberikan langkah-langkah untuk mereproduksi.

AWS tautan pasar

Dokumentasi mitra

JFrog – Xray

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>::product/jfrog/jfrog-xray`

JFrog Xrayadalah alat Analisis Komposisi Perangkat Lunak keamanan aplikasi universal (SCA) yang terus memindai binari untuk kepatuhan lisensi dan kerentanan keamanan sehingga Anda dapat menjalankan rantai pasokan perangkat lunak yang aman.

AWS Tautan Marketplace

Dokumentasi mitra

Juniper Networks – vSRX Next Generation Firewall

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>::product/juniper-networks/vsrx-next-generation-firewall`

Juniper Networks'VsRx Virtual Next Generation Firewall menghadirkan firewall virtual berbasis cloud lengkap dengan keamanan canggih, SD-WAN yang aman, jaringan yang kuat, dan otomatisasi bawaan.

AWS Tautan Marketplace

Dokumentasi mitra

Tautan produk

k9 Security – Access Analyzer

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>::product/k9-security/access-analyzer`

k9 Securitymemberi tahu Anda ketika perubahan akses penting terjadi di AWS Identity and Access Management akun Anda. Dengank9 Security, Anda dapat memahami akses yang dimiliki pengguna dan peran IAM ke kritis Layanan AWS dan data Anda.

k9 Securitydibangun untuk pengiriman berkelanjutan, memungkinkan Anda untuk mengoperasionalkan IAM dengan audit akses yang dapat ditindaklanjuti dan otomatisasi kebijakan sederhana untuk dan Terraform. AWS CDK

Tautan produk

Dokumentasi mitra

Lacework – Lacework

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>::product/lacework/lacework`

Laceworkadalah platform keamanan berbasis data untuk cloud. Platform Keamanan Cloud Lacework mengotomatiskan keamanan cloud dalam skala besar sehingga Anda dapat berinovasi dengan kecepatan dan keamanan.

Tautan produk

Dokumentasi mitra

McAfee – MVISION Cloud Native Application Protection Platform (CNAPP)

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>::product/mcafee-skyhigh/mcafee-mvision-cloud-aws`

McAfee MVISION Cloud Native Application Protection Platform (CNAPP)menawarkan Cloud Security Posture Management (CSPM) dan Cloud Workload Protection Platform (CWPP) untuk lingkungan Anda. AWS

Tautan produk

Dokumentasi mitra

NETSCOUT – NETSCOUT Cyber Investigator

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>::product/netscout/netscout-cyber-investigator`

NETSCOUT Cyber Investigatoradalah ancaman jaringan di seluruh perusahaan, investigasi risiko, dan platform analisis forensik yang membantu mengurangi dampak ancaman dunia maya pada bisnis.

Tautan produk

Dokumentasi mitra

Palo Alto Networks – Prisma Cloud Compute

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>:496947949261:product/twistlock/twistlock-enterprise`

Prisma Cloud Computeadalah platform keamanan siber asli cloud yang melindungi VM, wadah, dan platform tanpa server.

Tautan produk

Dokumentasi mitra

Palo Alto Networks – Prisma Cloud Enterprise

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>:188619942792:product/paloaltonetworks/redlock`

Melindungi AWS penyebaran Anda dengan analitik keamanan cloud, deteksi ancaman tingkat lanjut, dan pemantauan kepatuhan.

Tautan produk

Dokumentasi mitra

Plerion – Cloud Security Platform

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>::product/plerion/cloud-security-platform`

Plerionadalah Platform Keamanan Cloud dengan pendekatan unik yang dipimpin oleh ancaman dan berbasis risiko yang menawarkan tindakan pencegahan, detektif, dan korektif di seluruh beban kerja Anda. Integrasi antara Plerion dan Security Hub memungkinkan pelanggan untuk memusatkan dan bertindak atas temuan keamanan mereka di satu tempat.

AWS Tautan Marketplace

Dokumentasi mitra

Prowler – Prowler

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>::product/prowler/prowler`

Prowleradalah alat keamanan open source untuk melakukan AWS pemeriksaan terkait praktik terbaik keamanan, pengerasan, dan pemantauan berkelanjutan.

Tautan produk

Dokumentasi mitra

Qualys – Vulnerability Management

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>:805950163170:product/qualys/qualys-vm`

Qualys Vulnerability Management (VM)terus memindai dan mengidentifikasi kerentanan, melindungi aset Anda.

Tautan produk

Dokumentasi mitra

Rapid7 – InsightVM

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>:336818582268:product/rapid7/insightvm`

Rapid7 InsightVM menyediakan manajemen kerentanan untuk lingkungan modern, memungkinkan Anda menemukan, memprioritaskan, dan memulihkan kerentanan secara efisien.

Tautan produk

Dokumentasi mitra

SecureCloudDB – SecureCloudDB

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>::product/securecloudddb/securecloudddb`

SecureCloudDBadalah alat keamanan database asli cloud yang menyediakan visibilitas komprehensif postur dan aktivitas keamanan internal dan eksternal. Ini menandai pelanggaran keamanan dan memberikan remediasi pada kerentanan database yang dapat dieksploitasi.

Tautan produk

Dokumentasi mitra

SentinelOne – SentinelOne

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>::product/sentinelone/endpoint-protection`

SentinelOneadalah platform deteksi dan respons tambahan (XDR) otonom yang mencakup pencegahan, deteksi, respons, dan perburuan bertenaga AI di seluruh titik akhir, wadah, beban kerja cloud, dan perangkat IoT.

AWS Tautan Marketplace

Tautan produk

Snyk

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>::product/snyk/snyk`

Snykmenyediakan platform keamanan yang memindai komponen aplikasi untuk risiko keamanan dalam beban kerja yang berjalan. AWS Risiko ini dikirim ke Security Hub sebagai temuan, membantu pengembang dan tim keamanan memvisualisasikan dan memprioritaskannya bersama dengan sisa temuan keamanan mereka AWS .

AWS Tautan Marketplace

Dokumentasi mitra

Sonrai Security – Sonrai Dig

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>::product/sonrai-security/sonrai-dig`

Sonrai Digmemantau dan memulihkan kesalahan konfigurasi cloud dan pelanggaran kebijakan, sehingga Anda dapat meningkatkan keamanan dan postur kepatuhan Anda.

Tautan produk

Dokumentasi mitra

Sophos – Server Protection

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>:062897671886:product/sophos/sophos-server-protection`

Sophos Server Protectionmembela aplikasi dan data penting di inti organisasi Anda, menggunakan defense-in-depth teknik yang komprehensif.

Tautan produk

Dokumentasi mitra

StackRox – StackRox Kubernetes Security

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>::product/stackrox/kubernetes-security`

StackRoxmembantu perusahaan mengamankan container dan penerapan Kubernetes mereka dalam skala besar dengan menegakkan kebijakan kepatuhan dan keamanan mereka di seluruh siklus hidup container — build, deploy, dan run.

Tautan produk

Dokumentasi mitra

Sumo Logic – Machine Data Analytics

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>:956882708938:product/sumologicinc/sumologic-mda`

Sumo Logicadalah platform analisis data mesin yang aman yang memungkinkan tim operasi pengembangan dan keamanan untuk membangun, menjalankan, dan mengamankan AWS aplikasi mereka.

Tautan produk

Dokumentasi mitra

Symantec – Cloud Workload Protection

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>:754237914691:product/symantec-corp/symantec-cwp`

Cloud Workload Protectionmemberikan perlindungan lengkap untuk instans Amazon EC2 Anda dengan antimalware, pencegahan intrusi, dan pemantauan integritas file.

Tautan produk

Dokumentasi mitra

Tenable – Tenable.io

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>:422820575223:product/tenable/tenable-io`

Mengidentifikasi, menyelidiki, dan memprioritaskan kerentanan secara akurat. Dikelola di cloud.

Tautan produk

Dokumentasi mitra

Trend Micro – Cloud One

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>::product/trend-micro/cloud-one`

Trend Micro Cloud Onememberikan informasi keamanan yang tepat kepada tim pada waktu dan tempat yang tepat. Integrasi ini mengirimkan temuan keamanan ke Security Hub secara real time, meningkatkan visibilitas ke AWS sumber daya dan detail Trend Micro Cloud One acara Anda di Security Hub.

AWS Tautan Marketplace

Dokumentasi mitra

Vectra – Cognito Detect

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>:978576646331:product/vectra-ai/cognito-detect`

Vectramengubah keamanan siber dengan menerapkan AI canggih untuk mendeteksi dan merespons penyerang siber tersembunyi sebelum mereka dapat mencuri atau menyebabkan kerusakan.

AWS Tautan Marketplace

Dokumentasi mitra

Wiz – Wiz Security

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>::product/wiz-security/wiz-security`

Wizterus menganalisis konfigurasi, kerentanan, jaringan, pengaturan IAM, rahasia, dan lainnya di seluruh Anda, pengguna Akun AWS, dan beban kerja untuk menemukan masalah penting yang mewakili risiko aktual. Integrasikan Wiz dengan Security Hub untuk memvisualisasikan dan menanggapi masalah yang dideteksi Wiz dari konsol Security Hub.

AWS Tautan Marketplace

Dokumentasi mitra

Integrasi pihak ketiga yang menerima temuan dari Security Hub

Integrasi produk mitra pihak ketiga berikut menerima temuan dari Security Hub. Jika dicatat, produk juga dapat memperbarui temuan. Dalam hal ini, menemukan pembaruan yang Anda buat di produk mitra juga akan tercermin di Security Hub.

Atlassian - Jira Service Management

Jenis integrasi: Terima dan perbarui

The AWS Service Management Connector for Jira mengirimkan temuan dari Security Hub keJira. Jiramasalah dibuat berdasarkan temuan. Saat Jira masalah diperbarui, temuan terkait diperbarui di Security Hub.

Integrasi hanya mendukung Jira Server dan Jira Data Center.

Untuk gambaran umum tentang integrasi dan cara kerjanya, tonton video AWS Security Hub — Integrasi dua arah dengan. Atlassian Jira Service Management

Tautan produk

Dokumentasi mitra

Atlassian - Jira Service Management Cloud

Jenis integrasi: Terima dan perbarui

Jira Service Management Cloudadalah komponen cloud dari Jira Service Management.

The AWS Service Management Connector for Jira mengirimkan temuan dari Security Hub keJira. Temuan tersebut memicu terciptanya masalah diJira Service Management Cloud. Saat Anda memperbarui masalah tersebutJira Service Management Cloud, temuan terkait juga diperbarui di Security Hub.

Tautan produk

Dokumentasi mitra

Atlassian – Opsgenie

Jenis integrasi: Terima

Opsgenieadalah solusi manajemen insiden modern untuk mengoperasikan layanan selalu aktif, memberdayakan tim pengembangan dan operasi untuk merencanakan gangguan layanan dan tetap memegang kendali selama insiden.

Mengintegrasikan dengan Security Hub memastikan bahwa insiden terkait keamanan kritis misi diarahkan ke tim yang sesuai untuk penyelesaian segera.

Tautan produk

Dokumentasi mitra

Fortinet – FortiCNP

Jenis integrasi: Terima

FortiCNPadalah produk Cloud Native Protection yang menggabungkan temuan keamanan ke dalam wawasan yang dapat ditindaklanjuti dan memprioritaskan wawasan keamanan berdasarkan skor risiko untuk mengurangi kelelahan waspada dan mempercepat remediasi.

AWS Tautan Marketplace

Dokumentasi mitra

IBM – QRadar

Jenis integrasi: Terima

IBM QRadarSIEM memberi tim keamanan kemampuan untuk mendeteksi, memprioritaskan, menyelidiki, dan merespons ancaman dengan cepat dan akurat.

Tautan produk

Dokumentasi mitra

Logz.io Cloud SIEM

Jenis integrasi: Terima

Logz.ioadalah penyedia Cloud SIEM yang menyediakan korelasi lanjutan data log dan peristiwa untuk membantu tim keamanan mendeteksi, menganalisis, dan menanggapi ancaman keamanan secara real time.

Tautan produk

Dokumentasi mitra

MetricStream – CyberGRC

Jenis integrasi: Terima

MetricStream CyberGRCmembantu Anda mengelola, mengukur, dan mengurangi risiko keamanan siber. Dengan menerima temuan Security Hub, CyberGRC memberikan lebih banyak visibilitas terhadap risiko ini, sehingga Anda dapat memprioritaskan investasi keamanan siber dan mematuhi kebijakan TI.

AWS Tautan Marketplace

Tautan produk

MicroFocus – MicroFocus Arcsight

Jenis integrasi: Terima

ArcSightmempercepat deteksi dan respons ancaman yang efektif secara real time, mengintegrasikan korelasi peristiwa dan analitik yang diawasi dan tanpa pengawasan dengan otomatisasi respons dan orkestrasi.

Tautan produk

Dokumentasi mitra

New Relic Vulnerability Management

Jenis integrasi: Terima

New Relic Vulnerability Managementmenerima temuan keamanan dari Security Hub, sehingga Anda bisa mendapatkan tampilan keamanan terpusat di samping telemetri kinerja dalam konteks di seluruh tumpukan Anda.

AWS Tautan Marketplace

Dokumentasi mitra

PagerDuty – PagerDuty

Jenis integrasi: Terima

Platform manajemen operasi PagerDuty digital memberdayakan tim untuk secara proaktif mengurangi masalah yang berdampak pelanggan dengan secara otomatis mengubah sinyal apa pun menjadi wawasan dan tindakan yang tepat.

AWS pengguna dapat menggunakan PagerDuty serangkaian AWS integrasi untuk menskalakan lingkungan mereka AWS dan hibrida dengan percaya diri.

Ketika digabungkan dengan peringatan keamanan teragregasi dan terorganisir Security Hub, PagerDuty memungkinkan tim untuk mengotomatiskan proses respons ancaman mereka dan dengan cepat mengatur tindakan khusus untuk mencegah potensi masalah.

PagerDutypengguna yang melakukan proyek migrasi cloud dapat bergerak dengan cepat, sekaligus mengurangi dampak masalah yang terjadi di seluruh siklus hidup migrasi.

Tautan produk

Dokumentasi mitra

Palo Alto Networks – Cortex XSOAR

Jenis integrasi: Terima

Cortex XSOARadalah platform Security Orchestration, Automation, and Response (SOAR) yang terintegrasi dengan seluruh tumpukan produk keamanan Anda untuk mempercepat respons insiden dan operasi keamanan.

Tautan produk

Dokumentasi mitra

Palo Alto Networks – VM-Series

Jenis integrasi: Terima

Palo Alto VM-SeriesIntegrasi dengan Security Hub mengumpulkan intelijen ancaman dan mengirimkannya ke firewall VM-Series generasi berikutnya sebagai pembaruan kebijakan keamanan otomatis yang memblokir aktivitas alamat IP berbahaya.

Tautan produk

Dokumentasi mitra

Rackspace Technology – Cloud Native Security

Jenis integrasi: Terima

Rackspace Technology menyediakan layanan keamanan terkelola di atas produk AWS keamanan asli untuk pemantauan 24x7x365 oleh Rackspace SOC, analisis lanjutan, dan remediasi ancaman.

Tautan produk

Rapid7 – InsightConnect

Jenis integrasi: Terima

Rapid7 InsightConnectadalah solusi orkestrasi dan otomatisasi keamanan yang memungkinkan tim Anda mengoptimalkan operasi SOC dengan sedikit atau tanpa kode.

Tautan produk

Dokumentasi mitra

RSA – RSA Archer

Jenis integrasi: Terima

RSA ArcherManajemen Risiko TI dan Keamanan memungkinkan Anda untuk menentukan aset mana yang penting bagi bisnis Anda, menetapkan dan mengkomunikasikan kebijakan dan standar keamanan, mendeteksi dan menanggapi serangan, mengidentifikasi dan memulihkan kekurangan keamanan, dan menetapkan praktik terbaik manajemen risiko TI yang jelas.

Tautan produk

Dokumentasi mitra

ServiceNow – ITSM

Jenis integrasi: Terima dan perbarui

ServiceNowIntegrasi dengan Security Hub memungkinkan temuan keamanan dari Security Hub untuk dilihat di dalamnyaServiceNow ITSM. Anda juga dapat mengonfigurasi ServiceNow untuk secara otomatis membuat insiden atau masalah saat menerima temuan dari Security Hub.

Setiap pembaruan untuk insiden dan masalah ini menghasilkan pembaruan temuan di Security Hub.

Untuk ikhtisar integrasi dan cara kerjanya, tonton video AWS Security Hub - Integrasi dua arah dengan. ServiceNow ITSM

Tautan produk

Dokumentasi mitra

Slack – Slack

Jenis integrasi: Terima

Slackadalah lapisan tumpukan teknologi bisnis yang menyatukan orang, data, dan aplikasi. Ini adalah satu tempat di mana orang dapat bekerja sama secara efektif, menemukan informasi penting, dan mengakses ratusan ribu aplikasi dan layanan penting untuk melakukan pekerjaan terbaik mereka.

Tautan produk

Dokumentasi mitra

Splunk – Splunk Enterprise

Jenis integrasi: Terima

Splunkmenggunakan Amazon CloudWatch Events sebagai konsumen temuan Security Hub. Kirim data Anda ke Splunk untuk analitik keamanan tingkat lanjut dan SIEM.

Tautan produk

Dokumentasi mitra

Splunk – Splunk Phantom

Jenis integrasi: Terima

Dengan Splunk Phantom aplikasi untuk AWS Security Hub, temuan dikirim ke Phantom untuk pengayaan konteks otomatis dengan informasi intelijen ancaman tambahan atau untuk melakukan tindakan respons otomatis.

Tautan produk

Dokumentasi mitra

ThreatModeler

Jenis integrasi: Terima

ThreatModeleradalah solusi pemodelan ancaman otomatis yang mengamankan dan meningkatkan skala perangkat lunak perusahaan dan siklus hidup pengembangan cloud.

Tautan produk

Dokumentasi mitra

Trellix – Trellix Helix

Jenis integrasi: Terima

Trellix Helixadalah platform operasi keamanan yang dihosting cloud yang memungkinkan organisasi mengendalikan insiden apa pun dari peringatan untuk diperbaiki.

Tautan produk

Dokumentasi mitra

Integrasi pihak ketiga yang mengirimkan temuan ke dan menerima temuan dari Security Hub

Integrasi produk mitra pihak ketiga berikut mengirimkan temuan ke dan menerima temuan dari Security Hub.

Caveonix – Caveonix Cloud

Jenis integrasi: Kirim dan terima

Produk ARN: `arn:aws:securityhub:<REGION>::product/caveonix/caveonix-cloud`

Platform yang Caveonix didukung AI mengotomatiskan visibilitas, penilaian, dan mitigasi di cloud hybrid, yang mencakup layanan cloud-native, VM, dan container. Terintegrasi dengan AWS Security Hub, Caveonix menggabungkan AWS data dan analitik lanjutan untuk wawasan tentang peringatan keamanan dan kepatuhan.

AWS Tautan Marketplace

Dokumentasi mitra

Cloud Custodian – Cloud Custodian

Jenis integrasi: Kirim dan terima

Produk ARN: `arn:aws:securityhub:<REGION>::product/cloud-custodian/cloud-custodian`

Cloud Custodianmemungkinkan pengguna untuk dikelola dengan baik di cloud. YAMM DSL yang sederhana memungkinkan aturan yang mudah didefinisikan untuk memungkinkan infrastruktur cloud yang dikelola dengan baik yang aman dan dioptimalkan biaya.

Tautan produk

Dokumentasi mitra

DisruptOps, Inc. – DisruptOPS

Jenis integrasi: Kirim dan terima

Produk ARN: `arn:aws:securityhub:<REGION>::product/disruptops-inc/disruptops`

Platform Operasi DisruptOps Keamanan membantu organisasi mempertahankan praktik keamanan terbaik di cloud Anda melalui penggunaan pagar pembatas otomatis.

Tautan produk

Dokumentasi mitra

Kion

Jenis integrasi: Kirim dan terima

Produk ARN: `arn:aws:securityhub:<REGION>::product/cloudtamerio/cloudtamerio`

Kion(sebelumnya cloudtamer.io) adalah solusi tata kelola cloud lengkap untuk. AWSKionmemberikan visibilitas pemangku kepentingan ke dalam operasi cloud dan membantu pengguna cloud mengelola akun, mengontrol anggaran dan biaya, dan memastikan kepatuhan berkelanjutan.

Tautan produk

Dokumentasi mitra

Turbot – Turbot

Jenis integrasi: Kirim dan terima

Produk ARN: `arn:aws:securityhub:<REGION>::product/turbot/turbot`

Turbotmemastikan bahwa infrastruktur cloud Anda aman, sesuai, terukur, dan dioptimalkan biaya.

Tautan produk

Dokumentasi mitra

Menggunakan integrasi produk khusus untuk mengirim temuan ke AWS Security Hub

Selain temuan yang dihasilkan oleh AWS layanan terintegrasi dan produk pihak ketiga, Security Hub dapat mengkonsumsi temuan yang dihasilkan oleh produk keamanan khusus lainnya.

Anda dapat mengirimkan temuan ini ke Security Hub secara manual dengan menggunakan operasi `BatchImportFindings`API.

Saat menyiapkan integrasi kustom, gunakan pedoman dan daftar periksa yang disediakan dalam Panduan Integrasi Mitra Security Hub.

Persyaratan dan rekomendasi untuk mengirimkan temuan dari produk keamanan khusus

Sebelum Anda berhasil menjalankan operasi `BatchImportFindings`API, Anda harus mengaktifkan Security Hub.

Anda harus memberikan rincian temuan menggunakanthe section called “Menemukan format”. Untuk temuan dari integrasi kustom Anda, gunakan persyaratan dan rekomendasi berikut.

Mengatur ARN produk

Saat Anda mengaktifkan Security Hub, produk default Nama Sumber Daya Amazon (ARN) untuk Security Hub akan dibuat di akun Anda saat ini.

Produk ARN ini memiliki format sebagai berikut:. `arn:aws:securityhub:<region>:<account-id>:product/<account-id>/default` Misalnya, `arn:aws:securityhub:us-west-2:123456789012:product/123456789012/default`.

Gunakan ARN produk ini sebagai nilai untuk `ProductArn`atribut saat menjalankan operasi API. `BatchImportFindings`

Mendefinisikan nama perusahaan dan produk

Anda dapat menggunakan `BatchImportFindings` untuk menetapkan nama perusahaan dan nama produk pilihan untuk integrasi kustom yang mengirimkan temuan ke Security Hub.

Nama yang Anda tentukan menggantikan nama perusahaan dan nama produk yang telah dikonfigurasi sebelumnya, masing-masing disebut nama pribadi dan nama default, dan muncul di konsol Security Hub dan JSON dari setiap temuan. Lihat Menggunakan BatchImportFindings untuk membuat dan memperbarui temuan.

Mengatur ID temuan

Anda harus menyediakan, mengelola, dan menambah ID temuan Anda sendiri, menggunakan `Id`atribut.

Setiap temuan baru harus memiliki ID temuan unik. Jika produk kustom mengirimkan beberapa temuan dengan ID temuan yang sama, Security Hub hanya memproses temuan pertama.

Mengatur ID akun

Anda harus menentukan ID akun Anda sendiri, menggunakan `AwsAccountId`atribut.

Mengatur yang dibuat pada dan diperbarui pada tanggal

Anda harus menyediakan stempel waktu Anda sendiri untuk atribut `CreatedAt`dan `UpdatedAt`.

Memperbarui temuan dari produk khusus

Selain mengirimkan temuan baru dari produk kustom, Anda juga dapat menggunakan operasi `BatchImportFindings`API untuk memperbarui temuan yang ada dari produk kustom.

Untuk memperbarui temuan yang ada, gunakan ID temuan yang ada (melalui `Id`atribut). Kirim ulang temuan lengkap dengan informasi yang sesuai yang diperbarui dalam permintaan, termasuk `UpdatedAt`stempel waktu yang dimodifikasi.

Contoh integrasi kustom

Anda dapat menggunakan contoh integrasi produk kustom berikut sebagai panduan untuk membuat solusi kustom Anda sendiri.

Mengirim temuan dari Chef InSpec pemindaian ke Security Hub

Anda dapat membuat AWS CloudFormation template yang menjalankan pemindaian Chef InSpec kepatuhan dan kemudian mengirimkan temuan ke Security Hub.

Untuk detail selengkapnya, lihat Pemantauan kepatuhan berkelanjutan dengan Chef InSpec dan AWS Security Hub.

Mengirim kerentanan kontainer terdeteksi oleh Trivy ke Security Hub

Anda dapat membuat AWS CloudFormation templat yang digunakan AquaSecurity Trivy untuk memindai kerentanan kontainer, lalu mengirimkan temuan kerentanan tersebut ke Security Hub.

Untuk detail selengkapnya, lihat Cara membuat pipeline CI/CD untuk pemindaian kerentanan kontainer dengan dan Security Trivy Hub AWS.

Kontrol dan standar keamanan di AWS Security Hub

AWS Security Hub mengkonsumsi, mengumpulkan, dan menganalisis temuan keamanan dari berbagai produk yang didukung AWS dan pihak ketiga.

Security Hub juga menghasilkan temuannya sendiri dengan menjalankan pemeriksaan keamanan otomatis dan berkelanjutan terhadap aturan. Aturan diwakili oleh kontrol keamanan. Kontrol dapat, pada gilirannya, diaktifkan dalam satu atau lebih standar keamanan. Kontrol membantu Anda menentukan apakah persyaratan dalam suatu standar terpenuhi.

Pemeriksaan keamanan terhadap kontrol menghasilkan temuan yang dapat Anda gunakan untuk memantau postur keamanan Anda dan mengidentifikasi spesifik Akun AWS atau sumber daya yang memerlukan perhatian. Setiap kontrol terkait dengan AWS layanan dan sumber daya. Misalnya, pemeriksaan keamanan terhadap CloudTrailkontrol.4 menentukan apakah Anda telah mengonfigurasi validasi file log pada log Anda AWS CloudTrail . Untuk informasi selengkapnya tentang kontrol, lihatMelihat dan mengelola kontrol keamanan.

Anda dapat mengaktifkan kontrol dalam satu atau beberapa standar Security Hub yang diaktifkan. Saat Anda mengaktifkan standar, Security Hub secara otomatis mengaktifkan kontrol yang berlaku untuk standar. Standar keamanan memungkinkan Anda untuk fokus pada kerangka kepatuhan tertentu. Security Hub mendefinisikan kontrol yang berlaku untuk setiap standar. Untuk informasi selengkapnya tentang standar keamanan, lihatMelihat dan mengelola standar keamanan.

Berdasarkan hasil pemeriksaan keamanan, Security Hub menghitung skor keamanan keseluruhan dan skor keamanan khusus standar. Skor ini membantu Anda memahami postur keamanan Anda. Untuk informasi lebih lanjut tentang skor, lihatBagaimana skor keamanan dihitung.

Untuk informasi tentang harga Security Hub untuk pemeriksaan keamanan, lihat harga Security Hub.

Topik

Izin IAM untuk mengonfigurasi standar dan kontrol

Untuk melihat informasi tentang kontrol keamanan dan mengaktifkan serta menonaktifkan kontrol keamanan dalam standar, peran AWS Identity and Access Management (IAM) yang Anda gunakan untuk mengakses AWS Security Hub memerlukan izin untuk memanggil tindakan API berikut. Tanpa menambahkan izin untuk tindakan ini, Anda tidak akan dapat memanggil API ini. Untuk mendapatkan izin yang diperlukan, Anda dapat menggunakan kebijakan terkelola Security Hub. Atau, Anda dapat memperbarui kebijakan IAM khusus untuk menyertakan izin untuk tindakan ini. Kebijakan khusus juga harus menyertakan izin untuk `DescribeStandardsControls`dan `UpdateStandardsControl`API.

- **`BatchGetSecurityControls`**— Mengembalikan informasi tentang sekumpulan kontrol keamanan untuk akun saat ini dan Wilayah AWS.
- **`ListSecurityControlDefinitions`**— Mengembalikan informasi tentang kontrol keamanan yang berlaku untuk standar tertentu.
- **`ListStandardsControlAssociations`**— Mengidentifikasi apakah kontrol keamanan saat ini diaktifkan atau dinonaktifkan dari setiap standar yang diaktifkan di akun.
- **`BatchGetStandardsControlAssociations`**— Untuk sekumpulan kontrol keamanan, identifikasi apakah setiap kontrol saat ini diaktifkan atau dinonaktifkan dari standar yang ditentukan.
- **`BatchUpdateStandardsControlAssociations`**Digunakan untuk mengaktifkan kontrol keamanan dalam standar yang mencakup kontrol, atau untuk menonaktifkan kontrol dalam standar. Ini adalah pengganti batch untuk `UpdateStandardsControl`API yang ada jika administrator tidak ingin mengizinkan akun anggota untuk mengaktifkan atau menonaktifkan kontrol.

Selain API sebelumnya, Anda harus menambahkan izin untuk memanggil **`BatchGetControlEvaluations`**ke peran IAM Anda. Izin ini diperlukan untuk melihat status pemberdayaan dan kepatuhan kontrol, jumlah temuan untuk kontrol, dan skor keamanan keseluruhan untuk kontrol di konsol Security Hub. Karena hanya panggilan konsol **`BatchGetControlEvaluations`**, izin IAM ini tidak secara langsung sesuai dengan API atau AWS CLI perintah Security Hub yang didokumentasikan secara publik.

Untuk informasi selengkapnya tentang API yang terkait dengan kontrol dan standar, lihat Referensi AWS Security Hub API.

Pemeriksaan keamanan dan skor keamanan di Security Hub

Untuk setiap kontrol yang Anda aktifkan, AWS Security Hub jalankan pemeriksaan keamanan. Pemeriksaan keamanan menentukan apakah AWS sumber daya Anda sesuai dengan aturan yang termasuk dalam kontrol.

Beberapa pemeriksaan berjalan pada jadwal berkala. Pemeriksaan lain hanya berjalan ketika ada perubahan pada status sumber daya. Untuk informasi selengkapnya, lihat the section called “Jadwal untuk menjalankan pemeriksaan keamanan”.

Banyak pemeriksaan keamanan menggunakan aturan AWS Config terkelola atau kustom untuk menetapkan persyaratan kepatuhan. Untuk menjalankan pemeriksaan ini, Anda harus mengatur AWS Config. Untuk informasi selengkapnya, lihat the section called “AWS Config aturan dan pemeriksaan keamanan”. Lainnya menggunakan fungsi Lambda khusus, yang dikelola oleh Security Hub dan tidak terlihat oleh pelanggan.

Karena Security Hub menjalankan pemeriksaan keamanan, ia menghasilkan temuan dan memberi mereka status kepatuhan. Untuk informasi selengkapnya tentang status kepatuhan, lihatNilai untuk status kepatuhan suatu temuan.

Security Hub menggunakan status kepatuhan temuan kontrol untuk menentukan status kontrol secara keseluruhan. Security Hub juga menghitung skor keamanan di semua kontrol yang diaktifkan dan untuk standar tertentu. Untuk informasi selengkapnya, lihat the section called “Status kepatuhan dan status kontrol” dan the section called “Menentukan skor keamanan”.

Jika Anda mengaktifkan temuan kontrol konsolidasi, Security Hub menghasilkan satu temuan bahkan ketika kontrol dikaitkan dengan lebih dari satu standar. Untuk informasi selengkapnya, lihat Temuan kontrol terkonsolidasi.

Topik

- Bagaimana Security Hub menggunakan AWS Config aturan untuk menjalankan pemeriksaan keamanan
- AWS Config sumber daya yang dibutuhkan untuk menghasilkan temuan kontrol
- Jadwal untuk menjalankan pemeriksaan keamanan
- Menghasilkan dan memperbarui temuan kontrol
- Status kepatuhan dan status kontrol
- Menentukan skor keamanan

Bagaimana Security Hub menggunakan AWS Config aturan untuk menjalankan pemeriksaan keamanan

Untuk menjalankan pemeriksaan keamanan pada sumber daya lingkungan Anda, AWS Security Hub gunakan langkah-langkah yang ditentukan oleh standar, atau gunakan AWS Config aturan khusus. Beberapa aturan adalah aturan yang dikelola, yang dikelola oleh AWS Config. Aturan lainnya adalah aturan khusus yang dikembangkan Security Hub.

AWS Config Aturan yang digunakan Security Hub untuk kontrol disebut sebagai aturan terkait layanan, karena aturan tersebut diaktifkan dan dikendalikan oleh layanan Security Hub.

Untuk mengaktifkan pemeriksaan terhadap AWS Config aturan ini, Anda harus terlebih dahulu mengaktifkan AWS Config akun Anda dan mengaktifkan perekaman sumber daya untuk sumber daya yang diperlukan. Untuk informasi tentang cara mengaktifkan AWS Config, lihatMengkonfigurasi AWS Config. Untuk informasi tentang perekaman sumber daya yang diperlukan, lihat AWS Config sumber daya yang dibutuhkan untuk menghasilkan temuan kontrol

Cara Security Hub menghasilkan aturan terkait layanan

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

Aturan terkait layanan ini khusus untuk Security Hub. Ini menciptakan aturan terkait layanan ini bahkan jika contoh lain dari aturan yang sama sudah ada. Aturan terkait layanan ditambahkan `securityhub` sebelum nama aturan asli, dan pengidentifikasi unik setelah nama aturan. Misalnya, untuk aturan AWS Config terkelola aslivpc-flow-logs-enabled, nama aturan terkait layanan akan menjadi sesuatu seperti. `securityhub-vpc-flow-logs-enabled-12345`

Ada batasan jumlah AWS Config aturan yang dapat digunakan untuk mengevaluasi kontrol. AWS Config Aturan khusus yang dibuat Security Hub tidak diperhitungkan dalam batas tersebut. Anda dapat mengaktifkan standar keamanan meskipun Anda telah mencapai AWS Config batas untuk aturan terkelola di akun Anda. Untuk mempelajari lebih lanjut tentang batasan AWS Config aturan, lihat Batas Layanan di Panduan AWS Config Pengembang.

Melihat detail tentang AWS Config aturan untuk kontrol

Untuk kontrol yang menggunakan aturan AWS Config terkelola, deskripsi kontrol menyertakan tautan ke detail AWS Config aturan. Aturan kustom tidak ditautkan dari deskripsi kontrol. Untuk deskripsi kontrol, lihatReferensi kontrol Security Hub. Pilih kontrol dari daftar untuk melihat deskripsinya.

Untuk temuan yang dihasilkan dari kontrol tersebut, detail temuan mencakup tautan ke AWS Config aturan terkait. Perhatikan bahwa untuk menavigasi ke AWS Config aturan dari menemukan detail, Anda juga harus memiliki izin IAM di akun yang dipilih untuk menavigasi ke AWS Config.

Detail temuan di halaman Temuan, halaman Wawasan, dan halaman Integrasi menyertakan tautan Aturan ke detail AWS Config aturan. Lihat Meninjau detail temuan.

Pada halaman detail kontrol, kolom Selidiki daftar temuan berisi tautan ke detail AWS Config aturan. Lihat Melihat AWS Config aturan untuk menemukan sumber daya.

AWS Config sumber daya yang dibutuhkan untuk menghasilkan temuan kontrol

AWS Security Hub menghasilkan temuan kontrol dengan melakukan pemeriksaan keamanan terhadap kontrol Security Hub. Beberapa kontrol menggunakan AWS Config aturan yang mengevaluasi kepatuhan dengan sumber daya tertentu. Agar Security Hub menghasilkan temuan untuk kontrol yang memiliki jenis jadwal yang dipicu perubahan, Anda harus mengaktifkan perekaman untuk sumber daya yang diperlukan AWS Config. Anda tidak perlu merekam sumber daya untuk sebagian besar kontrol yang memiliki jenis jadwal berkala. Namun, beberapa kontrol berkala memerlukan perekaman sumber daya untuk mendeteksi perubahan kepatuhan.

Halaman ini menyediakan daftar sumber daya yang diperlukan di seluruh standar dan daftar sumber daya yang diperlukan dibagi dengan standar. Tabel pertama juga mencantumkan kontrol Security Hub yang menggunakan setiap sumber daya.

Jika temuan dihasilkan oleh pemeriksaan keamanan yang didasarkan pada AWS Config aturan, rincian temuan menyertakan tautan Aturan ke AWS Config aturan terkait. Untuk menavigasi ke AWS Config aturan, akun Anda harus memiliki izin AWS Identity and Access Management (IAM) untuk melihat AWS Config aturan.

> **Note**
>
> Di Wilayah AWS mana kontrol tidak tersedia, sumber daya yang sesuai tidak tersedia di AWS Config. Untuk mengetahui daftar batas Regional pada kontrol Security Hub, lihatKetersediaan kontrol berdasarkan Wilayah.

AWS Config sumber daya yang dibutuhkan untuk semua kontrol

Agar Security Hub menghasilkan temuan untuk kontrol yang dipicu perubahan Security Hub yang diaktifkan yang menggunakan AWS Config aturan, Anda harus merekam sumber daya ini AWS Config. Tabel ini juga menunjukkan kontrol mana yang memerlukan sumber daya tertentu. Kontrol mungkin memerlukan lebih dari satu sumber daya.

Layanan	Sumber daya yang dibutuhkan	Kontrol terkait
Amazon API Gateway	`AWS::ApiGateway::Stage`	ApiGateway.1 ApiGateway.2 ApiGateway.3 ApiGateway.4 ApiGateway.5
	`AWS::ApiGatewayV2::Stage`	ApiGateway.1 ApiGateway.9
AWS AppSync	`AWS::AppSync::GraphQLApi`	AppSync.2 AppSync.4 AppSync.5
AWS Backup (AWS Backup)	`AWS::Backup::BackupPlan`	Cadangan.5
	`AWS::Backup::BackupVault`	Cadangan.3
	`AWS::Backup::RecoveryPoint`	Backup.1 Backup.2

Layanan	Sumber daya yang dibutuhkan	Kontrol terkait
	`AWS::Backup::ReportPlan`	Cadangan.4
AWS Certificate Manager (ACM)	`AWS::ACM::Certificate`	ACM.1 ACM.2 ACM.3
Amazon Athena	`AWS::Athena::DataCatalog`	Athena.2
	`AWS::Athena::WorkGroup`	Athena.3
AWS CloudFormation	`AWS::CloudFormation::Stack`	CloudFormation.2

Layanan	Sumber daya yang dibutuhkan	Kontrol terkait
Amazon CloudFront	`AWS::CloudFront::Distribution`	CloudFront.1 CloudFront.3 CloudFront.4 CloudFront.5 CloudFront.6 CloudFront.7 CloudFront.8 CloudFront.9 CloudFront.10 CloudFront.13 CloudFront.14
AWS CloudTrail	`AWS::CloudTrail::Trail`	CloudTrail.9
Amazon CloudWatch	`AWS::CloudWatch::Alarm`	CloudWatch.15 CloudWatch.17
AWS CodeArtifact	`AWS::CodeArtifact::Repository`	CodeArtifact.1

Layanan	Sumber daya yang dibutuhkan	Kontrol terkait
AWS CodeBuild	`AWS::CodeBuild::Project`	CodeBuild.1 CodeBuild.2 CodeBuild.3 CodeBuild.4
Amazon Detective	`AWS::Detective::Graph`	Detektif.1
AWS Database Migration Service (AWS DMS)	`AWS::DMS::Certificate`	DMS.2

	`AWS::DMS::Endpoint`	`DMS.9`
		`DMS.10`
		`DMS.11`
		`DMS.12`

	`AWS::DMS::EventSubscription`	DMS.3
	`AWS::DMS::ReplicationInstance`	DMS.4 DMS.6
	`AWS::DMS::ReplicationSubnetGroup`	DMS.5
	`AWS::DMS::ReplicationTask`	DMS.7 DMS.8

Layanan	Sumber daya yang dibutuhkan	Kontrol terkait
Amazon DynamoDB	`AWS::DynamoDB::Table`	DynamoDB.1 DynamoDB.2 DynamoDb.5 DynamoDb.6
Amazon Elastic Compute Cloud (EC2)	`AWS::EC2::ClientVpnEndpoint`	EC2.51
	`AWS::EC2::CustomerGateway`	EC2.36
	`AWS::EC2::EIP`	EC2.12 EC2.37
	`AWS::EC2::FlowLog`	EC2.48
	`AWS::EC2::Instance`	EC2.4 EC2.8 EC2.9 EC2.17 EC2.24 EC2.38 EMR.1 SSM.1

Layanan	Sumber daya yang dibutuhkan	Kontrol terkait
	`AWS::EC2::InternetGateway`	EC2.39
	`AWS::EC2::LaunchTemplate`	EC2.25
	`AWS::EC2::NatGateway`	EC2.40
	`AWS::EC2::NetworkAcl`	EC2.16 EC2.21 EC2.41
	`AWS::EC2::NetworkInterface`	EC2.22 EC2.35
	`AWS::EC2::RouteTable`	EC2.42
	`AWS::EC2::SecurityGroup`	EC2.2 EC2.13 EC2.14 EC2.18 EC2.19 EC2.43

Layanan	Sumber daya yang dibutuhkan	Kontrol terkait
	`AWS::EC2::Subnet`	EC2.15 EC2.44 ElastiCache.7
	`AWS::EC2::TransitGateway`	EC2.23 EC2.52
	`AWS::EC2::TransitGatewayAttachment`	EC2.33
	`AWS::EC2::TransitGatewayRouteTable`	EC2.34
	`AWS::EC2::Volume`	EC2.3 EC2.45
	`AWS::EC2::VPC`	EC2.6 EC2.46
	`AWS::EC2::VPCEndpointService`	EC2.47
	`AWS::EC2::VPCPeeringConnection`	EC2.49

Layanan	Sumber daya yang dibutuhkan	Kontrol terkait
	`AWS::EC2::VPNConnection`	EC2.20
	`AWS::EC2::VPNGateway`	EC2.50
Amazon EC2 Auto Scaling	`AWS::AutoScaling::AutoScalingGroup`	AutoScaling.1 AutoScaling.2 AutoScaling.6 AutoScaling.9 AutoScaling.10
	`AWS::AutoScaling::LaunchConfiguration`	AutoScaling.3 Penskalaan otomatis.5
Amazon EC2 Systems Manager (SSM)	`AWS::SSM::AssociationCompliance`	SSM.3
	`AWS::SSM::ManagedInstanceInventory`	SSM.1
	`AWS::SSM::PatchCompliance`	SSM.2

Layanan	Sumber daya yang dibutuhkan	Kontrol terkait
Amazon Elastic Container Registry (Amazon ECR)	`AWS::ECR::PublicRepository`	ECR.4
	`AWS::ECR::Repository`	ECR.2 ECR.3
Amazon Elastic Container Service (Amazon ECS)	`AWS::ECS::Cluster`	ECS.12 ECS.14
	`AWS::ECS::Service`	ECS.2 ECS.10 ECS.13
	`AWS::ECS::TaskDefinition`	ECS.1 ECS.3 ECS.4 DLS.5 ECS.8 ECS.9 ECS.15
Amazon Elastic File System (Amazon EFS)	`AWS::EFS::AccessPoint`	EFS.3 EFS.4 EFS.5

Layanan	Sumber daya yang dibutuhkan	Kontrol terkait
Amazon Elastic Kubernetes Service (Amazon EKS)	`AWS::EKS::Cluster`	EKS.2 EKS.6 EKS.8
	`AWS::EKS::IdentityProviderConfig`	EKS.7
AWS Elastic Beanstalk	`AWS::ElasticBeanstalk::Environment`	ElasticBeanstalk.1 ElasticBeanstalk.2 ElasticBeanstalk.3
Penyeimbang Beban Elastis	`AWS::ElasticLoadBalancing::LoadBalancer`	ELB.2 ELB.3 ELB.5 ELB.7 ELB.8 ELB.9 ELB.10 ELB.14

Layanan	Sumber daya yang dibutuhkan	Kontrol terkait
	`AWS::ElasticLoadBalancingV2::LoadBalancer`	ELB.1 ELB.4 ELB.5 ELB.6 ELB.12 ELB.13 ELB.16
ElasticSearch	`AWS::Elasticsearch::Domain`	ES.3 ES.4 ES.5 ES.6 ES.7 ES.8 ES.9
Amazon EventBridge	`AWS::Events::EventBus`	EventBridge.2 EventBridge.3
	`AWS::Events::Endpoint`	EventBridge.4
`AWS Global Accelerator`	`AWS::GlobalAccelerator::Accelerator`	GlobalAccelerator.1

Layanan	Sumber daya yang dibutuhkan	Kontrol terkait
AWS Glue	AWS::Glue::Job	Lem. 1
Amazon GuardDuty	AWS::GuardDuty::Detector	GuardDuty.4
	AWS::GuardDuty::Filter	GuardDuty.2
	AWS::GuardDuty::IPSet	GuardDuty.3
AWS Identity and Access Management (IAM)	AWS::IAM::Group	IAM.27 KMS.2
	AWS::IAM::Policy	IAM.1 IAM.21 KMS.1
	AWS::IAM::Role	IAM.24 IAM.27 KMS.2

Layanan	Sumber daya yang dibutuhkan	Kontrol terkait
	`AWS::IAM::User`	IAM.2 IAM.3 IAM.5 IAM.8 IAM.19 IAM.22 IAM.25 IAM.27 KMS.2
AWS Identity and Access Management Access Analyzer	`AWS::AccessAnalyzer::Analyzer`	IAM.23
AWS IoT	`AWS::IoT::Authorizer`	IoT.4
	`AWS::IoT::Dimension`	IoT.3
	`AWS::IoT::MitigationAction`	IoT.2
	`AWS::IoT::Policy`	IoT.6
	`AWS::IoT::RoleAlias`	IoT.5

Layanan	Sumber daya yang dibutuhkan	Kontrol terkait
	`AWS::IoT::SecurityProfile`	IoT.1
AWS Key Management Service (AWS KMS)	`AWS::KMS::Alias`	S3.17
	`AWS::KMS::Key`	KMS.3 S3.17
Amazon Kinesis	`AWS::Kinesis::Stream`	Kinesis.1 Kinesis.2
AWS Lambda	`AWS::Lambda::Function`	Lambda.1 Lambda.2 Lambda.3 Lambda.5 Lambda.6
Amazon MSK	`AWS::MSK::Cluster`	MSK.1 MSK.2
Amazon MQ	`AWS::AmazonMQ::Broker`	MQ.2 MQ.3 MQ.4 MQ.5 MQ.6

Layanan	Sumber daya yang dibutuhkan	Kontrol terkait
AWS Network Firewall	`AWS::NetworkFirewall::Firewall`	NetworkFirewall.1 NetworkFirewall.7 NetworkFirewall.9
	`AWS::NetworkFirewall::FirewallPolicy`	NetworkFirewall.3 NetworkFirewall.4 NetworkFirewall.5 NetworkFirewall.8
	`AWS::NetworkFirewall::RuleGroup`	NetworkFirewall.6
OpenSearch Layanan Amazon	`AWS::OpenSearch::Domain`	Opensearch.1 Opensearch.2 Opensearch.3 Opensearch.4 Opensearch.5 Opensearch.6 Opensearch.7 Opensearch.8 Opensearch.9 Opensearch.10 Opensearch.11

Layanan	Sumber daya yang dibutuhkan	Kontrol terkait
Amazon Relational Database Service (Amazon RDS)	`AWS::RDS::DBCluster`	DokumenDB.1 DokumenDB.2 DokumenDB.4 DokumenDB.5 Neptunus.1 Neptunus.2 Neptunus.4 Neptunus.5 Neptunus.7 Neptunus.8 Neptunus.9 RDS.7 RDS.12 RDS.14 RDS.15 RDS.16 RDS.24 RDS.27 RDS.28 RDS.34

Layanan	Sumber daya yang dibutuhkan	Kontrol terkait
		RDS.35
	`AWS::RDS::DBClusterSnapshot`	DokumenDB.3 Neptunus.3 Neptunus.6 RDS.1 RDS.4 RDS.29

Layanan	Sumber daya yang dibutuhkan	Kontrol terkait
	`AWS::RDS::DBInstance`	RDS.2 RDS.3 RDS.5 RDS.6 RDS.8 RDS.9 RDS.10 RDS.11 RDS.13 RDS.17 RDS.18 RDS.23 RDS.25 RDS.30
	`AWS::RDS::DBSecurityGroup`	RDS.31
	`AWS::RDS::DBSnapshot`	RDS.1 RDS.4 RDS.32

Layanan	Sumber daya yang dibutuhkan	Kontrol terkait
	`AWS::RDS::DBSubnetGroup`	RDS.33
	`AWS::RDS::EventSubscription`	RDS.19 RDS.20 RDS.21 RDS.22
Amazon Redshift	`AWS::Redshift::Cluster`	Pergeseran merah.1 Pergeseran merah.2 Pergeseran merah.3 Pergeseran merah.4 Pergeseran Merah.6 Pergeseran Merah.7 Pergeseran Merah.8 Pergeseran Merah.9 Pergeseran Merah.10 Pergeseran Merah.11
	`AWS::Redshift::ClusterParameterGroup`	Pergeseran merah.2

Layanan	Sumber daya yang dibutuhkan	Kontrol terkait
	`AWS::Redshift::ClusterSnapshot`	Pergeseran Merah.13
	`AWS::Redshift::ClusterSubnetGroup`	Pergeseran Merah.14
	`AWS::Redshift::EventSubscription`	Pergeseran Merah.12
Amazon Route 53	`AWS::Route53::HostedZone`	Route53.2
	`AWS::Route53::HealthCheck`	Route53.1
Amazon Simple Storage Service (Amazon S3)	`AWS::S3::AccessPoint`	S3.19
	`AWS::S3::AccountPublicAccessBlock`	S3.2 S3.3

Layanan	Sumber daya yang dibutuhkan	Kontrol terkait
	`AWS::S3::Bucket`	S3.2 S3.3 S3.5 S3.6 S3.7 S3.8 S3.9 S3.10 S3.11 S3.12 S3.13 S3.14 S3.15 S3.17 S3.20
AWS Secrets Manager	`AWS::SecretsManager::Secret`	SecretsManager.1 SecretsManager.2 SecretsManager.5
AWS Service Catalog	`AWS::ServiceCatalog::Portfolio`	ServiceCatalog.1

Layanan	Sumber daya yang dibutuhkan	Kontrol terkait
Amazon Simple Email Service (Amazon SES)	`AWS::SES::ConfigurationSet`	SES.2
	`AWS::SES::ContactList`	SES.1
Amazon Simple Notification Service (Amazon SNS)	`AWS::SNS::Topic`	SNS.1 SNS.3
Amazon Simple Queue Service (Amazon SQS)	`AWS::SQS::Queue`	SQS.1 SQS.2
Amazon SageMaker	`AWS::SageMaker::NotebookInstance`	SageMaker.2 SageMaker.3
AWS Step Functions	`AWS::StepFunctions::StateMachine`	StepFunctions.1
	`AWS::StepFunctions::Activity`	StepFunctions.2
AWS Transfer Family	`AWS::Transfer::Workflow`	Transfer.1
AWS WAF	`AWS::WAF::Rule`	WAF.6
	`AWS::WAF::RuleGroup`	WAF.7

Layanan	Sumber daya yang dibutuhkan	Kontrol terkait
	`AWS::WAF::WebACL`	WAF.1 WAF.8
	`AWS::WAFRegional::Rule`	WAF.2
	`AWS::WAFRegional::RuleGroup`	WAF.3
	`AWS::WAFRegional::WebACL`	WAF.4
	`AWS::WAFv2::RuleGroup`	WAF.12
	`AWS::WAFv2::WebACL`	WAF.10 WAF.11

Sumber daya yang diperlukan untuk standar FSBP

Agar Security Hub dapat secara akurat melaporkan temuan untuk mengaktifkan kontrol yang dipicu oleh perubahan AWS Foundational Security Best Practices (FSBP) yang menggunakan AWS Config aturan, Anda harus mencatat sumber daya ini. AWS Config Untuk informasi lebih lanjut tentang standar ini, lihatAWS Standar Praktik Terbaik Keamanan Dasar (FSBP).

Layanan	Sumber daya yang dibutuhkan
Amazon API Gateway	`AWS::ApiGateway::Stage` `AWS::ApiGatewayV2::Stage`
AWS AppSync	`AWS::AppSync::GraphQLApi`

Layanan	Sumber daya yang dibutuhkan
AWS Backup	`AWS::Backup::RecoveryPoint`
AWS Certificate Manager (ACM)	`AWS::ACM::Certificate`
AWS CloudFormation	`AWS::CloudFormation::Stack`
Amazon CloudFront	`AWS::CloudFront::Distribution`
AWS CodeBuild	`AWS::CodeBuild::Project`

AWS Database Migration Service (AWS DMS)	`AWS::DMS::Endpoint`
	`AWS::DMS::ReplicationInstance`
	`AWS::DMS::ReplicationTask`

Amazon DynamoDB	`AWS::DynamoDB::Table`

Amazon EC2 Systems Manager (SSM)	`AWS::SSM::AssociationCompliance`
	`AWS::SSM::ManagedInstanceInventory`
	`AWS::SSM::PatchCompliance`

Layanan	Sumber daya yang dibutuhkan

Amazon Elastic Compute Cloud (EC2)	`AWS::EC2::ClientVpnEndpoint`
	`AWS::EC2::Instance`
	`AWS::EC2::LaunchTemplate`
	`AWS::EC2::NetworkAcl`
	`AWS::EC2::NetworkInterface`
	`AWS::EC2::SecurityGroup`
	`AWS::EC2::Subnet`
	`AWS::EC2::TransitGateway`
	`AWS::EC2::VPNConnection`
	`AWS::EC2::Volume`

Amazon EC2 Auto Scaling	`AWS::AutoScaling::AutoScalingGroup` `AWS::AutoScaling::LaunchConfiguration`
Amazon Elastic Container Registry (Amazon ECR)	`AWS::ECR::Repository`

Amazon Elastic Container Service (Amazon ECS)	`AWS::ECS::Cluster`
	`AWS::ECS::Service`
	`AWS::ECS::TaskDefinition`

Amazon Elastic File System (Amazon EFS)	`AWS::EFS::AccessPoint`
Amazon EKS	`AWS::EKS::Cluster`

Layanan	Sumber daya yang dibutuhkan
ElasticBeanstalk	`AWS::ElasticBeanstalk::Environment`
Penyeimbang Beban Elastis	`AWS::ElasticLoadBalancing::LoadBalancer` `AWS::ElasticLoadBalancingV2::LoadBalancer`
ElasticSearch	`AWS::Elasticsearch::Domain`

AWS Identity and Access Management (IAM)	`AWS::IAM::Group`
	`AWS::IAM::Policy`
	`AWS::IAM::Role`
	`AWS::IAM::User`

AWS Key Management Service (AWS KMS)	`AWS::KMS::Key`
Amazon Kinesis	`AWS::Kinesis::Stream`
AWS Lambda	`AWS::Lambda::Function`
Amazon MSK	`AWS::MSK::Cluster`

AWS Network Firewall	`AWS::NetworkFirewall::Firewall`
	`AWS::NetworkFirewall::FirewallPolicy`
	`AWS::NetworkFirewall::RuleGroup`

OpenSearch Layanan Amazon	`AWS::OpenSearch::Domain`

Layanan	Sumber daya yang dibutuhkan

Amazon Relational Database Service (Amazon RDS)	`AWS::RDS::DBCluster`
	`AWS::RDS::DBClusterSnapshot`
	`AWS::RDS::DBInstance`
	`AWS::RDS::DBSnapshot`
	`AWS::RDS::EventSubscription`

Amazon Redshift	`AWS::Redshift::Cluster`
Amazon Route 53	`AWS::Route53::HostedZone`

Amazon Simple Storage Service (Amazon S3)	`AWS::S3::AccessPoint`
	`AWS::S3::AccountPublicAccessBlock`
	`AWS::S3::Bucket`

Amazon Simple Notification Service (Amazon SNS)	`AWS::SNS::Topic`
Amazon Simple Queue Service (Amazon SQS)	`AWS::SQS::Queue`
Amazon SageMaker	`AWS::SageMaker::NotebookInstance`
AWS Secrets Manager	`AWS::SecretsManager::Secret`
AWS Step Functions	`AWS::StepFunctions::StateMachine`

Layanan	Sumber daya yang dibutuhkan

AWS WAF	`AWS::WAF::Rule`
	`AWS::WAF::RuleGroup`
	`AWS::WAF::WebACL`
	`AWS::WAFRegional::Rule`
	`AWS::WAFRegional::RuleGroup`
	`AWS::WAFRegional::WebACL`
	`AWS::WAFv2::RuleGroup`
	`AWS::WAFv2::WebACL`

Sumber daya yang diperlukan untuk Tolok Ukur AWS Yayasan CIS

Untuk menjalankan pemeriksaan keamanan untuk kontrol yang diaktifkan yang berlaku pada Tolok Ukur AWS Yayasan Center for Internet Security (CIS), Security Hub menjalankan langkah-langkah audit yang tepat yang ditentukan untuk pemeriksaan di Securing Amazon Web Services atau menggunakan aturan terkelola tertentu AWS Config .

Untuk informasi lebih lanjut tentang standar ini, lihatTolok Ukur AWS Yayasan CIS.

Sumber daya yang diperlukan untuk CIS v3.0.0

Agar Security Hub melaporkan temuan secara akurat untuk kontrol yang dipicu perubahan CIS v3.0.0 yang diaktifkan yang menggunakan AWS Config aturan, Anda harus mencatat sumber daya ini. AWS Config

Layanan	Sumber daya yang dibutuhkan

Amazon Elastic Compute Cloud (Amazon EC2)	`AWS::EC2::Instance`
	`AWS::EC2::NetworkAcl`
	`AWS::EC2::SecurityGroup`

Layanan	Sumber daya yang dibutuhkan

AWS Identity and Access Management (IAM)	`AWS::IAM::Group`
	`AWS::IAM::User`
	`AWS::IAM::Role`

Amazon Relational Database Service (Amazon RDS)	`AWS::RDS::DBInstance`
Amazon Simple Storage Service (Amazon S3)	`AWS::S3::Bucket`

Sumber daya yang dibutuhkan untuk CIS v1.4.0

Agar Security Hub melaporkan temuan secara akurat untuk kontrol yang dipicu perubahan CIS v1.4.0 yang diaktifkan yang menggunakan AWS Config aturan, Anda harus mencatat sumber daya ini. AWS Config

Layanan	Sumber daya yang dibutuhkan
Amazon Elastic Compute Cloud (EC2)	`AWS::EC2::NetworkAcl` `AWS::EC2::SecurityGroup`
AWS Identity and Access Management (IAM)	`AWS::IAM::Policy` `AWS::IAM::User`
Amazon Relational Database Service (Amazon RDS)	`AWS::RDS::DBInstance`
Amazon Simple Storage Service (Amazon S3)	`AWS::S3::Bucket`

Sumber daya yang diperlukan untuk CIS v1.2.0

Agar Security Hub melaporkan temuan secara akurat untuk kontrol yang dipicu perubahan CIS v1.2.0 yang diaktifkan yang menggunakan AWS Config aturan, Anda harus mencatat sumber daya ini. AWS Config

Layanan	Sumber daya yang dibutuhkan
Amazon Elastic Compute Cloud (EC2)	`AWS::EC2::SecurityGroup`
AWS Identity and Access Management (IAM)	`AWS::IAM::Policy` `AWS::IAM::User`

Sumber daya yang diperlukan untuk NIST SP 800-53 Rev. 5

Agar Security Hub dapat secara akurat melaporkan temuan untuk mengaktifkan National Institute of Standards and Technology (NIST) SP 800-53 Rev. 5 mengubah kontrol yang dipicu yang menggunakan AWS Config aturan, Anda harus mencatat sumber daya ini. AWS Config Anda hanya perlu merekam sumber daya untuk kontrol yang memiliki jenis perubahan jadwal yang dipicu. Untuk informasi lebih lanjut tentang standar ini, lihatInstitut Nasional Standar dan Teknologi (NIST) SP 800-53 Rev. 5.

Layanan	Sumber daya yang dibutuhkan
Amazon API Gateway	`AWS::ApiGateway::Stage` `AWS::ApiGatewayV2::Stage`
AWS AppSync	`AWS::AppSync::GraphQLApi`
AWS Backup	`AWS::Backup::RecoveryPoint`
AWS Certificate Manager (ACM)	`AWS::ACM::Certificate`
AWS CloudFormation	`AWS::CloudFormation::Stack`
Amazon CloudFront	`AWS::CloudFront::Distribution`
Amazon CloudWatch	`AWS::CloudWatch::Alarm`
AWS CodeBuild	`AWS::CodeBuild::Project`
AWS Database Migration Service (AWS DMS)	`AWS::DMS::Endpoint` `AWS::DMS::ReplicationInstance`

Layanan	Sumber daya yang dibutuhkan
	`AWS::DMS::ReplicationTask`
Amazon DynamoDB	`AWS::DynamoDB::Table`

Amazon Elastic Compute Cloud (EC2)	`AWS::EC2::ClientVpnEndpoint`
	`AWS::EC2::EIP`
	`AWS::EC2::Instance`
	`AWS::EC2::LaunchTemplate`
	`AWS::EC2::NetworkAcl`
	`AWS::EC2::NetworkInterface`
	`AWS::EC2::SecurityGroup`
	`AWS::EC2::Subnet`
	`AWS::EC2::TransitGateway`
	`AWS::EC2::VPNConnection`
	`AWS::EC2::Volume`

Amazon EC2 Auto Scaling	`AWS::AutoScaling::AutoScalingGroup` `AWS::AutoScaling::LaunchConfiguration`
Amazon Elastic Container Registry (Amazon ECR)	`AWS::ECR::Repository`

Amazon Elastic Container Service (Amazon ECS)	`AWS::ECS::Cluster`
	`AWS::ECS::Service`
	`AWS::ECS::TaskDefinition`

Layanan	Sumber daya yang dibutuhkan
Amazon Elastic File System (Amazon EFS)	`AWS::EFS::AccessPoint`
Amazon EKS	`AWS::EKS::Cluster`
ElasticBeanstalk	`AWS::ElasticBeanstalk::Environment`
Penyeimbang Beban Elastis	`AWS::ElasticLoadBalancing::LoadBalancer` `AWS::ElasticLoadBalancingV2::LoadBalancer`
ElasticSearch	`AWS::Elasticsearch::Domain`
Amazon EventBridge	`AWS::Events::Endpoint` `AWS::Events::EventBus`

AWS Identity and Access Management (IAM)	`AWS::IAM::Group`
	`AWS::IAM::Policy`
	`AWS::IAM::Role`
	`AWS::IAM::User`

AWS Key Management Service (AWS KMS)	`AWS::KMS::Alias` `AWS::KMS::Key`
Amazon Kinesis	`AWS::Kinesis::Stream`
AWS Lambda	`AWS::Lambda::Function`
Amazon MSK	`AWS::MSK::Cluster`
Amazon MQ	`AWS::AmazonMQ::Broker`

Layanan	Sumber daya yang dibutuhkan

AWS Network Firewall	`AWS::NetworkFirewall::Firewall`
	`AWS::NetworkFirewall::FirewallPolicy`
	`AWS::NetworkFirewall::RuleGroup`

OpenSearch Layanan Amazon	`AWS::OpenSearch::Domain`

Amazon Relational Database Service (Amazon RDS)	`AWS::RDS::DBCluster`
	`AWS::RDS::DBClusterSnapshot`
	`AWS::RDS::DBInstance`
	`AWS::RDS::DBSnapshot`
	`AWS::RDS::EventSubscription`

Amazon Redshift	`AWS::Redshift::Cluster`
Amazon Route 53	`AWS::Route53::HostedZone`

Amazon Simple Storage Service (Amazon S3)	`AWS::S3::AccountPublicAccessBlock`
	`AWS::S3::AccessPoint`
	`AWS::S3::Bucket`

AWS Service Catalog	`AWS::ServiceCatalog::Portfolio`
Amazon Simple Notification Service (Amazon SNS)	`AWS::SNS::Topic`
Amazon Simple Queue Service (Amazon SQS)	`AWS::SQS::Queue`

Layanan	Sumber daya yang dibutuhkan

Amazon EC2 Systems Manager (SSM)	`AWS::SSM::AssociationCompliance`
	`AWS::SSM::ManagedInstanceInventory`
	`AWS::SSM::PatchCompliance`

Amazon SageMaker	`AWS::SageMaker::NotebookInstance`
AWS Secrets Manager	`AWS::SecretsManager::Secret`

AWS WAF	`AWS::WAF::Rule`
	`AWS::WAF::RuleGroup`
	`AWS::WAF::WebACL`
	`AWS::WAFRegional::Rule`
	`AWS::WAFRegional::RuleGroup`
	`AWS::WAFRegional::WebACL`
	`AWS::WAFv2::RuleGroup`
	`AWS::WAFv2::WebACL`

Sumber daya yang dibutuhkan untuk PCI DSS v3.2.1

Agar Security Hub melaporkan temuan secara akurat untuk kontrol Standar Keamanan Data Industri Kartu Pembayaran (PCI DSS) yang diaktifkan yang menggunakan AWS Config aturan, Anda harus mencatat sumber daya ini. AWS Config Untuk informasi lebih lanjut tentang standar ini, lihatStandar Keamanan Data Industri Kartu Pembayaran (PCI DSS).

Layanan	Sumber daya yang dibutuhkan
AWS CodeBuild	`AWS::CodeBuild::Project`

Layanan	Sumber daya yang dibutuhkan

Amazon Elastic Compute Cloud (EC2)	`AWS::EC2::EIP`
	`AWS::EC2::Instance`
	`AWS::EC2::SecurityGroup`

Amazon EC2 Auto Scaling	`AWS::AutoScaling::AutoScalingGroup`
AWS Identity and Access Management (IAM)	`AWS::IAM::Policy` `AWS::IAM::User`
AWS Lambda	`AWS::Lambda::Function`
OpenSearch Layanan Amazon	`AWS::OpenSearch::Domain`

Amazon Relational Database Service (Amazon RDS)	`AWS::RDS::DBClusterSnapshot`
	`AWS::RDS::DBInstance`
	`AWS::RDS::DBSnapshot`

Amazon Redshift	`AWS::Redshift::Cluster`
Amazon Simple Storage Service (Amazon S3)	`AWS::S3::AccountPublicAccesssBlock` `AWS::S3::Bucket`

Amazon EC2 Systems Manager (SSM)	`AWS::SSM::AssociationCompliance`
	`AWS::SSM::ManagedInstanceInventory`
	`AWS::SSM::PatchCompliance`

Sumber daya yang diperlukan untuk AWS Standar Penandaan Sumber Daya

Semua kontrol dalam Standar Penandaan AWS Sumber Daya dipicu perubahan dan menggunakan AWS Config aturan. Agar Security Hub melaporkan temuan untuk kontrol ini secara akurat, Anda harus mencatat sumber daya berikut AWS Config. Anda hanya perlu merekam sumber daya untuk kontrol yang memiliki jenis perubahan jadwal yang dipicu. Untuk informasi lebih lanjut tentang standar ini, lihatAWS Standar Penandaan Sumber Daya.

Layanan	Sumber daya yang dibutuhkan
AWS AppSync	`AWS::AppSync::GraphQLApi`
Amazon Athena	`AWS::Athena::DataCatalog` `AWS::Athena::WorkGroup`
AWS Certificate Manager (ACM)	`AWS::ACM::Certificate`

AWS Backup (AWS Backup)	`AWS::Backup::BackupPlan`
	`AWS::Backup::BackupVault`
	`AWS::Backup::RecoveryPlan`
	`AWS::Backup::ReportPlan`

AWS CloudFormation	`AWS::CloudFormation::Stack`
Amazon CloudFront	`AWS::CloudFront::Distribution`
AWS CloudTrail	`AWS::CloudTrail::Trail`
AWS CodeArtifact	`AWS::CodeArtifact::Repository`
Amazon Detective	`AWS::Detective::Graph`

AWS Database Migration Service (AWS DMS)	`AWS::DMS::Certificate`
	`AWS::DMS::EventSubscription`
	`AWS::DMS::ReplicationInstance`

Layanan	Sumber daya yang dibutuhkan
	`AWS::DMS::ReplicationSubnetGroup`
Amazon DynamoDB	`AWS::DynamoDB::Trail`

Layanan	Sumber daya yang dibutuhkan

Amazon Elastic Compute Cloud (EC2)	`AWS::EC2::CustomerGateway`
	`AWS::EC2::EIP`
	`AWS::EC2::FlowLog`
	`AWS::EC2::Instance`
	`AWS::EC2::InternetGateway`
	`AWS::EC2::NatGateway`
	`AWS::EC2::NetworkAcl`
	`AWS::EC2::NetworkInterface`
	`AWS::EC2::RouteTable`
	`AWS::EC2::SecurityGroup`
	`AWS::EC2::Subnet`
	`AWS::EC2::TransitGateway`
	`AWS::EC2::TransitGatewayAttachment`
	`AWS::EC2::TransitGatewayRouteTable`
	`AWS::EC2::Volume`
	`AWS::EC2::VPC`
	`AWS::EC2::VPCEndpointService`
	`AWS::EC2::VPCPeeringConnection`
	`AWS::EC2::VPNGateway`

Layanan	Sumber daya yang dibutuhkan
Amazon EC2 Auto Scaling	`AWS::AutoScaling::AutoScalingGroup`
Amazon Elastic Container Registry (Amazon ECR)	`AWS::ECR::PublicRepository`

Amazon Elastic Container Service (Amazon ECS)	`AWS::ECS::Cluster`
	`AWS::ECS::Service`
	`AWS::ECS::TaskDefinition`

Amazon Elastic File System (Amazon EFS)	`AWS::EFS::AccessPoint`
Amazon Elastic Kubernetes Service (Amazon EKS)	`AWS::EKS::Cluster` `AWS::EKS::IdentityProviderConfig`
AWS Elastic Beanstalk (Elastic Beanstalk)	`AWS::ElasticBeanstalk::Environment`
ElasticSearch	`AWS::Elasticsearch::Domain`
Amazon EventBridge	`AWS::Events::EventBus`
AWS Global Accelerator	`AWS::GlobalAccelerator::Accelerator`
AWS Glue	`AWS::Glue::Job`

Amazon GuardDuty	`AWS::GuardDuty::Detector`
	`AWS::GuardDuty::Filter`
	`AWS::GuardDuty::IPSet`

AWS Identity and Access Management (IAM)	`AWS::IAM::Role` `AWS::IAM::User`

Layanan	Sumber daya yang dibutuhkan
AWS Identity and Access Management Access Analyzer (Penganalisis Akses IAM)	`AWS::AccessAnalyzer::Analyzer`

AWS IoT	`AWS::IoT::Authorizer`
	`AWS::IoT::Dimension`
	`AWS::IoT::MitigationAction`
	`AWS::IoT::Policy`
	`AWS::IoT::RoleAlias`
	`AWS::IoT::SecurityProfile`

Amazon Kinesis	`AWS::Kinesis::Stream`
AWS Lambda	`AWS::Lambda::Function`
Amazon MQ	`AWS::AmazonMQ::Broker`
AWS Network Firewall	`AWS::NetworkFirewall::Firewall` `AWS::NetworkFirewall::FirewallPolicy`
OpenSearch Layanan Amazon	`AWS::OpenSearch::Domain`

Amazon Relational Database Service	`AWS::RDS::DBCluster`
	`AWS::RDS::DBClusterSnapshot`
	`AWS::RDS::DBInstance`
	`AWS::RDS::DBSecurityGroup`
	`AWS::RDS::DBSnapshot`
	`AWS::RDS::DBSubnetGroup`

Layanan	Sumber daya yang dibutuhkan

Amazon Redshift	`AWS::Redshift::Cluster`
	`AWS::Redshift::ClusterSnapshot`
	`AWS::Redshift::ClusterSubnetGroup`
	`AWS::Redshift::EventSubscription`

Amazon Route 53	`AWS::Route53::HealthCheck`
AWS Secrets Manager	`AWS::SecretsManager::Secret`
Amazon Simple Email Service (Amazon SES)	`AWS::SES::ConfigurationSet` `AWS::SES::ContactList`
Amazon Simple Notification Service (Amazon SNS)	`AWS::SNS::Topic`
Amazon Simple Queue Service (Amazon SQS)	`AWS::SQS::Queue`
AWS Step Functions	`AWS::StepFunctions::Activity`
AWS Transfer Family	`AWS::Transfer::Workflow`

Sumber daya yang diperlukan untuk Standar yang Dikelola Layanan: AWS Control Tower

Agar Security Hub melaporkan temuan secara akurat untuk Standar yang Dikelola Layanan yang diaktifkan: AWS Control Tower ubah kontrol yang dipicu yang menggunakan AWS Config aturan, Anda harus mencatat sumber daya berikut. AWS Config Untuk informasi lebih lanjut tentang standar ini, lihatStandar yang Dikelola Layanan: AWS Control Tower.

Layanan	Sumber daya yang dibutuhkan
Amazon API Gateway	`AWS::ApiGateway::Stage`

Layanan	Sumber daya yang dibutuhkan
	`AWS::ApiGatewayV2::Stage`
AWS Certificate Manager (ACM)	`AWS::ACM::Certificate`
AWS CodeBuild	`AWS::CodeBuild::Project`
Amazon DynamoDB	`AWS::DynamoDB::Table`

Amazon Elastic Compute Cloud (EC2)	`AWS::EC2::Instance`
	`AWS::EC2::NetworkAcl`
	`AWS::EC2::NetworkInterface`
	`AWS::EC2::SecurityGroup`
	`AWS::EC2::Subnet`
	`AWS::EC2::VPNConnection`
	`AWS::EC2::Volume`

Amazon EC2 Auto Scaling	`AWS::AutoScaling::AutoScalingGroup` `AWS::AutoScaling::LaunchConfiguration`
Amazon Elastic Container Registry (Amazon ECR)	`AWS::ECR::Repository`

Amazon Elastic Container Service (Amazon ECS)	`AWS::ECS::Cluster`
	`AWS::ECS::Service`
	`AWS::ECS::TaskDefinition`

Amazon Elastic File System (Amazon EFS)	`AWS::EFS::AccessPoint`
Amazon EKS	`AWS::EKS::Cluster`

Layanan	Sumber daya yang dibutuhkan
ElasticBeanstalk	`AWS::ElasticBeanstalk::Environment`
Penyeimbang Beban Elastis	`AWS::ElasticLoadBalancing::LoadBalancer` `AWS::ElasticLoadBalancingV2::LoadBalancer`
ElasticSearch	`AWS::Elasticsearch::Domain`

AWS Identity and Access Management (IAM)	`AWS::IAM::Group`
	`AWS::IAM::Policy`
	`AWS::IAM::Role`
	`AWS::IAM::User`

AWS Key Management Service (AWS KMS)	`AWS::KMS::Alias` `AWS::KMS::Key`
Amazon Kinesis	`AWS::Kinesis::Stream`
AWS Lambda	`AWS::Lambda::Function`
AWS Network Firewall	`AWS::NetworkFirewall::FirewallPolicy` `AWS::NetworkFirewall::RuleGroup`
OpenSearch Layanan Amazon	`AWS::OpenSearch::Domain`

Layanan	Sumber daya yang dibutuhkan

Amazon Relational Database Service (Amazon RDS)	`AWS::RDS::DBCluster`
	`AWS::RDS::DBClusterSnapshot`
	`AWS::RDS::DBInstance`
	`AWS::RDS::DBSnapshot`
	`AWS::RDS::EventSubscription`

Amazon Redshift	`AWS::Redshift::Cluster`
Amazon Simple Storage Service (Amazon S3)	`AWS::S3::AccountPublicAccessBlock` `AWS::S3::Bucket`
Amazon Simple Notification Service (Amazon SNS)	`AWS::SNS::Topic`
Amazon Simple Queue Service (Amazon SQS)	`AWS::SQS::Queue`

Amazon EC2 Systems Manager (SSM)	`AWS::SSM::AssociationCompliance`
	`AWS::SSM::ManagedInstanceInventory`
	`AWS::SSM::PatchCompliance`

AWS Secrets Manager	`AWS::SecretsManager::Secret`

AWS WAF	`AWS::WAFRegional::Rule`
	`AWS::WAFRegional::RuleGroup`
	`AWS::WAFRegional::WebACL`
	`AWS::WAFv2::WebACL`

Jadwal untuk menjalankan pemeriksaan keamanan

Setelah Anda mengaktifkan standar keamanan, AWS Security Hub mulai menjalankan semua pemeriksaan dalam waktu dua jam. Sebagian besar pemeriksaan mulai berjalan dalam 25 menit. Security Hub menjalankan pemeriksaan dengan mengevaluasi aturan yang mendasari kontrol. Sampai kontrol menyelesaikan pemeriksaan pertamanya, statusnya adalah Tidak ada data.

Saat Anda mengaktifkan standar baru, Security Hub mungkin membutuhkan waktu hingga 24 jam untuk menghasilkan temuan untuk kontrol yang menggunakan aturan AWS Config terkait layanan dasar yang sama dengan kontrol yang diaktifkan dari standar lain yang diaktifkan. Misalnya, jika Anda mengaktifkan Lambda.1 dalam standar Praktik Terbaik Keamanan AWS Dasar (FSBP), Security Hub akan membuat aturan terkait layanan dan biasanya menghasilkan temuan dalam hitungan menit. Setelah ini, jika Anda mengaktifkan Lambda.1 di Standar Keamanan Data Industri Kartu Pembayaran (PCI DSS), Security Hub dapat memakan waktu hingga 24 jam untuk menghasilkan temuan untuk kontrol ini karena menggunakan aturan terkait layanan yang sama dengan Lambda.1.

Setelah pemeriksaan awal, jadwal untuk setiap kontrol dapat berupa periodik atau perubahan yang dipicu.

- Pemeriksaan berkala — Pemeriksaan ini berjalan secara otomatis dalam waktu 12 atau 24 jam setelah proses terbaru. Security Hub menentukan periodisitas, dan Anda tidak dapat mengubahnya. Kontrol periodik mencerminkan evaluasi pada saat pemeriksaan berjalan. Jika Anda memperbarui status alur kerja dari temuan kontrol berkala, dan kemudian pada pemeriksaan berikutnya status kepatuhan temuan tetap sama, status alur kerja tetap dalam status yang diubah. Misalnya, jika Anda memiliki temuan gagal untuk KMS.4 - AWS KMS key rotasi harus diaktifkan, dan kemudian memulihkan temuan, Security Hub mengubah status alur kerja dari ke. `NEW` `RESOLVED` Jika Anda menonaktifkan rotasi kunci KMS sebelum pemeriksaan berkala berikutnya, status alur kerja temuan tetap ada. `RESOLVED`
- Pemeriksaan yang dipicu perubahan - Pemeriksaan ini berjalan saat sumber daya terkait mengubah status. AWS Config memungkinkan Anda memilih antara perekaman terus menerus dari perubahan status sumber daya dan perekaman harian. Jika Anda memilih perekaman harian, AWS Config mengirimkan data konfigurasi sumber daya pada akhir setiap periode 24 jam jika ada perubahan status sumber daya. Jika tidak ada perubahan, tidak ada data yang dikirimkan. Ini dapat menunda pembuatan temuan Security Hub hingga periode 24 jam selesai. Terlepas dari periode perekaman yang Anda pilih, Security Hub memeriksa setiap 18 jam untuk memastikan tidak ada pembaruan sumber daya yang AWS Config terlewatkan.

Secara umum, Security Hub menggunakan aturan yang dipicu perubahan bila memungkinkan. Agar sumber daya menggunakan aturan yang dipicu perubahan, ia harus mendukung item AWS Config konfigurasi.

Untuk kontrol yang didasarkan pada AWS Config aturan terkelola, deskripsi kontrol menyertakan tautan ke deskripsi aturan di Panduan AWS Config Pengembang. Deskripsi itu mencakup apakah aturan tersebut dipicu perubahan atau periodik.

Pemeriksaan yang menggunakan fungsi Lambda kustom Security Hub bersifat periodik.

Menghasilkan dan memperbarui temuan kontrol

AWS Security Hub menghasilkan temuan dengan menjalankan pemeriksaan terhadap kontrol keamanan. Temuan ini menggunakan AWS Security Finding Format (ASFF). Perhatikan bahwa jika ukuran temuan melebihi maksimum 240 KB, maka `Resource.Details` objek dihapus. Untuk kontrol yang didukung oleh AWS Config sumber daya, Anda dapat melihat detail sumber daya di AWS Config konsol.

Security Hub biasanya mengenakan biaya untuk setiap pemeriksaan keamanan untuk kontrol. Namun, jika beberapa kontrol menggunakan AWS Config aturan yang sama, maka Security Hub hanya mengenakan biaya sekali untuk setiap pemeriksaan terhadap AWS Config aturan tersebut. Jika Anda mengaktifkan temuan kontrol konsolidasi, Security Hub menghasilkan satu temuan untuk pemeriksaan keamanan meskipun kontrol disertakan dalam beberapa standar yang diaktifkan.

Misalnya, AWS Config aturan `iam-password-policy` ini digunakan oleh beberapa kontrol dalam standar Tolok Ukur AWS Yayasan Center for Internet Security (CIS) dan standar Praktik Terbaik Keamanan Dasar. Setiap kali Security Hub menjalankan pemeriksaan terhadap AWS Config aturan itu, ia menghasilkan temuan terpisah untuk setiap kontrol terkait, tetapi hanya mengenakan biaya sekali untuk pemeriksaan.

Temuan kontrol terkonsolidasi

Ketika temuan kontrol konsolidasi diaktifkan di akun Anda, Security Hub menghasilkan satu temuan baru atau menemukan pembaruan untuk setiap pemeriksaan keamanan kontrol, bahkan jika kontrol berlaku untuk beberapa standar yang diaktifkan. Untuk melihat daftar kontrol dan standar yang mereka terapkan, lihatReferensi kontrol Security Hub. Anda dapat mengaktifkan atau menonaktifkan temuan kontrol terkonsolidasi. Kami merekomendasikan untuk menyalakannya untuk mengurangi kebisingan temuan.

Jika Anda mengaktifkan Security Hub Akun AWS sebelum 23 Februari 2023, Anda harus mengaktifkan temuan kontrol konsolidasi dengan mengikuti petunjuk nanti di bagian ini. Jika Anda mengaktifkan Security Hub pada atau setelah 23 Februari 2023, temuan kontrol konsolidasi diaktifkan secara otomatis di akun Anda. Namun, jika Anda menggunakan integrasi Security Hub dengan AWS Organizations atau akun anggota yang diundang melalui proses undangan manual, temuan kontrol konsolidasi diaktifkan di akun anggota hanya jika diaktifkan di akun administrator. Jika fitur dimatikan di akun administrator, itu dimatikan di akun anggota. Perilaku ini berlaku untuk akun anggota baru dan yang sudah ada.

Jika Anda menonaktifkan temuan kontrol konsolidasi di akun Anda, Security Hub akan menghasilkan temuan terpisah per pemeriksaan keamanan untuk setiap standar yang diaktifkan yang menyertakan kontrol. Misalnya, jika empat standar yang diaktifkan berbagi kontrol dengan AWS Config aturan dasar yang sama, Anda menerima empat temuan terpisah setelah pemeriksaan keamanan kontrol. Jika Anda mengaktifkan temuan kontrol terkonsolidasi, Anda hanya menerima satu temuan. Untuk informasi lebih lanjut tentang bagaimana konsolidasi memengaruhi temuan Anda, lihatTemuan kontrol sampel.

Saat Anda mengaktifkan temuan kontrol konsolidasi, Security Hub menciptakan temuan agnostik standar baru dan mengarsipkan temuan berbasis standar asli. Beberapa bidang dan nilai pencarian kontrol akan berubah dan dapat memengaruhi alur kerja yang ada. Untuk informasi lebih lanjut tentang perubahan ini, lihatTemuan kontrol konsolidasi - perubahan ASFF.

Mengaktifkan temuan kontrol konsolidasi juga dapat memengaruhi temuan yang diterima integrasi pihak ketiga dari Security Hub. Respon Keamanan Otomatis pada AWS v2.0.0 mendukung temuan kontrol terkonsolidasi.

Mengaktifkan temuan kontrol terkonsolidasi

Untuk mengaktifkan temuan kontrol konsolidasi, Anda harus masuk ke akun administrator atau akun mandiri.

> **Note**
>
> Setelah mengaktifkan temuan kontrol konsolidasi, mungkin diperlukan waktu hingga 24 jam untuk Security Hub untuk menghasilkan temuan baru yang terkonsolidasi dan mengarsipkan temuan asli berbasis standar. Selama waktu itu, Anda mungkin melihat campuran temuan agnostik standar dan berbasis standar di akun Anda.

Security Hub console

1. Buka AWS Security Hub konsol di https://console.aws.amazon.com/securityhub/.
2. Pada panel navigasi, silakan pilih Pengaturan.
3. Pilih tab Umum.
4. Untuk Kontrol, aktifkan Temuan kontrol konsolidasi.
5. Pilih Simpan.

Security Hub API

1. Jalankan `UpdateSecurityHubConfiguration`.
2. Tetapkan `ControlFindingGenerator` sama dengan`SECURITY_CONTROL`.

   Permintaan contoh:

```
{
   "ControlFindingGenerator": "SECURITY_CONTROL"
}
```

AWS CLI

1. Jalankan perintah `update-security-hub-configuration`.
2. Tetapkan `control-finding-generator` sama dengan`SECURITY_CONTROL`.

```
aws securityhub  --region us-east-1 update-security-hub-configuration --control-finding-generator SECURITY_CONTROL
```

Mematikan temuan kontrol konsolidasi

Untuk menonaktifkan temuan kontrol konsolidasi, Anda harus masuk ke akun administrator atau akun mandiri.

> **Note**
>
> Setelah mematikan temuan kontrol konsolidasi, mungkin diperlukan waktu hingga 24 jam untuk Security Hub untuk menghasilkan temuan baru berbasis standar dan mengarsipkan

temuan konsolidasi. Selama waktu itu, Anda mungkin melihat campuran temuan berbasis standar dan konsolidasi di akun Anda.

Security Hub console

1. Buka AWS Security Hub konsol di https://console.aws.amazon.com/securityhub/.
2. Pada panel navigasi, silakan pilih Pengaturan.
3. Pilih tab Umum.
4. Untuk Kontrol, pilih Edit dan matikan Temuan kontrol konsolidasi.
5. Pilih Simpan.

Security Hub API

1. Jalankan `UpdateSecurityHubConfiguration`.
2. Tetapkan `ControlFindingGenerator` sama dengan`STANDARD_CONTROL`.

   Permintaan contoh:

```
{
   "ControlFindingGenerator": "STANDARD_CONTROL"
}
```

AWS CLI

1. Jalankan perintah `update-security-hub-configuration`.
2. Tetapkan `control-finding-generator` sama dengan`STANDARD_CONTROL`.

```
aws securityhub  --region us-east-1 update-security-hub-configuration --control-finding-generator STANDARD_CONTROL
```

`Compliance`rincian untuk temuan kontrol

Untuk temuan yang dihasilkan oleh pemeriksaan keamanan kontrol, `Compliance`bidang dalam AWS Security Finding Format (ASFF) berisi rincian yang terkait dengan temuan kontrol. `Compliance`Bidang ini mencakup informasi berikut.

`AssociatedStandards`

Standar yang diaktifkan di mana kontrol diaktifkan.

`RelatedRequirements`

Daftar persyaratan terkait untuk kontrol di semua standar yang diaktifkan. Persyaratannya berasal dari kerangka keamanan pihak ketiga untuk kontrol, seperti Standar Keamanan Data Industri Kartu Pembayaran (PCI DSS).

`SecurityControlId`

Pengidentifikasi untuk kontrol di seluruh standar keamanan yang didukung Security Hub.

`Status`

Hasil pemeriksaan terbaru bahwa Security Hub berjalan untuk kontrol yang diberikan. Hasil pemeriksaan sebelumnya disimpan dalam keadaan diarsipkan selama 90 hari.

`StatusReasons`

Berisi daftar alasan untuk nilai`Compliance.Status`. Untuk setiap alasan, `StatusReasons` sertakan kode alasan dan deskripsi.

Tabel berikut mencantumkan kode alasan status dan deskripsi yang tersedia. Langkah-langkah remediasi tergantung pada kontrol mana yang menghasilkan temuan dengan kode alasan. Pilih kontrol dari Referensi kontrol Security Hub untuk melihat langkah-langkah remediasi untuk kontrol itu.

Kode alasan	Compliance.Status	Deskripsi
`CLOUDTRAIL_METRIC_FILTER_NOT_VALID`	`FAILED`	CloudTrail Jejak Multi-wilayah tidak memiliki filter metrik yang valid.
`CLOUDTRAIL_METRIC_FILTERS_NOT_PRESENT`	`FAILED`	Filter metrik tidak ada untuk CloudTrail jejak Multi-wilayah.
`CLOUDTRAIL_MULTI_REGION_NOT_PRESENT`	`FAILED`	Akun tidak memiliki CloudTrail jejak Multi-wilayah dengan konfigurasi yang diperlukan.

Kode alasan	Compliance.Status	Deskripsi
CLOUDTRAIL_REGION_INVAILD	WARNING	CloudTrail Jalur Multi-Region tidak berada di Wilayah saat ini.
CLOUDWATCH_ALARM_ACTIONS_NOT_VALID	FAILED	Tidak ada tindakan alarm yang valid.
CLOUDWATCH_ALARMS_NOT_PRESENT	FAILED	CloudWatch alarm tidak ada di akun.
CONFIG_ACCESS_DENIED	NOT_AVAILABLE AWS Config Status adalah ConfigError	AWS Config akses ditolak. Verifikasi bahwa AWS Config diaktifkan dan telah diberikan izin yang cukup.
CONFIG_EVALUATIONS_EMPTY	PASSED	AWS Config mengevaluasi sumber daya Anda berdasarkan aturan. Aturan tidak berlaku untuk AWS sumber daya dalam ruang lingkupnya, sumber daya yang ditentukan dihapus, atau hasil evaluasi dihapus.

Kode alasan	Compliance.Status	Deskripsi
`CONFIG_RETURNS_NOT_APPLICABLE`	`NOT_AVAILABLE`	Status kepatuhan adalah `NOT_AVAILABLE` karena AWS Config mengembalikan status Tidak Berlaku. AWS Config tidak memberikan alasan untuk status tersebut. Berikut adalah beberapa kemungkinan alasan untuk status Tidak Berlaku: • Sumber daya telah dihapus dari ruang lingkup AWS Config aturan. • AWS Config Aturan itu dihapus. • Sumber daya telah dihapus. • Logika AWS Config aturan dapat menghasilkan status Tidak Berlaku.

Kode alasan	Compliance.Status	Deskripsi
`CONFIG_RULE_EVALUATION_ERROR`	`NOT_AVAILABLE` AWS Config Status adalah `ConfigError`	Kode alasan ini digunakan untuk beberapa jenis kesalahan evaluasi. Deskripsi memberikan informasi alasan spesifik. Jenis kesalahan dapat berupa salah satu dari yang berikut: • Ketidakmampuan untuk melakukan evaluasi karena kurangnya izin. Deskripsi memberikan izin khusus yang hilang. • Nilai yang hilang atau tidak valid untuk parameter. Deskripsi memberikan parameter dan persyaratan untuk nilai parameter. • Kesalahan membaca dari ember S3. Deskripsi mengidentifikasi ember dan memberikan kesalahan spesifik. • AWS Langganan yang hilang. • Batas waktu umum pada evaluasi. • Akun yang ditangguhkan.
`CONFIG_RULE_NOT_FOUND`	`NOT_AVAILABLE` AWS Config Status adalah `ConfigError`	AWS Config Aturannya sedang dalam proses diciptakan.
`INTERNAL_SERVICE_ERROR`	`NOT_AVAILABLE`	Terjadi kesalahan yang tidak diketahui.

Kode alasan	Complianc e.Status	Deskripsi
`LAMBDA_CUSTOM_RUNT IME_DETAILS_NOT_AV AILABLE`	FAILED	Security Hub tidak dapat melakukan pemeriksaan terhadap runtime Lambda kustom.
`S3_BUCKET_CROSS_AC COUNT_CROSS_REGION`	`WARNING`	Temuan ini dalam `WARNING` keadaan, karena bucket S3 yang dikaitkan dengan aturan ini berada di Wilayah atau akun yang berbeda. Aturan ini tidak mendukung pemeriksaan lintas wilayah atau lintas akun. Disarankan agar Anda menonakti fkan kontrol ini di Wilayah atau akun ini. Jalankan saja di Wilayah atau akun tempat sumber daya berada.
`SNS_SUBSCRIPTION_N OT_PRESENT`	`FAILED`	Filter metrik CloudWatch Log tidak memiliki langganan Amazon SNS yang valid.
`SNS_TOPIC_CROSS_ACCOUNT`	WARNING	Temuan itu dalam `WARNING` keadaan. Topik SNS yang terkait dengan aturan ini dimiliki oleh akun yang berbeda. Akun saat ini tidak dapat memperoleh informasi berlangganan. Akun yang memiliki topik SNS harus memberikan `sns:ListS ubscriptionsByTopic` izin kepada akun saat ini untuk topik SNS.

Kode alasan	Complianc e.Status	Deskripsi
`SNS_TOPIC_CROSS_AC COUNT_CROSS_REGION`	`WARNING`	Temuan ini dalam `WARNING` keadaan karena topik SNS yang terkait dengan aturan ini berada di Wilayah atau akun yang berbeda. Aturan ini tidak mendukung pemeriksaan lintas wilayah atau lintas akun. Disarankan agar Anda menonakti fkan kontrol ini di Wilayah atau akun ini. Jalankan saja di Wilayah atau akun tempat sumber daya berada.
`SNS_TOPIC_INVALID`	`FAILED`	Topik SNS yang terkait dengan aturan ini tidak valid.
`THROTTLING_ERROR`	`NOT_AVAIL ABLE`	Operasi API yang relevan melebihi tarif yang diizinkan.

`ProductFields`rincian untuk temuan kontrol

Saat Security Hub menjalankan pemeriksaan keamanan dan menghasilkan temuan kontrol, `ProductFields` atribut di ASFF menyertakan bidang berikut:

`ArchivalReasons:0/Description`

Menjelaskan mengapa Security Hub telah mengarsipkan temuan yang ada.

Misalnya, Security Hub mengarsipkan temuan yang ada saat Anda menonaktifkan kontrol atau standar dan saat Anda mengaktifkan atau menonaktifkan temuan kontrol konsolidasi.

`ArchivalReasons:0/ReasonCode`

Memberikan alasan mengapa Security Hub telah mengarsipkan temuan yang ada.

Misalnya, Security Hub mengarsipkan temuan yang ada saat Anda menonaktifkan kontrol atau standar dan saat Anda mengaktifkan atau menonaktifkan temuan kontrol konsolidasi.

`StandardsGuideArn` atau `StandardsArn`

ARN dari standar yang terkait dengan kontrol.

Untuk standar CIS AWS Foundations Benchmark, bidangnya adalah. `StandardsGuideArn`

Untuk standar PCI DSS dan AWS Foundational Security Best Practices, bidangnya adalah. `StandardsArn`

Bidang ini dihapus demi `Compliance.AssociatedStandards` jika Anda mengaktifkan temuan kontrol terkonsolidasi.

`StandardsGuideSubscriptionArn` atau `StandardsSubscriptionArn`

ARN berlangganan akun ke standar.

Untuk standar CIS AWS Foundations Benchmark, bidangnya adalah. `StandardsGuideSubscriptionArn`

Untuk standar PCI DSS dan AWS Foundational Security Best Practices, bidangnya adalah. `StandardsSubscriptionArn`

Bidang ini dihapus jika Anda mengaktifkan temuan kontrol konsolidasi.

`RuleId` atau `ControlId`

Pengidentifikasi kontrol.

Untuk standar CIS AWS Foundations Benchmark, bidangnya adalah. `RuleId`

Untuk standar lain, bidangnya`ControlId`.

Bidang ini dihapus demi `Compliance.SecurityControlId` jika Anda mengaktifkan temuan kontrol terkonsolidasi.

`RecommendationUrl`

URL ke informasi remediasi untuk kontrol. Bidang ini dihapus demi `Remediation.Recommendation.Url` jika Anda mengaktifkan temuan kontrol terkonsolidasi.

`RelatedAWSResources:0/name`

Nama sumber daya yang terkait dengan temuan.

`RelatedAWSResource:0/type`

Jenis sumber daya yang terkait dengan kontrol.

`StandardsControlArn`

ARN kontrol. Bidang ini dihapus jika Anda mengaktifkan temuan kontrol konsolidasi.

`aws/securityhub/ProductName`

Untuk temuan berbasis kontrol, nama produknya adalah Security Hub.

`aws/securityhub/CompanyName`

Untuk temuan berbasis kontrol, nama perusahaan adalah. AWS

`aws/securityhub/annotation`

Deskripsi masalah yang ditemukan oleh kontrol.

`aws/securityhub/FindingId`

Pengidentifikasi temuan. Bidang ini tidak mereferensikan standar jika Anda mengaktifkan temuan kontrol terkonsolidasi.

Menetapkan tingkat keparahan untuk mengontrol temuan

Tingkat keparahan yang ditetapkan ke kontrol Security Hub mengidentifikasi pentingnya kontrol. Tingkat keparahan kontrol menentukan label keparahan yang ditetapkan untuk temuan kontrol.

Kriteria keparahan

Tingkat keparahan kontrol ditentukan berdasarkan penilaian kriteria berikut:

- Seberapa sulit bagi aktor ancaman untuk memanfaatkan kelemahan konfigurasi yang terkait dengan kontrol?

  Kesulitan ditentukan oleh jumlah kecanggihan atau kompleksitas yang diperlukan untuk menggunakan kelemahan untuk melakukan skenario ancaman.
- Seberapa besar kemungkinan kelemahan itu akan menyebabkan kompromi terhadap sumber daya Anda Akun AWS atau sumber daya?

  Kompromi terhadap sumber daya Anda Akun AWS berarti kerahasiaan, integritas, atau ketersediaan data atau AWS infrastruktur Anda rusak dalam beberapa cara.

Kemungkinan kompromi menunjukkan seberapa besar kemungkinan skenario ancaman akan mengakibatkan gangguan atau pelanggaran AWS layanan atau sumber daya Anda.

Sebagai contoh, pertimbangkan kelemahan konfigurasi berikut:

- Kunci akses pengguna tidak diputar setiap 90 hari.
- Kunci pengguna root IAM ada.

Kedua kelemahan sama-sama sulit untuk dimanfaatkan musuh. Dalam kedua kasus, musuh dapat menggunakan pencurian kredenal atau metode lain untuk memperoleh kunci pengguna. Mereka kemudian dapat menggunakannya untuk mengakses sumber daya Anda dengan cara yang tidak sah.

Namun, kemungkinan kompromi jauh lebih tinggi jika aktor ancaman memperoleh kunci akses pengguna root karena ini memberi mereka akses yang lebih besar. Akibatnya, kelemahan kunci pengguna root memiliki tingkat keparahan yang lebih tinggi.

Tingkat keparahannya tidak memperhitungkan kekritisan sumber daya yang mendasarinya. Kritikalitas adalah tingkat pentingnya sumber daya yang terkait dengan temuan tersebut. Misalnya, sumber daya yang terkait dengan aplikasi kritis misi lebih penting daripada sumber daya yang terkait dengan pengujian nonproduksi. Untuk menangkap informasi kekritisan sumber daya, gunakan `Criticality` bidang AWS Security Finding Format (ASFF).

Tabel berikut memetakan kesulitan untuk mengeksploitasi dan kemungkinan kompromi dengan label keamanan.

	Kompromi sangat mungkin	Kemungkinan kompromi	Kompromi tidak mungkin	Kompromi sangat tidak mungkin
Sangat mudah untuk dieksploi tasi	Kritis	Kritis	Tinggi	Sedang
Agak mudah untuk dieksploi tasi	Kritis	Tinggi	Sedang	Sedang

Agak sulit untuk dieksploitasi	Tinggi	Sedang	Sedang	Rendah
Sangat sulit untuk dieksploi tasi	Sedang	Sedang	Rendah	Rendah

Definisi keparahan

Label keparahan didefinisikan sebagai berikut.

Kritis — Masalah ini harus segera diperbaiki untuk menghindari eskalasi.

Misalnya, bucket S3 terbuka dianggap sebagai temuan tingkat keparahan kritis. Karena begitu banyak pelaku ancaman memindai bucket S3 terbuka, data dalam bucket S3 yang terbuka kemungkinan akan ditemukan dan diakses oleh orang lain.

Secara umum, sumber daya yang dapat diakses publik dianggap sebagai masalah keamanan kritis. Anda harus memperlakukan temuan kritis dengan sangat mendesak. Anda juga harus mempertimbangkan kekritisan sumber daya.

Tinggi — Masalah ini harus ditangani sebagai prioritas jangka pendek.

Misalnya, jika grup keamanan VPC default terbuka untuk lalu lintas masuk dan keluar, itu dianggap tingkat keparahan tinggi. Agak mudah bagi aktor ancaman untuk mengkompromikan VPC menggunakan metode ini. Kemungkinan juga aktor ancaman akan dapat mengganggu atau mengeksfiltrasi sumber daya begitu mereka berada di VPC.

Security Hub merekomendasikan agar Anda memperlakukan temuan tingkat keparahan tinggi sebagai prioritas jangka pendek. Anda harus segera mengambil langkah-langkah remediasi. Anda juga harus mempertimbangkan kekritisan sumber daya.

Medium — Masalah ini harus ditangani sebagai prioritas jangka menengah.

Misalnya, kurangnya enkripsi untuk data dalam perjalanan dianggap sebagai temuan tingkat keparahan sedang. Dibutuhkan man-in-the-middle serangan canggih untuk memanfaatkan kelemahan ini. Dengan kata lain, ini agak sulit. Kemungkinan beberapa data akan dikompromikan jika skenario ancaman berhasil.

Security Hub merekomendasikan agar Anda menyelidiki sumber daya yang terlibat secepatnya. Anda juga harus mempertimbangkan kekritisan sumber daya.

Rendah — Masalah ini tidak memerlukan tindakan sendiri.

Misalnya, kegagalan untuk mengumpulkan informasi forensik dianggap tingkat keparahan rendah. Kontrol ini dapat membantu mencegah kompromi di masa depan, tetapi tidak adanya forensik tidak mengarah langsung pada kompromi.

Anda tidak perlu mengambil tindakan segera pada temuan tingkat keparahan rendah, tetapi mereka dapat memberikan konteks ketika Anda menghubungkannya dengan masalah lain.

Informasi - Tidak ada kelemahan konfigurasi yang ditemukan.

Dengan kata lain, statusnya adalah`PASSED`,`WARNING`, atau`NOT AVAILABLE`.

Tidak ada tindakan yang disarankan. Temuan informasi membantu pelanggan untuk menunjukkan bahwa mereka berada dalam keadaan patuh.

Aturan untuk memperbarui temuan kontrol

Pemeriksaan berikutnya terhadap aturan yang diberikan mungkin menghasilkan hasil baru. Misalnya, status “Hindari penggunaan pengguna root” dapat berubah dari `FAILED` ke`PASSED`. Dalam hal ini, temuan baru dihasilkan yang berisi hasil terbaru.

Jika pemeriksaan berikutnya terhadap aturan yang diberikan menghasilkan hasil yang identik dengan hasil saat ini, temuan yang ada diperbarui. Tidak ada temuan baru yang dihasilkan.

Security Hub secara otomatis mengarsipkan temuan dari kontrol jika sumber daya terkait dihapus, sumber daya tidak ada, atau kontrol dinonaktifkan. Sumber daya mungkin tidak ada lagi karena layanan terkait saat ini tidak digunakan. Temuan diarsipkan secara otomatis berdasarkan salah satu kriteria berikut:

- Temuan ini tidak diperbarui selama tiga hingga lima hari (perhatikan bahwa ini adalah upaya terbaik dan tidak dijamin).
- AWS Config Evaluasi terkait kembali`NOT_APPLICABLE`.

Status kepatuhan dan status kontrol

`Compliance.Status`Bidang Format Pencarian AWS Keamanan menjelaskan hasil temuan kontrol. Security Hub menggunakan status kepatuhan temuan kontrol untuk menentukan status kontrol secara keseluruhan. Status kontrol ditampilkan di halaman detail kontrol di konsol Security Hub.

Untuk akun administrator, status kontrol mencerminkan status kontrol di akun administrator dan akun anggota. Secara khusus, status keseluruhan kontrol muncul sebagai Gagal jika kontrol memiliki satu atau lebih temuan gagal di akun administrator atau salah satu akun anggota. Jika Anda telah menetapkan Wilayah agregasi, status kontrol di Wilayah agregasi mencerminkan status kontrol di Wilayah agregasi dan Wilayah yang ditautkan. Secara khusus, status keseluruhan kontrol muncul sebagai Gagal jika kontrol memiliki satu atau lebih temuan gagal di Wilayah agregasi atau salah satu Wilayah terkait.

Security Hub biasanya menghasilkan status kontrol awal dalam waktu 30 menit setelah kunjungan pertama Anda ke halaman Ringkasan atau halaman standar Keamanan konsol Security Hub. Anda harus memiliki perekaman AWS Config sumber daya yang dikonfigurasi agar status kontrol muncul. Setelah status kontrol dibuat untuk pertama kalinya, Security Hub memperbarui status kontrol setiap 24 jam berdasarkan temuan dari 24 jam sebelumnya. Stempel waktu pada halaman detail kontrol menunjukkan kapan status kontrol terakhir diperbarui.

> **Note**
>
> Ini dapat memakan waktu hingga 24 jam setelah memungkinkan kontrol untuk status kontrol pertama kali yang akan dihasilkan di Wilayah China dan. AWS GovCloud (US) Region

Nilai untuk status kepatuhan suatu temuan

Status kepatuhan untuk setiap temuan diberikan salah satu dari nilai berikut:

- `PASSED`— Menunjukkan bahwa kontrol melewati pemeriksaan keamanan untuk temuan ini. Secara otomatis menyetel Security Hub `Workflow.Status` ke`RESOLVED`.

  Jika `Compliance.Status` untuk temuan berubah dari `PASSED` ke`FAILED`,, atau `WARNING`ke`NOT_AVAILABLE`, dan `Workflow.Status` salah satu `NOTIFIED` atau`RESOLVED`, maka Security Hub secara otomatis disetel `Workflow.Status` ke`NEW`.

  Jika Anda tidak memiliki sumber daya yang sesuai dengan kontrol, Security Hub menghasilkan `PASSED` temuan di tingkat akun. Jika Anda memiliki sumber daya yang sesuai dengan kontrol tetapi kemudian menghapus sumber daya, Security Hub membuat `NOT_AVAILABLE` temuan dan mengarsipkannya segera. Setelah 18 jam, Anda menerima `PASSED` temuan karena Anda tidak lagi memiliki sumber daya yang sesuai dengan kontrol.
- `FAILED`— Menunjukkan bahwa kontrol tidak lulus pemeriksaan keamanan untuk temuan ini.

- `WARNING`— Menunjukkan bahwa pemeriksaan telah selesai, tetapi Security Hub tidak dapat menentukan apakah sumber daya dalam `FAILED` status `PASSED` atau tidak.
- `NOT_AVAILABLE`— Menunjukkan bahwa pemeriksaan tidak dapat diselesaikan karena server gagal, sumber daya dihapus, atau hasil AWS Config evaluasi`NOT_APPLICABLE`.

  Jika hasil AWS Config evaluasi adalah`NOT_APPLICABLE`, Security Hub secara otomatis mengarsipkan temuan tersebut.

Nilai untuk status kontrol

Security Hub memperoleh status kontrol keseluruhan dari status kepatuhan temuan kontrol. Saat menentukan status kontrol, Security Hub mengabaikan temuan yang memiliki `RecordState` of `ARCHIVED` dan temuan yang memiliki a `Workflow.Status` of. `SUPPRESSED`

Status kontrol diberikan salah satu nilai berikut:

- Lulus — Menunjukkan bahwa semua temuan memiliki status kepatuhan`PASSED`.
- Gagal - Menunjukkan bahwa setidaknya satu temuan memiliki status kepatuhan`FAILED`.
- Tidak diketahui - Menunjukkan bahwa setidaknya satu temuan memiliki status kepatuhan `WARNING` atau`NOT_AVAILABLE`. Tidak ada temuan yang memiliki status kepatuhan`FAILED`.
- Tidak ada data — Menunjukkan bahwa tidak ada temuan untuk kontrol. Misalnya, kontrol yang baru diaktifkan memiliki status ini hingga Security Hub mulai menghasilkan temuan untuknya. Kontrol juga memiliki status ini jika semua temuan `SUPPRESSED` atau jika tidak tersedia di Wilayah saat ini.
- Dinonaktifkan - Menunjukkan bahwa kontrol dinonaktifkan di akun saat ini dan Wilayah. Saat ini tidak ada pemeriksaan keamanan yang dilakukan untuk kontrol ini di akun saat ini dan Wilayah. Namun, temuan kontrol yang dinonaktifkan mungkin memiliki nilai untuk status kepatuhan hingga 24 jam setelah penonaktifan.

Menentukan skor keamanan

Halaman Ringkasan dan halaman Kontrol konsol Security Hub menampilkan skor keamanan ringkasan di semua standar yang diaktifkan. Pada halaman standar Keamanan, Security Hub juga menampilkan skor keamanan dari 0-100 persen untuk setiap standar yang diaktifkan.

Saat pertama kali mengaktifkan Security Hub, Security Hub menghitung skor keamanan ringkasan dan skor keamanan standar dalam waktu 30 menit setelah kunjungan pertama Anda ke halaman

Ringkasan atau halaman standar Keamanan di konsol Security Hub. Skor hanya dihasilkan untuk standar yang diaktifkan saat Anda mengunjungi halaman tersebut. Untuk melihat daftar standar yang saat ini diaktifkan, panggil operasi `GetEnabledStandards`API. Selain itu, perekaman AWS Config sumber daya harus dikonfigurasi agar skor muncul. Skor keamanan ringkasan adalah rata-rata skor keamanan standar.

Setelah menghasilkan skor pertama kali, Security Hub memperbarui skor keamanan setiap 24 jam. Security Hub menampilkan stempel waktu untuk menunjukkan kapan skor keamanan terakhir diperbarui.

> **Note**
>
> Mungkin diperlukan waktu hingga 24 jam untuk skor keamanan pertama kali dihasilkan di Wilayah China dan AWS GovCloud (US) Region.

Jika Anda mengaktifkan temuan kontrol konsolidasi, mungkin diperlukan waktu hingga 24 jam agar skor keamanan Anda diperbarui. Selain itu, mengaktifkan Wilayah agregasi baru atau memperbarui Wilayah tertaut akan me-reset skor keamanan yang ada. Diperlukan waktu hingga 24 jam bagi Security Hub untuk menghasilkan skor keamanan baru yang menyertakan data dari Wilayah yang diperbarui.

Bagaimana skor keamanan dihitung

Skor keamanan mewakili proporsi kontrol Lulus ke kontrol yang diaktifkan. Skor ditampilkan sebagai persentase yang dibulatkan ke atas atau ke bawah ke bilangan bulat terdekat.

Security Hub menghitung skor keamanan ringkasan di semua standar yang diaktifkan. Security Hub juga menghitung skor keamanan untuk setiap standar yang diaktifkan. Untuk tujuan perhitungan skor, kontrol yang diaktifkan menyertakan kontrol dengan status Lulus, Gagal, dan Tidak Diketahui. Kontrol dengan status Tidak ada data dikecualikan dari perhitungan skor.

Security Hub mengabaikan temuan yang diarsipkan dan ditekan saat menghitung status kontrol. Ini dapat memengaruhi skor keamanan. Misalnya, jika Anda menekan semua temuan yang gagal untuk kontrol, statusnya menjadi Lulus, yang pada gilirannya dapat meningkatkan skor keamanan Anda. Untuk informasi selengkapnya tentang status kontrol, lihatStatus kepatuhan dan status kontrol.

Contoh penilaian:

Standar	Kontrol yang lulus	Kontrol gagal	Kontrol tidak diketahui	Skor standar
AWS Praktik Terbaik Keamanan Dasar v1.0.0	168	22	0	88%
Tolok Ukur AWS Yayasan CIS v1.4.0	8	29	0	22%
Tolok Ukur AWS Yayasan CIS v1.2.0	6	35	0	15%
Publikasi Khusus NIST 800-53 Revisi 5	159	56	0	74%
PCI DSS v3.2.1	28	17	0	62%

Saat menghitung skor keamanan ringkasan, Security Hub menghitung setiap kontrol hanya sekali di seluruh standar. Misalnya, jika Anda telah mengaktifkan kontrol yang berlaku untuk tiga standar yang diaktifkan, itu hanya dihitung sebagai satu kontrol yang diaktifkan untuk tujuan penilaian.

Dalam contoh ini, meskipun jumlah total kontrol yang diaktifkan di seluruh standar yang diaktifkan adalah 528, Security Hub menghitung setiap kontrol unik hanya sekali untuk tujuan penilaian. Jumlah kontrol unik yang diaktifkan kemungkinan lebih rendah dari 528. Jika kita menganggap jumlah kontrol unik yang diaktifkan adalah 515, dan jumlah kontrol unik yang dilewati adalah 357, skor ringkasan adalah 69%. Skor ini dihitung dengan membagi jumlah kontrol unik yang dilewatkan dengan jumlah kontrol unik yang diaktifkan.

Anda mungkin memiliki skor ringkasan yang berbeda dari skor keamanan standar meskipun Anda hanya mengaktifkan satu standar di akun Anda di Wilayah saat ini. Hal ini dapat terjadi jika Anda masuk ke akun administrator dan akun anggota memiliki standar tambahan atau standar yang berbeda diaktifkan. Hal ini juga dapat terjadi jika Anda melihat skor dari Wilayah agregasi dan standar tambahan atau standar yang berbeda diaktifkan di Wilayah tertaut.

Skor keamanan untuk akun administrator

Jika Anda masuk ke akun administrator, skor keamanan ringkasan dan skor standar akun untuk status kontrol di akun administrator dan semua akun anggota.

Jika status kontrol Gagal bahkan di satu akun anggota, statusnya Gagal di akun administrator dan berdampak pada skor akun administrator.

Jika Anda masuk ke akun administrator dan melihat skor di Wilayah agregasi, skor keamanan akan memperhitungkan status kontrol di semua akun anggota dan semua Wilayah yang ditautkan.

Skor keamanan jika Anda telah menetapkan Wilayah agregasi

Jika Anda telah menetapkan agregasi Wilayah AWS, skor keamanan ringkasan dan skor standar memperhitungkan status kontrol di semua Wilayah terkait.

Jika status kontrol Gagal bahkan di satu Wilayah yang ditautkan, statusnya Gagal di Wilayah agregasi dan berdampak pada skor Wilayah agregasi.

Jika Anda masuk ke akun administrator dan melihat skor di Wilayah agregasi, skor keamanan akan memperhitungkan status kontrol di semua akun anggota dan semua Wilayah yang ditautkan.

Referensi standar Security Hub

AWS Security Hub saat ini mendukung standar keamanan yang dirinci di bagian ini.

Pilih standar untuk melihat detail lebih lanjut tentang itu dan kontrol yang berlaku untuk itu.

Standar dan kontrol Security Hub tidak menjamin kepatuhan terhadap kerangka kerja peraturan atau audit apa pun. Sebaliknya, kontrol menyediakan cara untuk memantau keadaan Anda saat ini Akun AWS dan sumber daya.

Standar yang didukung

- AWS Standar Praktik Terbaik Keamanan Dasar (FSBP)
- Tolok Ukur AWS Yayasan CIS
- Institut Nasional Standar dan Teknologi (NIST) SP 800-53 Rev. 5
- Standar Keamanan Data Industri Kartu Pembayaran (PCI DSS)
- AWS Standar Penandaan Sumber Daya
- Standar yang dikelola layanan

AWS Standar Praktik Terbaik Keamanan Dasar (FSBP)

Standar Praktik Terbaik Keamanan AWS Dasar adalah seperangkat kontrol yang mendeteksi kapan Anda Akun AWS dan sumber daya menyimpang dari praktik terbaik keamanan.

Standar ini memungkinkan Anda terus mengevaluasi semua beban kerja Akun AWS dan beban kerja Anda untuk dengan cepat mengidentifikasi area penyimpangan dari praktik terbaik. Ini memberikan panduan yang dapat ditindaklanjuti dan preskriptif tentang bagaimana meningkatkan dan mempertahankan postur keamanan organisasi Anda.

Kontrol mencakup praktik terbaik keamanan untuk sumber daya dari beberapa sumber daya Layanan AWS. Setiap kontrol juga diberi kategori yang mencerminkan fungsi keamanan yang berlaku. Untuk informasi selengkapnya, lihat the section called “Kategori kontrol”.

Kontrol yang berlaku untuk standar FSBP

[Akun.1] Informasi kontak keamanan harus disediakan untuk Akun AWS

[ACM.1] Sertifikat yang diimpor dan diterbitkan ACM harus diperbarui setelah jangka waktu tertentu

[ACM.2] Sertifikat RSA yang dikelola oleh ACM harus menggunakan panjang kunci minimal 2.048 bit

[ApiGateway.1] API Gateway REST WebSocket dan pencatatan eksekusi API harus diaktifkan

[ApiGateway.2] Tahapan API Gateway REST API harus dikonfigurasi untuk menggunakan sertifikat SSL untuk otentikasi backend

[ApiGateway.3] Tahapan API Gateway REST API harus mengaktifkan penelusuran AWS X-Ray

[ApiGateway.4] API Gateway harus dikaitkan dengan ACL Web WAF

[ApiGateway.5] Data cache API Gateway REST API harus dienkripsi saat istirahat

[ApiGateway.8] Rute API Gateway harus menentukan jenis otorisasi

[ApiGateway.9] Pencatatan akses harus dikonfigurasi untuk Tahapan API Gateway V2

[AppSync.2] AWS AppSync harus mengaktifkan logging tingkat lapangan

[AppSync.5] AWS AppSync GraphQL API tidak boleh diautentikasi dengan kunci API

[AutoScaling.1] Grup Auto Scaling yang terkait dengan penyeimbang beban harus menggunakan pemeriksaan kesehatan ELB

[AutoScaling.2] Grup Auto Scaling Amazon EC2 harus mencakup beberapa Availability Zone

[AutoScaling.3] Konfigurasi peluncuran grup Auto Scaling harus mengonfigurasi instans EC2 agar memerlukan Layanan Metadata Instans Versi 2 (IMDSv2)

[Autoscaling.5] Instans Amazon EC2 yang diluncurkan menggunakan konfigurasi peluncuran grup Auto Scaling seharusnya tidak memiliki alamat IP Publik

[AutoScaling.6] Grup Auto Scaling harus menggunakan beberapa jenis instance di beberapa Availability Zone

[AutoScaling.9] Grup Auto Scaling Amazon EC2 harus menggunakan templat peluncuran Amazon EC2

[Backup.1] titik AWS Backup pemulihan harus dienkripsi saat istirahat

[CloudFront.1] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi

[CloudFront.3] CloudFront distribusi harus memerlukan enkripsi dalam perjalanan

[CloudFront.4] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi

[CloudFront.5] CloudFront distribusi seharusnya mengaktifkan logging

[CloudFront.6] CloudFront distribusi harus mengaktifkan WAF

[CloudFront.7] CloudFront distribusi harus menggunakan sertifikat SSL/TLS khusus

[CloudFront.8] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS

[CloudFront.9] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus

[CloudFront.10] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal khusus

[CloudFront.12] CloudFront distribusi seharusnya tidak menunjukkan asal S3 yang tidak ada

[CloudFront.13] CloudFront distribusi harus menggunakan kontrol akses asal

[CloudTrail.1] CloudTrail harus diaktifkan dan dikonfigurasi dengan setidaknya satu jejak Multi-wilayah yang mencakup acara manajemen baca dan tulis

[CloudTrail.2] CloudTrail harus mengaktifkan enkripsi saat istirahat

[CloudTrail.4] validasi file CloudTrail log harus diaktifkan

[CloudTrail.5] CloudTrail jalur harus diintegrasikan dengan Amazon Logs CloudWatch

[CodeBuild.1] URL repositori sumber CodeBuild Bitbucket tidak boleh berisi kredensyal sensitif

[CodeBuild.2] variabel lingkungan CodeBuild proyek tidak boleh berisi kredensil teks yang jelas

[CodeBuild.3] Log CodeBuild S3 harus dienkripsi

[CodeBuild.4] lingkungan CodeBuild proyek harus memiliki urasi logging AWS Config

[Config.1] AWS Config harus diaktifkan dan menggunakan peran terkait layanan untuk perekaman sumber daya

[DataFirehose.1] Aliran pengiriman Firehose harus dienkripsi saat istirahat

[DMS.1] Instans replikasi Layanan Migrasi Database tidak boleh bersifat publik

[DMS.6] Instans replikasi DMS harus mengaktifkan peningkatan versi minor otomatis

[DMS.7] Tugas replikasi DMS untuk database target seharusnya mengaktifkan logging

[DMS.8] Tugas replikasi DMS untuk database sumber seharusnya mengaktifkan logging

[DMS.9] Titik akhir DMS harus menggunakan SSL

[DMS.10] Titik akhir DMS untuk database Neptunus harus mengaktifkan otorisasi IAM

[DMS.11] Titik akhir DMS untuk MongoDB harus mengaktifkan mekanisme otentikasi

[DMS.12] Titik akhir DMS untuk Redis harus mengaktifkan TLS

[DocumentDB.1] Cluster Amazon DocumentDB harus dienkripsi saat istirahat

[DocumentDB.2] Cluster Amazon DocumentDB harus memiliki periode retensi cadangan yang memadai

[DocumentDB.3] Cuplikan cluster manual Amazon DocumentDB seharusnya tidak bersifat publik

[DocumentDB.4] Cluster Amazon DocumentDB harus mempublikasikan log audit ke Log CloudWatch

[DocumentDB.5] Cluster Amazon DocumentDB harus mengaktifkan perlindungan penghapusan

[DynamoDB.1] Tabel DynamoDB harus secara otomatis menskalakan kapasitas sesuai permintaan

[DynamoDB.2] Tabel DynamoDB harus mengaktifkan pemulihan point-in-time

[DynamoDB.3] Cluster DynamoDB Accelerator (DAX) harus dienkripsi saat istirahat

[DynamoDB.6] Tabel DynamoDB harus mengaktifkan perlindungan penghapusan

[DynamoDB.7] Cluster DynamoDB Accelerator harus dienkripsi saat transit

[EC2.1] Snapshot Amazon EBS tidak boleh dipulihkan secara publik

[EC2.2] Grup keamanan default VPC tidak boleh mengizinkan lalu lintas masuk atau keluar

[EC2.3] Volume Amazon EBS yang terpasang harus dienkripsi saat istirahat

[EC2.4] Instans EC2 yang dihentikan harus dihapus setelah periode waktu tertentu

[EC2.6] Pencatatan aliran VPC harus diaktifkan di semua VPC

[EC2.7] Enkripsi default EBS harus diaktifkan

[EC2.8] Instans EC2 harus menggunakan Layanan Metadata Instance Versi 2 (IMDSv2)

[EC2.9] Instans Amazon EC2 seharusnya tidak memiliki alamat IPv4 publik

[EC2.10] Amazon EC2 harus dikonfigurasi untuk menggunakan titik akhir VPC yang dibuat untuk layanan Amazon EC2

[EC2.15] Subnet Amazon EC2 seharusnya tidak secara otomatis menetapkan alamat IP publik

[EC2.16] Daftar Kontrol Akses Jaringan yang Tidak Digunakan harus dihapus

[EC2.17] Instans Amazon EC2 tidak boleh menggunakan beberapa ENI

[EC2.18] Grup keamanan seharusnya hanya mengizinkan lalu lintas masuk yang tidak terbatas untuk port resmi

[EC2.19] Grup keamanan tidak boleh mengizinkan akses tidak terbatas ke port dengan risiko tinggi

[EC2.20] Kedua terowongan VPN untuk koneksi VPN Site-to-Site harus AWS aktif

[EC2.21] ACL jaringan seharusnya tidak mengizinkan masuknya dari 0.0.0.0/0 ke port 22 atau port 3389

[EC2.23] Amazon EC2 Transit Gateways seharusnya tidak secara otomatis menerima permintaan lampiran VPC

[EC2.24] Jenis instans paravirtual Amazon EC2 tidak boleh digunakan

[EC2.25] Templat peluncuran Amazon EC2 tidak boleh menetapkan IP publik ke antarmuka jaringan

[EC2.51] Titik akhir EC2 Client VPN harus mengaktifkan pencatatan koneksi klien

[ECR.1] Repositori pribadi ECR harus memiliki pemindaian gambar yang dikonfigurasi

[ECR.2] Repositori pribadi ECR harus memiliki kekekalan tag yang dikonfigurasi

[ECR.3] Repositori ECR harus memiliki setidaknya satu kebijakan siklus hidup yang dikonfigurasi

[ECS.1] Definisi tugas Amazon ECS harus memiliki mode jaringan yang aman dan definisi pengguna.

[ECS.2] Layanan ECS seharusnya tidak memiliki alamat IP publik yang ditetapkan kepadanya secara otomatis

[ECS.3] Definisi tugas ECS tidak boleh membagikan namespace proses host

[ECS.4] Kontainer ECS harus berjalan sebagai non-hak istimewa

[ECS.5] Wadah ECS harus dibatasi pada akses hanya-baca ke sistem file root

[ECS.8] Rahasia tidak boleh diteruskan sebagai variabel lingkungan kontainer

[ECS.9] Definisi tugas ECS harus memiliki konfigurasi logging

[ECS.10] Layanan ECS Fargate harus berjalan pada versi platform Fargate terbaru

[ECS.12] Cluster ECS harus menggunakan Wawasan Kontainer

[EFS.1] Sistem File Elastis harus dikonfigurasi untuk mengenkripsi data file saat istirahat menggunakan AWS KMS

[EFS.2] Volume Amazon EFS harus dalam rencana cadangan

[EFS.3] Titik akses EFS harus menegakkan direktori root

[EFS.4] Titik akses EFS harus menegakkan identitas pengguna

[EFS.6] Target pemasangan EFS tidak boleh dikaitkan dengan subnet publik

[EKS.1] Titik akhir klaster EKS seharusnya tidak dapat diakses publik

[EKS.2] Kluster EKS harus berjalan pada versi Kubernetes yang didukung

[EKS.3] Kluster EKS harus menggunakan rahasia Kubernetes terenkripsi

[EKS.8] Kluster EKS harus mengaktifkan pencatatan audit

[ElastiCache.1] Cluster ElastiCache Redis harus mengaktifkan pencadangan otomatis

[ElastiCache.2] ElastiCache untuk kluster cache Redis harus mengaktifkan peningkatan versi minor otomatis

[ElastiCache.3] ElastiCache untuk grup replikasi Redis harus mengaktifkan failover otomatis

[ElastiCache.4] ElastiCache untuk grup replikasi Redis harus dienkripsi saat istirahat

[ElastiCache.5] ElastiCache untuk grup replikasi Redis harus dienkripsi saat transit

[ElastiCache.6] ElastiCache untuk grup replikasi Redis sebelum versi 6.0 harus menggunakan Redis AUTH

[ElastiCache.7] ElastiCache cluster tidak boleh menggunakan grup subnet default

[ElasticBeanstalk.1] Lingkungan Elastic Beanstalk seharusnya mengaktifkan pelaporan kesehatan yang ditingkatkan

[ElasticBeanstalk.2] Pembaruan platform yang dikelola Elastic Beanstalk harus diaktifkan

[ElasticBeanstalk.3] Elastic Beanstalk harus mengalirkan log ke CloudWatch

[ELB.1] Application Load Balancer harus dikonfigurasi untuk mengalihkan semua permintaan HTTP ke HTTPS

[ELB.2] Classic Load Balancer dengan pendengar SSL/HTTPS harus menggunakan sertifikat yang disediakan oleh AWS Certificate Manager

[ELB.3] Pendengar Classic Load Balancer harus dikonfigurasi dengan penghentian HTTPS atau TLS

[ELB.4] Application Load Balancer harus dikonfigurasi untuk menjatuhkan header http

[ELB.5] Pencatatan aplikasi dan Classic Load Balancer harus diaktifkan

[ELB.6] Aplikasi, Gateway, dan Network Load Balancer harus mengaktifkan perlindungan penghapusan

[ELB.7] Classic Load Balancers harus mengaktifkan pengurasan koneksi

[ELB.8] Classic Load Balancer dengan pendengar SSL harus menggunakan kebijakan keamanan yang telah ditentukan sebelumnya yang memiliki urasi yang kuat AWS Config

[ELB.9] Classic Load Balancer harus mengaktifkan penyeimbangan beban lintas zona

[ELB.10] Classic Load Balancer harus menjangkau beberapa Availability Zone

[ELB.12] Application Load Balancer harus dikonfigurasi dengan mode mitigasi desync defensif atau paling ketat

[ELB.13] Penyeimbang Beban Aplikasi, Jaringan, dan Gateway harus mencakup beberapa Availability Zone

[ELB.14] Classic Load Balancer harus dikonfigurasi dengan mode mitigasi desync defensif atau paling ketat

[EMR.1] Node primer cluster EMR Amazon seharusnya tidak memiliki alamat IP publik

[EMR.2] Pengaturan akses publik blok EMR Amazon harus diaktifkan

[ES.1] Domain Elasticsearch harus mengaktifkan enkripsi saat istirahat

[ES.2] Domain Elasticsearch tidak boleh diakses publik

[ES.3] Domain Elasticsearch harus mengenkripsi data yang dikirim antar node

[ES.4] Kesalahan domain Elasticsearch yang masuk ke CloudWatch Log harus diaktifkan

[ES.5] Domain Elasticsearch harus mengaktifkan pencatatan audit

[ES.6] Domain Elasticsearch harus memiliki setidaknya tiga node data

[ES.7] Domain Elasticsearch harus dikonfigurasi dengan setidaknya tiga node master khusus

[ES.8] Koneksi ke domain Elasticsearch harus dienkripsi menggunakan kebijakan keamanan TLS terbaru

[EventBridge.3] bus acara EventBridge khusus harus memiliki kebijakan berbasis sumber daya terlampir

[FSX.1] FSx untuk sistem file OpenZFS harus dikonfigurasi untuk menyalin tag ke cadangan dan volume

[FSX.2] Sistem file FSx for Lustre harus dikonfigurasi untuk menyalin tag ke cadangan

[GuardDuty.1] GuardDuty harus diaktifkan

[IAM.1] Kebijakan IAM seharusnya tidak mengizinkan hak administratif “*” penuh

[IAM.2] Pengguna IAM seharusnya tidak memiliki kebijakan IAM yang dilampirkan

[IAM.3] Kunci akses pengguna IAM harus diputar setiap 90 hari atau kurang

[IAM.4] Kunci akses pengguna root IAM seharusnya tidak ada

[IAM.5] MFA harus diaktifkan untuk semua pengguna IAM yang memiliki kata sandi konsol

[IAM.6] MFA perangkat keras harus diaktifkan untuk pengguna root

[IAM.7] Kebijakan kata sandi untuk pengguna IAM harus memiliki konfigurasi yang kuat

[IAM.8] Kredensyal pengguna IAM yang tidak digunakan harus dihapus

[IAM.21] Kebijakan terkelola pelanggan IAM yang Anda buat seharusnya tidak mengizinkan tindakan wildcard untuk layanan

[Kinesis.1] Aliran kinesis harus dienkripsi saat istirahat

[KMS.1] Kebijakan yang dikelola pelanggan IAM tidak boleh mengizinkan tindakan dekripsi pada semua kunci KMS

[KMS.2] Prinsipal IAM tidak boleh memiliki kebijakan inline IAM yang memungkinkan tindakan dekripsi pada semua kunci KMS

[KMS.3] tidak AWS KMS keys boleh dihapus secara tidak sengaja

[Lambda.1] Kebijakan fungsi Lambda harus melarang akses publik

[Lambda.2] Fungsi Lambda harus menggunakan runtime yang didukung

[Lambda.5] Fungsi VPC Lambda harus beroperasi di beberapa Availability Zone

[Macie.1] Amazon Macie harus diaktifkan

[Macie.2] Penemuan data sensitif otomatis Macie harus diaktifkan

[MQ.2] Broker ActiveMQ harus mengalirkan log audit ke CloudWatch

[MQ.3] Broker Amazon MQ harus mengaktifkan peningkatan versi minor otomatis

[MSK.1] Cluster MSK harus dienkripsi saat transit di antara node broker

[Neptunus.1] Cluster DB Neptunus harus dienkripsi saat istirahat

[Neptune.2] Cluster DB Neptunus harus menerbitkan log audit ke Log CloudWatch

[Neptune.3] Snapshot cluster Neptunus DB seharusnya tidak publik

[Neptunus.4] Cluster DB Neptunus harus mengaktifkan perlindungan penghapusan

[Neptunus.5] Cluster DB Neptunus harus mengaktifkan cadangan otomatis

[Neptune.6] Snapshot cluster Neptunus DB harus dienkripsi saat istirahat

[Neptunus.7] Cluster DB Neptunus harus mengaktifkan otentikasi basis data IAM

[Neptunus.8] Cluster DB Neptunus harus dikonfigurasi untuk menyalin tag ke snapshot

[NetworkFirewall.2] Pencatatan Firewall Jaringan harus diaktifkan

[NetworkFirewall.3] Kebijakan Network Firewall harus memiliki setidaknya satu kelompok aturan yang terkait

[NetworkFirewall.4] Tindakan stateless default untuk kebijakan Network Firewall harus drop atau forward untuk paket penuh

[NetworkFirewall.5] Tindakan stateless default untuk kebijakan Network Firewall harus drop atau forward untuk paket yang terfragmentasi

[NetworkFirewall.6] Grup aturan Stateless Network Firewall tidak boleh kosong

[NetworkFirewall.9] Firewall Firewall Jaringan harus mengaktifkan perlindungan penghapusan

[Opensearch.1] OpenSearch domain harus mengaktifkan enkripsi saat istirahat

[Opensearch.2] OpenSearch domain tidak boleh diakses publik

[Opensearch.3] OpenSearch domain harus mengenkripsi data yang dikirim antar node

[Opensearch.4] login kesalahan OpenSearch domain ke Log harus diaktifkan CloudWatch

[Opensearch.5] OpenSearch domain harus mengaktifkan pencatatan audit

[Opensearch.6] OpenSearch domain harus memiliki setidaknya tiga node data

[Opensearch.7] OpenSearch domain harus mengaktifkan kontrol akses berbutir halus

[Opensearch.8] Koneksi ke OpenSearch domain harus dienkripsi menggunakan kebijakan keamanan TLS terbaru

[Opensearch.10] OpenSearch domain harus memiliki pembaruan perangkat lunak terbaru yang diinstal

[PCA.1] otoritas sertifikat AWS Private CA root harus dinonaktifkan

[Route53.2] Route 53 zona yang dihosting publik harus mencatat kueri DNS

[RDS.1] Snapshot RDS harus pribadi

[RDS.2] Instans RDS DB harus melarang akses publik, sebagaimana ditentukan oleh urasi PubliclyAccessible AWS Config

[RDS.3] Instans RDS DB harus mengaktifkan enkripsi saat istirahat

[RDS.4] Snapshot cluster RDS dan snapshot database harus dienkripsi saat istirahat

[RDS.5] Instans RDS DB harus dikonfigurasi dengan beberapa Availability Zone

[RDS.6] Pemantauan yang ditingkatkan harus dikonfigurasi untuk instans RDS DB

[RDS.7] Cluster RDS harus mengaktifkan perlindungan penghapusan

[RDS.8] Instans RDS DB harus mengaktifkan perlindungan penghapusan

[RDS.9] Instans RDS DB harus menerbitkan log ke Log CloudWatch

[RDS.10] Otentikasi IAM harus dikonfigurasi untuk instance RDS

[RDS.11] Instans RDS harus mengaktifkan pencadangan otomatis

[RDS.12] Otentikasi IAM harus dikonfigurasi untuk cluster RDS

[RDS.13] Peningkatan versi minor otomatis RDS harus diaktifkan

[RDS.14] Cluster Amazon Aurora seharusnya mengaktifkan backtracking

[RDS.15] Cluster RDS DB harus dikonfigurasi untuk beberapa Availability Zone

[RDS.16] Cluster RDS DB harus dikonfigurasi untuk menyalin tag ke snapshot

[RDS.17] Instans RDS DB harus dikonfigurasi untuk menyalin tag ke snapshot

[RDS.18] Instans RDS harus digunakan di VPC

[RDS.19] Langganan pemberitahuan acara RDS yang ada harus dikonfigurasi untuk peristiwa klaster penting

[RDS.20] Langganan pemberitahuan acara RDS yang ada harus dikonfigurasi untuk peristiwa instance basis data penting

[RDS.21] Langganan pemberitahuan acara RDS harus dikonfigurasi untuk peristiwa grup parameter basis data penting

[RDS.22] Langganan pemberitahuan acara RDS harus dikonfigurasi untuk acara grup keamanan basis data penting

[RDS.23] Instans RDS tidak boleh menggunakan port default mesin database

[RDS.24] Kluster Database RDS harus menggunakan nama pengguna administrator khusus

[RDS.25] Instans database RDS harus menggunakan nama pengguna administrator khusus

[RDS.27] Cluster RDS DB harus dienkripsi saat istirahat

[RDS.34] Cluster Aurora MySQL DB harus menerbitkan log audit ke Log CloudWatch

[RDS.35] Cluster RDS DB harus mengaktifkan peningkatan versi minor otomatis

[Redshift.1] Cluster Amazon Redshift harus melarang akses publik

[Redshift.2] Koneksi ke cluster Amazon Redshift harus dienkripsi saat transit

[Redshift.3] Cluster Amazon Redshift harus mengaktifkan snapshot otomatis

[Redshift.4] Cluster Amazon Redshift harus mengaktifkan pencatatan audit

[Redshift.6] Amazon Redshift harus mengaktifkan peningkatan otomatis ke versi utama

[Redshift.7] Cluster Redshift harus menggunakan perutean VPC yang ditingkatkan

[Redshift.8] Cluster Amazon Redshift tidak boleh menggunakan nama pengguna Admin default

[Redshift.9] Cluster Redshift tidak boleh menggunakan nama database default

[Redshift.10] Cluster Redshift harus dienkripsi saat istirahat

[Redshift.15] Grup keamanan Redshift harus mengizinkan masuknya port cluster hanya dari asal yang dibatasi

[S3.1] Bucket tujuan umum S3 harus mengaktifkan pengaturan akses publik blok

[S3.2] Bucket tujuan umum S3 harus memblokir akses baca publik

[S3.3] Bucket tujuan umum S3 harus memblokir akses tulis publik

[S3.5] Bucket tujuan umum S3 harus memerlukan permintaan untuk menggunakan SSL

[S3.6] Kebijakan bucket tujuan umum S3 harus membatasi akses ke yang lain Akun AWS

[S3.8] Bucket tujuan umum S3 harus memblokir akses publik

[S3.9] Bucket tujuan umum S3 harus mengaktifkan pencatatan akses server

[S3.12] ACL tidak boleh digunakan untuk mengelola akses pengguna ke bucket tujuan umum S3

[S3.13] Bucket tujuan umum S3 harus memiliki konfigurasi Siklus Hidup

[S3.19] Titik akses S3 harus mengaktifkan pengaturan akses publik blok

[SageMaker.1] Instans SageMaker notebook Amazon seharusnya tidak memiliki akses internet langsung

[SageMaker.2] instance SageMaker notebook harus diluncurkan dalam VPC khusus

[SageMaker.3] Pengguna seharusnya tidak memiliki akses root ke instance SageMaker notebook

[SageMaker.4] varian produksi SageMaker titik akhir harus memiliki jumlah instance awal yang lebih besar dari 1

[SecretsManager.1] Rahasia Secrets Manager harus mengaktifkan rotasi otomatis

[SecretsManager.2] Rahasia Secrets Manager yang dikonfigurasi dengan rotasi otomatis harus berhasil diputar

[SecretsManager.3] Hapus rahasia Secrets Manager yang tidak digunakan

[SecretsManager.4] Rahasia Secrets Manager harus diputar dalam jumlah hari tertentu

[ServiceCatalog.1] Portofolio Service Catalog harus dibagikan hanya dalam suatu organisasi AWS

[SQS.1] Antrian Amazon SQS harus dienkripsi saat istirahat

[SSM.1] Instans Amazon EC2 harus dikelola oleh AWS Systems Manager

[SSM.2] Instans Amazon EC2 yang dikelola oleh Systems Manager harus memiliki status kepatuhan patch COMPLIANT setelah instalasi patch

[SSM.3] Instans Amazon EC2 yang dikelola oleh Systems Manager harus memiliki status kepatuhan asosiasi COMPLIANT

[SSM.4] Dokumen SSM seharusnya tidak bersifat publik

[StepFunctions.1] Mesin status Step Functions seharusnya mengaktifkan logging

[Transfer.2] Server Transfer Family tidak boleh menggunakan protokol FTP untuk koneksi titik akhir

[WAF.1] Pencatatan ACL Web Global AWS WAF Klasik harus diaktifkan

[WAF.2] Aturan Regional AWS WAF Klasik harus memiliki setidaknya satu syarat

[WAF.3] Kelompok aturan Regional AWS WAF Klasik harus memiliki setidaknya satu aturan

[WAF.4] ACL web Regional AWS WAF klasik harus memiliki setidaknya satu aturan atau kelompok aturan

[WAF.6] Aturan global AWS WAF klasik harus memiliki setidaknya satu syarat

[WAF.7] Kelompok aturan global AWS WAF klasik harus memiliki setidaknya satu aturan

[WAF.8] ACL web global AWS WAF klasik harus memiliki setidaknya satu aturan atau kelompok aturan

[WAF.10] ACL AWS WAF web harus memiliki setidaknya satu aturan atau kelompok aturan

AWS WAF Aturan [WAF.12] harus mengaktifkan metrik CloudWatch

Tolok Ukur AWS Yayasan CIS

Tolok Ukur AWS Yayasan Center for Internet Security (CIS) berfungsi sebagai seperangkat praktik terbaik konfigurasi keamanan untuk. AWS Praktik terbaik yang diterima industri ini memberi Anda prosedur step-by-step implementasi, dan penilaian yang jelas. Mulai dari sistem operasi hingga layanan cloud dan perangkat jaringan, kontrol dalam tolok ukur ini membantu Anda melindungi sistem spesifik yang digunakan organisasi Anda.

AWS Security Hub mendukung CIS AWS Foundations Benchmark v3.0.0, 1.4.0, dan v1.2.0.

Halaman ini mencantumkan kontrol keamanan yang didukung setiap versi dan memberikan perbandingan versi.

Tolok Ukur AWS Yayasan CIS v3.0.0

Security Hub mendukung versi 3.0.0 dari CIS AWS Foundations Benchmark.

Security Hub telah memenuhi persyaratan Sertifikasi Perangkat Lunak Keamanan CIS dan telah dianugerahi Sertifikasi Perangkat Lunak Keamanan CIS untuk Tolok Ukur CIS berikut:

- Tolok Ukur CIS untuk Tolok Ukur AWS Yayasan CIS, v3.0.0, Level 1
- Tolok Ukur CIS untuk Tolok Ukur AWS Yayasan CIS, v3.0.0, Level 2

Kontrol yang berlaku untuk CIS AWS Foundations Benchmark v3.0.0

[Akun.1] Informasi kontak keamanan harus disediakan untuk Akun AWS

[CloudTrail.1] CloudTrail harus diaktifkan dan dikonfigurasi dengan setidaknya satu jejak Multi-wilayah yang mencakup acara manajemen baca dan tulis

[CloudTrail.2] CloudTrail harus mengaktifkan enkripsi saat istirahat

[CloudTrail.4] validasi file CloudTrail log harus diaktifkan

[CloudTrail.7] Pastikan pencatatan akses bucket S3 diaktifkan pada bucket CloudTrail S3

[Config.1] AWS Config harus diaktifkan dan menggunakan peran terkait layanan untuk perekaman sumber daya

[EC2.2] Grup keamanan default VPC tidak boleh mengizinkan lalu lintas masuk atau keluar

[EC2.6] Pencatatan aliran VPC harus diaktifkan di semua VPC

[EC2.7] Enkripsi default EBS harus diaktifkan

[EC2.8] Instans EC2 harus menggunakan Layanan Metadata Instance Versi 2 (IMDSv2)

[EC2.21] ACL jaringan seharusnya tidak mengizinkan masuknya dari 0.0.0.0/0 ke port 22 atau port 3389

[EC2.53] Grup keamanan EC2 tidak boleh mengizinkan masuknya dari 0.0.0.0/0 ke port administrasi server jarak jauh

[EC2.54] Grup keamanan EC2 tidak boleh mengizinkan masuknya dari: :/0 ke port administrasi server jarak jauh

[EFS.1] Sistem File Elastis harus dikonfigurasi untuk mengenkripsi data file saat istirahat menggunakan AWS KMS

[IAM.2] Pengguna IAM seharusnya tidak memiliki kebijakan IAM yang dilampirkan

[IAM.3] Kunci akses pengguna IAM harus diputar setiap 90 hari atau kurang

[IAM.4] Kunci akses pengguna root IAM seharusnya tidak ada

[IAM.5] MFA harus diaktifkan untuk semua pengguna IAM yang memiliki kata sandi konsol

[IAM.6] MFA perangkat keras harus diaktifkan untuk pengguna root

[IAM.9] MFA harus diaktifkan untuk pengguna root

[IAM.15] Pastikan kebijakan kata sandi IAM membutuhkan panjang kata sandi minimum 14 atau lebih

[IAM.16] Pastikan kebijakan kata sandi IAM mencegah penggunaan kembali kata sandi

[IAM.18] Memastikan peran dukungan telah dibuat untuk mengelola insiden dengan AWS Support

[IAM.22] Kredensyal pengguna IAM yang tidak digunakan selama 45 hari harus dihapus

[IAM.26] Sertifikat SSL/TLS kedaluwarsa yang dikelola di IAM harus dihapus

[IAM.27] Identitas IAM seharusnya tidak memiliki kebijakan yang dilampirkan AWSCloudShellFullAccess

[IAM.28] IAM Access Analyzer penganalisis akses eksternal harus diaktifkan

[KMS.4] rotasi AWS KMS tombol harus diaktifkan

[RDS.2] Instans RDS DB harus melarang akses publik, sebagaimana ditentukan oleh urasi PubliclyAccessible AWS Config

[RDS.3] Instans RDS DB harus mengaktifkan enkripsi saat istirahat

[RDS.13] Peningkatan versi minor otomatis RDS harus diaktifkan

[S3.1] Bucket tujuan umum S3 harus mengaktifkan pengaturan akses publik blok

[S3.5] Bucket tujuan umum S3 harus memerlukan permintaan untuk menggunakan SSL

[S3.8] Bucket tujuan umum S3 harus memblokir akses publik

[S3.20] Bucket tujuan umum S3 harus mengaktifkan penghapusan MFA

[S3.22] Bucket tujuan umum S3 harus mencatat peristiwa penulisan tingkat objek

[S3.23] Bucket tujuan umum S3 harus mencatat peristiwa pembacaan tingkat objek

Tolok Ukur AWS Yayasan CIS v1.4.0

Security Hub mendukung v1.4.0 dari CIS AWS Foundations Benchmark.

Kontrol yang berlaku untuk CIS AWS Foundations Benchmark v1.4.0

[CloudTrail.1] CloudTrail harus diaktifkan dan dikonfigurasi dengan setidaknya satu jejak Multi-wilayah yang mencakup acara manajemen baca dan tulis

[CloudTrail.2] CloudTrail harus mengaktifkan enkripsi saat istirahat

[CloudTrail.4] validasi file CloudTrail log harus diaktifkan

[CloudTrail.5] CloudTrail jalur harus diintegrasikan dengan Amazon Logs CloudWatch

[CloudTrail.6] Pastikan bucket S3 yang digunakan untuk menyimpan CloudTrail log tidak dapat diakses publik

[CloudTrail.7] Pastikan pencatatan akses bucket S3 diaktifkan pada bucket CloudTrail S3

[CloudWatch.1] Filter metrik log dan alarm harus ada untuk penggunaan pengguna “root”

[CloudWatch.4] Pastikan filter metrik log dan alarm ada untuk perubahan kebijakan IAM

[CloudWatch.5] Pastikan filter metrik log dan alarm ada untuk perubahan CloudTrail AWS Config urasi

[CloudWatch.6] Pastikan filter metrik log dan alarm ada untuk kegagalan AWS Management Console otentikasi

[CloudWatch.7] Pastikan filter metrik log dan alarm ada untuk menonaktifkan atau menjadwalkan penghapusan kunci yang dikelola pelanggan

[CloudWatch.8] Pastikan filter metrik log dan alarm ada untuk perubahan kebijakan bucket S3

[CloudWatch.9] Pastikan filter metrik log dan alarm ada untuk perubahan AWS Config konfigurasi

[CloudWatch.10] Pastikan filter metrik log dan alarm ada untuk perubahan grup keamanan

[CloudWatch.11] Pastikan filter metrik log dan alarm ada untuk perubahan pada Daftar Kontrol Akses Jaringan (NACL)

[CloudWatch.12] Pastikan filter metrik log dan alarm ada untuk perubahan pada gateway jaringan

[CloudWatch.13] Pastikan filter metrik log dan alarm ada untuk perubahan tabel rute

[CloudWatch.14] Pastikan filter metrik log dan alarm ada untuk perubahan VPC

[Config.1] AWS Config harus diaktifkan dan menggunakan peran terkait layanan untuk perekaman sumber daya

[EC2.2] Grup keamanan default VPC tidak boleh mengizinkan lalu lintas masuk atau keluar

[EC2.6] Pencatatan aliran VPC harus diaktifkan di semua VPC

[EC2.7] Enkripsi default EBS harus diaktifkan

[EC2.21] ACL jaringan seharusnya tidak mengizinkan masuknya dari 0.0.0.0/0 ke port 22 atau port 3389

[IAM.1] Kebijakan IAM seharusnya tidak mengizinkan hak administratif “*” penuh

[IAM.3] Kunci akses pengguna IAM harus diputar setiap 90 hari atau kurang

[IAM.4] Kunci akses pengguna root IAM seharusnya tidak ada

[IAM.5] MFA harus diaktifkan untuk semua pengguna IAM yang memiliki kata sandi konsol

[IAM.6] MFA perangkat keras harus diaktifkan untuk pengguna root

[IAM.9] MFA harus diaktifkan untuk pengguna root

[IAM.15] Pastikan kebijakan kata sandi IAM membutuhkan panjang kata sandi minimum 14 atau lebih

[IAM.16] Pastikan kebijakan kata sandi IAM mencegah penggunaan kembali kata sandi

[IAM.18] Memastikan peran dukungan telah dibuat untuk mengelola insiden dengan AWS Support

[IAM.22] Kredensyal pengguna IAM yang tidak digunakan selama 45 hari harus dihapus

[KMS.4] rotasi AWS KMS tombol harus diaktifkan

[RDS.3] Instans RDS DB harus mengaktifkan enkripsi saat istirahat

[S3.1] Bucket tujuan umum S3 harus mengaktifkan pengaturan akses publik blok

[S3.5] Bucket tujuan umum S3 harus memerlukan permintaan untuk menggunakan SSL

[S3.8] Bucket tujuan umum S3 harus memblokir akses publik

[S3.20] Bucket tujuan umum S3 harus mengaktifkan penghapusan MFA

Tolok Ukur AWS Yayasan Pusat Keamanan Internet (CIS) v1.2.0

Security Hub mendukung versi 1.2.0 dari CIS AWS Foundations Benchmark.

Security Hub telah memenuhi persyaratan Sertifikasi Perangkat Lunak Keamanan CIS dan telah dianugerahi Sertifikasi Perangkat Lunak Keamanan CIS untuk Tolok Ukur CIS berikut:

- Tolok Ukur CIS untuk Tolok Ukur AWS Yayasan CIS, v1.2.0, Level 1
- Tolok Ukur CIS untuk Tolok Ukur AWS Yayasan CIS, v1.2.0, Level 2

Kontrol yang berlaku untuk CIS AWS Foundations Benchmark v1.2.0

[CloudTrail.1] CloudTrail harus diaktifkan dan dikonfigurasi dengan setidaknya satu jejak Multi-wilayah yang mencakup acara manajemen baca dan tulis

[CloudTrail.2] CloudTrail harus mengaktifkan enkripsi saat istirahat

[CloudTrail.4] validasi file CloudTrail log harus diaktifkan

[CloudTrail.5] CloudTrail jalur harus diintegrasikan dengan Amazon Logs CloudWatch

[CloudTrail.6] Pastikan bucket S3 yang digunakan untuk menyimpan CloudTrail log tidak dapat diakses publik

[CloudTrail.7] Pastikan pencatatan akses bucket S3 diaktifkan pada bucket CloudTrail S3

[CloudWatch.1] Filter metrik log dan alarm harus ada untuk penggunaan pengguna “root”

[CloudWatch.2] Pastikan filter metrik log dan alarm ada untuk panggilan API yang tidak sah

[CloudWatch.3] Pastikan filter metrik log dan alarm ada untuk login Konsol Manajemen tanpa MFA

[CloudWatch.4] Pastikan filter metrik log dan alarm ada untuk perubahan kebijakan IAM

[CloudWatch.5] Pastikan filter metrik log dan alarm ada untuk perubahan CloudTrail AWS Config urasi

[CloudWatch.6] Pastikan filter metrik log dan alarm ada untuk kegagalan AWS Management Console otentikasi

[CloudWatch.7] Pastikan filter metrik log dan alarm ada untuk menonaktifkan atau menjadwalkan penghapusan kunci yang dikelola pelanggan

[CloudWatch.8] Pastikan filter metrik log dan alarm ada untuk perubahan kebijakan bucket S3

[CloudWatch.9] Pastikan filter metrik log dan alarm ada untuk perubahan AWS Config konfigurasi

[CloudWatch.10] Pastikan filter metrik log dan alarm ada untuk perubahan grup keamanan

[CloudWatch.11] Pastikan filter metrik log dan alarm ada untuk perubahan pada Daftar Kontrol Akses Jaringan (NACL)

[CloudWatch.12] Pastikan filter metrik log dan alarm ada untuk perubahan pada gateway jaringan

[CloudWatch.13] Pastikan filter metrik log dan alarm ada untuk perubahan tabel rute

[CloudWatch.14] Pastikan filter metrik log dan alarm ada untuk perubahan VPC

[Config.1] AWS Config harus diaktifkan dan menggunakan peran terkait layanan untuk perekaman sumber daya

[EC2.2] Grup keamanan default VPC tidak boleh mengizinkan lalu lintas masuk atau keluar

[EC2.6] Pencatatan aliran VPC harus diaktifkan di semua VPC

[EC2.13] Grup keamanan tidak boleh mengizinkan masuknya dari 0.0.0.0/0 atau: :/0 ke port 22

[EC2.14] Grup keamanan tidak boleh mengizinkan masuknya dari 0.0.0.0/0 atau: :/0 ke port 3389

[IAM.1] Kebijakan IAM seharusnya tidak mengizinkan hak administratif “*” penuh

[IAM.2] Pengguna IAM seharusnya tidak memiliki kebijakan IAM yang dilampirkan

[IAM.3] Kunci akses pengguna IAM harus diputar setiap 90 hari atau kurang

[IAM.4] Kunci akses pengguna root IAM seharusnya tidak ada

[IAM.5] MFA harus diaktifkan untuk semua pengguna IAM yang memiliki kata sandi konsol

[IAM.6] MFA perangkat keras harus diaktifkan untuk pengguna root

[IAM.8] Kredensyal pengguna IAM yang tidak digunakan harus dihapus

[IAM.9] MFA harus diaktifkan untuk pengguna root

[IAM.11] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu huruf besar

[IAM.12] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu huruf kecil

[IAM.13] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu simbol

[IAM.14] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu nomor

[IAM.15] Pastikan kebijakan kata sandi IAM membutuhkan panjang kata sandi minimum 14 atau lebih

[IAM.16] Pastikan kebijakan kata sandi IAM mencegah penggunaan kembali kata sandi

[IAM.17] Pastikan kebijakan kata sandi IAM kedaluwarsa kata sandi dalam waktu 90 hari atau kurang

[IAM.18] Memastikan peran dukungan telah dibuat untuk mengelola insiden dengan AWS Support

[KMS.4] rotasi AWS KMS tombol harus diaktifkan

Perbandingan versi untuk CIS AWS Foundations Benchmark

Bagian ini merangkum perbedaan antara Center for Internet Security (CIS) AWS Foundations Benchmark v3.0.0, v1.4.0, dan v1.2.0.

Security Hub mendukung masing-masing versi Tolok Ukur AWS Yayasan CIS ini, tetapi kami sarankan menggunakan v3.0.0 untuk tetap mengikuti praktik terbaik keamanan. Anda mungkin memiliki beberapa versi standar yang diaktifkan secara bersamaan. Untuk informasi selengkapnya, lihat Mengaktifkan dan menonaktifkan standar keamanan. Jika Anda ingin memutakhirkan ke v3.0.0, yang terbaik adalah mengaktifkannya terlebih dahulu sebelum menonaktifkan versi yang lebih lama. Jika Anda menggunakan integrasi Security Hub AWS Organizations untuk mengelola beberapa

secara terpusat Akun AWS dan Anda ingin mengaktifkan v3.0.0 secara batch di semua akun, Anda dapat menggunakan konfigurasi pusat.

Pemetaan kontrol ke persyaratan CIS di setiap versi

Memahami kontrol mana yang mendukung setiap versi CIS AWS Foundations Benchmark.

Kontrol ID dan judul	Persyaratan CIS v3.0.0	Persyaratan CIS v1.4.0	Persyaratan CIS v1.2.0
[Akun.1] Informasi kontak keamanan harus disediakan untuk Akun AWS	1.2	1.2	1.18
[CloudTrail.1] CloudTrail harus diaktifkan dan dikonfigurasi dengan setidaknya satu jejak Multi-wilayah yang mencakup acara manajemen baca dan tulis	3.1	3.1	2.1
[CloudTrail.1] CloudTrail harus diaktifkan dan dikonfigurasi dengan setidaknya satu jejak Multi-wilayah yang mencakup acara manajemen baca dan tulis	3.1	3.1	2.1
[CloudTrail.2] CloudTrail harus mengaktifkan enkripsi saat istirahat	3.5	3.7	2.7
[CloudTrail.4] validasi file CloudTrail log harus diaktifkan	3.2	3.2	2.2
[CloudTrail.5] CloudTrail jalur harus diintegrasikan dengan Amazon Logs CloudWatch	Tidak didukung - CIS menghapus persyaratan ini	3.4	2.4
[CloudTrail.6] Pastikan bucket S3 yang digunakan untuk menyimpan CloudTrail log tidak dapat diakses publik	Tidak didukung - CIS menghapus persyaratan ini	3.3	2.3

Kontrol ID dan judul	Persyaratan CIS v3.0.0	Persyaratan CIS v1.4.0	Persyaratan CIS v1.2.0
[CloudTrail.7] Pastikan pencatatan akses bucket S3 diaktifkan pada bucket CloudTrail S3	3.4	3.6	2.6
[CloudWatch.1] Filter metrik log dan alarm harus ada untuk penggunaan pengguna “root”	Tidak didukung - pemeriksaan manual	4.3	3.3
[CloudWatch.2] Pastikan filter metrik log dan alarm ada untuk panggilan API yang tidak sah	Tidak didukung - pemeriksaan manual	Tidak didukung - pemeriksaan manual	3.1
[CloudWatch.3] Pastikan filter metrik log dan alarm ada untuk login Konsol Manajemen tanpa MFA	Tidak didukung - pemeriksaan manual	Tidak didukung - pemeriksaan manual	3.2
[CloudWatch.4] Pastikan filter metrik log dan alarm ada untuk perubahan kebijakan IAM	Tidak didukung - pemeriksaan manual	4.4	3.4
[CloudWatch.5] Pastikan filter metrik log dan alarm ada untuk perubahan CloudTrail AWS Config urasi	Tidak didukung - pemeriksaan manual	4,5	3.5
[CloudWatch.6] Pastikan filter metrik log dan alarm ada untuk kegagalan AWS Management Console otentikasi	Tidak didukung - pemeriksaan manual	4.6	3.6
[CloudWatch.7] Pastikan filter metrik log dan alarm ada untuk menonaktifkan atau menjadwalkan penghapusan kunci yang dikelola pelanggan	Tidak didukung - pemeriksaan manual	4.7	3.7

Kontrol ID dan judul	Persyaratan CIS v3.0.0	Persyaratan CIS v1.4.0	Persyaratan CIS v1.2.0
[CloudWatch.8] Pastikan filter metrik log dan alarm ada untuk perubahan kebijakan bucket S3	Tidak didukung - pemeriksaan manual	4.8	3.8
[CloudWatch.9] Pastikan filter metrik log dan alarm ada untuk perubahan AWS Config konfigurasi	Tidak didukung - pemeriksaan manual	4.9	3.9
[CloudWatch.10] Pastikan filter metrik log dan alarm ada untuk perubahan grup keamanan	Tidak didukung - pemeriksaan manual	4.10	3.10
[CloudWatch.11] Pastikan filter metrik log dan alarm ada untuk perubahan pada Daftar Kontrol Akses Jaringan (NACL)	Tidak didukung - pemeriksaan manual	4.11	3.11
[CloudWatch.12] Pastikan filter metrik log dan alarm ada untuk perubahan pada gateway jaringan	Tidak didukung - pemeriksaan manual	4.12	3.12
[CloudWatch.13] Pastikan filter metrik log dan alarm ada untuk perubahan tabel rute	Tidak didukung - pemeriksaan manual	4.13	3.13
[CloudWatch.14] Pastikan filter metrik log dan alarm ada untuk perubahan VPC	Tidak didukung - pemeriksaan manual	4.14	3.14
[Config.1] AWS Config harus diaktifkan dan menggunakan peran terkait layanan untuk perekaman sumber daya	3.3	3.5	2.5

Kontrol ID dan judul	Persyaratan CIS v3.0.0	Persyaratan CIS v1.4.0	Persyaratan CIS v1.2.0
[EC2.2] Grup keamanan default VPC tidak boleh mengizinkan lalu lintas masuk atau keluar	5.4	5.3	4.3
[EC2.6] Pencatatan aliran VPC harus diaktifkan di semua VPC	3.7	3.9	2.9
[EC2.7] Enkripsi default EBS harus diaktifkan	2.2.1	2.2.1	Tidak didukung
[EC2.8] Instans EC2 harus menggunakan Layanan Metadata Instance Versi 2 (IMDSv2)	5.6	Tidak didukung	Tidak didukung
[EC2.13] Grup keamanan tidak boleh mengizinkan masuknya dari 0.0.0.0/0 atau: :/0 ke port 22	Tidak didukung - digantikan oleh persyaratan 5.2 dan 5.3	Tidak didukung - digantikan oleh persyaratan 5.2 dan 5.3	4.1
[EC2.14] Grup keamanan tidak boleh mengizinkan masuknya dari 0.0.0.0/0 atau: :/0 ke port 3389	Tidak didukung - digantikan oleh persyaratan 5.2 dan 5.3	Tidak didukung - digantikan oleh persyaratan 5.2 dan 5.3	4.2
[EC2.21] ACL jaringan seharusnya tidak mengizinkan masuknya dari 0.0.0.0/0 ke port 22 atau port 3389	5.1	5.1	Tidak didukung
[EC2.53] Grup keamanan EC2 tidak boleh mengizinkan masuknya dari 0.0.0.0/0 ke port administrasi server jarak jauh	5.2	Tidak didukung	Tidak didukung

Kontrol ID dan judul	Persyaratan CIS v3.0.0	Persyaratan CIS v1.4.0	Persyaratan CIS v1.2.0
[EC2.54] Grup keamanan EC2 tidak boleh mengizinkan masuknya dari: :/0 ke port administrasi server jarak jauh	5.3	Tidak didukung	Tidak didukung
[EFS.1] Sistem File Elastis harus dikonfigurasi untuk mengenkripsi data file saat istirahat menggunakan AWS KMS	2.4.1	Tidak didukung	Tidak didukung
[IAM.1] Kebijakan IAM seharusnya tidak mengizinkan hak administratif “*” penuh	Tidak didukung	1.16	1.22
[IAM.2] Pengguna IAM seharusnya tidak memiliki kebijakan IAM yang dilampirkan	1.15	Tidak didukung	1.16
[IAM.3] Kunci akses pengguna IAM harus diputar setiap 90 hari atau kurang	1.14	1.14	1.4
[IAM.4] Kunci akses pengguna root IAM seharusnya tidak ada	1.4	1.4	1.12
[IAM.5] MFA harus diaktifkan untuk semua pengguna IAM yang memiliki kata sandi konsol	1.10	1.10	1.2
[IAM.6] MFA perangkat keras harus diaktifkan untuk pengguna root	1.6	1.6	1.14

Kontrol ID dan judul	Persyaratan CIS v3.0.0	Persyaratan CIS v1.4.0	Persyaratan CIS v1.2.0
[IAM.8] Kredensyal pengguna IAM yang tidak digunakan harus dihapus	Tidak didukung — lihat [IAM.22] Kredensyal pengguna IAM yang tidak digunakan selama 45 hari harus dihapus sebagai gantinya	Tidak didukung — lihat [IAM.22] Kredensyal pengguna IAM yang tidak digunakan selama 45 hari harus dihapus sebagai gantinya	1.3
[IAM.9] MFA harus diaktifkan untuk pengguna root	1.5	1.5	1.13
[IAM.11] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu huruf besar	Tidak didukung - CIS menghapus persyaratan ini	Tidak didukung - CIS menghapus persyaratan ini	1.5
[IAM.12] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu huruf kecil	Tidak didukung - CIS menghapus persyaratan ini	Tidak didukung - CIS menghapus persyaratan ini	1.6
[IAM.13] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu simbol	Tidak didukung - CIS menghapus persyaratan ini	Tidak didukung - CIS menghapus persyaratan ini	1.7
[IAM.14] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu nomor	Tidak didukung - CIS menghapus persyaratan ini	Tidak didukung - CIS menghapus persyaratan ini	1.8
[IAM.15] Pastikan kebijakan kata sandi IAM membutuhkan panjang kata sandi minimum 14 atau lebih	1.8	1.8	1.9

Kontrol ID dan judul	Persyaratan CIS v3.0.0	Persyaratan CIS v1.4.0	Persyaratan CIS v1.2.0
[IAM.16] Pastikan kebijakan kata sandi IAM mencegah penggunaan kembali kata sandi	1.9	1.9	1.10
[IAM.17] Pastikan kebijakan kata sandi IAM kedaluwarsa kata sandi dalam waktu 90 hari atau kurang	Tidak didukung - CIS menghapus persyaratan ini	Tidak didukung - CIS menghapus persyaratan ini	1.11
[IAM.18] Memastikan peran dukungan telah dibuat untuk mengelola insiden dengan AWS Support	1.17	1.17	1.2
[IAM.20] Hindari penggunaan pengguna root	Tidak didukung - CIS menghapus persyaratan ini	Tidak didukung - CIS menghapus persyaratan ini	1.1
[IAM.22] Kredensyal pengguna IAM yang tidak digunakan selama 45 hari harus dihapus	1.12	1.12	Tidak didukung - CIS menambahkan persyaratan ini di versi yang lebih baru
[IAM.26] Sertifikat SSL/TLS kedaluwarsa yang dikelola di IAM harus dihapus	1.19	Tidak didukung - CIS menambahkan persyaratan ini di versi yang lebih baru	Tidak didukung - CIS menambahkan persyaratan ini di versi yang lebih baru
[IAM.27] Identitas IAM seharusnya tidak memiliki kebijakan yang dilampirkan AWSCloudShellFullAccess	1.22	Tidak didukung - CIS menambahkan persyaratan ini di versi yang lebih baru	Tidak didukung - CIS menambahkan persyaratan ini di versi yang lebih baru

Kontrol ID dan judul	Persyaratan CIS v3.0.0	Persyaratan CIS v1.4.0	Persyaratan CIS v1.2.0
[IAM.28] IAM Access Analyzer penganalisis akses eksternal harus diaktifkan	1.20	Tidak didukung - CIS menambahkan persyaratan ini di versi yang lebih baru	Tidak didukung - CIS menambahkan persyaratan ini di versi yang lebih baru
[KMS.4] rotasi AWS KMS tombol harus diaktifkan	3.6	3.8	2.8
[Macie.1] Amazon Macie harus diaktifkan	Tidak didukung - pemeriksaan manual	Tidak didukung - pemeriksaan manual	Tidak didukung - pemeriksaan manual
[RDS.2] Instans RDS DB harus melarang akses publik, sebagaimana ditentukan oleh urasi PubliclyAccessible AWS Config	2.3.3	Tidak didukung - CIS menambahkan persyaratan ini di versi yang lebih baru	Tidak didukung - CIS menambahkan persyaratan ini di versi yang lebih baru
[RDS.3] Instans RDS DB harus mengaktifkan enkripsi saat istirahat	2.3.1	2.3.1	Tidak didukung - CIS menambahkan persyaratan ini di versi yang lebih baru
[RDS.13] Peningkatan versi minor otomatis RDS harus diaktifkan	2.3.2	Tidak didukung - CIS menambahkan persyaratan ini di versi yang lebih baru	Tidak didukung - CIS menambahkan persyaratan ini di versi yang lebih baru

Kontrol ID dan judul	Persyaratan CIS v3.0.0	Persyaratan CIS v1.4.0	Persyaratan CIS v1.2.0
[S3.1] Bucket tujuan umum S3 harus mengaktifkan pengaturan akses publik blok	2.1.4	2.1.5	Tidak didukung - CIS menambahkan persyaratan ini di versi yang lebih baru
[S3.5] Bucket tujuan umum S3 harus memerlukan permintaan untuk menggunakan SSL	2.1.1	2.1.2	Tidak didukung - CIS menambahkan persyaratan ini di versi yang lebih baru
[S3.8] Bucket tujuan umum S3 harus memblokir akses publik	2.1.4	2.1.5	Tidak didukung - CIS menambahkan persyaratan ini di versi yang lebih baru
[S3.20] Bucket tujuan umum S3 harus mengaktifkan penghapusan MFA	2.1.2	2.1.3	Tidak didukung - CIS menambahkan persyaratan ini di versi yang lebih baru

ARN untuk Tolok Ukur Yayasan CIS AWS

Ketika Anda mengaktifkan satu atau beberapa versi CIS AWS Foundations Benchmark, Anda akan mulai menerima temuan dalam AWS Security Finding Format (ASFF). Di ASFF, setiap versi menggunakan Amazon Resource Name (ARN) berikut:

Tolok Ukur AWS Yayasan CIS v3.0.0

```
arn:aws:securityhub:region::standards/cis-aws-foundations-benchmark/
v/3.0.0
```

Tolok Ukur AWS Yayasan CIS v1.4.0

```
arn:aws:securityhub:region::standards/cis-aws-foundations-benchmark/
v/1.4.0
```

Tolok Ukur AWS Yayasan CIS v1.2.0

```
arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0
```

Anda dapat menggunakan GetEnabledStandardspengoperasian Security Hub API untuk mengetahui ARN dari standar yang diaktifkan.

Nilai-nilai sebelumnya adalah untuk. `StandardsArn` Namun, `StandardsSubscriptionArn` mengacu pada sumber daya langganan standar yang dibuat Security Hub saat Anda berlangganan standar dengan menelepon BatchEnableStandardsdi Wilayah.

> **Note**
>
> Saat Anda mengaktifkan versi Tolok Ukur AWS Yayasan CIS, Security Hub dapat memakan waktu hingga 18 jam untuk menghasilkan temuan untuk kontrol yang menggunakan aturan AWS Config terkait layanan yang sama dengan kontrol yang diaktifkan dalam standar lain yang diaktifkan. Untuk informasi selengkapnya, lihat Jadwal untuk menjalankan pemeriksaan keamanan.

Menemukan bidang berbeda jika Anda mengaktifkan temuan kontrol konsolidasi. Untuk informasi selengkapnya tentang metrik ini, lihat Dampak konsolidasi pada bidang dan nilai ASFF. Untuk temuan kontrol sampel, lihatTemuan kontrol sampel.

Persyaratan CIS yang tidak didukung di Security Hub

Seperti disebutkan dalam tabel sebelumnya, Security Hub tidak mendukung setiap persyaratan CIS di setiap versi CIS Foundations Benchmark. AWS Banyak persyaratan yang tidak didukung hanya dapat dievaluasi secara manual dengan meninjau status sumber daya Anda. AWS

Institut Nasional Standar dan Teknologi (NIST) SP 800-53 Rev. 5

NIST SP 800-53 Rev. 5 adalah kerangka kerja keamanan siber dan kepatuhan yang dikembangkan oleh National Institute of Standards and Technology (NIST), sebuah lembaga yang merupakan bagian dari Departemen Perdagangan AS. Kerangka kepatuhan ini membantu Anda melindungi

ketersediaan, kerahasiaan, dan integritas sistem informasi dan sumber daya penting Anda. Lembaga dan kontraktor pemerintah federal AS harus mematuhi NIST SP 800-53 untuk melindungi sistem mereka, tetapi perusahaan swasta dapat secara sukarela menggunakannya sebagai kerangka panduan untuk mengurangi risiko keamanan siber.

Security Hub menyediakan kontrol yang mendukung persyaratan NIST SP 800-53 tertentu. Kontrol ini dievaluasi melalui pemeriksaan keamanan otomatis. Kontrol Security Hub tidak mendukung persyaratan NIST SP 800-53 yang memerlukan pemeriksaan manual. Selain itu, kontrol Security Hub hanya mendukung persyaratan NIST SP 800-53 otomatis yang terdaftar sebagai persyaratan Terkait dalam detail untuk setiap kontrol. Pilih kontrol dari daftar berikut untuk melihat detailnya. Persyaratan terkait yang tidak disebutkan dalam detail kontrol saat ini tidak didukung oleh Security Hub.

Tidak seperti kerangka kerja lainnya, NIST SP 800-53 tidak preskriptif tentang bagaimana persyaratannya harus dievaluasi. Sebaliknya, kerangka kerja menyediakan pedoman, dan kontrol Security Hub NIST SP 800-53 mewakili pemahaman layanan tentang mereka.

Jika Anda menggunakan integrasi Security Hub AWS Organizations untuk mengelola beberapa akun secara terpusat dan ingin mengaktifkan NIST SP 800-53 secara batch di semuanya, Anda dapat menjalankan skrip multi-akun Security Hub dari akun administrator.

Untuk informasi lebih lanjut tentang NIST SP 800-53 Rev. 5, lihat Pusat Sumber Daya Keamanan Komputer NIST.

Kontrol yang berlaku untuk NIST SP 800-53 Rev. 5

[Akun.1] Informasi kontak keamanan harus disediakan untuk Akun AWS

[Akun.2] Akun AWS harus menjadi bagian dari organisasi AWS Organizations

[ACM.1] Sertifikat yang diimpor dan diterbitkan ACM harus diperbarui setelah jangka waktu tertentu

[ApiGateway.1] API Gateway REST WebSocket dan pencatatan eksekusi API harus diaktifkan

[ApiGateway.2] Tahapan API Gateway REST API harus dikonfigurasi untuk menggunakan sertifikat SSL untuk otentikasi backend

[ApiGateway.3] Tahapan API Gateway REST API harus mengaktifkan penelusuran AWS X-Ray

[ApiGateway.4] API Gateway harus dikaitkan dengan ACL Web WAF

[ApiGateway.5] Data cache API Gateway REST API harus dienkripsi saat istirahat

[ApiGateway.8] Rute API Gateway harus menentukan jenis otorisasi

[ApiGateway.9] Pencatatan akses harus dikonfigurasi untuk Tahapan API Gateway V2

[AppSync.5] AWS AppSync GraphQL API tidak boleh diautentikasi dengan kunci API

[AutoScaling.1] Grup Auto Scaling yang terkait dengan penyeimbang beban harus menggunakan pemeriksaan kesehatan ELB

[AutoScaling.2] Grup Auto Scaling Amazon EC2 harus mencakup beberapa Availability Zone

[AutoScaling.3] Konfigurasi peluncuran grup Auto Scaling harus mengonfigurasi instans EC2 agar memerlukan Layanan Metadata Instans Versi 2 (IMDSv2)

[Autoscaling.5] Instans Amazon EC2 yang diluncurkan menggunakan konfigurasi peluncuran grup Auto Scaling seharusnya tidak memiliki alamat IP Publik

[AutoScaling.6] Grup Auto Scaling harus menggunakan beberapa jenis instance di beberapa Availability Zone

[AutoScaling.9] Grup Auto Scaling Amazon EC2 harus menggunakan templat peluncuran Amazon EC2

[Backup.1] titik AWS Backup pemulihan harus dienkripsi saat istirahat

[CloudFront.1] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi

[CloudFront.3] CloudFront distribusi harus memerlukan enkripsi dalam perjalanan

[CloudFront.4] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi

[CloudFront.5] CloudFront distribusi seharusnya mengaktifkan logging

[CloudFront.6] CloudFront distribusi harus mengaktifkan WAF

[CloudFront.7] CloudFront distribusi harus menggunakan sertifikat SSL/TLS khusus

[CloudFront.8] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS

[CloudFront.9] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus

[CloudFront.10] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal khusus

[CloudFront.12] CloudFront distribusi seharusnya tidak menunjukkan asal S3 yang tidak ada

[CloudTrail.1] CloudTrail harus diaktifkan dan dikonfigurasi dengan setidaknya satu jejak Multi-wilayah yang mencakup acara manajemen baca dan tulis

[CloudTrail.2] CloudTrail harus mengaktifkan enkripsi saat istirahat

[CloudTrail.4] validasi file CloudTrail log harus diaktifkan

[CloudTrail.5] CloudTrail jalur harus diintegrasikan dengan Amazon Logs CloudWatch

[CloudWatch.15] CloudWatch alarm harus memiliki tindakan tertentu yang dikonfigurasi

[CloudWatch.16] grup CloudWatch log harus dipertahankan untuk jangka waktu tertentu

[CloudWatch.17] tindakan CloudWatch alarm harus diaktifkan

[CodeBuild.1] URL repositori sumber CodeBuild Bitbucket tidak boleh berisi kredensyal sensitif

[CodeBuild.2] variabel lingkungan CodeBuild proyek tidak boleh berisi kredensil teks yang jelas

[CodeBuild.3] Log CodeBuild S3 harus dienkripsi

[CodeBuild.4] lingkungan CodeBuild proyek harus memiliki urasi logging AWS Config

[Config.1] AWS Config harus diaktifkan dan menggunakan peran terkait layanan untuk perekaman sumber daya

[DataFirehose.1] Aliran pengiriman Firehose harus dienkripsi saat istirahat

[DMS.1] Instans replikasi Layanan Migrasi Database tidak boleh bersifat publik

[DMS.6] Instans replikasi DMS harus mengaktifkan peningkatan versi minor otomatis

[DMS.7] Tugas replikasi DMS untuk database target seharusnya mengaktifkan logging

[DMS.8] Tugas replikasi DMS untuk database sumber seharusnya mengaktifkan logging

[DMS.9] Titik akhir DMS harus menggunakan SSL

[DMS.10] Titik akhir DMS untuk database Neptunus harus mengaktifkan otorisasi IAM

[DMS.11] Titik akhir DMS untuk MongoDB harus mengaktifkan mekanisme otentikasi

[DMS.12] Titik akhir DMS untuk Redis harus mengaktifkan TLS

[DocumentDB.1] Cluster Amazon DocumentDB harus dienkripsi saat istirahat

[DocumentDB.2] Cluster Amazon DocumentDB harus memiliki periode retensi cadangan yang memadai

[DocumentDB.3] Cuplikan cluster manual Amazon DocumentDB seharusnya tidak bersifat publik

[DocumentDB.4] Cluster Amazon DocumentDB harus mempublikasikan log audit ke Log CloudWatch

[DocumentDB.5] Cluster Amazon DocumentDB harus mengaktifkan perlindungan penghapusan

[DynamoDB.1] Tabel DynamoDB harus secara otomatis menskalakan kapasitas sesuai permintaan

[DynamoDB.2] Tabel DynamoDB harus mengaktifkan pemulihan point-in-time

[DynamoDB.3] Cluster DynamoDB Accelerator (DAX) harus dienkripsi saat istirahat

[DynamoDB.4] Tabel DynamoDB harus ada dalam rencana cadangan

[DynamoDB.6] Tabel DynamoDB harus mengaktifkan perlindungan penghapusan

[DynamoDB.7] Cluster DynamoDB Accelerator harus dienkripsi saat transit

[EC2.1] Snapshot Amazon EBS tidak boleh dipulihkan secara publik

[EC2.2] Grup keamanan default VPC tidak boleh mengizinkan lalu lintas masuk atau keluar

[EC2.3] Volume Amazon EBS yang terpasang harus dienkripsi saat istirahat

[EC2.4] Instans EC2 yang dihentikan harus dihapus setelah periode waktu tertentu

[EC2.6] Pencatatan aliran VPC harus diaktifkan di semua VPC

[EC2.7] Enkripsi default EBS harus diaktifkan

[EC2.8] Instans EC2 harus menggunakan Layanan Metadata Instance Versi 2 (IMDSv2)

[EC2.9] Instans Amazon EC2 seharusnya tidak memiliki alamat IPv4 publik

[EC2.10] Amazon EC2 harus dikonfigurasi untuk menggunakan titik akhir VPC yang dibuat untuk layanan Amazon EC2

[EC2.12] EIP Amazon EC2 yang tidak digunakan harus dihapus

[EC2.13] Grup keamanan tidak boleh mengizinkan masuknya dari 0.0.0.0/0 atau: :/0 ke port 22

[EC2.15] Subnet Amazon EC2 seharusnya tidak secara otomatis menetapkan alamat IP publik

[EC2.16] Daftar Kontrol Akses Jaringan yang Tidak Digunakan harus dihapus

[EC2.17] Instans Amazon EC2 tidak boleh menggunakan beberapa ENI

[EC2.18] Grup keamanan seharusnya hanya mengizinkan lalu lintas masuk yang tidak terbatas untuk port resmi

[EC2.19] Grup keamanan tidak boleh mengizinkan akses tidak terbatas ke port dengan risiko tinggi

[EC2.20] Kedua terowongan VPN untuk koneksi VPN Site-to-Site harus AWS aktif

[EC2.21] ACL jaringan seharusnya tidak mengizinkan masuknya dari 0.0.0.0/0 ke port 22 atau port 3389

[EC2.23] Amazon EC2 Transit Gateways seharusnya tidak secara otomatis menerima permintaan lampiran VPC

[EC2.24] Jenis instans paravirtual Amazon EC2 tidak boleh digunakan

[EC2.25] Templat peluncuran Amazon EC2 tidak boleh menetapkan IP publik ke antarmuka jaringan

[EC2.28] Volume EBS harus dicakup oleh rencana cadangan

[EC2.51] Titik akhir EC2 Client VPN harus mengaktifkan pencatatan koneksi klien

[ECR.1] Repositori pribadi ECR harus memiliki pemindaian gambar yang dikonfigurasi

[ECR.2] Repositori pribadi ECR harus memiliki kekekalan tag yang dikonfigurasi

[ECR.3] Repositori ECR harus memiliki setidaknya satu kebijakan siklus hidup yang dikonfigurasi

[ECS.1] Definisi tugas Amazon ECS harus memiliki mode jaringan yang aman dan definisi pengguna.

[ECS.2] Layanan ECS seharusnya tidak memiliki alamat IP publik yang ditetapkan kepadanya secara otomatis

[ECS.3] Definisi tugas ECS tidak boleh membagikan namespace proses host

[ECS.4] Kontainer ECS harus berjalan sebagai non-hak istimewa

[ECS.5] Wadah ECS harus dibatasi pada akses hanya-baca ke sistem file root

[ECS.8] Rahasia tidak boleh diteruskan sebagai variabel lingkungan kontainer

[ECS.9] Definisi tugas ECS harus memiliki konfigurasi logging

[ECS.10] Layanan ECS Fargate harus berjalan pada versi platform Fargate terbaru

[ECS.12] Cluster ECS harus menggunakan Wawasan Kontainer

[EFS.1] Sistem File Elastis harus dikonfigurasi untuk mengenkripsi data file saat istirahat menggunakan AWS KMS

[EFS.2] Volume Amazon EFS harus dalam rencana cadangan

[EFS.3] Titik akses EFS harus menegakkan direktori root

[EFS.4] Titik akses EFS harus menegakkan identitas pengguna

[EFS.6] Target pemasangan EFS tidak boleh dikaitkan dengan subnet publik

[EKS.1] Titik akhir klaster EKS seharusnya tidak dapat diakses publik

[EKS.2] Kluster EKS harus berjalan pada versi Kubernetes yang didukung

[EKS.3] Kluster EKS harus menggunakan rahasia Kubernetes terenkripsi

[EKS.8] Kluster EKS harus mengaktifkan pencatatan audit

[ElastiCache.1] Cluster ElastiCache Redis harus mengaktifkan pencadangan otomatis

[ElastiCache.2] ElastiCache untuk kluster cache Redis harus mengaktifkan peningkatan versi minor otomatis

[ElastiCache.3] ElastiCache untuk grup replikasi Redis harus mengaktifkan failover otomatis

[ElastiCache.4] ElastiCache untuk grup replikasi Redis harus dienkripsi saat istirahat

[ElastiCache.5] ElastiCache untuk grup replikasi Redis harus dienkripsi saat transit

[ElastiCache.6] ElastiCache untuk grup replikasi Redis sebelum versi 6.0 harus menggunakan Redis AUTH

[ElastiCache.7] ElastiCache cluster tidak boleh menggunakan grup subnet default

[ElasticBeanstalk.1] Lingkungan Elastic Beanstalk seharusnya mengaktifkan pelaporan kesehatan yang ditingkatkan

[ElasticBeanstalk.2] Pembaruan platform yang dikelola Elastic Beanstalk harus diaktifkan

[ELB.1] Application Load Balancer harus dikonfigurasi untuk mengalihkan semua permintaan HTTP ke HTTPS

[ELB.2] Classic Load Balancer dengan pendengar SSL/HTTPS harus menggunakan sertifikat yang disediakan oleh AWS Certificate Manager

[ELB.3] Pendengar Classic Load Balancer harus dikonfigurasi dengan penghentian HTTPS atau TLS

[ELB.4] Application Load Balancer harus dikonfigurasi untuk menjatuhkan header http

[ELB.5] Pencatatan aplikasi dan Classic Load Balancer harus diaktifkan

[ELB.6] Aplikasi, Gateway, dan Network Load Balancer harus mengaktifkan perlindungan penghapusan

[ELB.7] Classic Load Balancers harus mengaktifkan pengurasan koneksi

[ELB.8] Classic Load Balancer dengan pendengar SSL harus menggunakan kebijakan keamanan yang telah ditentukan sebelumnya yang memiliki urasi yang kuat AWS Config

[ELB.9] Classic Load Balancer harus mengaktifkan penyeimbangan beban lintas zona

[ELB.10] Classic Load Balancer harus menjangkau beberapa Availability Zone

[ELB.12] Application Load Balancer harus dikonfigurasi dengan mode mitigasi desync defensif atau paling ketat

[ELB.13] Penyeimbang Beban Aplikasi, Jaringan, dan Gateway harus mencakup beberapa Availability Zone

[ELB.14] Classic Load Balancer harus dikonfigurasi dengan mode mitigasi desync defensif atau paling ketat

[ELB.16] Application Load Balancers harus dikaitkan dengan ACL web AWS WAF

[EMR.1] Node primer cluster EMR Amazon seharusnya tidak memiliki alamat IP publik

[EMR.2] Pengaturan akses publik blok EMR Amazon harus diaktifkan

[ES.1] Domain Elasticsearch harus mengaktifkan enkripsi saat istirahat

[ES.2] Domain Elasticsearch tidak boleh diakses publik

[ES.3] Domain Elasticsearch harus mengenkripsi data yang dikirim antar node

[ES.4] Kesalahan domain Elasticsearch yang masuk ke CloudWatch Log harus diaktifkan

[ES.5] Domain Elasticsearch harus mengaktifkan pencatatan audit

[ES.6] Domain Elasticsearch harus memiliki setidaknya tiga node data

[ES.7] Domain Elasticsearch harus dikonfigurasi dengan setidaknya tiga node master khusus

[ES.8] Koneksi ke domain Elasticsearch harus dienkripsi menggunakan kebijakan keamanan TLS terbaru

[EventBridge.3] bus acara EventBridge khusus harus memiliki kebijakan berbasis sumber daya terlampir

[EventBridge.4] titik akhir EventBridge global harus mengaktifkan replikasi acara

[FSX.1] FSx untuk sistem file OpenZFS harus dikonfigurasi untuk menyalin tag ke cadangan dan volume

[FSX.2] Sistem file FSx for Lustre harus dikonfigurasi untuk menyalin tag ke cadangan

[GuardDuty.1] GuardDuty harus diaktifkan

[IAM.1] Kebijakan IAM seharusnya tidak mengizinkan hak administratif “*” penuh

[IAM.2] Pengguna IAM seharusnya tidak memiliki kebijakan IAM yang dilampirkan

[IAM.3] Kunci akses pengguna IAM harus diputar setiap 90 hari atau kurang

[IAM.4] Kunci akses pengguna root IAM seharusnya tidak ada

[IAM.5] MFA harus diaktifkan untuk semua pengguna IAM yang memiliki kata sandi konsol

[IAM.6] MFA perangkat keras harus diaktifkan untuk pengguna root

[IAM.7] Kebijakan kata sandi untuk pengguna IAM harus memiliki konfigurasi yang kuat

[IAM.8] Kredensyal pengguna IAM yang tidak digunakan harus dihapus

[IAM.9] MFA harus diaktifkan untuk pengguna root

[IAM.19] MFA harus diaktifkan untuk semua pengguna IAM

[IAM.21] Kebijakan terkelola pelanggan IAM yang Anda buat seharusnya tidak mengizinkan tindakan wildcard untuk layanan

[Kinesis.1] Aliran kinesis harus dienkripsi saat istirahat

[KMS.1] Kebijakan yang dikelola pelanggan IAM tidak boleh mengizinkan tindakan dekripsi pada semua kunci KMS

[KMS.2] Prinsipal IAM tidak boleh memiliki kebijakan inline IAM yang memungkinkan tindakan dekripsi pada semua kunci KMS

[KMS.3] tidak AWS KMS keys boleh dihapus secara tidak sengaja

[KMS.4] rotasi AWS KMS tombol harus diaktifkan

[Lambda.1] Kebijakan fungsi Lambda harus melarang akses publik

[Lambda.2] Fungsi Lambda harus menggunakan runtime yang didukung

[Lambda.3] Fungsi Lambda harus dalam VPC

[Lambda.5] Fungsi VPC Lambda harus beroperasi di beberapa Availability Zone

[Macie.1] Amazon Macie harus diaktifkan

[Macie.2] Penemuan data sensitif otomatis Macie harus diaktifkan

[MSK.1] Cluster MSK harus dienkripsi saat transit di antara node broker

[MSK.2] Kluster MSK seharusnya telah meningkatkan pemantauan yang dikonfigurasi

[MQ.2] Broker ActiveMQ harus mengalirkan log audit ke CloudWatch

[MQ.3] Broker Amazon MQ harus mengaktifkan peningkatan versi minor otomatis

[MQ.5] Broker ActiveMQ harus menggunakan mode penerapan aktif/siaga

[MQ.6] Broker RabbitMQ harus menggunakan mode penerapan cluster

[Neptunus.1] Cluster DB Neptunus harus dienkripsi saat istirahat

[Neptune.2] Cluster DB Neptunus harus menerbitkan log audit ke Log CloudWatch

[Neptune.3] Snapshot cluster Neptunus DB seharusnya tidak publik

[Neptunus.4] Cluster DB Neptunus harus mengaktifkan perlindungan penghapusan

[Neptunus.5] Cluster DB Neptunus harus mengaktifkan cadangan otomatis

[Neptune.6] Snapshot cluster Neptunus DB harus dienkripsi saat istirahat

[Neptunus.7] Cluster DB Neptunus harus mengaktifkan otentikasi basis data IAM

[Neptunus.8] Cluster DB Neptunus harus dikonfigurasi untuk menyalin tag ke snapshot

[Neptunus.9] Cluster DB Neptunus harus digunakan di beberapa Availability Zone

[NetworkFirewall.1] Firewall Firewall Jaringan harus digunakan di beberapa Availability Zone

[NetworkFirewall.2] Pencatatan Firewall Jaringan harus diaktifkan

[NetworkFirewall.3] Kebijakan Network Firewall harus memiliki setidaknya satu kelompok aturan yang terkait

[NetworkFirewall.4] Tindakan stateless default untuk kebijakan Network Firewall harus drop atau forward untuk paket penuh

[NetworkFirewall.5] Tindakan stateless default untuk kebijakan Network Firewall harus drop atau forward untuk paket yang terfragmentasi

[NetworkFirewall.6] Grup aturan Stateless Network Firewall tidak boleh kosong

[NetworkFirewall.9] Firewall Firewall Jaringan harus mengaktifkan perlindungan penghapusan

[Opensearch.1] OpenSearch domain harus mengaktifkan enkripsi saat istirahat

[Opensearch.2] OpenSearch domain tidak boleh diakses publik

[Opensearch.3] OpenSearch domain harus mengenkripsi data yang dikirim antar node

[Opensearch.4] login kesalahan OpenSearch domain ke Log harus diaktifkan CloudWatch

[Opensearch.5] OpenSearch domain harus mengaktifkan pencatatan audit

[Opensearch.6] OpenSearch domain harus memiliki setidaknya tiga node data

[Opensearch.7] OpenSearch domain harus mengaktifkan kontrol akses berbutir halus

[Opensearch.8] Koneksi ke OpenSearch domain harus dienkripsi menggunakan kebijakan keamanan TLS terbaru

[Opensearch.10] OpenSearch domain harus memiliki pembaruan perangkat lunak terbaru yang diinstal

[Opensearch.11] OpenSearch domain harus memiliki setidaknya tiga node primer khusus

[PCA.1] otoritas sertifikat AWS Private CA root harus dinonaktifkan

[RDS.1] Snapshot RDS harus pribadi

[RDS.2] Instans RDS DB harus melarang akses publik, sebagaimana ditentukan oleh urasi PubliclyAccessible AWS Config

[RDS.3] Instans RDS DB harus mengaktifkan enkripsi saat istirahat

[RDS.4] Snapshot cluster RDS dan snapshot database harus dienkripsi saat istirahat

[RDS.5] Instans RDS DB harus dikonfigurasi dengan beberapa Availability Zone

[RDS.6] Pemantauan yang ditingkatkan harus dikonfigurasi untuk instans RDS DB

[RDS.7] Cluster RDS harus mengaktifkan perlindungan penghapusan

[RDS.8] Instans RDS DB harus mengaktifkan perlindungan penghapusan

[RDS.9] Instans RDS DB harus menerbitkan log ke Log CloudWatch

[RDS.10] Otentikasi IAM harus dikonfigurasi untuk instance RDS

[RDS.11] Instans RDS harus mengaktifkan pencadangan otomatis

[RDS.12] Otentikasi IAM harus dikonfigurasi untuk cluster RDS

[RDS.13] Peningkatan versi minor otomatis RDS harus diaktifkan

[RDS.14] Cluster Amazon Aurora seharusnya mengaktifkan backtracking

[RDS.15] Cluster RDS DB harus dikonfigurasi untuk beberapa Availability Zone

[RDS.16] Cluster RDS DB harus dikonfigurasi untuk menyalin tag ke snapshot

[RDS.17] Instans RDS DB harus dikonfigurasi untuk menyalin tag ke snapshot

[RDS.18] Instans RDS harus digunakan di VPC

[RDS.19] Langganan pemberitahuan acara RDS yang ada harus dikonfigurasi untuk peristiwa klaster penting

[RDS.20] Langganan pemberitahuan acara RDS yang ada harus dikonfigurasi untuk peristiwa instance basis data penting

[RDS.21] Langganan pemberitahuan acara RDS harus dikonfigurasi untuk peristiwa grup parameter basis data penting

[RDS.22] Langganan pemberitahuan acara RDS harus dikonfigurasi untuk acara grup keamanan basis data penting

[RDS.23] Instans RDS tidak boleh menggunakan port default mesin database

[RDS.24] Kluster Database RDS harus menggunakan nama pengguna administrator khusus

[RDS.25] Instans database RDS harus menggunakan nama pengguna administrator khusus

[RDS.26] Instans RDS DB harus dilindungi oleh rencana cadangan

[RDS.27] Cluster RDS DB harus dienkripsi saat istirahat

[RDS.34] Cluster Aurora MySQL DB harus menerbitkan log audit ke Log CloudWatch

[RDS.35] Cluster RDS DB harus mengaktifkan peningkatan versi minor otomatis

[Redshift.1] Cluster Amazon Redshift harus melarang akses publik

[Redshift.2] Koneksi ke cluster Amazon Redshift harus dienkripsi saat transit

[Redshift.3] Cluster Amazon Redshift harus mengaktifkan snapshot otomatis

[Redshift.4] Cluster Amazon Redshift harus mengaktifkan pencatatan audit

[Redshift.6] Amazon Redshift harus mengaktifkan peningkatan otomatis ke versi utama

[Redshift.7] Cluster Redshift harus menggunakan perutean VPC yang ditingkatkan

[Redshift.8] Cluster Amazon Redshift tidak boleh menggunakan nama pengguna Admin default

[Redshift.9] Cluster Redshift tidak boleh menggunakan nama database default

[Redshift.10] Cluster Redshift harus dienkripsi saat istirahat

[Route53.2] Route 53 zona yang dihosting publik harus mencatat kueri DNS

[S3.1] Bucket tujuan umum S3 harus mengaktifkan pengaturan akses publik blok

[S3.2] Bucket tujuan umum S3 harus memblokir akses baca publik

[S3.3] Bucket tujuan umum S3 harus memblokir akses tulis publik

[S3.5] Bucket tujuan umum S3 harus memerlukan permintaan untuk menggunakan SSL

[S3.6] Kebijakan bucket tujuan umum S3 harus membatasi akses ke yang lain Akun AWS

[S3.7] Ember tujuan umum S3 harus menggunakan replikasi lintas wilayah

[S3.8] Bucket tujuan umum S3 harus memblokir akses publik

[S3.9] Bucket tujuan umum S3 harus mengaktifkan pencatatan akses server

[S3.10] Bucket tujuan umum S3 dengan versi diaktifkan harus memiliki konfigurasi Siklus Hidup

[S3.11] Bucket tujuan umum S3 harus mengaktifkan pemberitahuan acara

[S3.12] ACL tidak boleh digunakan untuk mengelola akses pengguna ke bucket tujuan umum S3

[S3.13] Bucket tujuan umum S3 harus memiliki konfigurasi Siklus Hidup

[S3.14] Bucket tujuan umum S3 harus mengaktifkan versi

[S3.15] Bucket tujuan umum S3 harus mengaktifkan Object Lock

[S3.17] Ember tujuan umum S3 harus dienkripsi saat istirahat AWS KMS keys

[S3.19] Titik akses S3 harus mengaktifkan pengaturan akses publik blok

[S3.20] Bucket tujuan umum S3 harus mengaktifkan penghapusan MFA

[SageMaker.1] Instans SageMaker notebook Amazon seharusnya tidak memiliki akses internet langsung

[SageMaker.2] instance SageMaker notebook harus diluncurkan dalam VPC khusus

[SageMaker.3] Pengguna seharusnya tidak memiliki akses root ke instance SageMaker notebook

[SageMaker.4] varian produksi SageMaker titik akhir harus memiliki jumlah instance awal yang lebih besar dari 1

[SecretsManager.1] Rahasia Secrets Manager harus mengaktifkan rotasi otomatis

[SecretsManager.2] Rahasia Secrets Manager yang dikonfigurasi dengan rotasi otomatis harus berhasil diputar

[SecretsManager.3] Hapus rahasia Secrets Manager yang tidak digunakan

[SecretsManager.4] Rahasia Secrets Manager harus diputar dalam jumlah hari tertentu

[ServiceCatalog.1] Portofolio Service Catalog harus dibagikan hanya dalam suatu organisasi AWS

[SNS.1] Topik SNS harus dienkripsi saat istirahat menggunakan AWS KMS

[SQS.1] Antrian Amazon SQS harus dienkripsi saat istirahat

[SSM.1] Instans Amazon EC2 harus dikelola oleh AWS Systems Manager

[SSM.2] Instans Amazon EC2 yang dikelola oleh Systems Manager harus memiliki status kepatuhan patch COMPLIANT setelah instalasi patch

[SSM.3] Instans Amazon EC2 yang dikelola oleh Systems Manager harus memiliki status kepatuhan asosiasi COMPLIANT

[SSM.4] Dokumen SSM seharusnya tidak bersifat publik

[Transfer.2] Server Transfer Family tidak boleh menggunakan protokol FTP untuk koneksi titik akhir

[WAF.1] Pencatatan ACL Web Global AWS WAF Klasik harus diaktifkan

[WAF.2] Aturan Regional AWS WAF Klasik harus memiliki setidaknya satu syarat

[WAF.3] Kelompok aturan Regional AWS WAF Klasik harus memiliki setidaknya satu aturan

[WAF.4] ACL web Regional AWS WAF klasik harus memiliki setidaknya satu aturan atau kelompok aturan

[WAF.6] Aturan global AWS WAF klasik harus memiliki setidaknya satu syarat

[WAF.7] Kelompok aturan global AWS WAF klasik harus memiliki setidaknya satu aturan

[WAF.8] ACL web global AWS WAF klasik harus memiliki setidaknya satu aturan atau kelompok aturan

[WAF.10] ACL AWS WAF web harus memiliki setidaknya satu aturan atau kelompok aturan

[WAF.11] pencatatan ACL AWS WAF web harus diaktifkan

AWS WAF Aturan [WAF.12] harus mengaktifkan metrik CloudWatch

Standar Keamanan Data Industri Kartu Pembayaran (PCI DSS)

Standar Keamanan Data Industri Kartu Pembayaran (PCI DSS) di Security Hub menyediakan serangkaian praktik terbaik AWS keamanan untuk menangani data pemegang kartu. Anda dapat menggunakan standar ini untuk menemukan kerentanan keamanan dalam sumber daya yang menangani data pemegang kartu. Security Hub saat ini mencakup kontrol di tingkat akun. Kami menyarankan Anda mengaktifkan kontrol ini di semua akun Anda yang memiliki sumber daya yang menyimpan, memproses, atau mengirimkan data pemegang kartu.

Standar ini divalidasi oleh AWS Security Assurance Services LLC (AWS SAS), yang merupakan tim Qualified Security Assesors (QSAs) yang disertifikasi untuk memberikan panduan PCI DSS, dan penilaian oleh PCI DSS Security Standards Council (PCI SSC). AWS SAS telah mengkonfirmasi bahwa pemeriksaan otomatis dapat membantu pelanggan dalam mempersiapkan penilaian PCI DSS.

Halaman ini berisi daftar ID dan judul kontrol keamanan. Di Wilayah AWS GovCloud (US) Region dan China, ID dan judul kontrol khusus standar digunakan. Untuk pemetaan ID kontrol keamanan dan judul ke ID dan judul kontrol khusus standar, lihat. Bagaimana konsolidasi memengaruhi ID dan judul kontrol

Kontrol yang berlaku untuk PCI DSS

[AutoScaling.1] Grup Auto Scaling yang terkait dengan penyeimbang beban harus menggunakan pemeriksaan kesehatan ELB

[CloudTrail.2] CloudTrail harus mengaktifkan enkripsi saat istirahat

[CloudTrail.3] Setidaknya satu CloudTrail jejak harus diaktifkan

[CloudTrail.4] validasi file CloudTrail log harus diaktifkan

[CloudTrail.5] CloudTrail jalur harus diintegrasikan dengan Amazon Logs CloudWatch

[CloudWatch.1] Filter metrik log dan alarm harus ada untuk penggunaan pengguna “root”

[CodeBuild.1] URL repositori sumber CodeBuild Bitbucket tidak boleh berisi kredensyal sensitif

[CodeBuild.2] variabel lingkungan CodeBuild proyek tidak boleh berisi kredensil teks yang jelas

[Config.1] AWS Config harus diaktifkan dan menggunakan peran terkait layanan untuk perekaman sumber daya

[DMS.1] Instans replikasi Layanan Migrasi Database tidak boleh bersifat publik

[EC2.1] Snapshot Amazon EBS tidak boleh dipulihkan secara publik

[EC2.2] Grup keamanan default VPC tidak boleh mengizinkan lalu lintas masuk atau keluar

[EC2.6] Pencatatan aliran VPC harus diaktifkan di semua VPC

[EC2.12] EIP Amazon EC2 yang tidak digunakan harus dihapus

[EC2.13] Grup keamanan tidak boleh mengizinkan masuknya dari 0.0.0.0/0 atau: :/0 ke port 22

[ELB.1] Application Load Balancer harus dikonfigurasi untuk mengalihkan semua permintaan HTTP ke HTTPS

[ES.1] Domain Elasticsearch harus mengaktifkan enkripsi saat istirahat

[ES.2] Domain Elasticsearch tidak boleh diakses publik

[GuardDuty.1] GuardDuty harus diaktifkan

[IAM.1] Kebijakan IAM seharusnya tidak mengizinkan hak administratif “*” penuh

[IAM.2] Pengguna IAM seharusnya tidak memiliki kebijakan IAM yang dilampirkan

[IAM.4] Kunci akses pengguna root IAM seharusnya tidak ada

[IAM.6] MFA perangkat keras harus diaktifkan untuk pengguna root

[IAM.8] Kredensyal pengguna IAM yang tidak digunakan harus dihapus

[IAM.9] MFA harus diaktifkan untuk pengguna root

[IAM.10] Kebijakan kata sandi untuk pengguna IAM harus memiliki urasi yang kuat AWS Config

[IAM.19] MFA harus diaktifkan untuk semua pengguna IAM

[KMS.4] rotasi AWS KMS tombol harus diaktifkan

[Lambda.1] Kebijakan fungsi Lambda harus melarang akses publik

[Lambda.3] Fungsi Lambda harus dalam VPC

[Opensearch.1] OpenSearch domain harus mengaktifkan enkripsi saat istirahat

[Opensearch.2] OpenSearch domain tidak boleh diakses publik

[RDS.1] Snapshot RDS harus pribadi

[RDS.2] Instans RDS DB harus melarang akses publik, sebagaimana ditentukan oleh urasi PubliclyAccessible AWS Config

[Redshift.1] Cluster Amazon Redshift harus melarang akses publik

[S3.1] Bucket tujuan umum S3 harus mengaktifkan pengaturan akses publik blok

[S3.2] Bucket tujuan umum S3 harus memblokir akses baca publik

[S3.3] Bucket tujuan umum S3 harus memblokir akses tulis publik

[S3.5] Bucket tujuan umum S3 harus memerlukan permintaan untuk menggunakan SSL

[S3.7] Ember tujuan umum S3 harus menggunakan replikasi lintas wilayah

[SageMaker.1] Instans SageMaker notebook Amazon seharusnya tidak memiliki akses internet langsung

[SSM.1] Instans Amazon EC2 harus dikelola oleh AWS Systems Manager

[SSM.2] Instans Amazon EC2 yang dikelola oleh Systems Manager harus memiliki status kepatuhan patch COMPLIANT setelah instalasi patch

[SSM.3] Instans Amazon EC2 yang dikelola oleh Systems Manager harus memiliki status kepatuhan asosiasi COMPLIANT

AWS Standar Penandaan Sumber Daya

Bagian ini memberikan informasi tentang Standar Penandaan AWS Sumber Daya.

> **Note**
>
> Standar Penandaan AWS Sumber Daya tidak tersedia di Kanada Barat (Calgary), China, dan. AWS GovCloud (US)

Apa itu Standar Penandaan AWS Sumber Daya?

Tag adalah pasangan kunci dan nilai yang bertindak sebagai metadata untuk mengatur sumber daya Anda AWS . Dengan sebagian besar AWS sumber daya, Anda memiliki opsi untuk menambahkan tag saat Anda membuat sumber daya atau setelah pembuatan. Contoh sumber daya termasuk CloudFront distribusi Amazon, instans Amazon Elastic Compute Cloud (Amazon EC2), atau rahasia di. AWS Secrets Manager

Tanda dapat membantu Anda mengelola, mengidentifikasi, mengatur, dan memfilter sumber daya.

Setiap tag memiliki dua bagian:

- Kunci tag (misalnya,, `CostCenter` `Environment`, atau`Project`). Kunci tag peka huruf besar dan kecil.
- Nilai tag (misalnya, `111122223333` atau`Production`). Seperti kunci tag, nilai tag peka huruf besar dan kecil.

Anda dapat menggunakan tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya.

Untuk petunjuk cara menambahkan tag ke AWS sumber daya, lihat Cara menambahkan tag ke AWS sumber daya Anda di Panduan Pengguna AWS Security Hub.

Standar Penandaan AWS Sumber Daya, yang dikembangkan oleh AWS Security Hub, membantu Anda mengidentifikasi dengan cepat jika ada AWS sumber daya yang hilang kunci tag. Anda dapat menyesuaikan `requiredTagKeys` parameter untuk menentukan kunci tag tertentu yang diperiksa oleh kontrol. Jika tag tertentu tidak disediakan, kontrol hanya memeriksa keberadaan setidaknya satu kunci tag.

Saat Anda mengaktifkan Standar Penandaan AWS Sumber Daya, Anda akan mulai menerima temuan di AWS Security Finding Format (ASFF).

> **Note**
>
> Saat Anda mengaktifkan Standar Penandaan AWS Sumber Daya, Security Hub mungkin memerlukan waktu hingga 18 jam untuk menghasilkan temuan untuk kontrol yang menggunakan aturan AWS Config terkait layanan yang sama dengan kontrol yang diaktifkan dalam standar lain yang diaktifkan. Untuk informasi selengkapnya, lihat Jadwal untuk menjalankan pemeriksaan keamanan.

Standar ini memiliki Nama Sumber Daya Amazon (ARN) berikut:.
`arn:aws:securityhub:region::standards/aws-resource-tagging-standard/v/1.0.0`

Anda juga dapat menggunakan GetEnabledStandardspengoperasian Security Hub API untuk mengetahui ARN dari standar yang diaktifkan.

Kontrol dalam Standar Penandaan AWS Sumber Daya

Standar Penandaan AWS Sumber Daya mencakup kontrol berikut. Pilih kontrol untuk melihat deskripsi rinci tentang itu.

- [ACM.3] Sertifikat ACM harus ditandai
- [AppSync.4] AWS AppSync GraphQL API harus diberi tag
- [Athena.2] Katalog data Athena harus diberi tag
- [Athena.3] Kelompok kerja Athena harus ditandai
- [AutoScaling.10] Grup Penskalaan Otomatis EC2 harus diberi tag
- [Backup.2] poin AWS Backup pemulihan harus ditandai
- [Backup.3] AWS Backup brankas harus ditandai
- [Backup.4] rencana AWS Backup laporan harus ditandai
- [Backup.5] rencana AWS Backup cadangan harus ditandai
- [CloudFormation.2] CloudFormation tumpukan harus ditandai
- [CloudFront.14] CloudFront distribusi harus ditandai
- [CloudTrail.9] CloudTrail jejak harus ditandai
- [CodeArtifact.1] CodeArtifact repositori harus diberi tag
- [Detective.1] Grafik perilaku detektif harus diberi tag
- [DMS.2] Sertifikat DMS harus ditandai
- [DMS.3] Langganan acara DMS harus ditandai
- [DMS.4] Contoh replikasi DMS harus ditandai
- [DMS.5] Grup subnet replikasi DMS harus ditandai
- [DynamoDB.5] Tabel DynamoDB harus diberi tag
- [EC2.33] Lampiran gateway transit EC2 harus ditandai
- [EC2.34] Tabel rute gateway transit EC2 harus ditandai
- [EC2.35] Antarmuka jaringan EC2 harus ditandai

- [EC2.36] Gateway pelanggan EC2 harus ditandai
- [EC2.37] Alamat IP Elastis EC2 harus ditandai
- [EC2.38] Instans EC2 harus ditandai
- [EC2.39] Gerbang internet EC2 harus ditandai
- [EC2.40] Gerbang EC2 NAT harus ditandai
- [EC2.41] ACL jaringan EC2 harus ditandai
- [EC2.42] Tabel rute EC2 harus ditandai
- [EC2.43] Grup keamanan EC2 harus ditandai
- [EC2.44] Subnet EC2 harus ditandai
- [EC2.45] Volume EC2 harus ditandai
- [EC2.46] VPC Amazon harus ditandai
- [EC2.47] Layanan titik akhir Amazon VPC harus ditandai
- [EC2.48] Log aliran VPC Amazon harus ditandai
- [EC2.49] Koneksi peering VPC Amazon harus ditandai
- [EC2.50] Gateway EC2 VPN harus ditandai
- [EC2.52] Gerbang transit EC2 harus ditandai
- [ECR.4] Repositori publik ECR harus ditandai
- [ECS.13] Layanan ECS harus ditandai
- [ECS.14] Cluster ECS harus ditandai
- [ECS.15] Definisi tugas ECS harus ditandai
- [EFS.5] Titik akses EFS harus ditandai
- [EKS.6] Kluster EKS harus ditandai
- [EKS.7] Konfigurasi penyedia identitas EKS harus ditandai
- [ES.9] Domain Elasticsearch harus diberi tag
- [EventBridge.2] bus EventBridge acara harus diberi tag
- [GlobalAccelerator.1] Akselerator Akselerator Global harus diberi tag
- AWS Glue Pekerjaan [Glue.1] harus ditandai
- [GuardDuty.2] GuardDuty filter harus diberi tag
- [GuardDuty.3] GuardDuty IPset harus ditandai

- [GuardDuty.4] GuardDuty detektor harus ditandai
- [IAM.23] Penganalisis Akses IAM harus ditandai
- [IAM.24] Peran IAM harus ditandai
- [IAM.25] Pengguna IAM harus diberi tag
- [IoT.1] profil AWS IoT Core keamanan harus ditandai
- [IoT.2] tindakan AWS IoT Core mitigasi harus ditandai
- AWS IoT Core Dimensi [IoT.3] harus ditandai
- [IoT.4] AWS IoT Core otorisasi harus diberi tag
- [IoT.5] alias AWS IoT Core peran harus ditandai
- AWS IoT Core Kebijakan [IoT.6] harus ditandai
- [Kinesis.2] Aliran kinesis harus ditandai
- [Lambda.6] Fungsi Lambda harus ditandai
- [MQ.4] Broker Amazon MQ harus diberi tag
- [NetworkFirewall.7] Firewall Firewall Jaringan harus diberi tag
- [NetworkFirewall.8] Kebijakan firewall Network Firewall harus ditandai
- [Opensearch.9] domain harus ditandai OpenSearch
- [RDS.28] Cluster RDS DB harus ditandai
- [RDS.29] Snapshot cluster RDS DB harus ditandai
- [RDS.30] Instans RDS DB harus ditandai
- [RDS.31] Grup keamanan RDS DB harus ditandai
- [RDS.32] Snapshot RDS DB harus ditandai
- [RDS.33] Grup subnet RDS DB harus ditandai
- [Redshift.11] Cluster Redshift harus ditandai
- [Redshift.12] Langganan pemberitahuan acara Redshift harus ditandai
- [Redshift.13] Snapshot cluster Redshift harus ditandai
- [Redshift.14] Grup subnet cluster Redshift harus ditandai
- [Route53.1] Pemeriksaan kesehatan rute 53 harus ditandai
- [SecretsManager.5] Rahasia Secrets Manager harus diberi tag
- [SES.1] Daftar kontak SES harus ditandai

- [SES.2] Set konfigurasi SES harus ditandai
- [SNS.3] Topik SNS harus ditandai
- [SQS.2] Antrian SQS harus ditandai
- [StepFunctions.2] Aktivitas Step Functions harus diberi tag
- [Transfer.1] AWS Transfer Family alur kerja harus ditandai

Standar yang dikelola layanan

Standar yang dikelola layanan adalah standar keamanan yang dikelola orang lain Layanan AWS . Misalnya, Service-Managed Standard: AWS Control Tower adalah standar yang dikelola layanan yang mengelola. AWS Control Tower Standar yang dikelola layanan berbeda dari standar keamanan yang dikelola AWS Security Hub dengan cara berikut:

- Pembuatan dan penghapusan standar — Anda membuat dan menghapus standar yang dikelola layanan dengan konsol atau API layanan pengelola, atau dengan. AWS CLI Sampai Anda membuat standar dalam layanan pengelolaan dengan salah satu cara tersebut, standar tidak muncul di konsol Security Hub dan tidak dapat diakses oleh Security Hub API atau AWS CLI.
- Tidak ada pengaktifan kontrol otomatis — Saat Anda membuat standar yang dikelola layanan, Security Hub dan layanan pengelola tidak secara otomatis mengaktifkan kontrol yang berlaku pada standar. Selain itu, ketika Security Hub merilis kontrol baru untuk standar, kontrol tersebut tidak diaktifkan secara otomatis. Ini adalah penyimpangan dari standar yang dikelola Security Hub. Untuk informasi selengkapnya tentang cara biasa mengonfigurasi kontrol di Security Hub, lihatMelihat dan mengelola kontrol keamanan.
- Mengaktifkan dan menonaktifkan kontrol — Kami menyarankan untuk mengaktifkan dan menonaktifkan kontrol dalam layanan pengelolaan untuk menghindari penyimpangan.
- Ketersediaan kontrol — Layanan pengelola memilih kontrol mana yang tersedia sebagai bagian dari standar yang dikelola layanan. Kontrol yang tersedia dapat mencakup semua, atau sebagian dari, kontrol Security Hub yang ada.

Setelah layanan pengelolaan membuat standar yang dikelola layanan dan menyediakan kontrol untuknya, Anda dapat mengakses temuan kontrol, status kontrol, dan skor keamanan standar di konsol Security Hub, Security Hub API, atau. AWS CLI Beberapa atau semua informasi ini mungkin juga tersedia di layanan pengelolaan.

Pilih standar yang dikelola layanan dari daftar berikut untuk melihat detail selengkapnya.

Standar yang dikelola layanan

- Standar yang Dikelola Layanan: AWS Control Tower

Standar yang Dikelola Layanan: AWS Control Tower

Bagian ini memberikan informasi tentang Standar yang Dikelola Layanan:. AWS Control Tower

Apa itu Standar yang Dikelola Layanan:? AWS Control Tower

Standar ini dirancang untuk pengguna AWS Security Hub dan AWS Control Tower. Ini memungkinkan Anda mengonfigurasi kontrol proaktif AWS Control Tower di samping kontrol detektif Security Hub dalam layanan. AWS Control Tower

Kontrol proaktif membantu memastikan bahwa Anda Akun AWS mempertahankan kepatuhan karena mereka menandai tindakan yang dapat menyebabkan pelanggaran kebijakan atau kesalahan konfigurasi. Kontrol Detektif mendeteksi ketidakpatuhan sumber daya (misalnya, kesalahan konfigurasi) di dalam Anda. Akun AWS Dengan mengaktifkan kontrol proaktif dan detektif untuk AWS lingkungan Anda, Anda dapat meningkatkan postur keamanan Anda pada berbagai tahap pengembangan.

> **Tip**
>
> Standar yang dikelola layanan berbeda dari standar yang dikelola AWS Security Hub. Misalnya, Anda harus membuat dan menghapus standar yang dikelola layanan di layanan pengelolaan. Untuk informasi selengkapnya, lihat Standar yang dikelola layanan.

Di konsol Security Hub dan API, Anda dapat melihat Standar yang Dikelola Layanan: AWS Control Tower bersama standar Security Hub lainnya.

Menciptakan standar

Standar ini hanya tersedia jika Anda membuat standar di AWS Control Tower. AWS Control Tower membuat standar saat Anda pertama kali mengaktifkan kontrol yang berlaku dengan menggunakan salah satu metode berikut:

- AWS Control Tower konsol
- AWS Control Tower API (panggil `EnableControl`API)

- AWS CLI (jalankan `enable-control`perintah)

Kontrol Security Hub diidentifikasi di AWS Control Tower konsol sebagai SH. ***`ControlId`*** (misalnya, SH. CodeBuild.1).

Bila Anda membuat standar, jika Anda belum mengaktifkan Security Hub, AWS Control Tower juga mengaktifkan Security Hub untuk Anda.

Jika belum menyiapkan AWS Control Tower, Anda tidak dapat melihat atau mengakses standar ini di konsol Security Hub, Security Hub API, atau AWS CLI. Bahkan jika Anda telah menyiapkan AWS Control Tower, Anda tidak dapat melihat atau mengakses standar ini di Security Hub tanpa terlebih dahulu membuat standar dalam AWS Control Tower menggunakan salah satu metode sebelumnya.

Standar ini hanya tersedia di Wilayah AWS tempat yang AWS Control Tower tersedia, termasuk AWS GovCloud (US).

Mengaktifkan dan menonaktifkan kontrol dalam standar

Setelah Anda membuat standar di AWS Control Tower konsol, Anda dapat melihat standar dan kontrol yang tersedia di kedua layanan.

Setelah Anda pertama kali membuat standar, itu tidak memiliki kontrol apa pun yang diaktifkan secara otomatis. Selain itu, saat Security Hub menambahkan kontrol baru, kontrol tersebut tidak diaktifkan secara otomatis untuk Standar yang Dikelola Layanan:. AWS Control Tower Anda harus mengaktifkan dan menonaktifkan kontrol untuk standar AWS Control Tower dengan menggunakan salah satu metode berikut:

- AWS Control Tower konsol
- AWS Control Tower API (panggil `EnableControl`dan `DisableControl`API)
- AWS CLI (jalankan `enable-control`dan `disable-control`perintah)

Saat Anda mengubah status pengaktifan kontrol AWS Control Tower, perubahan tersebut juga tercermin di Security Hub.

Namun, menonaktifkan kontrol di Security Hub yang diaktifkan akan AWS Control Tower menghasilkan penyimpangan kontrol. Status kontrol di AWS Control Tower menunjukkan sebagai`Drifted`. Anda dapat mengatasi penyimpangan ini dengan memilih Registrasi ulang OU di AWS Control Tower konsol, atau dengan menonaktifkan dan mengaktifkan kembali kontrol dalam AWS Control Tower menggunakan salah satu metode sebelumnya.

Menyelesaikan tindakan pemberdayaan dan penonaktifan AWS Control Tower membantu Anda menghindari penyimpangan kontrol.

Saat Anda mengaktifkan atau menonaktifkan kontrol AWS Control Tower, tindakan akan berlaku di seluruh akun dan Wilayah. Jika Anda mengaktifkan dan menonaktifkan kontrol di Security Hub (tidak disarankan untuk standar ini), tindakan hanya berlaku untuk akun saat ini dan Wilayah.

> **Note**
>
> Konfigurasi pusat tidak dapat digunakan untuk mengelola Standar yang Dikelola Layanan:. AWS Control Tower Jika Anda menggunakan konfigurasi pusat, Anda hanya dapat menggunakan AWS Control Tower layanan untuk mengaktifkan dan menonaktifkan kontrol dalam standar ini untuk akun yang dikelola secara terpusat.

Melihat status pemberdayaan dan status kontrol

Anda dapat melihat status pemberdayaan kontrol dengan menggunakan salah satu metode berikut:

- Konsol Security Hub, Security Hub API, atau AWS CLI
- AWS Control Tower konsol
- AWS Control Tower API untuk melihat daftar kontrol yang diaktifkan (panggil `ListEnabledControls`API)
- AWS CLI untuk melihat daftar kontrol yang diaktifkan (jalankan `list-enabled-controls`perintah)

Kontrol yang Anda nonaktifkan AWS Control Tower memiliki status pengaktifan `Disabled` di Security Hub kecuali Anda secara eksplisit mengaktifkan kontrol tersebut di Security Hub.

Security Hub menghitung status kontrol berdasarkan status alur kerja dan status kepatuhan temuan kontrol. Untuk informasi selengkapnya tentang status pemberdayaan dan status kontrol, lihatMelihat detail untuk kontrol.

Berdasarkan status kontrol, Security Hub menghitung skor keamanan untuk Service-Managed Standard:. AWS Control Tower Skor ini hanya tersedia di Security Hub. Selain itu, Anda hanya dapat melihat temuan kontrol di Security Hub. Skor keamanan standar dan temuan kontrol tidak tersedia di AWS Control Tower.

> **Note**
>
> Saat Anda mengaktifkan kontrol untuk Standar yang Dikelola Layanan: AWS Control Tower, Security Hub mungkin memerlukan waktu hingga 18 jam untuk menghasilkan temuan untuk kontrol yang menggunakan aturan terkait AWS Config layanan yang ada. Anda mungkin memiliki aturan terkait layanan yang ada jika Anda telah mengaktifkan standar dan kontrol lain di Security Hub. Untuk informasi selengkapnya, lihat Jadwal untuk menjalankan pemeriksaan keamanan.

Menghapus standar

Anda dapat menghapus standar ini AWS Control Tower dengan menonaktifkan semua kontrol yang berlaku menggunakan salah satu metode berikut:

- AWS Control Tower konsol
- AWS Control Tower API (panggil `DisableControl`API)
- AWS CLI (jalankan `disable-control`perintah)

Menonaktifkan semua kontrol akan menghapus standar di semua akun terkelola dan Wilayah yang diatur di. AWS Control Tower Menghapus standar di AWS Control Tower menghapusnya dari halaman Standar konsol Security Hub, dan Anda tidak dapat lagi mengaksesnya dengan menggunakan Security Hub API atau AWS CLI.

> **Note**
>
> Menonaktifkan semua kontrol dari standar di Security Hub tidak menonaktifkan atau menghapus standar.

Menonaktifkan layanan Security Hub akan menghapus Standar yang Dikelola Layanan: AWS Control Tower dan standar lain yang telah Anda aktifkan.

Menemukan format bidang untuk Standar yang Dikelola Layanan: AWS Control Tower

Saat Anda membuat Service-Managed Standard: AWS Control Tower dan mengaktifkan kontrol untuk itu, Anda akan mulai menerima temuan kontrol di Security Hub. Security Hub melaporkan

temuan kontrol diAWS Format Pencarian Keamanan (ASFF). Ini adalah nilai ASFF untuk Amazon Resource Name (ARN) standar ini dan: `GeneratorId`

- ARN standar — *`arn:aws:us-east-1`*`:securityhub:::standards/service-managed-aws-control-tower/v/1.0.0`
- GeneratorId – `service-managed-aws-control-tower/v/1.0.0/`*`CodeBuild.1`*

Untuk contoh temuan Standar yang Dikelola Layanan: AWS Control Tower, lihat. Temuan kontrol sampel

Kontrol yang berlaku untuk Standar yang Dikelola Layanan: AWS Control Tower

Service-Managed Standard: AWS Control Tower mendukung subset kontrol yang merupakan bagian dari standar AWS Foundational Security Best Practices (FSBP). Pilih kontrol dari tabel berikut untuk melihat informasi tentangnya, termasuk langkah-langkah perbaikan untuk temuan yang gagal.

Daftar berikut menunjukkan kontrol yang tersedia untuk Standar yang Dikelola Layanan:. AWS Control Tower Batas regional pada kontrol cocok dengan batas Regional pada kontrol wajar dalam standar FSBP. Daftar ini menunjukkan ID kontrol keamanan agnostik standar. Di AWS Control Tower konsol, ID kontrol diformat sebagai SH. ***`ControlId`*** (misalnya SH. CodeBuild.1). Di Security Hub, jika temuan kontrol konsolidasi dimatikan di akun Anda, `ProductFields.ControlId` bidang tersebut menggunakan ID kontrol berbasis standar. ID kontrol berbasis standar diformat sebagai CT. ***`ControlId`***(misalnya, CT. CodeBuild.1).

- [Akun.1] Informasi kontak keamanan harus disediakan untuk Akun AWS
- [ACM.1] Sertifikat yang diimpor dan diterbitkan ACM harus diperbarui setelah jangka waktu tertentu
- [ACM.2] Sertifikat RSA yang dikelola oleh ACM harus menggunakan panjang kunci minimal 2.048 bit
- [ApiGateway.1] API Gateway REST WebSocket dan pencatatan eksekusi API harus diaktifkan
- [ApiGateway.2] Tahapan API Gateway REST API harus dikonfigurasi untuk menggunakan sertifikat SSL untuk otentikasi backend
- [ApiGateway.3] Tahapan API Gateway REST API harus mengaktifkan penelusuran AWS X-Ray
- [ApiGateway.4] API Gateway harus dikaitkan dengan ACL Web WAF
- [ApiGateway.5] Data cache API Gateway REST API harus dienkripsi saat istirahat
- [ApiGateway.8] Rute API Gateway harus menentukan jenis otorisasi
- [ApiGateway.9] Pencatatan akses harus dikonfigurasi untuk Tahapan API Gateway V2

- [AppSync.5] AWS AppSync GraphQL API tidak boleh diautentikasi dengan kunci API
- [AutoScaling.1] Grup Auto Scaling yang terkait dengan penyeimbang beban harus menggunakan pemeriksaan kesehatan ELB
- [AutoScaling.2] Grup Auto Scaling Amazon EC2 harus mencakup beberapa Availability Zone
- [AutoScaling.3] Konfigurasi peluncuran grup Auto Scaling harus mengonfigurasi instans EC2 agar memerlukan Layanan Metadata Instans Versi 2 (IMDSv2)
- [Autoscaling.5] Instans Amazon EC2 yang diluncurkan menggunakan konfigurasi peluncuran grup Auto Scaling seharusnya tidak memiliki alamat IP Publik
- [AutoScaling.6] Grup Auto Scaling harus menggunakan beberapa jenis instance di beberapa Availability Zone
- [AutoScaling.9] Grup Auto Scaling Amazon EC2 harus menggunakan templat peluncuran Amazon EC2
- [CloudTrail.1] CloudTrail harus diaktifkan dan dikonfigurasi dengan setidaknya satu jejak Multi-wilayah yang mencakup acara manajemen baca dan tulis
- [CloudTrail.2] CloudTrail harus mengaktifkan enkripsi saat istirahat
- [CloudTrail.4] validasi file CloudTrail log harus diaktifkan
- [CloudTrail.5] CloudTrail jalur harus diintegrasikan dengan Amazon Logs CloudWatch
- [CloudTrail.6] Pastikan bucket S3 yang digunakan untuk menyimpan CloudTrail log tidak dapat diakses publik
- [CodeBuild.1] URL repositori sumber CodeBuild Bitbucket tidak boleh berisi kredensyal sensitif
- [CodeBuild.2] variabel lingkungan CodeBuild proyek tidak boleh berisi kredensil teks yang jelas
- [CodeBuild.3] Log CodeBuild S3 harus dienkripsi
- [CodeBuild.4] lingkungan CodeBuild proyek harus memiliki urasi logging AWS Config
- [DMS.1] Instans replikasi Layanan Migrasi Database tidak boleh bersifat publik
- [DMS.9] Titik akhir DMS harus menggunakan SSL
- [DocumentDB.1] Cluster Amazon DocumentDB harus dienkripsi saat istirahat
- [DocumentDB.2] Cluster Amazon DocumentDB harus memiliki periode retensi cadangan yang memadai
- [DocumentDB.3] Cuplikan cluster manual Amazon DocumentDB seharusnya tidak bersifat publik
- [DynamoDB.1] Tabel DynamoDB harus secara otomatis menskalakan kapasitas sesuai permintaan
- [DynamoDB.2] Tabel DynamoDB harus mengaktifkan pemulihan point-in-time

- [DynamoDB.3] Cluster DynamoDB Accelerator (DAX) harus dienkripsi saat istirahat
- [EC2.1] Snapshot Amazon EBS tidak boleh dipulihkan secara publik
- [EC2.2] Grup keamanan default VPC tidak boleh mengizinkan lalu lintas masuk atau keluar
- [EC2.3] Volume Amazon EBS yang terpasang harus dienkripsi saat istirahat
- [EC2.4] Instans EC2 yang dihentikan harus dihapus setelah periode waktu tertentu
- [EC2.6] Pencatatan aliran VPC harus diaktifkan di semua VPC
- [EC2.7] Enkripsi default EBS harus diaktifkan
- [EC2.8] Instans EC2 harus menggunakan Layanan Metadata Instance Versi 2 (IMDSv2)
- [EC2.9] Instans Amazon EC2 seharusnya tidak memiliki alamat IPv4 publik
- [EC2.10] Amazon EC2 harus dikonfigurasi untuk menggunakan titik akhir VPC yang dibuat untuk layanan Amazon EC2
- [EC2.15] Subnet Amazon EC2 seharusnya tidak secara otomatis menetapkan alamat IP publik
- [EC2.16] Daftar Kontrol Akses Jaringan yang Tidak Digunakan harus dihapus
- [EC2.17] Instans Amazon EC2 tidak boleh menggunakan beberapa ENI
- [EC2.18] Grup keamanan seharusnya hanya mengizinkan lalu lintas masuk yang tidak terbatas untuk port resmi
- [EC2.19] Grup keamanan tidak boleh mengizinkan akses tidak terbatas ke port dengan risiko tinggi
- [EC2.20] Kedua terowongan VPN untuk koneksi VPN Site-to-Site harus AWS aktif
- [EC2.21] ACL jaringan seharusnya tidak mengizinkan masuknya dari 0.0.0.0/0 ke port 22 atau port 3389
- [EC2.22] Grup keamanan Amazon EC2 yang tidak digunakan harus dihapus
- [EC2.23] Amazon EC2 Transit Gateways seharusnya tidak secara otomatis menerima permintaan lampiran VPC
- [EC2.25] Templat peluncuran Amazon EC2 tidak boleh menetapkan IP publik ke antarmuka jaringan
- [ECR.1] Repositori pribadi ECR harus memiliki pemindaian gambar yang dikonfigurasi
- [ECR.2] Repositori pribadi ECR harus memiliki kekekalan tag yang dikonfigurasi
- [ECR.3] Repositori ECR harus memiliki setidaknya satu kebijakan siklus hidup yang dikonfigurasi
- [ECS.1] Definisi tugas Amazon ECS harus memiliki mode jaringan yang aman dan definisi pengguna.

- [ECS.2] Layanan ECS seharusnya tidak memiliki alamat IP publik yang ditetapkan kepadanya secara otomatis
- [ECS.3] Definisi tugas ECS tidak boleh membagikan namespace proses host
- [ECS.4] Kontainer ECS harus berjalan sebagai non-hak istimewa
- [ECS.5] Wadah ECS harus dibatasi pada akses hanya-baca ke sistem file root
- [ECS.8] Rahasia tidak boleh diteruskan sebagai variabel lingkungan kontainer
- [ECS.10] Layanan ECS Fargate harus berjalan pada versi platform Fargate terbaru
- [ECS.12] Cluster ECS harus menggunakan Wawasan Kontainer
- [EFS.1] Sistem File Elastis harus dikonfigurasi untuk mengenkripsi data file saat istirahat menggunakan AWS KMS
- [EFS.2] Volume Amazon EFS harus dalam rencana cadangan
- [EFS.3] Titik akses EFS harus menegakkan direktori root
- [EFS.4] Titik akses EFS harus menegakkan identitas pengguna
- [EKS.1] Titik akhir klaster EKS seharusnya tidak dapat diakses publik
- [EKS.2] Kluster EKS harus berjalan pada versi Kubernetes yang didukung
- [ElastiCache.3] ElastiCache untuk grup replikasi Redis harus mengaktifkan failover otomatis
- [ElastiCache.4] ElastiCache untuk grup replikasi Redis harus dienkripsi saat istirahat
- [ElastiCache.5] ElastiCache untuk grup replikasi Redis harus dienkripsi saat transit
- [ElastiCache.6] ElastiCache untuk grup replikasi Redis sebelum versi 6.0 harus menggunakan Redis AUTH
- [ElasticBeanstalk.1] Lingkungan Elastic Beanstalk seharusnya mengaktifkan pelaporan kesehatan yang ditingkatkan
- [ElasticBeanstalk.2] Pembaruan platform yang dikelola Elastic Beanstalk harus diaktifkan
- [ELB.1] Application Load Balancer harus dikonfigurasi untuk mengalihkan semua permintaan HTTP ke HTTPS
- [ELB.2] Classic Load Balancer dengan pendengar SSL/HTTPS harus menggunakan sertifikat yang disediakan oleh AWS Certificate Manager
- [ELB.3] Pendengar Classic Load Balancer harus dikonfigurasi dengan penghentian HTTPS atau TLS
- [ELB.4] Application Load Balancer harus dikonfigurasi untuk menjatuhkan header http
- [ELB.5] Pencatatan aplikasi dan Classic Load Balancer harus diaktifkan

- [ELB.6] Aplikasi, Gateway, dan Network Load Balancer harus mengaktifkan perlindungan penghapusan
- [ELB.7] Classic Load Balancers harus mengaktifkan pengurasan koneksi
- [ELB.8] Classic Load Balancer dengan pendengar SSL harus menggunakan kebijakan keamanan yang telah ditentukan sebelumnya yang memiliki urasi yang kuat AWS Config
- [ELB.9] Classic Load Balancer harus mengaktifkan penyeimbangan beban lintas zona
- [ELB.10] Classic Load Balancer harus menjangkau beberapa Availability Zone
- [ELB.12] Application Load Balancer harus dikonfigurasi dengan mode mitigasi desync defensif atau paling ketat
- [ELB.13] Penyeimbang Beban Aplikasi, Jaringan, dan Gateway harus mencakup beberapa Availability Zone
- [ELB.14] Classic Load Balancer harus dikonfigurasi dengan mode mitigasi desync defensif atau paling ketat
- [EMR.1] Node primer cluster EMR Amazon seharusnya tidak memiliki alamat IP publik
- [ES.1] Domain Elasticsearch harus mengaktifkan enkripsi saat istirahat
- [ES.2] Domain Elasticsearch tidak boleh diakses publik
- [ES.3] Domain Elasticsearch harus mengenkripsi data yang dikirim antar node
- [ES.4] Kesalahan domain Elasticsearch yang masuk ke CloudWatch Log harus diaktifkan
- [ES.5] Domain Elasticsearch harus mengaktifkan pencatatan audit
- [ES.6] Domain Elasticsearch harus memiliki setidaknya tiga node data
- [ES.7] Domain Elasticsearch harus dikonfigurasi dengan setidaknya tiga node master khusus
- [ES.8] Koneksi ke domain Elasticsearch harus dienkripsi menggunakan kebijakan keamanan TLS terbaru
- [EventBridge.3] bus acara EventBridge khusus harus memiliki kebijakan berbasis sumber daya terlampir
- [GuardDuty.1] GuardDuty harus diaktifkan
- [IAM.1] Kebijakan IAM seharusnya tidak mengizinkan hak administratif “*” penuh
- [IAM.2] Pengguna IAM seharusnya tidak memiliki kebijakan IAM yang dilampirkan
- [IAM.3] Kunci akses pengguna IAM harus diputar setiap 90 hari atau kurang
- [IAM.4] Kunci akses pengguna root IAM seharusnya tidak ada
- [IAM.5] MFA harus diaktifkan untuk semua pengguna IAM yang memiliki kata sandi konsol

- [IAM.6] MFA perangkat keras harus diaktifkan untuk pengguna root
- [IAM.7] Kebijakan kata sandi untuk pengguna IAM harus memiliki konfigurasi yang kuat
- [IAM.8] Kredensyal pengguna IAM yang tidak digunakan harus dihapus
- [IAM.21] Kebijakan terkelola pelanggan IAM yang Anda buat seharusnya tidak mengizinkan tindakan wildcard untuk layanan
- [Kinesis.1] Aliran kinesis harus dienkripsi saat istirahat
- [KMS.1] Kebijakan yang dikelola pelanggan IAM tidak boleh mengizinkan tindakan dekripsi pada semua kunci KMS
- [KMS.2] Prinsipal IAM tidak boleh memiliki kebijakan inline IAM yang memungkinkan tindakan dekripsi pada semua kunci KMS
- [KMS.3] tidak AWS KMS keys boleh dihapus secara tidak sengaja
- [KMS.4] rotasi AWS KMS tombol harus diaktifkan
- [Lambda.1] Kebijakan fungsi Lambda harus melarang akses publik
- [Lambda.2] Fungsi Lambda harus menggunakan runtime yang didukung
- [Lambda.3] Fungsi Lambda harus dalam VPC
- [Lambda.5] Fungsi VPC Lambda harus beroperasi di beberapa Availability Zone
- [MSK.1] Cluster MSK harus dienkripsi saat transit di antara node broker
- [MQ.5] Broker ActiveMQ harus menggunakan mode penerapan aktif/siaga
- [MQ.6] Broker RabbitMQ harus menggunakan mode penerapan cluster
- [Neptunus.1] Cluster DB Neptunus harus dienkripsi saat istirahat
- [Neptune.2] Cluster DB Neptunus harus menerbitkan log audit ke Log CloudWatch
- [Neptunus.4] Cluster DB Neptunus harus mengaktifkan perlindungan penghapusan
- [Neptunus.4] Cluster DB Neptunus harus mengaktifkan perlindungan penghapusan
- [Neptunus.5] Cluster DB Neptunus harus mengaktifkan cadangan otomatis
- [Neptune.6] Snapshot cluster Neptunus DB harus dienkripsi saat istirahat
- [Neptunus.7] Cluster DB Neptunus harus mengaktifkan otentikasi basis data IAM
- [Neptunus.8] Cluster DB Neptunus harus dikonfigurasi untuk menyalin tag ke snapshot
- [NetworkFirewall.3] Kebijakan Network Firewall harus memiliki setidaknya satu kelompok aturan yang terkait
- [NetworkFirewall.4] Tindakan stateless default untuk kebijakan Network Firewall harus drop atau forward untuk paket penuh

- [NetworkFirewall.5] Tindakan stateless default untuk kebijakan Network Firewall harus drop atau forward untuk paket yang terfragmentasi
- [NetworkFirewall.6] Grup aturan Stateless Network Firewall tidak boleh kosong
- [Opensearch.1] OpenSearch domain harus mengaktifkan enkripsi saat istirahat
- [Opensearch.2] OpenSearch domain tidak boleh diakses publik
- [Opensearch.3] OpenSearch domain harus mengenkripsi data yang dikirim antar node
- [Opensearch.4] login kesalahan OpenSearch domain ke Log harus diaktifkan CloudWatch
- [Opensearch.5] OpenSearch domain harus mengaktifkan pencatatan audit
- [Opensearch.6] OpenSearch domain harus memiliki setidaknya tiga node data
- [Opensearch.7] OpenSearch domain harus mengaktifkan kontrol akses berbutir halus
- [Opensearch.8] Koneksi ke OpenSearch domain harus dienkripsi menggunakan kebijakan keamanan TLS terbaru
- [RDS.1] Snapshot RDS harus pribadi
- [RDS.2] Instans RDS DB harus melarang akses publik, sebagaimana ditentukan oleh urasi PubliclyAccessible AWS Config
- [RDS.3] Instans RDS DB harus mengaktifkan enkripsi saat istirahat
- [RDS.4] Snapshot cluster RDS dan snapshot database harus dienkripsi saat istirahat
- [RDS.5] Instans RDS DB harus dikonfigurasi dengan beberapa Availability Zone
- [RDS.6] Pemantauan yang ditingkatkan harus dikonfigurasi untuk instans RDS DB
- [RDS.8] Instans RDS DB harus mengaktifkan perlindungan penghapusan
- [RDS.9] Instans RDS DB harus menerbitkan log ke Log CloudWatch
- [RDS.10] Otentikasi IAM harus dikonfigurasi untuk instance RDS
- [RDS.11] Instans RDS harus mengaktifkan pencadangan otomatis
- [RDS.12] Otentikasi IAM harus dikonfigurasi untuk cluster RDS
- [RDS.13] Peningkatan versi minor otomatis RDS harus diaktifkan
- [RDS.15] Cluster RDS DB harus dikonfigurasi untuk beberapa Availability Zone
- [RDS.17] Instans RDS DB harus dikonfigurasi untuk menyalin tag ke snapshot
- [RDS.18] Instans RDS harus digunakan di VPC
- [RDS.19] Langganan pemberitahuan acara RDS yang ada harus dikonfigurasi untuk peristiwa klaster penting

- [RDS.20] Langganan pemberitahuan acara RDS yang ada harus dikonfigurasi untuk peristiwa instance basis data penting
- [RDS.21] Langganan pemberitahuan acara RDS harus dikonfigurasi untuk peristiwa grup parameter basis data penting
- [RDS.22] Langganan pemberitahuan acara RDS harus dikonfigurasi untuk acara grup keamanan basis data penting
- [RDS.23] Instans RDS tidak boleh menggunakan port default mesin database
- [RDS.25] Instans database RDS harus menggunakan nama pengguna administrator khusus
- [RDS.27] Cluster RDS DB harus dienkripsi saat istirahat
- [Redshift.1] Cluster Amazon Redshift harus melarang akses publik
- [Redshift.2] Koneksi ke cluster Amazon Redshift harus dienkripsi saat transit
- [Redshift.4] Cluster Amazon Redshift harus mengaktifkan pencatatan audit
- [Redshift.6] Amazon Redshift harus mengaktifkan peningkatan otomatis ke versi utama
- [Redshift.7] Cluster Redshift harus menggunakan perutean VPC yang ditingkatkan
- [Redshift.8] Cluster Amazon Redshift tidak boleh menggunakan nama pengguna Admin default
- [Redshift.9] Cluster Redshift tidak boleh menggunakan nama database default
- [Redshift.10] Cluster Redshift harus dienkripsi saat istirahat
- [S3.1] Bucket tujuan umum S3 harus mengaktifkan pengaturan akses publik blok
- [S3.2] Bucket tujuan umum S3 harus memblokir akses baca publik
- [S3.3] Bucket tujuan umum S3 harus memblokir akses tulis publik
- [S3.5] Bucket tujuan umum S3 harus memerlukan permintaan untuk menggunakan SSL
- [S3.6] Kebijakan bucket tujuan umum S3 harus membatasi akses ke yang lain Akun AWS
- [S3.8] Bucket tujuan umum S3 harus memblokir akses publik
- [S3.9] Bucket tujuan umum S3 harus mengaktifkan pencatatan akses server
- [S3.12] ACL tidak boleh digunakan untuk mengelola akses pengguna ke bucket tujuan umum S3
- [S3.13] Bucket tujuan umum S3 harus memiliki konfigurasi Siklus Hidup
- [S3.17] Ember tujuan umum S3 harus dienkripsi saat istirahat AWS KMS keys
- [SageMaker.1] Instans SageMaker notebook Amazon seharusnya tidak memiliki akses internet langsung
- [SageMaker.2] instance SageMaker notebook harus diluncurkan dalam VPC khusus
- [SageMaker.3] Pengguna seharusnya tidak memiliki akses root ke instance SageMaker notebook

- [SecretsManager.1] Rahasia Secrets Manager harus mengaktifkan rotasi otomatis
- [SecretsManager.2] Rahasia Secrets Manager yang dikonfigurasi dengan rotasi otomatis harus berhasil diputar
- [SecretsManager.3] Hapus rahasia Secrets Manager yang tidak digunakan
- [SecretsManager.4] Rahasia Secrets Manager harus diputar dalam jumlah hari tertentu
- [SQS.1] Antrian Amazon SQS harus dienkripsi saat istirahat
- [SSM.1] Instans Amazon EC2 harus dikelola oleh AWS Systems Manager
- [SSM.2] Instans Amazon EC2 yang dikelola oleh Systems Manager harus memiliki status kepatuhan patch COMPLIANT setelah instalasi patch
- [SSM.3] Instans Amazon EC2 yang dikelola oleh Systems Manager harus memiliki status kepatuhan asosiasi COMPLIANT
- [SSM.4] Dokumen SSM seharusnya tidak bersifat publik
- [WAF.2] Aturan Regional AWS WAF Klasik harus memiliki setidaknya satu syarat
- [WAF.3] Kelompok aturan Regional AWS WAF Klasik harus memiliki setidaknya satu aturan
- [WAF.4] ACL web Regional AWS WAF klasik harus memiliki setidaknya satu aturan atau kelompok aturan
- [WAF.10] ACL AWS WAF web harus memiliki setidaknya satu aturan atau kelompok aturan

Untuk informasi selengkapnya tentang standar ini, lihat Kontrol Security Hub di Panduan AWS Control Tower Pengguna.

Melihat dan mengelola standar keamanan

Standar keamanan mencakup serangkaian persyaratan untuk menentukan kepatuhan terhadap kerangka peraturan, praktik terbaik industri, atau kebijakan perusahaan. AWS Security Hub memetakan persyaratan ini untuk mengontrol dan menjalankan pemeriksaan keamanan pada kontrol untuk menilai apakah persyaratan standar terpenuhi. Kontrol dapat diaktifkan dalam satu atau lebih standar. Jika Anda mengaktifkan temuan kontrol konsolidasi, Security Hub menghasilkan satu temuan per pemeriksaan keamanan bahkan ketika kontrol merupakan bagian dari beberapa standar yang diaktifkan. Untuk informasi selengkapnya, lihat Temuan kontrol terkonsolidasi.

Untuk daftar standar yang tersedia dan kontrol yang berlaku untuk mereka, lihatReferensi standar. Halaman standar Keamanan di konsol Security Hub juga menampilkan semua standar keamanan yang didukung di Security Hub dan status pengaktifannya. Untuk setiap standar keamanan yang

diaktifkan di akun Anda (atau jika Anda menggunakan integrasi dengan AWS Organizations, setidaknya dalam satu akun di organisasi Anda), Anda dapat melihat informasi berikut:

- Status pengaktifan standar dalam kebijakan konfigurasi Security Hub yang berbeda jika Anda menggunakan konfigurasi pusat
- Deskripsi standar yang dinonaktifkan
- Daftar kontrol yang saat ini diaktifkan dalam standar dan status keseluruhan kontrol tersebut berdasarkan status kepatuhan temuan mereka
- daftar kontrol yang berlaku untuk standar tetapi saat ini dinonaktifkan
- Skor keamanan untuk standar

Security Hub menghasilkan skor keamanan untuk setiap standar. Akun administrator melihat skor keamanan gabungan dan status kontrol di seluruh akun anggota mereka. Jika Anda telah menetapkan Wilayah agregasi, skor keamanan Anda mencerminkan status kepatuhan kontrol di semua Wilayah yang ditautkan. Untuk informasi selengkapnya, lihat Bagaimana skor keamanan dihitung.

Topik

- Mengaktifkan dan menonaktifkan standar keamanan
- Melihat detail untuk standar
- Mengaktifkan dan menonaktifkan kontrol dalam standar tertentu

Mengaktifkan dan menonaktifkan standar keamanan

Anda dapat mengaktifkan atau menonaktifkan setiap standar keamanan yang tersedia di Security Hub.

Sebelum Anda mengaktifkan standar keamanan apa pun, pastikan Anda telah mengaktifkan AWS Config dan mengonfigurasi perekaman sumber daya. Jika tidak, Security Hub mungkin tidak dapat menghasilkan temuan untuk kontrol yang berlaku untuk standar. Untuk informasi selengkapnya, lihat Mengkonfigurasi AWS Config.

> **Note**
>
> Petunjuk untuk mengaktifkan dan menonaktifkan standar bervariasi berdasarkan apakah Anda menggunakan konfigurasi pusat atau tidak. Bagian ini menjelaskan perbedaannya.

Konfigurasi pusat tersedia untuk pengguna yang mengintegrasikan Security Hub dan AWS Organizations. Kami merekomendasikan penggunaan konfigurasi pusat untuk menyederhanakan proses mengaktifkan dan menonaktifkan standar di lingkungan multi-akun, Multi-wilayah.

Mengaktifkan standar keamanan

Ketika Anda mengaktifkan standar keamanan, semua kontrol yang berlaku untuk standar secara otomatis diaktifkan di dalamnya. Security Hub juga mulai menghasilkan temuan untuk kontrol yang berlaku untuk standar.

Anda dapat memilih kontrol mana yang akan diaktifkan dan dinonaktifkan di setiap standar. Menonaktifkan kontrol menghentikan temuan untuk kontrol yang dihasilkan, dan kontrol diabaikan saat menghitung skor keamanan.

Saat Anda mengaktifkan Security Hub, Security Hub menghitung skor keamanan awal untuk standar dalam waktu 30 menit setelah kunjungan pertama Anda ke halaman Ringkasan atau halaman standar Keamanan di konsol Security Hub. Diperlukan waktu hingga 24 jam untuk skor keamanan pertama kali dihasilkan di Wilayah China dan AWS GovCloud (US) Region. Skor hanya dihasilkan untuk standar yang diaktifkan saat Anda mengunjungi halaman tersebut. Selain itu, perekaman AWS Config sumber daya harus dikonfigurasi agar skor muncul. Setelah menghasilkan skor pertama kali, Security Hub memperbarui skor keamanan setiap 24 jam. Security Hub menampilkan stempel waktu untuk menunjukkan kapan skor keamanan terakhir diperbarui. Untuk melihat daftar standar yang saat ini diaktifkan di akun Anda, panggil GetEnabledStandardsAPI.

Mengaktifkan standar di beberapa akun dan Wilayah

Untuk mengaktifkan standar keamanan di beberapa akun dan Wilayah AWS, Anda harus menggunakan konfigurasi pusat.

Bila Anda menggunakan konfigurasi pusat, administrator yang didelegasikan dapat membuat kebijakan konfigurasi Security Hub yang mengaktifkan satu atau beberapa standar. Anda kemudian dapat mengaitkan kebijakan konfigurasi dengan akun tertentu dan unit organisasi (OU) atau root. Kebijakan konfigurasi berlaku di Wilayah asal Anda (juga disebut Wilayah agregasi) dan semua Wilayah yang ditautkan.

Kebijakan konfigurasi menawarkan penyesuaian. Misalnya, Anda dapat memilih untuk mengaktifkan hanya AWS Foundational Security Best Practices (FSBP) di satu OU, dan Anda dapat memilih untuk

mengaktifkan FSBP dan Center for Internet Security (CIS) AWS Foundations Benchmark v1.4.0 di OU lain. Untuk petunjuk cara membuat kebijakan konfigurasi yang memungkinkan standar tertentu, lihat Membuat dan mengaitkan kebijakan konfigurasi Security Hub

Jika Anda menggunakan konfigurasi pusat, Security Hub tidak secara otomatis mengaktifkan standar apa pun di akun baru atau yang sudah ada. Sebagai gantinya, saat membuat kebijakan konfigurasi, administrator yang didelegasikan menentukan standar mana yang akan diaktifkan di akun yang berbeda. Security Hub menawarkan kebijakan konfigurasi yang direkomendasikan di mana hanya FSBP yang diaktifkan. Untuk informasi selengkapnya, lihat Jenis kebijakan konfigurasi.

> **Note**
>
> Administrator yang didelegasikan dapat membuat kebijakan konfigurasi untuk mengaktifkan standar apa pun kecuali Standar yang Dikelola Layanan:. AWS Control Tower Anda dapat mengaktifkan standar ini hanya dalam AWS Control Tower layanan. Jika Anda menggunakan konfigurasi pusat, Anda dapat mengaktifkan dan menonaktifkan kontrol dalam standar ini untuk akun yang dikelola secara terpusat hanya di AWS Control Tower.

Jika Anda ingin beberapa akun mengonfigurasi standarnya sendiri daripada administrator yang didelegasikan, administrator yang didelegasikan dapat menetapkan akun tersebut sebagai dikelola sendiri. Akun yang dikelola sendiri harus mengonfigurasi standar secara terpisah di setiap Wilayah.

Mengaktifkan standar dalam satu akun dan Wilayah

Jika Anda tidak menggunakan konfigurasi pusat atau jika Anda adalah akun yang dikelola sendiri, Anda tidak dapat menggunakan kebijakan konfigurasi untuk mengaktifkan standar secara terpusat di beberapa akun dan Wilayah. Namun, Anda dapat menggunakan langkah-langkah berikut untuk mengaktifkan standar dalam satu akun dan Wilayah.

Security Hub console

Untuk mengaktifkan standar dalam satu akun dan Wilayah

1. Buka AWS Security Hub konsol di https://console.aws.amazon.com/securityhub/.
2. Konfirmasikan bahwa Anda menggunakan Security Hub di Wilayah tempat Anda ingin mengaktifkan standar.
3. Di panel navigasi Security Hub, pilih Standar keamanan.

4. Untuk standar yang ingin Anda aktifkan, pilih Aktifkan. Ini juga memungkinkan semua kontrol dalam standar itu.
5. Ulangi di setiap Wilayah di mana Anda ingin mengaktifkan standar.

Security Hub API

Untuk mengaktifkan standar dalam satu akun dan Wilayah

1. Memanggil BatchEnableStandardsAPI.
2. Berikan Nama Sumber Daya Amazon (ARN) dari standar yang ingin Anda aktifkan. Untuk mendapatkan ARN standar, panggil API. DescribeStandards
3. Ulangi di setiap Wilayah di mana Anda ingin mengaktifkan standar.

AWS CLI

Untuk mengaktifkan standar dalam satu akun dan Wilayah

1. Jalankan perintah batch-enable-standards.
2. Berikan Nama Sumber Daya Amazon (ARN) dari standar yang ingin Anda aktifkan. Untuk mendapatkan ARN standar, jalankan perintah. describe-standards

```
aws securityhub batch-enable-standards --standards-subscription-requests
 '{"StandardsArn": "standard ARN"}'
```

Contoh

```
aws securityhub batch-enable-standards --standards-subscription-requests
 '{"StandardsArn":"arn:aws:securityhub:us-east-1::standards/aws-foundational-
security-best-practices/v/1.0.0"}'
```

3. Ulangi di setiap Wilayah di mana Anda ingin mengaktifkan standar.

Secara otomatis mengaktifkan standar keamanan default

Jika Anda tidak menggunakan konfigurasi pusat, Security Hub secara otomatis mengaktifkan standar keamanan default di akun baru saat mereka bergabung dengan organisasi Anda. Semua kontrol yang merupakan bagian dari standar default juga diaktifkan secara otomatis. Saat ini, standar

keamanan default yang diaktifkan secara otomatis adalah AWS Foundational Security Best Practices (FSBP) dan Center for Internet Security (CIS) AWS Foundations Benchmark v1.2.0. Anda dapat menonaktifkan standar yang diaktifkan secara otomatis jika Anda memilih untuk mengaktifkan standar secara manual di akun baru.

Jika Anda menggunakan konfigurasi pusat, Anda dapat membuat kebijakan konfigurasi yang mengaktifkan standar default dan mengaitkan kebijakan ini dengan root. Semua akun organisasi dan OU Anda akan mewarisi kebijakan konfigurasi ini kecuali jika dikaitkan dengan kebijakan yang berbeda atau dikelola sendiri.

Matikan standar yang diaktifkan secara otomatis

Langkah-langkah berikut hanya berlaku jika Anda mengintegrasikan dengan AWS Organizations tetapi tidak menggunakan konfigurasi pusat. Jika Anda tidak menggunakan integrasi Organizations, Anda dapat menonaktifkan standar default saat pertama kali mengaktifkan Security Hub, atau Anda dapat mengikuti langkah-langkah untuk menonaktifkan standar.

Security Hub console

Untuk mematikan standar yang diaktifkan secara otomatis

1. Buka AWS Security Hub konsol di https://console.aws.amazon.com/securityhub/.

   Masuk menggunakan kredensyal akun administrator.
2. Di panel navigasi Security Hub, di bawah Pengaturan, pilih Konfigurasi.
3. Di bagian Akun, matikan standar default Aktifkan otomatis.

Security Hub API

Untuk mematikan standar yang diaktifkan secara otomatis

1. Memanggil UpdateOrganizationConfigurationAPI dari akun administrator Security Hub.
2. Untuk mematikan standar yang diaktifkan secara otomatis di akun anggota baru, tetapkan `AutoEnableStandards` sama dengan`NONE`.

AWS CLI

Untuk mematikan standar yang diaktifkan secara otomatis

1. Jalankan perintah update-organization-configuration.
2. Sertakan `auto-enable-standards` parameter untuk mematikan standar yang diaktifkan secara otomatis di akun anggota baru.

```
aws securityhub update-organization-configuration --auto-enable-standards
```

Menonaktifkan standar keamanan

Saat Anda menonaktifkan standar keamanan di Security Hub, hal berikut akan terjadi:

- Semua kontrol yang berlaku untuk standar juga dinonaktifkan kecuali jika dikaitkan dengan standar lain.
- Pemeriksaan untuk kontrol yang dinonaktifkan tidak lagi dilakukan, dan tidak ada temuan tambahan yang dihasilkan untuk kontrol yang dinonaktifkan.
- Temuan yang ada untuk kontrol yang dinonaktifkan diarsipkan secara otomatis setelah sekitar 3-5 hari.
- AWS Config Aturan yang dibuat oleh Security Hub untuk kontrol yang dinonaktifkan akan dihapus.

  Ini biasanya terjadi dalam beberapa menit setelah Anda menonaktifkan standar, tetapi mungkin memakan waktu lebih lama. Jika permintaan pertama untuk menghapus AWS Config aturan gagal, maka Security Hub mencoba ulang setiap 12 jam. Namun, jika Anda menonaktifkan Security Hub atau tidak mengaktifkan standar lain, maka Security Hub tidak dapat mencoba lagi permintaan tersebut, artinya tidak dapat menghapus AWS Config aturan. Jika ini terjadi, dan Anda perlu menghapus AWS Config aturan, hubungi AWS Support.

Menonaktifkan standar di beberapa akun dan Wilayah

Untuk menonaktifkan standar keamanan di beberapa akun dan Wilayah, Anda harus menggunakan konfigurasi pusat.

Bila Anda menggunakan konfigurasi pusat, administrator yang didelegasikan dapat membuat kebijakan konfigurasi yang menonaktifkan satu atau beberapa standar. Anda dapat mengaitkan

kebijakan konfigurasi dengan akun tertentu dan OU atau root. Kebijakan konfigurasi berlaku di Wilayah asal Anda (juga disebut Wilayah agregasi) dan semua Wilayah yang ditautkan.

Kebijakan konfigurasi menawarkan penyesuaian. Misalnya, Anda dapat memilih untuk menonaktifkan Standar Keamanan Data Industri Kartu Pembayaran (PCI DSS) dalam satu OU, dan Anda dapat memilih untuk menonaktifkan PCI DSS dan National Institute of Standards and Technology (NIST) SP 800-53 Rev. 5 di OU lain. Untuk petunjuk cara membuat kebijakan konfigurasi yang menonaktifkan standar tertentu, lihatMembuat dan mengaitkan kebijakan konfigurasi Security Hub.

> **Note**
>
> Administrator yang didelegasikan dapat membuat kebijakan konfigurasi untuk menonaktifkan standar apa pun kecuali Standar yang Dikelola Layanan:. AWS Control Tower Anda dapat menonaktifkan standar ini hanya dalam AWS Control Tower layanan. Jika Anda menggunakan konfigurasi pusat, Anda dapat mengaktifkan dan menonaktifkan kontrol dalam standar ini untuk akun yang dikelola secara terpusat hanya di AWS Control Tower.

Jika Anda ingin beberapa akun mengonfigurasi standarnya sendiri daripada administrator yang didelegasikan, administrator yang didelegasikan dapat menetapkan akun tersebut sebagai dikelola sendiri. Akun yang dikelola sendiri harus mengonfigurasi standar secara terpisah di setiap Wilayah.

Menonaktifkan standar dalam satu akun dan Wilayah

Jika Anda tidak menggunakan konfigurasi pusat atau akun yang dikelola sendiri, Anda tidak dapat menggunakan kebijakan konfigurasi untuk menonaktifkan standar secara terpusat di beberapa akun dan Wilayah. Namun, Anda dapat menggunakan langkah-langkah berikut untuk menonaktifkan standar dalam satu akun dan Wilayah.

Security Hub console

Untuk menonaktifkan standar dalam satu akun dan Wilayah

1. Buka AWS Security Hub konsol di https://console.aws.amazon.com/securityhub/.
2. Konfirmasikan bahwa Anda menggunakan Security Hub di Wilayah tempat Anda ingin menonaktifkan standar.
3. Di panel navigasi Security Hub, pilih Standar keamanan.
4. Untuk standar yang ingin Anda nonaktifkan, pilih Nonaktifkan.
5. Ulangi di setiap Wilayah di mana Anda ingin menonaktifkan standar.

Security Hub API

Untuk menonaktifkan standar dalam satu akun dan Wilayah

1. Memanggil BatchDisableStandardsAPI.
2. Untuk setiap standar yang ingin Anda nonaktifkan, berikan ARN berlangganan standar. Untuk mendapatkan ARN langganan untuk standar yang diaktifkan, panggil API. GetEnabledStandards
3. Ulangi di setiap Wilayah di mana Anda ingin menonaktifkan standar.

AWS CLI

Untuk menonaktifkan standar dalam satu akun dan Wilayah

1. Jalankan perintah batch-disable-standards.
2. Untuk setiap standar yang ingin Anda nonaktifkan, berikan ARN berlangganan standar. Untuk mendapatkan ARN langganan untuk standar yang diaktifkan, jalankan get-enabled-standardsperintah.

```
aws securityhub batch-disable-standards --standards-subscription-arns "standard
 subscription ARN"
```

Contoh

```
aws securityhub batch-disable-standards --standards-subscription-arns
 "arn:aws:securityhub:us-west-1:123456789012:subscription/aws-foundational-
security-best-practices/v/1.0.0"
```

3. Ulangi di setiap Wilayah di mana Anda ingin menonaktifkan standar.

Melihat detail untuk standar

Di AWS Security Hub konsol, halaman detail untuk standar mencakup informasi berikut:

- Skor keamanan standar dan ringkasan visual pemeriksaan keamanan untuk kontrol yang diaktifkan dalam standar. Jika Anda mengintegrasikan dengan AWS Organizations, kontrol yang diaktifkan di setidaknya satu akun organisasi dianggap diaktifkan.
- Pengaturan untuk mengaktifkan atau menonaktifkan kontrol yang berlaku untuk standar.

- Daftar kontrol yang berlaku untuk standar. Kontrol dibagi menjadi tab yang berbeda berdasarkan status pemberdayaan. Jumlah kontrol di kolom Semua diaktifkan adalah jumlah kontrol di kolom Gagal, Tidak Dikenal, Tidak Ada data, dan Lulus.

Anda juga dapat menggunakan Security Hub API dan AWS CLI untuk mengambil detail untuk standar. Bagian berikut menjelaskan cara mendapatkan detail untuk standar.

Menampilkan halaman detail untuk standar yang diaktifkan (konsol)

Dari halaman Standar keamanan, Anda dapat menampilkan halaman detail untuk standar yang diaktifkan.

Jika Anda masuk ke akun administrator, Anda dapat melihat detail untuk standar apa pun yang diaktifkan di setidaknya satu akun anggota.

1. Buka AWS Security Hub konsol di https://console.aws.amazon.com/securityhub/.
2. Di panel navigasi Security Hub, pilih Standar keamanan.
3. Untuk standar yang ingin Anda tampilkan detailnya, pilih Lihat hasil.

Skor keamanan standar dan ringkasan pemeriksaan keamanan

Di bagian atas halaman detail standar adalah skor keamanan untuk standar. Skor adalah persentase kontrol yang diteruskan relatif terhadap jumlah kontrol yang diaktifkan (yang memiliki data) untuk standar.

Security Hub biasanya menghitung skor keamanan awal dalam waktu 30 menit setelah kunjungan pertama Anda ke halaman Ringkasan atau halaman standar Keamanan di konsol Security Hub. Skor hanya dihasilkan untuk standar yang diaktifkan saat Anda mengunjungi halaman tersebut. Untuk melihat daftar standar yang saat ini diaktifkan, gunakan operasi `GetEnabledStandards`API. Selain itu, perekaman AWS Config sumber daya harus dikonfigurasi agar skor muncul. Setelah menghasilkan skor pertama kali, Security Hub memperbarui skor keamanan setiap 24 jam. Security Hub menampilkan stempel waktu untuk menunjukkan kapan skor keamanan terakhir diperbarui. Untuk informasi selengkapnya, lihat the section called “Menentukan skor keamanan”.

> **Note**
>
> Diperlukan waktu hingga 24 jam untuk skor keamanan pertama kali dihasilkan di Wilayah China dan AWS GovCloud (US) Region.

Di sebelah skor adalah bagan yang merangkum pemeriksaan keamanan untuk kontrol yang diaktifkan untuk standar. Bagan menunjukkan persentase pemeriksaan keamanan yang gagal dan lulus. Saat Anda berhenti sejenak pada bagan, pop-up menampilkan yang berikut:

- Jumlah pemeriksaan keamanan yang gagal untuk kontrol setiap tingkat keparahan
- Jumlah pemeriksaan keamanan untuk kontrol dengan status Tidak Dikenal
- Jumlah pemeriksaan keamanan yang lolos

Untuk akun administrator, skor dan bagan standar digabungkan di seluruh akun administrator dan semua akun anggota.

Semua data pada halaman detail standar Keamanan khusus untuk Wilayah saat ini kecuali Anda telah menetapkan Wilayah agregasi. Jika Anda telah menetapkan Wilayah agregasi, skor keamanan berlaku di seluruh Wilayah dan menyertakan temuan di semua Wilayah yang ditautkan. Status kepatuhan kontrol pada halaman detail standar juga mencerminkan temuan dari Wilayah terkait, dan jumlah pemeriksaan keamanan mencakup temuan dari Wilayah terkait.

Melihat kontrol dalam standar yang diaktifkan

Saat Anda mengunjungi halaman detail untuk standar, Anda dapat melihat daftar kontrol keamanan yang berlaku untuk standar. Daftar ini diurutkan berdasarkan status kepatuhan kontrol dan tingkat keparahan yang ditetapkan untuk setiap kontrol. Security Hub memperbarui status kontrol dan jumlah pemeriksaan keamanan setiap 24 jam. Stempel waktu pada setiap tab menunjukkan kapan status kontrol dan jumlah pemeriksaan keamanan terbaru diperbarui. Untuk informasi selengkapnya, lihat the section called “Status kepatuhan dan status kontrol”.

Untuk akun administrator, status kepatuhan kontrol dan jumlah pemeriksaan keamanan dikumpulkan di seluruh akun administrator dan semua akun anggota.

Tab Semua diaktifkan mencantumkan semua kontrol yang saat ini diaktifkan dalam standar. Untuk akun administrator, tab Semua diaktifkan mencakup kontrol yang diaktifkan dalam standar di akun mereka atau setidaknya satu akun anggota.

Pada tab Gagal, Tidak Dikenal, Tidak Ada Data, dan Lulus, kontrol dari tab Semua diaktifkan disaring untuk menyertakan hanya kontrol yang diaktifkan dengan status tertentu.

Tab Dinonaktifkan berisi daftar kontrol yang dinonaktifkan dalam standar. Untuk akun administrator, tab Dinonaktifkan mencakup kontrol yang dinonaktifkan dalam standar di akun mereka dan semua akun anggota.

Untuk setiap kontrol, tab menampilkan informasi berikut:

- Status kontrol (lihatthe section called “Status kepatuhan dan status kontrol”)
- Tingkat keparahan yang ditetapkan untuk kontrol
- ID kontrol dan judul
- Jumlah temuan aktif yang gagal dari jumlah total temuan aktif. Jika berlaku, kolom Cek gagal juga mencantumkan jumlah temuan dengan status Tidak Diketahui.

Selain filter pencarian di setiap tab, Anda dapat mengurutkan daftar berdasarkan bidang berikut:

- Status Kepatuhan
- Keparahan
- ID
- Judul
- Cek gagal

Anda dapat mengurutkan setiap daftar menggunakan salah satu kolom. Secara default, tab Semua diaktifkan diurutkan sehingga kontrol yang gagal berada di bagian atas daftar. Ini membantu Anda untuk segera fokus pada masalah yang memerlukan perbaikan.

Pada tab yang tersisa, kontrol diurutkan secara default dalam urutan menurun berdasarkan tingkat keparahan. Dengan kata lain, kontrol kritis adalah yang pertama, diikuti oleh kontrol tingkat keparahan tinggi, kemudian sedang, lalu rendah.

Pilih metode akses pilihan Anda, dan ikuti langkah-langkah untuk menampilkan kontrol yang tersedia untuk standar yang diaktifkan. Sebagai pengganti petunjuk ini, Anda juga dapat menggunakan operasi DescribeStandardsControlAPI.

Security Hub console

1. Buka AWS Security Hub konsol di https://console.aws.amazon.com/securityhub/.
2. Pilih Standar keamanan di panel navigasi.
3. Pilih Lihat hasil untuk standar. Bagian bawah halaman mencantumkan kontrol (dibagi dengan tab) yang berlaku untuk standar.

Security Hub API

1. Jalankan ListSecurityControlDefinitionsdan berikan Amazon Resource Name (ARN) standar untuk mendapatkan daftar ID kontrol untuk standar tersebut. Untuk mendapatkan ARN standar, jalankan DescribeStandards. Jika Anda tidak menyediakan ARN standar, API ini mengembalikan semua ID kontrol Security Hub. API ini mengembalikan ID kontrol keamanan agnostik standar, bukan ID kontrol khusus standar.

   Permintaan contoh:

   ```
   {
       "StandardsArn": "arn:aws:securityhub:::standards/aws-foundational-security-best-practices/v/1.0.0"
   }
   ```

2. Jalankan ListStandardsControlAssociations untuk mengetahui apakah kontrol diaktifkan di setiap standar yang telah Anda aktifkan di akun Anda.
3. Identifikasi kontrol dengan menyediakan `SecurityControlId` atau`SecurityControlArn`. Parameter pagination adalah opsional.

   Permintaan contoh:

   ```
   {
       SecurityControlId: Config.1
       NextToken: lkeyusdlk-sdlflsnd-ladfterb
       MaxResults: 5
   }
   ```

AWS CLI

1. Jalankan list-security-control-definitions perintah, dan berikan satu atau lebih ARN standar untuk mendapatkan daftar ID kontrol. Untuk mendapatkan ARN standar, jalankan `describe-standards` perintah. Jika Anda tidak menyediakan ARN standar, perintah ini mengembalikan semua ID kontrol Security Hub. Perintah ini mengembalikan ID kontrol keamanan agnostik standar, bukan ID kontrol khusus standar.

   ```
   aws securityhub --region us-east-1 list-security-control-definitions --standards-arn "arn:aws:securityhub:us-east-1::standards/aws-foundational-security-best-practices/v/1.0.0"
   ```

2. Jalankan `list-standards-control-associations` perintah untuk mengetahui apakah kontrol diaktifkan di setiap standar yang telah Anda aktifkan di akun Anda.
3. Identifikasi kontrol dengan menyediakan `security-control-id` atau`security-control-arn`.

   Contoh perintah:

   ```
   aws securityhub --region us-east-1 list-standards-control-associations --
   security-control-id Config.1
   ```

Mengunduh daftar kontrol

Anda dapat mengunduh halaman daftar kontrol saat ini ke `.csv` file.

Jika Anda memfilter daftar kontrol, maka file yang diunduh hanya menyertakan kontrol yang cocok dengan pengaturan filter.

Jika Anda memilih kontrol tertentu dari daftar, maka file yang diunduh hanya menyertakan kontrol itu.

Untuk mengunduh halaman daftar kontrol saat ini atau kontrol yang dipilih saat ini, pilih Unduh.

Mengaktifkan dan menonaktifkan kontrol dalam standar tertentu

Saat Anda mengaktifkan standar AWS Security Hub, semua kontrol yang berlaku padanya akan diaktifkan secara otomatis dalam standar tersebut (pengecualian untuk ini adalah standar yang dikelola layanan). Anda kemudian dapat menonaktifkan dan mengaktifkan kembali kontrol tertentu dalam standar. Namun, kami menyarankan untuk menyelaraskan status pemberdayaan kontrol di semua standar yang Anda aktifkan.

> **Note**
>
> Jika Anda menggunakan konfigurasi pusat Security Hub, administrator yang didelegasikan dapat mengaktifkan dan dan menonaktifkan kontrol untuk akun organisasi di semua standar yang diaktifkan. Kami merekomendasikan pendekatan ini sehingga status pemberdayaan kontrol selaras di seluruh standar. Namun, administrator yang didelegasikan dapat menunjuk akun sebagai dikelola sendiri, yang memberi mereka kemampuan untuk mengaktifkan dan menonaktifkan kontrol dalam standar tertentu. Untuk informasi selengkapnya, lihat Cara kerja konfigurasi pusat.

Halaman detail untuk standar berisi daftar kontrol yang berlaku untuk standar, dan informasi tentang kontrol mana yang saat ini diaktifkan dan dinonaktifkan dalam standar tersebut.

Pada halaman detail standar, Anda juga dapat mengaktifkan dan menonaktifkan kontrol dalam standar tertentu. Anda harus mengaktifkan dan menonaktifkan kontrol secara terpisah di masing-masing Akun AWS dan Wilayah AWS. Saat Anda mengaktifkan atau menonaktifkan kontrol, itu hanya memengaruhi akun saat ini dan Wilayah.

Anda dapat mengaktifkan dan menonaktifkan kontrol di setiap Wilayah menggunakan konsol Security Hub, Security Hub API, atau AWS CLI. Jika Anda telah menetapkan Wilayah agregasi, Anda akan melihat kontrol dari semua Wilayah tertaut. Jika kontrol tersedia di Wilayah tertaut tetapi tidak di Wilayah agregasi, Anda tidak dapat mengaktifkan atau menonaktifkan kontrol tersebut dari Wilayah agregasi. Untuk skrip penonaktifan kontrol multi-akun dan Multi-wilayah, lihat Menonaktifkan kontrol Security Hub di lingkungan multi-akun.

Mengaktifkan kontrol dalam standar tertentu

Untuk mengaktifkan kontrol dalam standar, Anda harus terlebih dahulu mengaktifkan setidaknya satu standar yang berlaku kontrol. Untuk informasi selengkapnya tentang mengaktifkan standar, lihatMengaktifkan dan menonaktifkan standar keamanan. Ketika Anda mengaktifkan kontrol dalam standar, AWS Security Hub mulailah menghasilkan temuan untuk kontrol itu. Security Hub mencakup status kontrol dalam perhitungan skor keamanan keseluruhan dan skor keamanan standar. Bahkan jika Anda mengaktifkan kontrol dalam beberapa standar, Anda akan menerima satu temuan per pemeriksaan keamanan di seluruh standar jika Anda mengaktifkan temuan kontrol konsolidasi. Untuk informasi lebih lanjut, lihat Temuan kontrol konsolidasi.

Untuk mengaktifkan kontrol dalam standar, kontrol harus tersedia di Wilayah Anda saat ini. Untuk informasi selengkapnya, lihat Ketersediaan kontrol menurut Wilayah.

Ikuti langkah-langkah ini untuk mengaktifkan kontrol Security Hub dalam standar tertentu. Sebagai pengganti langkah-langkah berikut, Anda juga dapat menggunakan tindakan `UpdateStandardsControl`API untuk mengaktifkan kontrol dalam standar tertentu. Untuk petunjuk tentang mengaktifkan kontrol di semua standar, lihatMengaktifkan kontrol di semua standar dalam satu akun dan Wilayah.

Security Hub console

Untuk mengaktifkan kontrol dalam standar tertentu

1. Buka AWS Security Hub konsol di https://console.aws.amazon.com/securityhub/.

2. Pilih Standar keamanan dari panel navigasi.
3. Pilih Lihat hasil untuk standar yang relevan.
4. Pilih kontrol.
5. Pilih Aktifkan Kontrol (opsi ini tidak muncul untuk kontrol yang sudah diaktifkan). Konfirmasikan dengan memilih Aktifkan.

Security Hub API

Untuk mengaktifkan kontrol dalam standar tertentu

1. Jalankan`ListSecurityControlDefinitions`, dan berikan ARN standar untuk mendapatkan daftar kontrol yang tersedia untuk standar tertentu. Untuk mendapatkan ARN standar, jalankan. `DescribeStandards` API ini mengembalikan ID kontrol keamanan agnostik standar, bukan ID kontrol khusus standar.

   Permintaan contoh:

   ```
   {
       "StandardsArn": "arn:aws:securityhub:::standards/aws-foundational-security-best-practices/v/1.0.0"
   }
   ```

2. Jalankan`ListStandardsControlAssociations`, dan berikan ID kontrol khusus untuk mengembalikan status pengaktifan kontrol saat ini di setiap standar.

   Permintaan contoh:

   ```
   {
       "SecurityControlId": "IAM.1"
   }
   ```

3. Jalankan `BatchUpdateStandardsControlAssociations`. Berikan ARN standar yang ingin Anda aktifkan kontrolnya.
4. Atur `AssociationStatus` parameter sama dengan`ENABLED`.

   Permintaan contoh:

   ```
   {
   ```

```
    "StandardsControlAssociationUpdates": [{"SecurityControlId": "IAM.1",
 "StandardsArn": "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0", "AssociationStatus": "ENABLED"}]
}
```

AWS CLI

Untuk mengaktifkan kontrol dalam standar tertentu

1. Jalankan `list-security-control-definitions` perintah, dan berikan ARN standar untuk mendapatkan daftar kontrol yang tersedia untuk standar tertentu. Untuk mendapatkan ARN standar, jalankan. `describe-standards` Perintah ini mengembalikan ID kontrol keamanan agnostik standar, bukan ID kontrol khusus standar.

   ```
   aws securityhub --region us-east-1 list-security-control-definitions --
   standards-arn "arn:aws:securityhub:us-east-1::standards/aws-foundational-
   security-best-practices/v/1.0.0"
   ```

2. Jalankan `list-standards-control-associations` perintah, dan berikan ID kontrol khusus untuk mengembalikan status pengaktifan kontrol saat ini di setiap standar.

   ```
   aws securityhub  --region us-east-1 list-standards-control-associations --
   security-control-id CloudTrail.1
   ```

3. Jalankan perintah `batch-update-standards-control-associations`. Berikan ARN standar yang ingin Anda aktifkan kontrolnya.
4. Atur `AssociationStatus` parameter sama dengan`ENABLED`.

   ```
   aws securityhub  --region us-east-1 batch-update-standards-control-associations
    --standards-control-association-updates '[{"SecurityControlId": "CloudTrail.1",
    "StandardsArn": "arn:aws:securityhub:us-east-1::standards/aws-foundational-
   security-best-practices/v/1.0.0", "AssociationStatus": "ENABLED"}]'
   ```

Menonaktifkan kontrol dalam standar tertentu

Saat Anda menonaktifkan kontrol dalam standar, Security Hub berhenti menghasilkan temuan untuk kontrol. Status kontrol tidak lagi digunakan dalam menghitung skor keamanan untuk standar.

Salah satu cara untuk menonaktifkan kontrol adalah dengan menonaktifkan semua standar yang berlaku untuk kontrol. Ketika Anda menonaktifkan standar, semua kontrol yang berlaku untuk standar dinonaktifkan (namun, kontrol tersebut mungkin masih tetap diaktifkan dalam standar lain). Untuk informasi tentang menonaktifkan standar, lihat. the section called “Mengaktifkan dan menonaktifkan standar”

Saat Anda menonaktifkan kontrol dengan menonaktifkan standar yang berlaku, hal berikut terjadi:

- Pemeriksaan keamanan untuk kontrol tidak lagi dilakukan untuk standar itu. Ini berarti status kontrol tidak akan memengaruhi skor keamanan standar (Security Hub akan terus menjalankan pemeriksaan keamanan untuk kontrol jika diaktifkan dalam standar lain).
- Tidak ada temuan tambahan yang dihasilkan untuk kontrol itu.
- Temuan yang ada diarsipkan secara otomatis setelah 3-5 hari (perhatikan bahwa ini adalah upaya terbaik dan tidak dijamin).
- AWS Config Aturan terkait yang dibuat Security Hub akan dihapus.

Saat Anda menonaktifkan standar, Security Hub tidak melacak kontrol mana yang dinonaktifkan. Jika Anda kemudian mengaktifkan standar lagi, semua kontrol yang berlaku untuk itu diaktifkan secara otomatis. Selain itu, menonaktifkan kontrol adalah tindakan satu kali. Misalkan Anda menonaktifkan kontrol, dan kemudian Anda mengaktifkan standar yang sebelumnya dinonaktifkan. Jika standar mencakup kontrol itu, itu akan diaktifkan dalam standar itu. Saat Anda mengaktifkan standar di Security Hub, semua kontrol yang berlaku untuk standar tersebut akan diaktifkan secara otomatis.

Alih-alih menonaktifkan kontrol dengan menonaktifkan standar yang berlaku, Anda bisa menonaktifkan kontrol dalam satu atau lebih standar spesifik.

Untuk mengurangi kebisingan temuan, akan berguna untuk menonaktifkan kontrol yang tidak relevan dengan lingkungan Anda. Untuk rekomendasi tentang kontrol mana yang harus dinonaktifkan, lihat Kontrol Security Hub yang mungkin ingin Anda nonaktifkan.

Ikuti langkah-langkah ini untuk menonaktifkan kontrol dalam standar tertentu. Sebagai pengganti langkah-langkah berikut, Anda juga dapat menggunakan tindakan `UpdateStandardsControl`API untuk menonaktifkan kontrol dalam standar tertentu. Untuk petunjuk tentang menonaktifkan kontrol di semua standar, lihat. Mengaktifkan dan menonaktifkan kontrol di semua standar

Security Hub console

Untuk menonaktifkan kontrol dalam standar tertentu

1. Buka AWS Security Hub konsol di https://console.aws.amazon.com/securityhub/.
2. Pilih Standar keamanan dari panel navigasi. Pilih Lihat hasil untuk standar yang relevan.
3. Pilih kontrol.
4. Pilih Nonaktifkan Kontrol (opsi ini tidak muncul untuk kontrol yang sudah dinonaktifkan).
5. Berikan alasan untuk menonaktifkan kontrol, dan konfirmasikan dengan memilih Nonaktifkan.

Security Hub API

Untuk menonaktifkan kontrol dalam standar tertentu

1. Jalankan`ListSecurityControlDefinitions`, dan berikan ARN standar untuk mendapatkan daftar kontrol yang tersedia untuk standar tertentu. Untuk mendapatkan ARN standar, jalankan. `DescribeStandards` API ini mengembalikan ID kontrol keamanan agnostik standar, bukan ID kontrol khusus standar.

   Permintaan contoh:

   ```
   {
       "StandardsArn": "arn:aws:securityhub:::standards/aws-foundational-security-best-practices/v/1.0.0"
   }
   ```

2. Jalankan`ListStandardsControlAssociations`, dan berikan ID kontrol khusus untuk mengembalikan status pengaktifan kontrol saat ini di setiap standar.

   Permintaan contoh:

   ```
   {
       "SecurityControlId": "IAM.1"
   }
   ```

3. Jalankan `BatchUpdateStandardsControlAssociations`. Berikan ARN standar di mana Anda ingin menonaktifkan kontrol.

4. Atur `AssociationStatus` parameter sama dengan`DISABLED`. Jika Anda mengikuti langkah-langkah ini untuk kontrol yang sudah dinonaktifkan, API akan mengembalikan respons kode status HTTP 200.

   Permintaan contoh:

```
{
    "StandardsControlAssociationUpdates": [{"SecurityControlId": "IAM.1",
 "StandardsArn": "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0", "AssociationStatus": "DISABLED",  "UpdatedReason": "Not applicable to
 environment"}]
}
```

AWS CLI

Untuk menonaktifkan kontrol dalam standar tertentu

1. Jalankan `list-security-control-definitions` perintah, dan berikan ARN standar untuk mendapatkan daftar kontrol yang tersedia untuk standar tertentu. Untuk mendapatkan ARN standar, jalankan. `describe-standards` Perintah ini mengembalikan ID kontrol keamanan agnostik standar, bukan ID kontrol khusus standar.

```
aws securityhub --region us-east-1 list-security-control-definitions --
standards-arn "arn:aws:securityhub:us-east-1::standards/aws-foundational-
security-best-practices/v/1.0.0"
```

2. Jalankan `list-standards-control-associations` perintah, dan berikan ID kontrol khusus untuk mengembalikan status pengaktifan kontrol saat ini di setiap standar.

```
aws securityhub  --region us-east-1 list-standards-control-associations --
security-control-id CloudTrail.1
```

3. Jalankan perintah `batch-update-standards-control-associations`. Berikan ARN standar di mana Anda ingin menonaktifkan kontrol.
4. Atur `AssociationStatus` parameter sama dengan`DISABLED`. Jika Anda mengikuti langkah-langkah ini untuk kontrol yang sudah diaktifkan, perintah akan mengembalikan respons kode status HTTP 200.

```
aws securityhub  --region us-east-1 batch-update-standards-control-
associations --standards-control-association-updates '[{"SecurityControlId":
 "CloudTrail.1", "StandardsArn": "arn:aws:securityhub:us-east-1::standards/aws-
foundational-security-best-practices/v/1.0.0", "AssociationStatus": "DISABLED",
 "UpdatedReason": "Not applicable to environment"}]'
```

Referensi kontrol Security Hub

Referensi kontrol ini menyediakan daftar AWS Security Hub kontrol yang tersedia dengan tautan ke informasi lebih lanjut tentang setiap kontrol. Tabel ikhtisar menampilkan kontrol dalam urutan abjad dengan ID kontrol. Hanya kontrol yang digunakan aktif oleh Security Hub yang disertakan di sini. Kontrol pensiun dikecualikan dari daftar ini. Tabel memberikan informasi berikut untuk setiap kontrol:

- ID kontrol keamanan — ID ini berlaku di seluruh standar dan menunjukkan Layanan AWS dan sumber daya yang terkait dengan kontrol. Konsol Security Hub menampilkan ID kontrol keamanan, terlepas dari apakah temuan kontrol konsolidasi diaktifkan atau dinonaktifkan di akun Anda. Namun, temuan Security Hub mereferensikan ID kontrol keamanan hanya jika temuan kontrol konsolidasi diaktifkan di akun Anda. Jika temuan kontrol konsolidasi dimatikan di akun Anda, beberapa ID kontrol bervariasi menurut standar dalam temuan kontrol Anda. Untuk pemetaan ID kontrol khusus standar ke ID kontrol keamanan, lihat. Bagaimana konsolidasi memengaruhi ID dan judul kontrol

  Jika Anda ingin mengatur otomatisasi untuk kontrol keamanan, sebaiknya filter berdasarkan ID kontrol daripada judul atau deskripsi. Sementara Security Hub kadang-kadang dapat memperbarui judul atau deskripsi kontrol, ID kontrol tetap sama.

  ID kontrol dapat melewati angka. Ini adalah placeholder untuk kontrol masa depan.
- Standar yang berlaku - Menunjukkan standar mana yang berlaku untuk kontrol. Pilih kontrol untuk melihat persyaratan spesifik dari kerangka kerja kepatuhan pihak ketiga.
- Judul kontrol keamanan - Judul ini berlaku di seluruh standar. Konsol Security Hub menampilkan judul kontrol keamanan, terlepas dari apakah temuan kontrol konsolidasi diaktifkan atau dinonaktifkan di akun Anda. Namun, temuan Security Hub merujuk judul kontrol keamanan hanya jika temuan kontrol konsolidasi diaktifkan di akun Anda. Jika temuan kontrol konsolidasi dimatikan di akun Anda, beberapa judul kontrol bervariasi menurut standar dalam temuan kontrol Anda.

Untuk pemetaan ID kontrol khusus standar ke ID kontrol keamanan, lihat. Bagaimana konsolidasi memengaruhi ID dan judul kontrol

- Keparahan — Tingkat keparahan kontrol mengidentifikasi pentingnya dari sudut pandang keamanan. Untuk informasi tentang cara Security Hub menentukan tingkat keparahan kontrol, lihatMenetapkan tingkat keparahan untuk mengontrol temuan.
- Jenis jadwal - Menunjukkan kapan kontrol dievaluasi. Untuk informasi selengkapnya, lihat Jadwal untuk menjalankan pemeriksaan keamanan.
- Mendukung parameter kustom - Menunjukkan apakah kontrol mendukung nilai kustom untuk satu atau beberapa parameter. Pilih kontrol untuk melihat detail parameter. Untuk informasi selengkapnya, lihat Parameter kontrol khusus.

Pilih kontrol untuk melihat detail lebih lanjut. Kontrol tercantum dalam urutan abjad dari nama layanan.

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
Akun.1	Informasi kontak keamanan harus disediakan untuk Akun AWS	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	Tidak	Berkala
Akun.2	Akun AWS harus menjadi bagian dari sebuah AWS Organizations organisasi	NIST SP 800-53 Wahyu 5	TINGGI	Tidak	Berkala
ACM.1	Sertifikat yang diimpor dan diterbitkan ACM harus diperbarui	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan:	MEDIUM	Ya	Perubahan dipicu dan periodik

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
	setelah jangka waktu tertentu	AWS Control Tower, NIST SP 800-53 Rev. 5			
ACM.2	Sertifikat RSA yang dikelola oleh ACM harus menggunakan panjang kunci minimal 2.048 bit	AWS Praktik Terbaik Keamanan Dasar v1.0.0	TINGGI	 Tidak	Perubahan dipicu
ACM.3	Sertifikat ACM harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
ApiGateway.1	API Gateway REST dan pencatatan eksekusi WebSocket API harus diaktifkan	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Ya	Perubahan dipicu
ApiGateway.2	Tahapan API Gateway REST API harus dikonfigurasi untuk menggunakan sertifikat SSL untuk otentikasi backend	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
ApiGateway.3	Tahapan API Gateway REST API harus mengaktifkan AWS X-Ray penelusuran	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	RENDAH	 Tidak	Perubahan dipicu
ApiGateway.4	API Gateway harus dikaitkan dengan WAF Web ACL	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
ApiGateway.5	Data cache API Gateway REST API harus dienkripsi saat istirahat	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
ApiGateway.8	Rute API Gateway harus menentukan jenis otorisasi	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Ya	Berkala

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
ApiGateway.9	Pencatatan akses harus dikonfigurasi untuk Tahap API Gateway V2	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
AppSync.2	AWS AppSync harus mengaktifkan logging tingkat lapangan	AWS Praktik Terbaik Keamanan Dasar v1.0.0	MEDIUM	 Ya	Perubahan dipicu
AppSync.4	AWS AppSync GraphQL API harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
AppSync.5	AWS AppSync GraphQL API tidak boleh diautentikasi dengan kunci API	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	TINGGI	 Tidak	Perubahan dipicu
Athena.2	Katalog data Athena harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
Athena.3	Kelompok kerja Athena harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
AutoScaling.1	Grup Auto Scaling yang terkait dengan penyeimbang beban harus menggunakan pemeriksaan kesehatan ELB	AWS Praktik Terbaik Keamanan Dasar, Standar yang Dikelola Layanan:, PCI DSS v3.2.1 AWS Control Tower, NIST SP 800-53 Rev. 5	RENDAH	 Tidak	Perubahan dipicu
AutoScaling.2	Grup Auto Scaling Amazon EC2 harus mencakup beberapa Availability Zone	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Ya	Perubahan dipicu
AutoScaling.3	Konfigurasi peluncuran grup Auto Scaling harus mengonfigurasi instans EC2 agar memerlukan Layanan Metadata Instans Versi 2 (IMDSv2)	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	TINGGI	 Tidak	Perubahan dipicu
Penskalaan otomatis.5	Instans Amazon EC2 yang diluncurkan menggunakan konfigurasi peluncuran grup Auto Scaling seharusnya tidak memiliki alamat IP Publik	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	TINGGI	 Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
AutoScaling.6	Grup Auto Scaling harus menggunakan beberapa jenis instance di beberapa Availability Zone	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
AutoScaling.9	Grup EC2 Auto Scaling harus menggunakan templat peluncuran EC2	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
AutoScaling.10	Grup EC2 Auto Scaling harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
Backup.1	AWS Backup titik pemulihan harus dienkripsi saat istirahat	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
Backup.2	AWS Backup poin pemulihan harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
Cadangan.3	AWS Backup brankas harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
Cadangan.4	AWS Backup rencana laporan harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
Cadangan.5	AWS Backup rencana cadangan harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
CloudFormation.2	CloudFormation tumpukan harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
CloudFront.1	CloudFront distribusi harus memiliki objek root default yang dikonfigurasi	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	TINGGI	 Tidak	Perubahan dipicu
CloudFront.3	CloudFront distribusi harus memerlukan enkripsi dalam perjalanan	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
CloudFront.4	CloudFront distribusi harus memiliki failover asal yang dikonfigurasi	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	RENDAH	 Tidak	Perubahan dipicu
CloudFront.5	CloudFront distribusi harus mengaktifkan logging	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
CloudFront.6	CloudFront distribusi harus mengaktifkan WAF	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	MEDIUM	Tidak	Perubahan dipicu
CloudFront.7	CloudFront distribusi harus menggunakan sertifikat SSL/TLS khusus	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	MEDIUM	Tidak	Perubahan dipicu
CloudFront.8	CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	RENDAH	Tidak	Perubahan dipicu
CloudFront.9	CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	MEDIUM	Tidak	Perubahan dipicu
CloudFront.10	CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal kustom	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	MEDIUM	Tidak	Perubahan dipicu
CloudFront.12	CloudFront distribusi seharusnya tidak menunjukkan asal S3 yang tidak ada	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	TINGGI	Tidak	Berkala

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
CloudFront.13	CloudFront distribusi harus menggunakan kontrol akses asal	AWS Praktik Terbaik Keamanan Dasar v1.0.0	MEDIUM	 Tidak	Perubahan dipicu
CloudFront.14	CloudFront Distribusi harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
CloudTrail.1	CloudTrail harus diaktifkan dan dikonfigurasi dengan setidaknya satu jejak Multi-wilayah yang mencakup acara manajemen baca dan tulis	Tolok Ukur AWS Yayasan CIS v1.2.0, Tolok Ukur AWS Yayasan CIS v1.4.0, Praktik Terbaik Keamanan AWS Dasar v1.0.0, Standar yang Dikelola Layanan:, NIST SP 800-53 Rev. 5 AWS Control Tower	TINGGI	 Tidak	Berkala
CloudTrail.2	CloudTrail harus mengaktifkan enkripsi saat istirahat	Tolok Ukur AWS Yayasan CIS v1.2.0, Praktik Terbaik Keamanan AWS Dasar v1.0.0, Standar yang Dikelola Layanan:, PCI DSS v3.2.1, Tolok Ukur Yayasan CIS AWS Control Tower v1.4.0, NIST SP 800-53 Rev. 5 AWS	MEDIUM	 Tidak	Berkala

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
CloudTrail.3	Setidaknya satu CloudTrail jejak harus diaktifkan	PCI DSS v3.2.1	TINGGI	 Tidak	Berkala
CloudTrail.4	CloudTrail validasi file log harus diaktifkan	Tolok Ukur AWS Yayasan CIS v1.2.0, Praktik Terbaik Keamanan AWS Dasar v1.0.0, Standar yang Dikelola Layanan:, PCI DSS v3.2.1, Tolok Ukur Yayasan CIS AWS Control Tower v1.4.0, NIST SP 800-53 Rev. 5 AWS	RENDAH	 Tidak	Berkala
CloudTrail.5	CloudTrail jalur harus diintegrasikan dengan Amazon Logs CloudWatch	Tolok Ukur AWS Yayasan CIS v1.2.0, Praktik Terbaik Keamanan AWS Dasar v1.0.0, Standar yang Dikelola Layanan:, PCI DSS v3.2.1, Tolok Ukur Yayasan CIS AWS Control Tower v1.4.0, NIST SP 800-53 Rev. 5 AWS	RENDAH	 Tidak	Berkala

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
CloudTrail.6	Pastikan bucket S3 yang digunakan untuk menyimpan CloudTrail log tidak dapat diakses publik	Tolok Ukur AWS Yayasan CIS v1.2.0, Tolok Ukur Yayasan CIS AWS v1.4.0	KRITIS	 Tidak	Perubahan dipicu dan periodik
CloudTrail.7	Pastikan pencatatan akses bucket S3 diaktifkan pada bucket CloudTrail S3	Tolok Ukur AWS Yayasan CIS v1.2.0, Tolok Ukur Yayasan CIS AWS v1.4.0	RENDAH	 Tidak	Berkala
CloudTrail.9	CloudTrail jalan setapak harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
CloudWatch.1	Filter metrik log dan alarm harus ada untuk penggunaan pengguna “root”	Tolok Ukur AWS Yayasan CIS v1.2.0, PCI DSS v3.2.1, Tolok Ukur Yayasan CIS v1.4.0 AWS	RENDAH	 Tidak	Berkala
CloudWatch.2	Pastikan filter metrik log dan alarm ada untuk panggilan API yang tidak sah	Tolok Ukur AWS Yayasan CIS v1.2.0	RENDAH	 Tidak	Berkala
CloudWatch.3	Pastikan ada filter metrik log dan alarm untuk login Management Console tanpa MFA	Tolok Ukur AWS Yayasan CIS v1.2.0	RENDAH	 Tidak	Berkala

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
CloudWatch.4	Pastikan filter metrik log dan alarm ada untuk perubahan kebijakan IAM	Tolok Ukur AWS Yayasan CIS v1.2.0, Tolok Ukur Yayasan CIS AWS v1.4.0	RENDAH	 Tidak	Berkala
CloudWatch.5	Pastikan filter metrik log dan alarm ada untuk perubahan CloudTrail konfigurasi	Tolok Ukur AWS Yayasan CIS v1.2.0, Tolok Ukur Yayasan CIS AWS v1.4.0	RENDAH	 Tidak	Berkala
CloudWatch.6	Pastikan filter metrik log dan alarm ada untuk kegagalan AWS Management Console otentikasi	Tolok Ukur AWS Yayasan CIS v1.2.0, Tolok Ukur Yayasan CIS AWS v1.4.0	RENDAH	 Tidak	Berkala
CloudWatch.7	Pastikan filter metrik log dan alarm ada untuk menonaktifkan atau menjadwalkan penghapusan CMK yang dibuat pelanggan	Tolok Ukur AWS Yayasan CIS v1.2.0, Tolok Ukur Yayasan CIS AWS v1.4.0	RENDAH	 Tidak	Berkala
CloudWatch.8	Pastikan filter metrik log dan alarm ada untuk perubahan kebijakan bucket S3	Tolok Ukur AWS Yayasan CIS v1.2.0, Tolok Ukur Yayasan CIS AWS v1.4.0	RENDAH	 Tidak	Berkala

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
CloudWatch.9	Pastikan filter metrik log dan alarm ada untuk perubahan AWS Config konfigurasi	Tolok Ukur AWS Yayasan CIS v1.2.0, Tolok Ukur Yayasan CIS AWS v1.4.0	RENDAH	 Tidak	Berkala
CloudWatch.10	Pastikan filter metrik log dan alarm ada untuk perubahan grup keamanan	Tolok Ukur AWS Yayasan CIS v1.2.0, Tolok Ukur Yayasan CIS AWS v1.4.0	RENDAH	 Tidak	Berkala
CloudWatch.11	Pastikan filter metrik log dan alarm ada untuk perubahan pada Daftar Kontrol Akses Jaringan (NACL)	Tolok Ukur AWS Yayasan CIS v1.2.0, Tolok Ukur Yayasan CIS AWS v1.4.0	RENDAH	 Tidak	Berkala
CloudWatch.12	Pastikan filter metrik log dan alarm ada untuk perubahan gateway jaringan	Tolok Ukur AWS Yayasan CIS v1.2.0, Tolok Ukur Yayasan CIS AWS v1.4.0	RENDAH	 Tidak	Berkala
CloudWatch.13	Pastikan filter metrik log dan alarm ada untuk perubahan tabel rute	Tolok Ukur AWS Yayasan CIS v1.2.0, Tolok Ukur Yayasan CIS AWS v1.4.0	RENDAH	 Tidak	Berkala
CloudWatch.14	Pastikan filter metrik log dan alarm ada untuk perubahan VPC	Tolok Ukur AWS Yayasan CIS v1.2.0, Tolok Ukur Yayasan CIS AWS v1.4.0	RENDAH	 Tidak	Berkala

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
CloudWatch.15	CloudWatch alarm harus memiliki tindakan tertentu yang dikonfigurasi	NIST SP 800-53 Wahyu 5	TINGGI	 Ya	Perubahan dipicu
CloudWatch.16	CloudWatch grup log harus dipertahankan untuk jangka waktu tertentu	NIST SP 800-53 Wahyu 5	MEDIUM	 Ya	Berkala
CloudWatch.17	CloudWatch tindakan alarm harus diaktifkan	NIST SP 800-53 Wahyu 5	TINGGI	 Tidak	Perubahan dipicu
CodeArtifact.1	CodeArtifact repositori harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
CodeBuild.1	CodeBuild URL repositori sumber Bitbucket tidak boleh berisi kredensyal sensitif	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan:, PCI DSS v3.2.1 AWS Control Tower, NIST SP 800-53 Rev. 5	KRITIS	 Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
CodeBuild.2	CodeBuild variabel lingkungan proyek tidak boleh berisi kredensyal teks yang jelas	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan:, PCI DSS v3.2.1 AWS Control Tower, NIST SP 800-53 Rev. 5	KRITIS	 Tidak	Perubahan dipicu
CodeBuild.3	CodeBuild Log S3 harus dienkripsi	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	RENDAH	 Tidak	Perubahan dipicu
CodeBuild.4	CodeBuild lingkungan proyek harus memiliki konfigurasi logging	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
Konfigurasi.1	AWS Config harus diaktifkan dan menggunakan peran terkait layanan untuk perekaman sumber daya	Tolok Ukur AWS Yayasan CIS v1.4.0, Tolok Ukur AWS Yayasan CIS v1.2.0, Praktik Terbaik Keamanan AWS Dasar, NIST SP 800-53 Rev. 5, PCI DSS v3.2.1	MEDIUM	 Tidak	Berkala

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
DataFirehose.1	Aliran pengiriman Firehose harus dienkripsi saat istirahat	AWS Praktik Terbaik Keamanan Dasar NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Berkala
Detektif.1	Grafik perilaku Detektif harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
DMS.1	Contoh replikasi Database Migration Service tidak boleh bersifat publik	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan:, PCI DSS v3.2.1 AWS Control Tower, NIST SP 800-53 Rev. 5	KRITIS	 Tidak	Berkala
DMS.2	Sertifikat DMS harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
DMS.3	Langganan acara DMS harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
DMS.4	Instans replikasi DMS harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
DMS.5	Grup subnet replikasi DMS harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
DMS.6	Instans replikasi DMS harus mengaktifkan peningkatan versi minor otomatis	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
DMS.7	Tugas replikasi DMS untuk database target harus mengaktifkan logging	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
DMS.8	Tugas replikasi DMS untuk database sumber harus mengaktifkan logging	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
DMS.9	Titik akhir DMS harus menggunakan SSL	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
DMS.10	Titik akhir DMS untuk database Neptunus harus mengaktifkan otorisasi IAM	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
DMS.11	Titik akhir DMS untuk MongoDB harus mengaktifkan mekanisme otentikasi	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
DMS.12	Titik akhir DMS untuk Redis harus mengaktifkan TLS	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5	MEDIUM	Tidak	Perubahan dipicu
DokumenD.1	Cluster Amazon DocumentDB harus dienkripsi saat istirahat	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5, Standar yang Dikelola Layanan: AWS Control Tower	MEDIUM	Tidak	Perubahan dipicu
DokumenD.2	Cluster Amazon DocumentDB harus memiliki periode retensi cadangan yang memadai	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5, Standar yang Dikelola Layanan: AWS Control Tower	MEDIUM	Ya	Perubahan dipicu
DokumenD.3	Cuplikan cluster manual Amazon DocumentDB seharusnya tidak bersifat publik	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	KRITIS	Tidak	Perubahan dipicu
DokumenD.4	Cluster Amazon DocumentDB harus mempublikasikan log audit ke Log CloudWatch	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	MEDIUM	Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
DokumenDB.5	Cluster Amazon DocumentDB harus mengaktifkan perlindungan penghapusan	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
DynamoDB.1	Tabel DynamoDB harus secara otomatis menskalakan kapasitas dengan permintaan	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Ya	Berkala
DynamoDB.2	Tabel DynamoDB harus mengaktifkan pemulihan point-in-time	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
DynamoDB.3	Cluster DynamoDB Accelerator (DAX) harus dienkripsi saat istirahat	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Berkala
DynamoDB.4	Tabel DynamoDB harus ada dalam rencana cadangan	NIST SP 800-53 Wahyu 5	MEDIUM	 Ya	Berkala

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
DynamoDb 5	Tabel DynamoDB harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
DynamoDb 6	Tabel DynamoDB harus mengaktif kan perlindungan penghapusan	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
DynamoDb 7	Cluster DynamoDB Accelerator harus dienkripsi saat transit	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Berkala
EC2.1	Snapshot EBS tidak boleh dipulihkan secara publik	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan:, PCI DSS v3.2.1 AWS Control Tower, NIST SP 800-53 Rev. 5	KRITIS	 Tidak	Berkala

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
EC2.2	Grup keamanan default VPC tidak boleh mengizinkan lalu lintas masuk atau keluar	Tolok Ukur AWS Yayasan CIS v1.2.0, Praktik Terbaik Keamanan AWS Dasar v1.0.0, Standar yang Dikelola Layanan:, PCI DSS v3.2.1, Tolok Ukur Yayasan CIS AWS Control Tower v1.4.0, NIST SP 800-53 Rev. 5 AWS	TINGGI	 Tidak	Perubahan dipicu
EC2.3	Volume EBS yang terpasang harus dienkripsi saat istirahat	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
EC2.4	Instans EC2 yang dihentikan harus dihapus setelah periode waktu tertentu	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Ya	Berkala

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
EC2.6	Pencatatan aliran VPC harus diaktifkan di semua VPC	Tolok Ukur AWS Yayasan CIS v1.2.0, Praktik Terbaik Keamanan AWS Dasar v1.0.0, Standar yang Dikelola Layanan:, PCI DSS v3.2.1, Tolok Ukur Yayasan CIS AWS Control Tower v1.4.0, NIST SP 800-53 Rev. 5 AWS	MEDIUM	 Tidak	Berkala
EC2.7	Enkripsi default EBS harus diaktifkan	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan:, Tolok Ukur AWS Yayasan CIS v1.4.0 AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Berkala
EC2.8	Instans EC2 harus menggunakan Layanan Metadata Instans Versi 2 (IMDSv2)	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	TINGGI	 Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
EC2.9	Instans EC2 seharusnya tidak memiliki alamat IPv4 publik	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	TINGGI	 Tidak	Perubahan dipicu
EC2.10	Amazon EC2 harus dikonfigurasi untuk menggunakan titik akhir VPC yang dibuat untuk layanan Amazon EC2	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Berkala
EC2.12	EIP EC2 yang tidak digunakan harus dihapus	PCI DSS v3.2.1, NIST SP 800-53 Wahyu 5	RENDAH	 Tidak	Perubahan dipicu
EC2.13	Grup keamanan tidak boleh mengizinkan masuknya dari 0.0.0.0/0 atau: :/0 ke port 22	Tolok Ukur AWS Yayasan CIS v1.2.0, PCI DSS v3.2.1, NIST SP 800-53 Rev. 5	TINGGI	 Tidak	Perubahan dipicu
EC2.14	Grup keamanan tidak boleh mengizinkan masuknya dari 0.0.0.0/0 atau: :/0 ke port 3389	Tolok Ukur AWS Yayasan CIS v1.2.0	TINGGI	 Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
EC2.15	Subnet EC2 seharusnya tidak secara otomatis menetapkan alamat IP publik	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
EC2.16	Daftar Kontrol Akses Jaringan yang Tidak Digunakan harus dihapus	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	RENDAH	 Tidak	Perubahan dipicu
EC2.17	Instans EC2 tidak boleh menggunakan beberapa ENI	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	RENDAH	 Tidak	Perubahan dipicu
EC2.18	Grup keamanan hanya boleh mengizinkan lalu lintas masuk yang tidak terbatas untuk port resmi	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	TINGGI	 Ya	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
EC2.19	Kelompok keamanan tidak boleh mengizinkan akses tidak terbatas ke port dengan risiko tinggi	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	KRITIS	 Tidak	Perubahan dipicu
EC2.20	Kedua terowongan VPN untuk koneksi VPN AWS Site-to-Site harus aktif	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
EC2.21	ACL jaringan seharusnya tidak mengizinkan masuknya dari 0.0.0.0/0 ke port 22 atau port 3389	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan:, Tolok Ukur AWS Yayasan CIS v1.4.0 AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
EC2.22	Grup keamanan EC2 yang tidak digunakan harus dihapus	Standar yang Dikelola Layanan: AWS Control Tower	MEDIUM	 Tidak	Berkala

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
EC2.23	EC2 Transit Gateways seharusnya tidak secara otomatis menerima permintaan lampiran VPC	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	TINGGI	 Tidak	Perubahan dipicu
EC2.24	Jenis instance paravirtual EC2 tidak boleh digunakan	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
EC2.25	Template peluncura n EC2 tidak boleh menetapkan IP publik ke antarmuka jaringan	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	TINGGI	 Tidak	Perubahan dipicu
EC2.28	Volume EBS harus dalam rencana cadangan	NIST SP 800-53 Wahyu 5	RENDAH	 Ya	Berkala
EC2.33	Lampiran gateway transit EC2 harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
EC2.34	Tabel rute gateway transit EC2 harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
EC2.35	Antarmuka jaringan EC2 harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
EC2.36	Gateway pelanggan EC2 harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
EC2.37	Alamat IP Elastis EC2 harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
EC2.38	Instans EC2 harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
EC2.39	Gerbang internet EC2 harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
EC2.40	Gerbang EC2 NAT harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
EC2.41	ACL jaringan EC2 harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
EC2.42	Tabel rute EC2 harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
EC2.43	Grup keamanan EC2 harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
EC2.44	Subnet EC2 harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
EC2.45	Volume EC2 harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
EC2.46	Amazon VPC harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
EC2.47	Layanan endpoint Amazon VPC harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
EC2.48	Log aliran VPC Amazon harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
EC2.49	Koneksi peering VPC Amazon harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
EC2.50	Gateway EC2 VPN harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
EC2.51	Titik akhir EC2 Client VPN harus mengaktif kan logging koneksi klien	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	RENDAH	 Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
EC2.52	Gerbang transit EC2 harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
EC2.53	Grup keamanan EC2 tidak boleh mengizinkan masuknya dari 0.0.0.0/0 ke port administrasi server jarak jauh	Tolok Ukur AWS Yayasan CIS v3.0.0	TINGGI	 Tidak	Berkala
EC2.54	Grup keamanan EC2 tidak boleh mengizinkan masuknya dari: :/0 ke port administrasi server jarak jauh	Tolok Ukur AWS Yayasan CIS v3.0.0	TINGGI	 Tidak	Berkala
ECR.1	Repositori pribadi ECR harus memiliki pemindaian gambar yang dikonfigurasi	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	TINGGI	 Tidak	Berkala
ECR.2	Repositori pribadi ECR harus memiliki kekekalan tag yang dikonfigurasi	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
ECR.3	Repositori ECR harus memiliki setidaknya satu kebijakan siklus hidup yang dikonfigurasi	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
ECR.4	Repositori publik ECR harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
ECS.1	Definisi tugas Amazon ECS harus memiliki mode jaringan yang aman dan definisi pengguna.	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	TINGGI	 Tidak	Perubahan dipicu
ECS.2	Layanan ECS seharusnya tidak memiliki alamat IP publik yang ditetapkan kepadanya secara otomatis	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	TINGGI	 Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
ECS.3	Definisi tugas ECS tidak boleh berbagi namespace proses host	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	TINGGI	 Tidak	Perubahan dipicu
ECS.4	Kontainer ECS harus berjalan sebagai non-hak istimewa	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	TINGGI	 Tidak	Perubahan dipicu
ECS.5	Kontainer ECS harus dibatasi pada akses hanya-baca ke sistem file root	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	TINGGI	 Tidak	Perubahan dipicu
ECS.8	Rahasia tidak boleh diteruskan sebagai variabel lingkungan kontainer	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	TINGGI	 Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
ECS.9	Definisi tugas ECS harus memiliki konfigurasi logging	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	TINGGI	 Tidak	Perubahan dipicu
ECS.10	Layanan ECS Fargate harus berjalan pada versi platform Fargate terbaru	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
ECS.12	Cluster ECS harus menggunakan Wawasan Kontainer	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
ECS.13	Layanan ECS harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
ECS.14	Cluster ECS harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
ECS.15	Definisi tugas ECS harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
EFS.1	Sistem File Elastis harus dikonfigurasi untuk mengenkripsi data file saat istirahat menggunakan AWS KMS	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Berkala
EFS.2	Volume Amazon EFS harus ada dalam paket cadangan	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Berkala
EFS.3	Titik akses EFS harus menerapkan direktori root	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
EFS.4	Titik akses EFS harus menegakkan identitas pengguna	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
EFS.5	Titik akses EFS harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
EFS.6	Target pemasangan EFS tidak boleh dikaitkan dengan subnet publik	AWS Praktik Terbaik Keamanan Dasar	MEDIUM	 Tidak	Berkala
EKS.1	Titik akhir kluster EKS tidak boleh diakses publik	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	TINGGI	 Tidak	Berkala
EKS.2	Kluster EKS harus berjalan pada versi Kubernetes yang didukung	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	TINGGI	 Tidak	Perubahan dipicu
EKS.3	Kluster EKS harus menggunakan rahasia Kubernetes terenkripsi	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Berkala
EKS.6	Kluster EKS harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
EKS.7	Konfigurasi penyedia identitas EKS harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
EKS.8	Kluster EKS harus mengaktifkan pencatatan audit	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Berkala
ElastiCache.1	ElastiCache Cluster Redis harus mengaktifkan pencadangan otomatis	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	TINGGI	 Ya	Berkala
ElastiCache.2	ElastiCache untuk kluster cache Redis harus mengaktifkan peningkatan versi minor otomatis	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	TINGGI	 Tidak	Berkala
ElastiCache.3	ElastiCache grup replikasi harus mengaktifkan failover otomatis	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Berkala
ElastiCache.4	ElastiCache grup replikasi seharusnya diaktifkan encryption-at-rest	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Berkala

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
ElastiCache.5	ElastiCache grup replikasi seharusnya diaktifkan encryption-in-transit	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Berkala
ElastiCache.6	ElastiCache grup replikasi versi Redis sebelumnya harus mengaktifkan Redis AUTH	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Berkala
ElastiCache.7	ElastiCache cluster tidak boleh menggunakan grup subnet default	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	TINGGI	 Tidak	Berkala
ElasticBeanstalk.1	Lingkungan Elastic Beanstalk seharusnya mengaktifkan pelaporan kesehatan yang ditingkatkan	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	RENDAH	 Tidak	Perubahan dipicu
ElasticBeanstalk.2	Pembaruan platform yang dikelola Elastic Beanstalk harus diaktifkan	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	TINGGI	 Ya	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
ElasticBeanstalk.3	Elastic Beanstalk harus mengalirkan log ke CloudWatch	AWS Praktik Terbaik Keamanan Dasar v1.0.0	TINGGI	 Ya	Perubahan dipicu
ELB.1	Application Load Balancer harus dikonfigurasi untuk mengalihkan semua permintaan HTTP ke HTTPS	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan:, PCI DSS v3.2.1 AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Berkala
ELB.2	Classic Load Balancer dengan pendengar SSL/HTTPS harus menggunakan sertifikat yang disediakan oleh AWS Certificate Manager	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
ELB.3	Pendengar Classic Load Balancer harus dikonfigurasi dengan penghentian HTTPS atau TLS	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
ELB.4	Application Load Balancer harus dikonfigurasi untuk menjatuhkan header http	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
ELB.5	Pencatatan aplikasi dan Classic Load Balancer harus diaktifkan	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
ELB.6	Aplikasi, Gateway, dan Network Load Balancer harus mengaktif kan perlindungan penghapusan	AWS Praktik Terbaik Keamanan Dasar, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
ELB.7	Classic Load Balancers harus mengaktifkan pengurasan koneksi	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
ELB.8	Classic Load Balancer dengan pendengar SSL harus menggunakan kebijakan keamanan yang telah ditentukan sebelumnya yang memiliki konfigurasi yang kuat	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
ELB.9	Penyeimbang Beban Klasik harus mengaktifkan penyeimbangan beban lintas zona	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
ELB.10	Classic Load Balancer harus menjangkau beberapa Availability Zone	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Ya	Perubahan dipicu
ELB.12	Application Load Balancer harus dikonfigurasi dengan mode mitigasi desync defensif atau paling ketat	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
ELB.13	Penyeimbang Beban Aplikasi, Jaringan, dan Gateway harus menjangkau beberapa Availability Zone	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Ya	Perubahan dipicu
ELB.14	Classic Load Balancer harus dikonfigurasi dengan mode mitigasi desync defensif atau paling ketat	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
ELB.16	Application Load Balancers harus dikaitkan dengan ACL web AWS WAF	NIST SP 800-53 Wahyu 5	MEDIUM	 Tidak	Perubahan dipicu
EMR.1	Node primer klaster EMR Amazon seharusnya tidak memiliki alamat IP publik	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	TINGGI	 Tidak	Berkala
EMR.2	Amazon EMR memblokir pengaturan akses publik harus diaktifkan	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	KRITIS	 Tidak	Berkala

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
ES.1	Domain Elasticsearch harus mengaktifkan enkripsi saat istirahat	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan:, PCI DSS v3.2.1 AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Berkala
ES.2	Domain Elasticsearch tidak boleh diakses publik	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan:, PCI DSS v3.2.1 AWS Control Tower, NIST SP 800-53 Rev. 5	KRITIS	 Tidak	Berkala
ES.3	Domain Elasticsearch harus mengenkripsi data yang dikirim antar node	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
ES.4	Kesalahan domain Elasticsearch yang masuk ke CloudWatch Log harus diaktifkan	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
ES.5	Domain Elasticsearch harus mengaktifkan pencatatan audit	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	Tidak	Perubahan dipicu
ES.6	Domain Elasticsearch harus memiliki setidaknya tiga node data	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	Tidak	Perubahan dipicu
ES.7	Domain Elasticsearch harus dikonfigurasi dengan setidakny a tiga node master khusus	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	Tidak	Perubahan dipicu
ES.8	Koneksi ke domain Elasticsearch harus dienkrips i menggunakan kebijakan keamanan TLS terbaru	AWS Praktik Terbaik Keamanan Dasar, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
ES.9	Domain Elasticsearch harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
EventBridge.2	EventBridge bus acara harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
EventBridge.3	EventBridge bus acara khusus harus memiliki kebijakan berbasis sumber daya terlampir	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	RENDAH	 Tidak	Perubahan dipicu
EventBridge.4	EventBridge titik akhir global harus mengaktifkan replikasi acara	NIST SP 800-53 Wahyu 5	MEDIUM	 Tidak	Perubahan dipicu
FSX.1	FSx untuk sistem file OpenZFS harus dikonfigurasi untuk menyalin tag ke backup dan volume	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	RENDAH	 Tidak	Perubahan dipicu
FSX.2	Sistem file FSx for Lustre harus dikonfigurasi untuk menyalin tag ke cadangan	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5	RENDAH	 Tidak	Perubahan dipicu
Lem. 1	AWS Glue pekerjaan harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
GlobalAccelerator.1	Akselerator Global Accelerator harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
GuardDuty.1	GuardDuty harus diaktifkan	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan:, PCI DSS v3.2.1 AWS Control Tower, NIST SP 800-53 Rev. 5	TINGGI	 Tidak	Berkala
GuardDuty.2	GuardDuty filter harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
GuardDuty.3	GuardDuty IPset harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
GuardDuty.4	GuardDuty detektor harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
IAM.1	Kebijakan IAM seharusnya tidak mengizinkan hak administratif “*” penuh	Tolok Ukur AWS Yayasan CIS v1.2.0, Praktik Terbaik Keamanan AWS Dasar v1.0.0, Standar yang Dikelola Layanan:, PCI DSS v3.2.1, Tolok Ukur Yayasan CIS AWS Control Tower v1.4.0, NIST SP 800-53 Rev. 5 AWS	TINGGI	 Tidak	Perubahan dipicu
IAM.2	Pengguna IAM seharusnya tidak memiliki kebijakan IAM yang dilampirkan	Tolok Ukur AWS Yayasan CIS v1.2.0, Praktik Terbaik Keamanan AWS Dasar v1.0.0, Standar yang Dikelola Layanan:, PCI DSS v3.2.1, NIST SP 800-53 AWS Control Tower Rev. 5	RENDAH	 Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
IAM.3	Kunci akses pengguna IAM harus diputar setiap 90 hari atau kurang	Tolok Ukur AWS Yayasan CIS v1.2.0, Praktik Terbaik Keamanan AWS Dasar v1.0.0, Standar yang Dikelola Layanan:, Tolok Ukur Yayasan CIS AWS v1.4.0, NIST SP AWS Control Tower 800-53 Rev. 5	MEDIUM	 Tidak	Berkala
IAM.4	Kunci akses pengguna root IAM seharusnya tidak ada	Tolok Ukur AWS Yayasan CIS v1.2.0, Praktik Terbaik Keamanan AWS Dasar v1.0.0, Standar yang Dikelola Layanan:, PCI DSS v3.2.1, Tolok Ukur Yayasan CIS AWS Control Tower v1.4.0, NIST SP 800-53 Rev. 5 AWS	KRITIS	 Tidak	Berkala

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
IAM.5	MFA harus diaktifkan untuk semua pengguna IAM yang memiliki kata sandi konsol	Tolok Ukur AWS Yayasan CIS v1.2.0, Praktik Terbaik Keamanan AWS Dasar v1.0.0, Standar yang Dikelola Layanan:, Tolok Ukur Yayasan CIS AWS v1.4.0, NIST SP AWS Control Tower 800-53 Rev. 5	MEDIUM	 Tidak	Berkala
IAM.6	MFA perangkat keras harus diaktifkan untuk pengguna root	Tolok Ukur AWS Yayasan CIS v1.2.0, Praktik Terbaik Keamanan AWS Dasar v1.0.0, Standar yang Dikelola Layanan:, PCI DSS v3.2.1, Tolok Ukur Yayasan CIS AWS Control Tower v1.4.0, NIST SP 800-53 Rev. 5 AWS	KRITIS	 Tidak	Berkala
IAM.7	Kebijakan kata sandi untuk pengguna IAM harus memiliki konfigurasi yang kuat	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Ya	Berkala

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
IAM.8	Kredensyal pengguna IAM yang tidak digunakan harus dihapus	Tolok Ukur AWS Yayasan CIS v1.2.0, Praktik Terbaik Keamanan AWS Dasar v1.0.0, Standar yang Dikelola Layanan:, PCI DSS v3.2.1, NIST SP 800-53 AWS Control Tower Rev. 5	MEDIUM	 Tidak	Berkala
IAM.9	MFA harus diaktifkan untuk pengguna root	Tolok Ukur AWS Yayasan CIS v1.2.0, PCI DSS v3.2.1, Tolok Ukur AWS Yayasan CIS v1.4.0, NIST SP 800-53 Rev. 5	KRITIS	 Tidak	Berkala
IAM.10	Kebijakan kata sandi untuk pengguna IAM harus memiliki konfigurasi yang kuat	PCI DSS v3.2.1	MEDIUM	 Tidak	Berkala
IAM.11	Pastikan kebijakan kata sandi IAM memerlukan setidaknya satu huruf besar	Tolok Ukur AWS Yayasan CIS v1.2.0	MEDIUM	 Tidak	Berkala

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
IAM.12	Pastikan kebijakan kata sandi IAM memerlukan setidaknya satu huruf kecil	Tolok Ukur AWS Yayasan CIS v1.2.0	MEDIUM	 Tidak	Berkala
IAM.13	Pastikan kebijakan kata sandi IAM memerlukan setidaknya satu simbol	Tolok Ukur AWS Yayasan CIS v1.2.0	MEDIUM	 Tidak	Berkala
IAM.14	Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu nomor	Tolok Ukur AWS Yayasan CIS v1.2.0	MEDIUM	 Tidak	Berkala
IAM.15	Pastikan kebijakan kata sandi IAM memerlukan panjang kata sandi minimum 14 atau lebih	Tolok Ukur AWS Yayasan CIS v1.2.0, Tolok Ukur Yayasan CIS AWS v1.4.0	MEDIUM	 Tidak	Berkala
IAM.16	Pastikan kebijakan kata sandi IAM mencegah penggunaan kembali kata sandi	Tolok Ukur AWS Yayasan CIS v1.2.0, Tolok Ukur Yayasan CIS AWS v1.4.0	RENDAH	 Tidak	Berkala

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
IAM.17	Pastikan kebijakan kata sandi IAM kedaluwarsa kata sandi dalam waktu 90 hari atau kurang	Tolok Ukur AWS Yayasan CIS v1.2.0	RENDAH	 Tidak	Berkala
IAM.18	Pastikan peran dukungan telah dibuat untuk mengelola insiden dengan AWS Support	Tolok Ukur AWS Yayasan CIS v1.2.0, Tolok Ukur Yayasan CIS AWS v1.4.0	RENDAH	 Tidak	Berkala
IAM.19	MFA harus diaktifkan untuk semua pengguna IAM	PCI DSS v3.2.1, NIST SP 800-53 Wahyu 5	MEDIUM	 Tidak	Berkala
IAM.21	Kebijakan terkelola pelanggan IAM yang Anda buat tidak boleh mengizinkan tindakan wildcard untuk layanan	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	RENDAH	 Tidak	Perubahan dipicu
IAM.22	Kredensyal pengguna IAM yang tidak digunakan selama 45 hari harus dihapus	Tolok Ukur AWS Yayasan CIS v1.4.0	MEDIUM	 Tidak	Berkala

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
IAM.23	Alat analisis IAM Access Analyzer harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
IAM.24	Peran IAM harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
IAM.25	Pengguna IAM harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	 Ya	Perubahan dipicu
IAM.26	Sertifikat SSL/TLS yang kedaluwarsa yang dikelola di IAM harus dihapus	Tolok Ukur AWS Yayasan CIS v3.0.0	MEDIUM	 Tidak	Berkala
IAM.27	Identitas IAM seharusnya tidak memiliki kebijakan yang dilampirkan AWSCloudShellFullAccess	Tolok Ukur AWS Yayasan CIS v3.0.0	MEDIUM	 Tidak	Perubahan dipicu
IAM.28	IAM Access Analyzer penganalisis akses eksternal harus diaktifkan	Tolok Ukur AWS Yayasan CIS v3.0.0	TINGGI	 Tidak	Berkala

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
IoT.1	AWS IoT Core profil keamanan harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
IoT.2	AWS IoT Core tindakan mitigasi harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
IoT.3	AWS IoT Core dimensi harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
IoT.4	AWS IoT Core pemberi otorisasi harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
IoT.5	AWS IoT Core alias peran harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
IoT.6	AWS IoT Core kebijakan harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
Kinesis.1	Aliran Kinesis harus dienkripsi saat istirahat	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
Kinesis.2	Aliran Kinesis harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
KMS.1	Kebijakan yang dikelola pelanggan IAM tidak boleh mengizinkan tindakan dekripsi pada semua kunci KMS	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
KMS.2	Prinsipal IAM seharusnya tidak memiliki kebijakan inline IAM yang memungkinkan tindakan dekripsi pada semua kunci KMS	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
KMS.3	AWS KMS keys tidak boleh dihapus secara tidak sengaja	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	KRITIS	 Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
KMS.4	AWS KMS key rotasi harus diaktifkan	Tolok Ukur AWS Yayasan CIS v1.2.0, PCI DSS v3.2.1, Tolok Ukur AWS Yayasan CIS v1.4.0, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Berkala
Lambda.1	Kebijakan fungsi Lambda harus melarang akses publik	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan:, PCI DSS v3.2.1 AWS Control Tower, NIST SP 800-53 Rev. 5	KRITIS	 Tidak	Perubahan dipicu
Lambda.2	Fungsi Lambda harus menggunakan runtime yang didukung	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
Lambda.3	Fungsi Lambda harus dalam VPC	PCI DSS v3.2.1, NIST SP 800-53 Wahyu 5	RENDAH	 Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
Lambda.5	Fungsi VPC Lambda harus beroperasi di beberapa Availability Zone	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Ya	Perubahan dipicu
Lambda.6	Fungsi Lambda harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
Macie.1	Amazon Macie harus diaktifkan	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Berkala
Macie.2	Penemuan data sensitif otomatis Macie harus diaktifkan	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	TINGGI	 Tidak	Berkala
MSK.1	Cluster MSK harus dienkripsi dalam perjalanan di antara node broker	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
MSK.2	Cluster MSK harus memiliki pemantauan yang ditingkatkan yang dikonfigurasi	NIST SP 800-53 Wahyu 5	RENDAH	 Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
MQ.2	Broker ActiveMQ harus mengalirkan log audit ke CloudWatch	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
MQ.3	Broker Amazon MQ harus mengaktifkan peningkatan versi minor otomatis	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5	RENDAH	 Tidak	Perubahan dipicu
MQ.4	Broker Amazon MQ harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
MQ.5	Broker ActiveMQ harus menggunakan mode penerapan aktif/siaga	NIST SP 800-53 Rev. 5, Standar yang Dikelola Layanan: AWS Control Tower	RENDAH	 Tidak	Perubahan dipicu
MQ.6	Broker RabbitMQ harus menggunakan mode penerapan cluster	NIST SP 800-53 Rev. 5, Standar yang Dikelola Layanan: AWS Control Tower	RENDAH	 Tidak	Perubahan dipicu
Neptunus.1	Cluster DB Neptunus harus dienkripsi saat istirahat	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5, Standar yang Dikelola Layanan: AWS Control Tower	MEDIUM	 Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
Neptunus.2	Cluster DB Neptunus harus mempublikasikan log audit ke Log CloudWatch	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5, Standar yang Dikelola Layanan: AWS Control Tower	MEDIUM	 Tidak	Perubahan dipicu
Neptunus.3	Cuplikan cluster Neptunus DB seharusnya tidak bersifat publik	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5, Standar yang Dikelola Layanan: AWS Control Tower	KRITIS	 Tidak	Perubahan dipicu
Neptunus.4	Cluster DB Neptunus harus mengaktifkan perlindungan penghapusan	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5, Standar yang Dikelola Layanan: AWS Control Tower	RENDAH	 Tidak	Perubahan dipicu
Neptunus.5	Cluster DB Neptunus harus mengaktifkan cadangan otomatis	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5, Standar yang Dikelola Layanan: AWS Control Tower	MEDIUM	 Ya	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
Neptunus.6	Snapshot cluster Neptunus DB harus dienkripsi saat istirahat	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5, Standar yang Dikelola Layanan: AWS Control Tower	MEDIUM	 Tidak	Perubahan dipicu
Neptunus.7	Cluster DB Neptunus harus mengaktifkan otentikasi database IAM	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5, Standar yang Dikelola Layanan: AWS Control Tower	MEDIUM	 Tidak	Perubahan dipicu
Neptunus.8	Cluster DB Neptunus harus dikonfigurasi untuk menyalin tag ke snapshot	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5, Standar yang Dikelola Layanan: AWS Control Tower	RENDAH	 Tidak	Perubahan dipicu
Neptunus.9	Cluster DB Neptunus harus digunakan di beberapa Availability Zone	NIST SP 800-53 Wahyu 5	MEDIUM	 Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
NetworkFirewall.1	Firewall Network Firewall harus digunakan di beberapa Availability Zone	NIST SP 800-53 Wahyu 5	MEDIUM	 Tidak	Perubahan dipicu
NetworkFirewall.2	Pencatatan Network Firewall harus diaktifkan	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Berkala
NetworkFirewall.3	Kebijakan Network Firewall harus memiliki setidaknya satu kelompok aturan yang terkait	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
NetworkFirewall.4	Tindakan stateless default untuk kebijakan Network Firewall harus dijatuhkan atau diteruskan untuk paket lengkap	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
NetworkFirewall.5	Tindakan stateless default untuk kebijakan Network Firewall harus dijatuhkan atau diteruskan untuk paket yang terfragmentasi	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
NetworkFirewall.6	Grup aturan firewall jaringan stateless tidak boleh kosong	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
NetworkFirewall.7	Firewall Network Firewall harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
NetworkFirewall.8	Kebijakan firewall Network Firewall harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
NetworkFirewall.9	Firewall Network Firewall harus mengaktifkan perlindungan penghapusan	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
Opensearch.1	OpenSearch domain harus mengaktifkan enkripsi saat istirahat	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan:, PCI DSS v3.2.1 AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
Opensearch.2	OpenSearch Domain tidak boleh diakses publik	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan:, PCI DSS v3.2.1 AWS Control Tower, NIST SP 800-53 Rev. 5	KRITIS	 Tidak	Perubahan dipicu
Opensearch.3	OpenSearch domain harus mengenkripsi data yang dikirim antar node	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
Opensearch.4	OpenSearch kesalahan domain saat masuk ke CloudWatch Log harus diaktifkan	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
Opensearch.5	OpenSearch domain harus mengaktifkan pencatatan audit	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
Opensearch.6	OpenSearch domain harus memiliki setidaknya tiga node data	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
Opensearch.7	OpenSearch domain harus mengaktifkan kontrol akses berbutir halus	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	TINGGI	 Tidak	Perubahan dipicu
Opensearch.8	Koneksi ke OpenSearch domain harus dienkripsi menggunakan kebijakan keamanan TLS terbaru	AWS Praktik Terbaik Keamanan Dasar, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
Opensearch.9	OpenSearch domain harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
Opensearch.10	OpenSearch domain harus memiliki pembaruan perangkat lunak terbaru yang diinstal	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	RENDAH	 Tidak	Perubahan dipicu
Opensearch.11	OpenSearch domain harus memiliki setidaknya tiga node primer khusus	NIST SP 800-53 Wahyu 5	MEDIUM	 Tidak	Berkala
PCA.1	AWS Private CA otoritas sertifikat root harus dinonaktifkan	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	RENDAH	 Tidak	Berkala
RDS.1	Cuplikan RDS harus bersifat pribadi	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan:, PCI DSS v3.2.1 AWS Control Tower, NIST SP 800-53 Rev. 5	KRITIS	 Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
RDS.2	Instans RDS DB harus melarang akses publik, sebagaimana ditentukan oleh konfigurasi PubliclyAccessible	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan:, PCI DSS v3.2.1 AWS Control Tower, NIST SP 800-53 Rev. 5	KRITIS	 Tidak	Perubahan dipicu
RDS.3	Instans RDS DB harus mengaktifkan enkripsi saat istirahat	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan:, Tolok Ukur AWS Yayasan CIS v1.4.0 AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
RDS.4	Snapshot cluster RDS dan snapshot database harus dienkripsi saat istirahat	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
RDS.5	Instans RDS DB harus dikonfigurasi dengan beberapa Availability Zone	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
RDS.6	Pemantauan yang ditingkatkan harus dikonfigurasi untuk instans RDS DB	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	RENDAH	 Ya	Perubahan dipicu
RDS.7	Cluster RDS harus mengaktif kan perlindungan penghapusan	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	RENDAH	 Tidak	Perubahan dipicu
RDS.8	Instans RDS DB harus mengaktif kan perlindungan penghapusan	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	RENDAH	 Tidak	Perubahan dipicu
RDS.9	Instans RDS DB harus menerbitkan log ke Log CloudWatch	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
RDS.10	Autentikasi IAM harus dikonfigurasi untuk instance RDS	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
RDS.11	Instans RDS harus mengaktifkan pencadangan otomatis	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Ya	Perubahan dipicu
RDS.12	Autentikasi IAM harus dikonfigurasi untuk cluster RDS	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
RDS.13	Peningkatan versi minor otomatis RDS harus diaktifkan	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	TINGGI	 Tidak	Perubahan dipicu
RDS.14	Cluster Amazon Aurora seharusnya mengaktifkan backtracking	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	MEDIUM	 Ya	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
RDS.15	Cluster RDS DB harus dikonfigurasi untuk beberapa Availability Zone	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
RDS.16	Cluster RDS DB harus dikonfigurasi untuk menyalin tag ke snapshot	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	RENDAH	 Tidak	Perubahan dipicu
RDS.17	Instans RDS DB harus dikonfigurasi untuk menyalin tag ke snapshot	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	RENDAH	 Tidak	Perubahan dipicu
RDS.18	Instans RDS harus digunakan dalam VPC	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	TINGGI	 Tidak	Perubahan dipicu
RDS.19	Langganan pemberitahuan acara RDS yang ada harus dikonfigurasi untuk peristiwa klaster kritis	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	RENDAH	 Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
RDS.20	Langganan pemberitahuan acara RDS yang ada harus dikonfigurasi untuk peristiwa instance database penting	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	RENDAH	 Tidak	Perubahan dipicu
RDS.21	Langganan pemberitahuan acara RDS harus dikonfigurasi untuk peristiwa grup parameter basis data kritis	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	RENDAH	 Tidak	Perubahan dipicu
RDS.22	Langganan pemberitahuan acara RDS harus dikonfigurasi untuk peristiwa grup keamanan basis data penting	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	RENDAH	 Tidak	Perubahan dipicu
RDS.23	Instans RDS tidak boleh menggunakan port default mesin database	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	RENDAH	 Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
RDS.24	Cluster Database RDS harus menggunakan nama pengguna administrator khusus	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
RDS.25	Instans database RDS harus menggunakan nama pengguna administrator khusus	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
RDS.26	Instans RDS DB harus dilindungi oleh rencana cadangan	NIST SP 800-53 Wahyu 5	MEDIUM	 Ya	Berkala
RDS.27	Cluster RDS DB harus dienkripsi saat istirahat	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5, Standar yang Dikelola Layanan: AWS Control Tower	MEDIUM	 Tidak	Perubahan dipicu
RDS.28	Cluster RDS DB harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
RDS.29	Snapshot cluster RDS DB harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
RDS.30	Instans RDS DB harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
RDS.31	Grup keamanan RDS DB harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
RDS.32	Snapshot RDS DB harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
RDS.33	Grup subnet RDS DB harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
RDS.34	Cluster Aurora MySQL DB harus mempublikasikan log audit ke Log CloudWatch	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
RDS.35	Cluster RDS DB harus mengaktifkan peningkatan versi minor otomatis	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
Pergeseran merah.1	Cluster Amazon Redshift harus melarang akses publik	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan:, PCI DSS v3.2.1 AWS Control Tower, NIST SP 800-53 Rev. 5	KRITIS	 Tidak	Perubahan dipicu
Pergeseran merah.2	Koneksi ke cluster Amazon Redshift harus dienkripsi saat transit	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
Pergeseran merah.3	Cluster Amazon Redshift harus mengaktifkan snapshot otomatis	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	MEDIUM	 Ya	Perubahan dipicu
Pergeseran merah.4	Cluster Amazon Redshift harus mengaktifkan pencatatan audit	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
Pergeseran Merah.6	Amazon Redshift harus mengaktifkan peningkatan otomatis ke versi utama	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
Pergeseran Merah.7	Cluster Redshift harus menggunakan perutean VPC yang disempurnakan	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
Pergeseran Merah.8	Cluster Amazon Redshift tidak boleh menggunakan nama pengguna Admin default	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
Pergeseran Merah.9	Cluster Redshift tidak boleh menggunakan nama database default	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
Pergeseran Merah.10	Cluster Redshift harus dienkripsi saat istirahat	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
Pergeseran Merah.11	Cluster Redshift harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
Pergeseran Merah.12	Pemberitahuan berlangganan acara Redshift harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
Pergeseran Merah.13	Cuplikan klaster Redshift harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
Pergeseran Merah.14	Grup subnet cluster Redshift harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
Pergeseran Merah.15	Grup keamanan Redshift harus mengizinkan masuknya pada port cluster hanya dari asal yang dibatasi	AWS Praktik Terbaik Keamanan Dasar	TINGGI	 Tidak	Berkala

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
Route53.1	Pemeriksaan kesehatan Route 53 harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
Route53.2	Rute 53 zona yang dihosting publik harus mencatat kueri DNS	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
S3.1	Bucket tujuan umum S3 harus mengaktif kan pengaturan akses publik blok	AWS Praktik Terbaik Keamanan Dasar, Standar yang Dikelola Layanan:, PCI DSS v3.2.1 AWS Control Tower, Tolok Ukur AWS Yayasan CIS v1.4.0, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Berkala
S3.2	Bucket tujuan umum S3 harus memblokir akses baca publik	AWS Praktik Terbaik Keamanan Dasar, Standar yang Dikelola Layanan:, PCI DSS v3.2.1 AWS Control Tower, NIST SP 800-53 Rev. 5	KRITIS	 Tidak	Perubahan dipicu dan periodik

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
S3.3	Bucket tujuan umum S3 harus memblokir akses tulis publik	AWS Praktik Terbaik Keamanan Dasar, Standar yang Dikelola Layanan:, PCI DSS v3.2.1 AWS Control Tower, NIST SP 800-53 Rev. 5	KRITIS	 Tidak	Perubahan dipicu dan periodik
S3.5	Bucket tujuan umum S3 harus memerlukan permintaan untuk menggunakan SSL	AWS Praktik Terbaik Keamanan Dasar, Standar yang Dikelola Layanan:, PCI DSS v3.2.1 AWS Control Tower, Tolok Ukur AWS Yayasan CIS v1.4.0, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
S3.6	Kebijakan bucket tujuan umum S3 harus membatasi akses ke yang lain Akun AWS	AWS Praktik Terbaik Keamanan Dasar, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	TINGGI	 Tidak	Perubahan dipicu
S3.7	Bucket tujuan umum S3 harus menggunakan replikasi lintas wilayah	PCI DSS v3.2.1, NIST SP 800-53 Wahyu 5	RENDAH	 Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
S3.8	Bucket tujuan umum S3 harus memblokir akses publik	AWS Praktik Terbaik Keamanan Dasar, Standar yang Dikelola Layanan:, Tolok Ukur AWS Yayasan CIS v1.4.0 AWS Control Tower, NIST SP 800-53 Rev. 5	TINGGI	 Tidak	Perubahan dipicu
S3.9	Bucket tujuan umum S3 harus mengaktif kan pencatatan akses server	AWS Praktik Terbaik Keamanan Dasar, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
S3.10	Bucket tujuan umum S3 dengan versi diaktifkan harus memiliki konfigurasi Siklus Hidup	NIST SP 800-53 Wahyu 5	MEDIUM	 Tidak	Perubahan dipicu
S3.11	Bucket tujuan umum S3 harus mengaktif kan pemberitahuan acara	NIST SP 800-53 Wahyu 5	MEDIUM	 Ya	Perubahan dipicu
S3.12	ACL tidak boleh digunakan untuk mengelola akses pengguna ke bucket tujuan umum S3	AWS Praktik Terbaik Keamanan Dasar, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
S3.13	Bucket tujuan umum S3 harus memiliki konfigurasi Siklus Hidup	AWS Praktik Terbaik Keamanan Dasar, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	RENDAH	 Ya	Perubahan dipicu
S3.14	Bucket tujuan umum S3 harus mengaktifkan versi	NIST SP 800-53 Wahyu 5	RENDAH	 Tidak	Perubahan dipicu
S3.15	Bucket tujuan umum S3 harus mengaktifkan Object Lock	NIST SP 800-53 Wahyu 5	MEDIUM	 Ya	Perubahan dipicu
S3.17	Bucket tujuan umum S3 harus dienkripsi saat istirahat dengan AWS KMS keys	Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
S3.19	Titik akses S3 harus mengaktifkan pengaturan akses publik blok	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5	KRITIS	 Tidak	Perubahan dipicu
S3.20	Bucket tujuan umum S3 harus mengaktifkan penghapusan MFA	Tolok Ukur AWS Yayasan CIS v1.4.0, NIST SP 800-53 Rev. 5	RENDAH	 Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
S3.22	Bucket tujuan umum S3 harus mencatat peristiwa penulisan tingkat objek	Tolok Ukur AWS Yayasan CIS v3.0.0	MEDIUM	 Tidak	Berkala
S3.23	Bucket tujuan umum S3 harus mencatat peristiwa pembacaan tingkat objek	Tolok Ukur AWS Yayasan CIS v3.0.0	MEDIUM	 Tidak	Berkala
SageMaker.1	Instans SageMaker notebook Amazon seharusnya tidak memiliki akses internet langsung	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan:, PCI DSS v3.2.1 AWS Control Tower, NIST SP 800-53 Rev. 5	TINGGI	 Tidak	Berkala
SageMaker.2	SageMaker instance notebook harus diluncurkan dalam VPC khusus	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	TINGGI	 Tidak	Perubahan dipicu
SageMaker.3	Pengguna seharusnya tidak memiliki akses root ke instance SageMaker notebook	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	TINGGI	 Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
SageMaker.4	SageMaker varian produksi endpoint harus memiliki jumlah instance awal yang lebih besar dari 1	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Berkala
SecretsManager.1	Rahasia Secrets Manager harus mengaktifkan rotasi otomatis	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Ya	Perubahan dipicu
SecretsManager.2	Rahasia Secrets Manager yang dikonfigurasi dengan rotasi otomatis harus berhasil diputar	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
SecretsManager.3	Hapus rahasia Secrets Manager yang tidak digunakan	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Ya	Berkala

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
SecretsManager.4	Rahasia Secrets Manager harus diputar dalam jumlah hari tertentu	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Ya	Berkala
SecretsManager.5	Rahasia Secrets Manager harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
ServiceCatalog.1	Portofolio Service Catalog harus dibagikan hanya dalam suatu organisasi AWS	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5	TINGGI	 Tidak	Berkala
SES.1	Daftar kontak SES harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
SES.2	Set konfigurasi SES harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
SNS.1	Topik SNS harus dienkripsi saat istirahat menggunakan AWS KMS	NIST SP 800-53 Wahyu 5	MEDIUM	 Tidak	Perubahan dipicu
SNS.3	Topik SNS harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
SQS.1	Antrian Amazon SQS harus dienkripsi saat istirahat	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
SQ.2	Antrian SQS harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
SSM.1	Instans EC2 harus dikelola oleh AWS Systems Manager	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan:, PCI DSS v3.2.1 AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
SSM.2	Instans EC2 yang dikelola oleh Systems Manager harus memiliki status kepatuhan patch COMPLIANT setelah instalasi patch	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan:, PCI DSS v3.2.1 AWS Control Tower, NIST SP 800-53 Rev. 5	TINGGI	 Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
SSM.3	Instans EC2 yang dikelola oleh Systems Manager harus memiliki status kepatuhan asosiasi COMPLIANT	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan:, PCI DSS v3.2.1 AWS Control Tower, NIST SP 800-53 Rev. 5	RENDAH	 Tidak	Perubahan dipicu
SSM.4	Dokumen SSM tidak boleh bersifat publik	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	KRITIS	 Tidak	Berkala
StepFunctions.1	Mesin status Step Functions harus mengaktifkan logging	AWS Praktik Terbaik Keamanan Dasar	MEDIUM	 Ya	Perubahan dipicu
StepFunctions.2	Aktivitas Step Functions harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
Transfer.1	Alur kerja Transfer Family harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
Transfer.2	Server Transfer Family tidak boleh menggunakan protokol FTP untuk koneksi endpoint	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Berkala
WAF.1	AWS WAF Pencatatan ACL Web Global Klasik harus diaktifkan	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Berkala
WAF.2	AWS WAF Aturan Regional Klasik harus memiliki setidaknya satu syarat	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
WAF.3	AWS WAF Kelompok aturan Regional klasik harus memiliki setidaknya satu aturan	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
WAF.4	AWS WAF ACL web Regional Klasik harus memiliki setidaknya satu aturan atau grup aturan	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
WAF.6	AWS WAF Aturan global klasik harus memiliki setidaknya satu syarat	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
WAF.7	AWS WAF Kelompok aturan global klasik harus memiliki setidaknya satu aturan	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
WAF.8	AWS WAF ACL web global klasik harus memiliki setidaknya satu aturan atau grup aturan	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu
WAF.10	AWS WAF ACL web harus memiliki setidaknya satu aturan atau kelompok aturan	AWS Praktik Terbaik Keamanan Dasar v1.0.0, Standar yang Dikelola Layanan: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
WAF.11	AWS WAF pencatatan ACL web harus diaktifkan	NIST SP 800-53 Wahyu 5	RENDAH	 Tidak	Berkala
WAF.12	AWS WAF aturan harus mengaktifkan CloudWatch metrik	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	MEDIUM	 Tidak	Perubahan dipicu

Topik

- Akun AWS kontrol
- AWS Certificate Manager kontrol
- Kontrol Amazon API Gateway
- AWS AppSync kontrol
- Kontrol Amazon Athena
- AWS Backup kontrol
- AWS CloudFormation kontrol
- CloudFront Kontrol Amazon
- AWS CloudTrail kontrol
- CloudWatch Kontrol Amazon
- AWS CodeArtifact kontrol
- AWS CodeBuild kontrol
- AWS Config kontrol
- Kontrol Firehose Data Amazon
- Kontrol Detektif Amazon
- AWS Database Migration Service kontrol
- Kontrol Amazon DocumentDB

- Kontrol Amazon DynamoDB
- Kontrol Registri Kontainer Elastis Amazon
- Kontrol Amazon ECS
- Kontrol Amazon Elastic Compute Cloud
- Kontrol Auto Scaling Amazon EC2
- Kontrol Manajer Sistem Amazon EC2
- Kontrol Amazon Elastic File System
- Kontrol Layanan Amazon Elastic Kubernetes
- ElastiCache Kontrol Amazon
- AWS Elastic Beanstalk kontrol
- Kontrol Elastic Load Balancing
- Kontrol EMR Amazon
- Kontrol Elasticsearch
- EventBridge Kontrol Amazon
- Kontrol Amazon FSx
- AWS Global Accelerator kontrol
- AWS Glue kontrol
- GuardDuty Kontrol Amazon
- AWS Identity and Access Management kontrol
- AWS IoT kontrol
- Kontrol Amazon Kinesis
- AWS Key Management Service kontrol
- AWS Lambda kontrol
- Kontrol Amazon Macie
- Kontrol MSK Amazon
- Kontrol Amazon MQ
- Kontrol Amazon Neptunus
- AWS Network Firewall kontrol
- Kontrol OpenSearch Layanan Amazon
- AWS Private Certificate Authority kontrol

- Kontrol Layanan Amazon Relational Database Service
- Kontrol Amazon Redshift
- Amazon Route 53 kontrol
- Kontrol Layanan Penyimpanan Sederhana Amazon
- SageMaker Kontrol Amazon
- AWS Secrets Manager kontrol
- AWS Service Catalog kontrol
- Kontrol Layanan Email Sederhana Amazon
- Kontrol Layanan Pemberitahuan Sederhana Amazon
- Kontrol Layanan Antrian Sederhana Amazon
- AWS Step Functions kontrol
- AWS Transfer Family kontrol
- AWS WAF kontrol

Akun AWS kontrol

Kontrol ini terkait dengan Akun AWS.

Kontrol ini mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[Akun.1] Informasi kontak keamanan harus disediakan untuk Akun AWS

Persyaratan terkait: Nist.800-53.r5 CM-2, Nist.800-53.r5 CM-2 (2)

Kategori: Identifikasi > Konfigurasi Sumber Daya

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::::Account`

AWS Config aturan: **`security-account-information-provided`**

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah akun Amazon Web Services (AWS) memiliki informasi kontak keamanan. Kontrol gagal jika informasi kontak keamanan tidak disediakan untuk akun.

Kontak keamanan alternatif memungkinkan AWS untuk menghubungi orang lain tentang masalah dengan akun Anda jika Anda tidak tersedia. Pemberitahuan dapat berasal dari AWS Support, atau Layanan AWS tim lain tentang topik terkait keamanan yang terkait dengan penggunaan Anda. Akun AWS

Remediasi

Untuk menambahkan kontak alternatif sebagai kontak keamanan ke kontak Anda Akun AWS, lihat Menambahkan, mengubah, atau menghapus kontak alternatif di Panduan Pengguna AWS Billing and Cost Management.

[Akun.2] Akun AWS harus menjadi bagian dari organisasi AWS Organizations

Kategori: Lindungi > Manajemen akses yang aman > Kontrol akses

Persyaratan terkait: NIST.800-53.R5 CA-9 (1), NIST.800-53.R5 CM-2

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::::Account`

AWS Config aturan: **`account-part-of-organizations`**

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa Akun AWS apakah suatu bagian dari organisasi yang dikelola AWS Organizations. Kontrol gagal jika akun bukan bagian dari organisasi.

Organizations membantu Anda mengelola lingkungan secara terpusat saat Anda meningkatkan beban kerja. AWS Anda dapat menggunakan beberapa Akun AWS untuk mengisolasi beban kerja yang memiliki persyaratan keamanan tertentu, atau untuk mematuhi kerangka kerja seperti HIPAA atau PCI. Dengan membuat organisasi, Anda dapat mengelola beberapa akun sebagai satu unit dan mengelola akses Layanan AWS, sumber daya, dan Wilayah secara terpusat.

Remediasi

Untuk membuat organisasi baru dan Akun AWS menambahkannya secara otomatis, lihat Membuat organisasi di Panduan AWS Organizations Pengguna. Untuk menambahkan akun ke organisasi

yang ada, lihat Mengundang Akun AWS untuk bergabung dengan organisasi Anda di Panduan AWS Organizations Pengguna.

AWS Certificate Manager kontrol

Kontrol ini terkait dengan sumber daya ACM.

Kontrol ini mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[ACM.1] Sertifikat yang diimpor dan diterbitkan ACM harus diperbarui setelah jangka waktu tertentu

Persyaratan terkait: Nist.800-53.r5 SC-28 (3), Nist.800-53.R5 SC-7 (16)

Kategori: Lindungi > Perlindungan Data > Enkripsi data-in-transit

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::ACM::Certificate`

AWS Config aturan: **`acm-certificate-expiration-check`**

Jenis jadwal: Perubahan yang dipicu dan berkala

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`daysToExpiration`	Jumlah hari di mana sertifikat ACM harus diperpanjang	Bilangan Bulat	`14` untuk `365`	`30`

Kontrol ini memeriksa apakah sertifikat AWS Certificate Manager (ACM) diperbarui dalam jangka waktu yang ditentukan. Ini memeriksa sertifikat impor dan sertifikat yang disediakan oleh ACM. Kontrol gagal jika sertifikat tidak diperpanjang dalam jangka waktu yang ditentukan. Kecuali Anda memberikan nilai parameter khusus untuk periode perpanjangan, Security Hub menggunakan nilai default 30 hari.

ACM dapat secara otomatis memperbarui sertifikat yang menggunakan validasi DNS. Untuk sertifikat yang menggunakan validasi email, Anda harus menanggapi email validasi domain. ACM tidak secara otomatis memperbarui sertifikat yang Anda impor. Anda harus memperbarui sertifikat yang diimpor secara manual.

Remediasi

ACM menyediakan perpanjangan terkelola untuk sertifikat SSL/TLS Anda yang dikeluarkan oleh Amazon. Ini berarti bahwa ACM memperbarui sertifikat Anda secara otomatis (jika Anda menggunakan validasi DNS), atau mengirimi Anda pemberitahuan email ketika kedaluwarsa sertifikat mendekati. Layanan ini disediakan untuk sertifikat ACM publik dan swasta.

Untuk domain yang divalidasi melalui email

Ketika sertifikat 45 hari dari kedaluwarsa, ACM mengirimkan email kepada pemilik domain untuk setiap nama domain. Untuk memvalidasi domain dan menyelesaikan pembaruan, Anda harus menanggapi pemberitahuan email.

Untuk informasi selengkapnya, lihat Perpanjangan domain yang divalidasi melalui email di Panduan Pengguna.AWS Certificate Manager

Untuk domain yang divalidasi oleh DNS

ACM secara otomatis memperbarui sertifikat yang menggunakan validasi DNS. 60 hari sebelum kedaluwarsa, ACM memverifikasi bahwa sertifikat dapat diperpanjang.

Jika tidak dapat memvalidasi nama domain, maka ACM mengirimkan pemberitahuan bahwa validasi manual diperlukan. Ini mengirimkan pemberitahuan ini 45 hari, 30 hari, 7 hari, dan 1 hari sebelum kedaluwarsa.

Untuk informasi selengkapnya, lihat Perpanjangan domain yang divalidasi oleh DNS di Panduan Pengguna.AWS Certificate Manager

[ACM.2] Sertifikat RSA yang dikelola oleh ACM harus menggunakan panjang kunci minimal 2.048 bit

Kategori: Identifikasi > Inventaris > Layanan inventaris

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::ACM::Certificate`

AWS Config aturan: **`acm-certificate-rsa-check`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah sertifikat RSA dikelola dengan AWS Certificate Manager menggunakan panjang kunci minimal 2.048 bit. Kontrol gagal jika panjang kunci lebih kecil dari 2.048 bit.

Kekuatan enkripsi berkorelasi langsung dengan ukuran kunci. Kami merekomendasikan panjang kunci setidaknya 2.048 bit untuk melindungi AWS sumber daya Anda karena daya komputasi menjadi lebih murah dan server menjadi lebih maju.

Remediasi

Panjang kunci minimum untuk sertifikat RSA yang dikeluarkan oleh ACM sudah 2.048 bit. Untuk petunjuk tentang menerbitkan sertifikat RSA baru dengan ACM, lihat Menerbitkan dan mengelola sertifikat di Panduan Pengguna.AWS Certificate Manager

Meskipun ACM memungkinkan Anda untuk mengimpor sertifikat dengan panjang kunci yang lebih pendek, Anda harus menggunakan kunci minimal 2.048 bit untuk melewati kontrol ini. Anda tidak dapat mengubah panjang kunci setelah mengimpor sertifikat. Sebagai gantinya, Anda harus menghapus sertifikat dengan panjang kunci lebih kecil dari 2.048 bit. Untuk informasi selengkapnya tentang mengimpor sertifikat ke ACM, lihat Prasyarat untuk mengimpor sertifikat di Panduan Pengguna.AWS Certificate Manager

[ACM.3] Sertifikat ACM harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::ACM::Certificate`

AWS Config aturan: `tagged-acm-certificate` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList	Daftar tag yang memenuhi AWS persyaratan	Tidak ada nilai default

Kontrol ini memeriksa apakah sertifikat AWS Certificate Manager (ACM) memiliki tag dengan kunci spesifik yang ditentukan dalam parameter`requiredTagKeys`. Kontrol gagal jika sertifikat tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika sertifikat tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke sertifikat ACM, lihat Menandai AWS Certificate Manager sertifikat di AWS Certificate Manager Panduan Pengguna.

Kontrol Amazon API Gateway

Kontrol ini terkait dengan sumber daya API Gateway.

Kontrol ini mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[ApiGateway.1] API Gateway REST WebSocket dan pencatatan eksekusi API harus diaktifkan

Persyaratan terkait: Nist.800-53.r5 AC-4 (26), Nist.800-53.R5 AU-10, Nist.800-53.R5 AU-12, Nist.800-53.r5 AU-2, Nist.800-53.r5 AU-3, Nist.800-53.r5 AU-6 (3), Nist.800-53.r5 AU-6 (4), NIST.800-53.R5 CA-7, NIST.800-53.R5 SC-7 (9), NIST.800-53.R5 SI-7 (8)

Kategori: Identifikasi > Logging

Tingkat keparahan: Sedang

Jenis sumber daya:`AWS::ApiGateway::Stage`, `AWS::ApiGatewayV2::Stage`

AWS Config aturan: **`api-gw-execution-logging-enabled`**

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`loggingLevel`	Tingkat pencatatan log	Enum	`ERROR`, `INFO`	`No default value`

Kontrol ini memeriksa apakah semua tahapan Amazon API Gateway REST atau WebSocket API telah diaktifkan pencatatan. Kontrol gagal jika `loggingLevel` tidak `ERROR` atau `INFO` untuk semua

tahapan API. Kecuali Anda memberikan nilai parameter khusus untuk menunjukkan bahwa jenis log tertentu harus diaktifkan, Security Hub akan menghasilkan temuan yang diteruskan jika tingkat logging adalah salah satu `ERROR` atau`INFO`.

API Gateway REST atau WebSocket API tahapan harus mengaktifkan log yang relevan. API Gateway REST dan pencatatan eksekusi WebSocket API menyediakan catatan terperinci tentang permintaan yang dibuat ke API Gateway REST dan tahapan WebSocket API. Tahapannya meliputi respons backend integrasi API, respons otorisasi Lambda, dan titik akhir untuk integrasi. `requestId` AWS

Remediasi

Untuk mengaktifkan logging untuk operasi REST dan WebSocket API, lihat Menyiapkan pencatatan CloudWatch API menggunakan konsol API Gateway di Panduan Pengembang API Gateway.

[ApiGateway.2] Tahapan API Gateway REST API harus dikonfigurasi untuk menggunakan sertifikat SSL untuk otentikasi backend

Persyaratan terkait: Nist.800-53.r5 AC-17 (2), Nist.800-53.r5 AC-4, Nist.800-53.r5 IA-5 (1), Nist.800-53.r5 SC-12 (3), Nist.800-53.r5 SC-13, Nist.800-53.r5 SC-23, Nist.800-53.r5 SC-23, Nist.800-53.r5 00-53.r5 SC-23 (3), NIST.800-53.R5 SC-7 (4), NIST.800-53.R5 SC-8, Nist.800-53.r5 SC-8 (1), NIST.800-53.R5 SC-8 (2), NIST.800-53.R5 SI-7 (6)

Kategori: Lindungi > Perlindungan Data > Enkripsi data-in-transit

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::ApiGateway::Stage`

AWS Config aturan: **`api-gw-ssl-enabled`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah tahapan API Amazon API Gateway REST memiliki sertifikat SSL yang dikonfigurasi. Sistem backend menggunakan sertifikat ini untuk mengautentikasi bahwa permintaan yang masuk berasal dari API Gateway.

Tahapan API Gateway REST API harus dikonfigurasi dengan sertifikat SSL untuk memungkinkan sistem backend mengautentikasi permintaan tersebut berasal dari API Gateway.

Remediasi

Untuk petunjuk terperinci tentang cara membuat dan mengonfigurasi sertifikat SSL API Gateway REST API, lihat Menghasilkan dan mengonfigurasi sertifikat SSL untuk autentikasi backend di Panduan Pengembang API Gateway.

[ApiGateway.3] Tahapan API Gateway REST API harus mengaktifkan penelusuran AWS X-Ray

Persyaratan terkait: Nist.800-53.r5 CA-7

Kategori: Deteksi > Layanan deteksi

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::ApiGateway::Stage`

AWS Config aturan: **`api-gw-xray-enabled`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah penelusuran AWS X-Ray aktif diaktifkan untuk tahapan API REST Amazon API Gateway Anda.

X-Ray active tracing memungkinkan respons yang lebih cepat terhadap perubahan kinerja pada infrastruktur yang mendasarinya. Perubahan kinerja dapat mengakibatkan kurangnya ketersediaan API. X-Ray active tracing menyediakan metrik real-time dari permintaan pengguna yang mengalir melalui operasi API API Gateway REST API dan layanan yang terhubung.

Remediasi

Untuk petunjuk terperinci tentang cara mengaktifkan penelusuran aktif X-Ray untuk operasi API Gateway REST API, lihat dukungan penelusuran aktif Amazon API Gateway AWS X-Ray di Panduan AWS X-Ray Pengembang.

[ApiGateway.4] API Gateway harus dikaitkan dengan ACL Web WAF

Persyaratan terkait: Nist.800-53.r5 AC-4 (21)

Kategori: Lindungi > Layanan pelindung

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::ApiGateway::Stage`

AWS Config aturan: **`api-gw-associated-with-waf`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah tahap API Gateway menggunakan daftar kontrol akses AWS WAF web (ACL). Kontrol ini gagal jika ACL AWS WAF web tidak dilampirkan ke tahap REST API Gateway.

AWS WAF adalah firewall aplikasi web yang membantu melindungi aplikasi web dan API dari serangan. Ini memungkinkan Anda untuk mengonfigurasi ACL, yang merupakan seperangkat aturan yang memungkinkan, memblokir, atau menghitung permintaan web berdasarkan aturan dan kondisi keamanan web yang dapat disesuaikan yang Anda tentukan. Pastikan tahap API Gateway Anda dikaitkan dengan ACL AWS WAF web untuk membantu melindunginya dari serangan berbahaya.

Remediasi

Untuk informasi tentang cara menggunakan konsol API Gateway untuk mengaitkan ACL web AWS WAF Regional dengan tahap API Gateway API yang ada, lihat Menggunakan AWS WAF untuk melindungi API Anda di Panduan Pengembang API Gateway.

[ApiGateway.5] Data cache API Gateway REST API harus dienkripsi saat istirahat

Persyaratan terkait: Nist.800-53.r5 CA-9 (1), NIST.800-53.R5 CM-3 (6), Nist.800-53.r5 SC-13, Nist.800-53.r5 SC-28, Nist.800-53.r5 SC-28 (1), Nist.800-53.r5 SC-7 (10), Nist.800-53.r5 SC-7 (10), Nist.800-53.r5 SC-7 (10), Nist.800-53.r5 SC-7 (10), Nist.800-53.r5 SC-7 (10), Nist.800-53.r5 SC-7 (10), Nist.800-53.r5 SC-7 (10), ST.800-53.R5 SI-7 (6)

Kategori: Lindungi > Perlindungan data > Enkripsi data saat istirahat

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::ApiGateway::Stage`

AWS Config aturan: `api-gw-cache-encrypted` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah semua metode dalam tahapan API Gateway REST API yang mengaktifkan cache dienkripsi. Kontrol gagal jika metode apa pun dalam tahap API Gateway REST API dikonfigurasi ke cache dan cache tidak dienkripsi. Security Hub mengevaluasi enkripsi metode tertentu hanya ketika caching diaktifkan untuk metode itu.

Mengenkripsi data saat istirahat mengurangi risiko data yang disimpan pada disk diakses oleh pengguna yang tidak diautentikasi. AWS Ini menambahkan satu set kontrol akses lain untuk membatasi kemampuan pengguna yang tidak sah mengakses data. Misalnya, izin API diperlukan untuk mendekripsi data sebelum dapat dibaca.

Cache API Gateway REST API harus dienkripsi saat istirahat untuk lapisan keamanan tambahan.

Remediasi

Untuk mengonfigurasi cache API untuk suatu tahap, lihat Mengaktifkan caching Amazon API Gateway di Panduan Pengembang API Gateway. Di Pengaturan Cache, pilih Enkripsi data cache.

[ApiGateway.8] Rute API Gateway harus menentukan jenis otorisasi

Persyaratan terkait: Nist.800-53.r5 AC-3, Nist.800-53.r5 CM-2, Nist.800-53.r5 CM-2 (2)

Kategori: Lindungi > Manajemen Akses Aman

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::ApiGatewayV2::Route`

AWS Config aturan: `api-gwv2-authorization-type-configured`

Jenis jadwal: Periodik

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`authorizationType`	Jenis otorisasi rute API	Enum	`AWS_IAM`, `CUSTOM`, `JWT`	Tidak ada nilai default

Kontrol ini memeriksa apakah rute Amazon API Gateway memiliki jenis otorisasi. Kontrol gagal jika rute API Gateway tidak memiliki jenis otorisasi apa pun. Secara opsional, Anda dapat memberikan nilai parameter khusus jika Anda ingin kontrol lulus hanya jika rute menggunakan jenis otorisasi yang ditentukan dalam parameter. `authorizationType`

API Gateway mendukung beberapa mekanisme untuk mengontrol dan mengelola akses ke API Anda. Dengan menentukan jenis otorisasi, Anda dapat membatasi akses ke API hanya untuk pengguna atau proses yang berwenang.

Remediasi

Untuk menetapkan jenis otorisasi untuk API HTTP, lihat Mengontrol dan mengelola akses ke API HTTP di API Gateway di Panduan Pengembang API Gateway. Untuk menetapkan jenis otorisasi untuk WebSocket API, lihat Mengontrol dan mengelola akses ke WebSocket API di API Gateway di Panduan Pengembang API Gateway.

[ApiGateway.9] Pencatatan akses harus dikonfigurasi untuk Tahapan API Gateway V2

Persyaratan terkait: Nist.800-53.r5 AC-4 (26), Nist.800-53.R5 AU-10, Nist.800-53.R5 AU-12, Nist.800-53.r5 AU-2, Nist.800-53.r5 AU-3, Nist.800-53.r5 AU-6 (3), Nist.800-53.r5 AU-6 (4), NIST.800-53.R5 CA-7, NIST.800-53.R5 SC-7 (9), NIST.800-53.R5 SI-7 (8)

Kategori: Identifikasi > Logging

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::ApiGatewayV2::Stage`

AWS Config aturan: `api-gwv2-access-logs-enabled`

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah tahapan Amazon API Gateway V2 memiliki pencatatan akses yang dikonfigurasi. Kontrol ini gagal jika pengaturan log akses tidak ditentukan.

Log akses API Gateway memberikan informasi terperinci tentang siapa yang telah mengakses API Anda dan bagaimana penelepon mengakses API. Log ini berguna untuk aplikasi seperti audit keamanan dan akses dan investigasi forensik. Aktifkan log akses ini untuk menganalisis pola lalu lintas dan memecahkan masalah.

Untuk praktik terbaik lainnya, lihat Memantau REST API di Panduan Pengembang API Gateway.

Remediasi

Untuk menyiapkan pencatatan akses, lihat Menyiapkan pencatatan CloudWatch API menggunakan konsol API Gateway di Panduan Pengembang API Gateway.

AWS AppSync kontrol

Kontrol ini terkait dengan AWS AppSync sumber daya.

Kontrol ini mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[AppSync.2] AWS AppSync harus mengaktifkan logging tingkat lapangan

Kategori: Identifikasi > Logging

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::AppSync::GraphQLApi`

AWS Config aturan: **`appsync-logging-enabled`**

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub	
`fieldLoggingLevel`	Tingkat pencatatan lapangan	Enum	`ERROR`, `ALL`	No `default value`	

Kontrol ini memeriksa apakah AWS AppSync API telah mengaktifkan logging tingkat bidang. Kontrol gagal jika tingkat log penyelesai bidang diatur ke Tidak Ada. Kecuali Anda memberikan nilai parameter khusus untuk menunjukkan bahwa jenis log tertentu harus diaktifkan, Security

Hub menghasilkan temuan yang diteruskan jika tingkat log penyelesai bidang adalah salah satu atau`ERROR`. `ALL`

Anda dapat menggunakan logging dan metrik untuk mengidentifikasi, memecahkan masalah, dan mengoptimalkan kueri GraphQL Anda. Mengaktifkan logging untuk AWS AppSync GraphQL membantu Anda mendapatkan informasi terperinci tentang permintaan dan tanggapan API, mengidentifikasi dan menanggapi masalah, dan mematuhi persyaratan peraturan.

Remediasi

Untuk mengaktifkan pencatatan AWS AppSync, lihat Pengaturan dan konfigurasi di Panduan AWS AppSync Pengembang.

[AppSync.4] AWS AppSync GraphQL API harus diberi tag

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::AppSync::GraphQLApi`

AWS Config aturan: `tagged-appsync-graphqlapi` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList	Daftar tag yang memenuhi AWS persyaratan	Tidak ada nilai default

Kontrol ini memeriksa apakah AWS AppSync GraphQL API memiliki tag dengan kunci spesifik yang ditentukan dalam parameter. `requiredTagKeys` Kontrol gagal jika GraphQL API tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter. `requiredTagKeys`

Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika GraphQL API tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke AWS AppSync GraphQL API, TagResourcelihat di AWS AppSync Referensi API.

[AppSync.5] AWS AppSync GraphQL API tidak boleh diautentikasi dengan kunci API

Persyaratan terkait: Nist.800-53.r5 AC-2 (1), Nist.800-53.r5 AC-3, Nist.800-53.r5 AC-3 (15), Nist.800-53.r5 AC-3 (7), Nist.800-53.r5 AC-6

Kategori: Lindungi > Manajemen akses aman > Otentikasi tanpa kata sandi

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::AppSync::GraphQLApi`

AWS Config aturan: **`appsync-authorization-check`**

Jenis jadwal: Perubahan dipicu

Parameter:

- `AllowedAuthorizationTypes: AWS_LAMBDA, AWS_IAM, OPENID_CONNECT, AMAZON_COGNITO_USER_POOLS` (tidak dapat disesuaikan)

Kontrol ini memeriksa apakah aplikasi Anda menggunakan kunci API untuk berinteraksi dengan AWS AppSync GraphQL API. Kontrol gagal jika AWS AppSync GraphQL API diautentikasi dengan kunci API.

Kunci API adalah nilai hard-code dalam aplikasi Anda yang dihasilkan oleh AWS AppSync layanan saat Anda membuat titik akhir GraphQL yang tidak diautentikasi. Jika kunci API ini dikompromikan, titik akhir Anda rentan terhadap akses yang tidak diinginkan. Kecuali Anda mendukung aplikasi atau situs web yang dapat diakses publik, kami tidak menyarankan menggunakan kunci API untuk otentikasi.

Remediasi

Untuk menetapkan opsi otorisasi untuk AWS AppSync GraphQL API Anda, lihat Otorisasi dan otentikasi di Panduan Pengembang.AWS AppSync

Kontrol Amazon Athena

Kontrol ini terkait dengan sumber daya Athena.

Kontrol ini mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[Athena.1] Kelompok kerja Athena harus dienkripsi saat istirahat

> **Important**
>
> Security Hub menghentikan kontrol ini pada April 2024. Untuk informasi selengkapnya, lihat Ubah log untuk kontrol Security Hub.

Kategori: Lindungi > Perlindungan data > Enkripsi data saat istirahat

Persyaratan terkait: Nist.800-53.r5 CA-9 (1), NIST.800-53.R5 CM-3 (6), Nist.800-53.r5 SC-13, Nist.800-53.r5 SC-28, Nist.800-53.r5 SC-28 (1), Nist.800-53.r5 SC-7 (10), Nist.800-53.r5 SC-7 (10), Nist.800-53.r5 SC-7 (10), Nist.800-53.r5 SC-7 (10), Nist.800-53.r5 SC-7 (10), Nist.800-53.r5 SC-7 (10), Nist.800-53.r5 SC-7 (10), ST.800-53.R5 SI-7 (6)

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::Athena::WorkGroup`

AWS Config aturan: **`athena-workgroup-encrypted-at-rest`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah workgroup Athena dienkripsi saat istirahat. Kontrol gagal jika workgroup Athena tidak dienkripsi saat istirahat.

Di Athena, Anda dapat membuat grup kerja untuk menjalankan kueri untuk tim, aplikasi, atau beban kerja yang berbeda. Setiap workgroup memiliki pengaturan untuk mengaktifkan enkripsi pada semua query. Anda memiliki opsi untuk menggunakan enkripsi sisi server dengan kunci terkelola Amazon Simple Storage Service (Amazon S3), enkripsi sisi server dengan kunci AWS KMS(), atau enkripsi sisi klien AWS Key Management Service dengan kunci KMS yang dikelola pelanggan. Data saat istirahat mengacu pada data apa pun yang disimpan dalam penyimpanan persisten dan tidak mudah menguap untuk durasi berapa pun. Enkripsi membantu Anda melindungi kerahasiaan data tersebut, mengurangi risiko bahwa pengguna yang tidak sah dapat mengaksesnya.

Remediasi

Untuk mengaktifkan enkripsi saat istirahat untuk grup kerja Athena, lihat Mengedit grup kerja di Panduan Pengguna Amazon Athena. Di bagian Konfigurasi Hasil Kueri, pilih Enkripsi hasil kueri.

[Athena.2] Katalog data Athena harus diberi tag

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::Athena::DataCatalog`

AWS Config aturan: `tagged-athena-datacatalog` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList	Daftar tag yang memenuhi AWS persyaratan	`No default value`

Kontrol ini memeriksa apakah katalog data Amazon Athena memiliki tag dengan kunci spesifik yang ditentukan dalam parameter. `requiredTagKeys` Kontrol gagal jika katalog data tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika katalog data tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS

Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke katalog data Athena, lihat Menandai sumber daya Athena di Panduan Pengguna Amazon Athena.

[Athena.3] Kelompok kerja Athena harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::Athena::WorkGroup`

AWS Config aturan: `tagged-athena-workgroup` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList	Daftar tag yang memenuhi AWS persyaratan	`No default value`

Kontrol ini memeriksa apakah workgroup Amazon Athena memiliki tag dengan kunci tertentu yang ditentukan dalam parameter. `requiredTagKeys` Kontrol gagal jika workgroup tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika workgroup tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke workgroup Athena, lihat Menambahkan dan menghapus tag pada grup kerja individual di Panduan Pengguna Amazon Athena.

AWS Backup kontrol

Kontrol ini terkait dengan AWS Backup sumber daya.

Kontrol ini mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[Backup.1] titik AWS Backup pemulihan harus dienkripsi saat istirahat

Persyaratan terkait: NIST.800-53.R5 CP-9 (8), NIST.800-53.R5 SI-12

Kategori: Lindungi > Perlindungan Data > Enkripsi data-at-rest

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::Backup::RecoveryPoint`

AWS Config aturan: **`backup-recovery-point-encrypted`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah titik AWS Backup pemulihan dienkripsi saat istirahat. Kontrol gagal jika titik pemulihan tidak dienkripsi saat istirahat.

Titik AWS Backup pemulihan mengacu pada salinan atau snapshot data tertentu yang dibuat sebagai bagian dari proses pencadangan. Ini merupakan momen tertentu ketika data dicadangkan dan berfungsi sebagai titik pemulihan jika data asli hilang, rusak, atau tidak dapat diakses. Mengenkripsi titik pemulihan cadangan menambahkan lapisan perlindungan ekstra terhadap akses yang tidak sah. Enkripsi adalah praktik terbaik untuk melindungi kerahasiaan, integritas, dan keamanan data cadangan.

Remediasi

Untuk mengenkripsi titik AWS Backup pemulihan, lihat Enkripsi untuk cadangan AWS Backup di Panduan Pengembang.AWS Backup

[Backup.2] poin AWS Backup pemulihan harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::Backup::RecoveryPoint`

AWS Config aturan: `tagged-backup-recoverypoint` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya	StringList	Daftar tag yang	Tidak ada nilai default

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
	yang dievaluasi. Kunci tag peka huruf besar dan kecil.		memenuhi AWS persyaratan	

Kontrol ini memeriksa apakah titik AWS Backup pemulihan memiliki tag dengan kunci spesifik yang ditentukan dalam parameter`requiredTagKeys`. Kontrol gagal jika titik pemulihan tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika titik pemulihan tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke titik AWS Backup pemulihan

1. Buka AWS Backup konsol di https://console.aws.amazon.com/backup.
2. Di panel navigasi, pilih Rencana cadangan.
3. Pilih paket cadangan dari daftar.
4. Di bagian Tag paket Backup, pilih Kelola tag.
5. Masukkan kunci dan nilai untuk tanda tersebut. Pilih Tambahkan tag baru untuk pasangan nilai kunci tambahan.
6. Setelah Anda selesai menambahkan tanda, pilih Simpan.

[Backup.3] AWS Backup brankas harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::Backup::BackupVault`

AWS Config aturan: `tagged-backup-backupvault` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList	Daftar tag yang memenuhi AWS persyaratan	Tidak ada nilai default

Kontrol ini memeriksa apakah AWS Backup vault memiliki tag dengan kunci spesifik yang ditentukan dalam parameter`requiredTagKeys`. Kontrol gagal jika titik pemulihan tidak memiliki kunci tag atau

jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika titik pemulihan tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke AWS Backup brankas

1. Buka AWS Backup konsol di https://console.aws.amazon.com/backup.
2. Di panel navigasi, pilih Brankas cadangan.
3. Pilih brankas cadangan dari daftar.
4. Di bagian Backup vault tags, pilih Kelola tag.
5. Masukkan kunci dan nilai untuk tanda tersebut. Pilih Tambahkan tag baru untuk pasangan nilai kunci tambahan.
6. Setelah Anda selesai menambahkan tanda, pilih Simpan.

[Backup.4] rencana AWS Backup laporan harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::Backup::ReportPlan`

AWS Config aturan: `tagged-backup-reportplan` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList	Daftar tag yang memenuhi AWS persyaratan	Tidak ada nilai default

Kontrol ini memeriksa apakah rencana AWS Backup laporan memiliki tag dengan kunci spesifik yang ditentukan dalam parameter`requiredTagKeys`. Kontrol gagal jika rencana laporan tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika rencana laporan tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke

AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke rencana AWS Backup laporan

1. Buka AWS Backup konsol di https://console.aws.amazon.com/backup.
2. Di panel navigasi, pilih Brankas cadangan.
3. Pilih brankas cadangan dari daftar.
4. Di bagian Backup vault tags, pilih Kelola tag.
5. Pilih Tambahkan tag baru. Masukkan kunci dan nilai untuk tanda tersebut. Ulangi untuk pasangan nilai kunci tambahan.
6. Setelah Anda selesai menambahkan tanda, pilih Simpan.

[Backup.5] rencana AWS Backup cadangan harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::Backup::BackupPlan`

AWS Config aturan: `tagged-backup-backupplan` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList	Daftar tag yang memenuhi AWS persyaratan	Tidak ada nilai default

Kontrol ini memeriksa apakah rencana AWS Backup cadangan memiliki tag dengan kunci spesifik yang ditentukan dalam parameter`requiredTagKeys`. Kontrol gagal jika paket cadangan tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika paket cadangan tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke rencana AWS Backup cadangan

1. Buka AWS Backup konsol di https://console.aws.amazon.com/backup.
2. Di panel navigasi, pilih Brankas cadangan.
3. Pilih brankas cadangan dari daftar.
4. Di bagian Backup vault tags, pilih Kelola tag.
5. Pilih Tambahkan tag baru. Masukkan kunci dan nilai untuk tanda tersebut. Ulangi untuk pasangan nilai kunci tambahan.
6. Setelah Anda selesai menambahkan tanda, pilih Simpan.

AWS CloudFormation kontrol

Kontrol ini terkait dengan CloudFormation sumber daya.

Kontrol ini mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[CloudFormation.1] CloudFormation tumpukan harus diintegrasikan dengan Simple Notification Service (SNS)

> **Important**
>
> Security Hub menghentikan kontrol ini pada April 2024. Untuk informasi selengkapnya, lihat Ubah log untuk kontrol Security Hub.

Persyaratan terkait: NIST.800-53.R5 SI-4 (12), NIST.800-53.R5 SI-4 (5)

Kategori: Deteksi > Layanan deteksi > Pemantauan aplikasi

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::CloudFormation::Stack`

AWS Config aturan: **`cloudformation-stack-notification-check`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah pemberitahuan Amazon Simple Notification Service terintegrasi dengan AWS CloudFormation tumpukan. Kontrol gagal untuk CloudFormation tumpukan jika tidak ada pemberitahuan SNS yang terkait dengannya.

Mengonfigurasi notifikasi SNS dengan CloudFormation tumpukan Anda membantu segera memberi tahu pemangku kepentingan tentang peristiwa atau perubahan apa pun yang terjadi dengan tumpukan.

Remediasi

Untuk mengintegrasikan CloudFormation tumpukan dan topik SNS, lihat Memperbarui tumpukan secara langsung di AWS CloudFormation Panduan Pengguna.

[CloudFormation.2] CloudFormation tumpukan harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::CloudFormation::Stack`

AWS Config aturan: `tagged-cloudformation-stack` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList	Daftar tag yang memenuhi AWS persyaratan	Tidak ada nilai default

Kontrol ini memeriksa apakah AWS CloudFormation tumpukan memiliki tag dengan kunci tertentu yang ditentukan dalam parameter`requiredTagKeys`. Kontrol gagal jika tumpukan tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika tumpukan tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke CloudFormation tumpukan, lihat CreateStackdi Referensi AWS CloudFormation API.

CloudFront Kontrol Amazon

Kontrol ini terkait dengan CloudFront sumber daya.

Kontrol ini mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[CloudFront.1] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi

Persyaratan terkait: Nist.800-53.r5 SC-7 (11), Nist.800-53.R5 SC-7 (16)

Kategori: Lindungi > Manajemen akses aman > Sumber daya tidak dapat diakses publik

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::CloudFront::Distribution`

AWS Config aturan: **`cloudfront-default-root-object-configured`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah CloudFront distribusi Amazon dikonfigurasi untuk mengembalikan objek tertentu yang merupakan objek root default. Kontrol gagal jika CloudFront distribusi tidak memiliki objek root default yang dikonfigurasi.

Pengguna terkadang meminta URL root distribusi alih-alih objek dalam distribusi. Ketika ini terjadi, menentukan objek root default dapat membantu Anda menghindari mengekspos konten distribusi web Anda.

Remediasi

Untuk mengonfigurasi objek root default untuk CloudFront distribusi, lihat Cara menentukan objek root default di Panduan CloudFront Pengembang Amazon.

[CloudFront.3] CloudFront distribusi harus memerlukan enkripsi dalam perjalanan

Persyaratan terkait: Nist.800-53.r5 AC-17 (2), Nist.800-53.r5 AC-4, Nist.800-53.r5 IA-5 (1), Nist.800-53.r5 SC-12 (3), Nist.800-53.r5 SC-13, Nist.800-53.r5 SC-23, Nist.800-53.r5 SC-23, Nist.800-53.r5 00-53.r5 SC-23 (3), NIST.800-53.R5 SC-7 (4), NIST.800-53.R5 SC-8, Nist.800-53.r5 SC-8 (1), NIST.800-53.R5 SC-8 (2), NIST.800-53.R5 SI-7 (6)

Kategori: Lindungi > Perlindungan Data > Enkripsi data-in-transit

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::CloudFront::Distribution`

AWS Config aturan: **`cloudfront-viewer-policy-https`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah CloudFront distribusi Amazon mengharuskan pemirsa untuk menggunakan HTTPS secara langsung atau menggunakan pengalihan. Kontrol gagal jika `ViewerProtocolPolicy` disetel ke `allow-all` untuk `defaultCacheBehavior` atau untuk`cacheBehaviors`.

HTTPS (TLS) dapat digunakan untuk membantu mencegah penyerang potensial menggunakan person-in-the-middle atau serangan serupa untuk menguping atau memanipulasi lalu lintas jaringan. Hanya koneksi terenkripsi melalui HTTPS (TLS) yang diizinkan. Mengenkripsi data dalam perjalanan dapat memengaruhi kinerja. Anda harus menguji aplikasi Anda dengan fitur ini untuk memahami profil kinerja dan dampak TLS.

Remediasi

Untuk mengenkripsi CloudFront distribusi saat transit, lihat Memerlukan HTTPS untuk komunikasi antara pemirsa dan CloudFront di Panduan CloudFront Pengembang Amazon.

[CloudFront.4] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi

Persyaratan terkait: Nist.800-53.R5 CP-10, Nist.800-53.R5 SC-36, Nist.800-53.R5 SC-5 (2), Nist.800-53.R5 SI-13 (5)

Kategori: Pulihkan > Ketahanan > Ketersediaan tinggi

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::CloudFront::Distribution`

AWS Config aturan: **`cloudfront-origin-failover-enabled`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah CloudFront distribusi Amazon dikonfigurasi dengan grup asal yang memiliki dua atau lebih asal.

CloudFront origin failover dapat meningkatkan ketersediaan. Origin failover secara otomatis mengalihkan lalu lintas ke asal sekunder jika asal primer tidak tersedia atau jika mengembalikan kode status respons HTTP tertentu.

Remediasi

Untuk mengonfigurasi failover asal untuk CloudFront distribusi, lihat Membuat grup asal di Panduan CloudFront Pengembang Amazon.

[CloudFront.5] CloudFront distribusi seharusnya mengaktifkan logging

Persyaratan terkait: Nist.800-53.r5 AC-2 (4), Nist.800-53.r5 AC-4 (26), Nist.800-53.r5 AC-6 (9), Nist.800-53.r5 AU-10, Nist.800-53.r5 AU-12, Nist.800-53.r5 AU-2, Nist.800-53.r5 5 AU-3, NIST.800-53.R5 AU-6 (3), NIST.800-53.R5 AU-6 (4), NIST.800-53.R5 CA-7, NIST.800-53.R5 SC-7 (9), NIST.800-53.R5 SI-4 (20), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-4 (20), nistST.800-53.R5 SI-7 (8)

Kategori: Identifikasi > Logging

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::CloudFront::Distribution`

AWS Config aturan: **`cloudfront-accesslogs-enabled`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah pencatatan akses server diaktifkan pada CloudFront distribusi. Kontrol gagal jika pencatatan akses tidak diaktifkan untuk distribusi.

CloudFront log akses memberikan informasi rinci tentang setiap permintaan pengguna yang CloudFront menerima. Setiap log berisi informasi seperti tanggal dan waktu permintaan diterima, alamat IP penampil yang membuat permintaan, sumber permintaan, dan nomor port permintaan dari penampil.

Log ini berguna untuk aplikasi seperti audit keamanan dan akses dan investigasi forensik. Untuk panduan tambahan tentang cara menganalisis log akses, lihat Menanyakan CloudFront log Amazon di Panduan Pengguna Amazon Athena.

Remediasi

Untuk mengonfigurasi pencatatan akses untuk CloudFront distribusi, lihat Mengonfigurasi dan menggunakan log standar (log akses) di Panduan CloudFront Pengembang Amazon.

[CloudFront.6] CloudFront distribusi harus mengaktifkan WAF

Persyaratan terkait: Nist.800-53.r5 AC-4 (21)

Kategori: Lindungi > Layanan pelindung

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::CloudFront::Distribution`

AWS Config aturan: **`cloudfront-associated-with-waf`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah CloudFront distribusi terkait dengan AWS WAF Classic atau AWS WAF web ACL. Kontrol gagal jika distribusi tidak terkait dengan ACL web.

AWS WAF adalah firewall aplikasi web yang membantu melindungi aplikasi web dan API dari serangan. Ini memungkinkan Anda untuk mengonfigurasi seperangkat aturan, yang disebut daftar kontrol akses web (web ACL), yang memungkinkan, memblokir, atau menghitung permintaan web berdasarkan aturan dan kondisi keamanan web yang dapat disesuaikan yang Anda tentukan. Pastikan CloudFront distribusi Anda dikaitkan dengan ACL AWS WAF web untuk membantu melindunginya dari serangan berbahaya.

Remediasi

Untuk mengaitkan ACL AWS WAF web dengan CloudFront distribusi, lihat Menggunakan AWS WAF untuk mengontrol akses ke konten Anda di Panduan CloudFront Pengembang Amazon.

[CloudFront.7] CloudFront distribusi harus menggunakan sertifikat SSL/TLS khusus

Persyaratan terkait: Nist.800-53.r5 AC-17 (2), Nist.800-53.r5 AC-4, Nist.800-53.r5 IA-5 (1), Nist.800-53.r5 SC-12 (3), Nist.800-53.r5 SC-13, Nist.800-53.r5 SC-23, Nist.800-53.r5 SC-23, Nist.800-53.r5 00-53.r5 SC-23 (3), NIST.800-53.R5 SC-7 (4), NIST.800-53.R5 SC-8, Nist.800-53.r5 SC-8 (1), NIST.800-53.R5 SC-8 (2), NIST.800-53.R5 SI-7 (6)

Kategori: Lindungi > Perlindungan Data > Enkripsi data-in-transit

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::CloudFront::Distribution`

AWS Config aturan: **`cloudfront-custom-ssl-certificate`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah CloudFront distribusi menggunakan sertifikat SSL/TLS default yang disediakan. CloudFront Kontrol ini lolos jika CloudFront distribusi menggunakan sertifikat SSL/TLS kustom. Kontrol ini gagal jika CloudFront distribusi menggunakan sertifikat SSL/TLS default.

SSL/TLS khusus memungkinkan pengguna Anda mengakses konten dengan menggunakan nama domain alternatif. Anda dapat menyimpan sertifikat khusus di AWS Certificate Manager (disarankan), atau di IAM.

Remediasi

Untuk menambahkan nama domain alternatif untuk CloudFront distribusi menggunakan sertifikat SSL/TLS kustom, lihat Menambahkan nama domain alternatif di Panduan Pengembang Amazon. CloudFront

[CloudFront.8] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS

Persyaratan terkait: NIST.800-53.R5 CA-9 (1), NIST.800-53.R5 CM-2

Kategori: Lindungi > Konfigurasi jaringan aman

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::CloudFront::Distribution`

AWS Config aturan: **`cloudfront-sni-enabled`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah CloudFront distribusi Amazon menggunakan sertifikat SSL/TLS kustom dan dikonfigurasi untuk menggunakan SNI untuk melayani permintaan HTTPS. Kontrol ini gagal jika sertifikat SSL/TLS khusus dikaitkan tetapi metode dukungan SSL/TLS adalah alamat IP khusus.

Indikasi Nama Server (Ser Server Name Indication atau SNI) adalah ekstensi untuk protokol TLS yang didukung oleh browser dan klien yang dirilis setelah tahun 2010. Jika Anda mengonfigurasi CloudFront untuk melayani permintaan HTTPS menggunakan SNI, CloudFront kaitkan nama domain

alternatif Anda dengan alamat IP untuk setiap lokasi tepi. Saat penampil mengirimkan permintaan HTTPS untuk konten Anda, DNS mengirimkan permintaan ke alamat IP untuk lokasi tepi yang benar. Alamat IP untuk nama domain Anda ditentukan selama negosiasi jabat tangan SSL/TLS; alamat IP tidak dikhususkan untuk distribusi Anda.

Remediasi

Untuk mengonfigurasi CloudFront distribusi agar menggunakan SNI untuk melayani permintaan HTTPS, lihat Menggunakan SNI untuk Melayani Permintaan HTTPS (berfungsi untuk Sebagian Besar Klien) di Panduan CloudFront Pengembang.

[CloudFront.9] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus

Persyaratan terkait: Nist.800-53.r5 AC-17 (2), Nist.800-53.r5 AC-4, Nist.800-53.r5 IA-5 (1), Nist.800-53.r5 SC-12 (3), Nist.800-53.r5 SC-13, Nist.800-53.r5 SC-23, Nist.800-53.r5 SC-23, Nist.800-53.r5 00-53.r5 SC-23 (3), NIST.800-53.R5 SC-7 (4), NIST.800-53.R5 SC-8, Nist.800-53.r5 SC-8 (1), NIST.800-53.R5 SC-8 (2), NIST.800-53.R5 SI-7 (6)

Kategori: Lindungi > Perlindungan Data > Enkripsi data-in-transit

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::CloudFront::Distribution`

AWS Config aturan: **`cloudfront-traffic-to-origin-encrypted`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah CloudFront distribusi Amazon mengenkripsi lalu lintas ke asal kustom. Kontrol ini gagal untuk CloudFront distribusi yang kebijakan protokol asalnya memungkinkan 'hanya http'. Kontrol ini juga gagal jika kebijakan protokol asal distribusi adalah 'penampil pencocokan' sedangkan kebijakan protokol penampil adalah 'izinkan semua'.

HTTPS (TLS) dapat digunakan untuk membantu mencegah penyadapan atau manipulasi lalu lintas jaringan. Hanya koneksi terenkripsi melalui HTTPS (TLS) yang diizinkan.

Remediasi

Untuk memperbarui Kebijakan Protokol Asal agar memerlukan enkripsi untuk CloudFront sambungan, lihat Memerlukan HTTPS untuk komunikasi antara CloudFront dan asal kustom Anda di Panduan CloudFront Pengembang Amazon.

[CloudFront.10] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal khusus

Persyaratan terkait: Nist.800-53.r5 AC-17 (2), Nist.800-53.r5 AC-4, Nist.800-53.r5 IA-5 (1), Nist.800-53.r5 SC-12 (3), Nist.800-53.r5 SC-13, Nist.800-53.r5 SC-23, Nist.800-53.r5 SC-23, Nist.800-53.r5 00-53.R5 SC-7 (4), NIST.800-53.R5 SC-8, NIST.800-53.R5 SC-8 (1), Nist.800-53.r5 SC-8 (2), NIST.800-53.R5 SI-7 (6)

Kategori: Lindungi > Perlindungan Data > Enkripsi data-in-transit

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::CloudFront::Distribution`

AWS Config aturan: **`cloudfront-no-deprecated-ssl-protocols`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah CloudFront distribusi Amazon menggunakan protokol SSL yang tidak digunakan lagi untuk komunikasi HTTPS antara CloudFront lokasi tepi dan asal kustom Anda. Kontrol ini gagal jika CloudFront distribusi memiliki `CustomOriginConfig` where `OriginSslProtocols` include`SSLv3`.

Pada tahun 2015, Internet Engineering Task Force (IETF) secara resmi mengumumkan bahwa SSL 3.0 harus dihentikan karena protokol tidak cukup aman. Disarankan agar Anda menggunakan TLSv1.2 atau yang lebih baru untuk komunikasi HTTPS ke asal kustom Anda.

Remediasi

Untuk memperbarui Protokol SSL Asal untuk CloudFront distribusi, lihat Memerlukan HTTPS untuk komunikasi antara CloudFront dan asal kustom Anda di Panduan Pengembang Amazon CloudFront .

[CloudFront.12] CloudFront distribusi seharusnya tidak menunjukkan asal S3 yang tidak ada

Persyaratan terkait: Nist.800-53.r5 CM-2, Nist.800-53.r5 CM-2 (2)

Kategori: Identifikasi > Konfigurasi sumber daya

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::CloudFront::Distribution`

AWS Config aturan: **`cloudfront-s3-origin-non-existent-bucket`**

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah CloudFront distribusi Amazon menunjuk ke asal Amazon S3 yang tidak ada. Kontrol gagal untuk CloudFront distribusi jika asal dikonfigurasi untuk menunjuk ke bucket yang tidak ada. Kontrol ini hanya berlaku untuk CloudFront distribusi di mana bucket S3 tanpa hosting situs web statis adalah asal S3.

Ketika CloudFront distribusi di akun Anda dikonfigurasi untuk menunjuk ke bucket yang tidak ada, pihak ketiga yang jahat dapat membuat bucket yang direferensikan dan menyajikan konten mereka sendiri melalui distribusi Anda. Sebaiknya periksa semua asal terlepas dari perilaku perutean untuk memastikan bahwa distribusi Anda mengarah ke asal yang sesuai.

Remediasi

Untuk mengubah CloudFront distribusi agar mengarah ke asal baru, lihat Memperbarui distribusi di Panduan CloudFront Pengembang Amazon.

[CloudFront.13] CloudFront distribusi harus menggunakan kontrol akses asal

Kategori: Lindungi > Manajemen akses aman > Sumber daya tidak dapat diakses publik

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::CloudFront::Distribution`

AWS Config aturan: **`cloudfront-s3-origin-access-control-enabled`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah CloudFront distribusi Amazon dengan asal Amazon S3 memiliki kontrol akses asal (OAC) yang dikonfigurasi. Kontrol gagal jika OAC tidak dikonfigurasi untuk CloudFront distribusi.

Saat menggunakan bucket S3 sebagai asal CloudFront distribusi Anda, Anda dapat mengaktifkan OAC. Ini memungkinkan akses ke konten dalam bucket hanya melalui CloudFront distribusi yang ditentukan, dan melarang akses langsung dari bucket atau distribusi lain. Meskipun CloudFront mendukung Origin Access Identity (OAI), OAC menawarkan fungsionalitas tambahan, dan distribusi menggunakan OAI dapat bermigrasi ke OAC. Meskipun OAI menyediakan cara aman untuk mengakses asal S3, ia memiliki keterbatasan, seperti kurangnya dukungan untuk konfigurasi kebijakan granular dan untuk permintaan HTTP/HTTPS yang menggunakan metode POST Wilayah AWS yang memerlukan AWS Signature Version 4 (SigV4). OAI juga tidak mendukung enkripsi dengan AWS Key Management Service. OAC didasarkan pada praktik AWS terbaik menggunakan prinsip layanan IAM untuk mengautentikasi dengan asal-usul S3.

Remediasi

Untuk mengonfigurasi OAC untuk CloudFront distribusi dengan asal S3, lihat Membatasi akses ke asal Amazon S3 di Panduan Pengembang Amazon. CloudFront

[CloudFront.14] CloudFront distribusi harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::CloudFront::Distribution`

AWS Config aturan: `tagged-cloudfront-distribution` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList	Daftar tag yang memenuhi AWS persyaratan	Tidak ada nilai default

Kontrol ini memeriksa apakah CloudFront distribusi Amazon memiliki tag dengan kunci tertentu yang ditentukan dalam parameter`requiredTagKeys`. Kontrol gagal jika distribusi tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika distribusi tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke CloudFront distribusi, lihat Menandai CloudFront distribusi Amazon di Panduan CloudFront Pengembang Amazon.

AWS CloudTrail kontrol

Kontrol ini terkait dengan CloudTrail sumber daya.

Kontrol ini mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[CloudTrail.1] CloudTrail harus diaktifkan dan dikonfigurasi dengan setidaknya satu jejak Multi-wilayah yang mencakup acara manajemen baca dan tulis

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v1.2.0/2.1, Tolok Ukur Yayasan CIS v1.4.0/3.1, Tolok Ukur AWS Yayasan CIS v3.0.0/3.1, Nist.800-53.r5 AC-2 (4), Nist.800-53.r5 AC-4 (26), Nist.800-53.r5 AC-6 (9), Nist.800-53.r5 AU-10, NiST.800-53.r5 ST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.R5 AU-3, Nist.800-53.r5 AU-6 (3), Nist.800-53.r5 AU-6 (4), Nist.800-53.r5 AU-14 (1), Nist.800-53.r5 CA-7, Nist.800-53.r5 ST.800-53.R5 SC-7 (9), NIST.800-53.R5 SI-3 (8), NIST.800-53.R5 SI-4 (20), NIST.800-53.R5 SI-7 (8), NIST.800-53.R5 SA-8 (22) AWS

Kategori: Identifikasi > Logging

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::::Account`

AWS Config aturan: **`multi-region-cloudtrail-enabled`**

Jenis jadwal: Periodik

Parameter:

- `readWriteType`: `ALL` (tidak dapat disesuaikan)

  `includeManagementEvents`: `true` (tidak dapat disesuaikan)

Kontrol ini memeriksa apakah ada setidaknya satu AWS CloudTrail jejak Multi-wilayah yang menangkap peristiwa manajemen baca dan tulis. Kontrol gagal jika CloudTrail dinonaktifkan atau jika tidak ada setidaknya satu CloudTrail jejak yang menangkap peristiwa manajemen baca dan tulis.

AWS CloudTrail merekam panggilan AWS API untuk akun Anda dan mengirimkan file log kepada Anda. Informasi yang direkam mencakup informasi berikut:

- Identitas pemanggil API
- Waktu panggilan API
- Alamat IP sumber pemanggil API
- Permintaan parameter
- Elemen respons yang dikembalikan oleh Layanan AWS

CloudTrail menyediakan riwayat panggilan AWS API untuk akun, termasuk panggilan API yang dibuat dari AWS Management Console, AWS SDK, alat baris perintah. Riwayat ini juga mencakup panggilan API dari tingkat yang lebih tinggi Layanan AWS seperti. AWS CloudFormation

Riwayat panggilan AWS API yang dihasilkan oleh CloudTrail memungkinkan analisis keamanan, pelacakan perubahan sumber daya, dan audit kepatuhan. Jalur Multi-Region juga memberikan manfaat berikut.

- Jejak multi-wilayah membantu mendeteksi aktivitas tak terduga yang terjadi di Wilayah yang tidak digunakan.
- Jejak multi-wilayah memastikan bahwa pencatatan peristiwa layanan global diaktifkan untuk jejak secara default. Pencatatan peristiwa layanan global mencatat peristiwa yang dihasilkan oleh layanan AWS global.
- Untuk jejak Multi-wilayah, acara manajemen untuk semua operasi baca dan tulis memastikan bahwa operasi manajemen CloudTrail catatan pada semua sumber daya dalam file Akun AWS.

Secara default, CloudTrail jalur yang dibuat menggunakan jalur Multi-wilayah. AWS Management Console

Remediasi

Untuk membuat jejak Multi-wilayah baru CloudTrail, lihat Membuat jejak di Panduan AWS CloudTrail Pengguna. Gunakan nilai berikut:

Bidang	Nilai
Pengaturan tambahan, Validasi file log	Diaktifkan
Pilih peristiwa log, Acara manajemen, aktivitas API	Baca dan Tulis. Kosongkan kotak centang untuk pengecualian.

Untuk memperbarui jejak yang ada, lihat Memperbarui jejak di Panduan AWS CloudTrail Pengguna. Di acara Manajemen, untuk aktivitas API, pilih Baca dan Tulis.

[CloudTrail.2] CloudTrail harus mengaktifkan enkripsi saat istirahat

Persyaratan terkait: PCI DSS v3.2.1/3.4, Tolok Ukur Yayasan CIS v1.2.0/2.7, Tolok Ukur Yayasan CIS v1.4.0/3.7, Tolok Ukur AWS Yayasan CIS v3.0.0/3.5, NIST.800-53.R5 AU-9, NIST.800-53.R5

AWS CA-9 (1), NIST.800-53.R5 AWS CM-3 (6), Nist.800-53.R5 SC-13, NIST.800-53.R5 SC-28, NIST.800-53.R5 SC-28 (1), NIST.800-53.R5 SC-7 (10), NIST.800-53.R5 SI-7 (6)

Kategori: Lindungi > Perlindungan Data > Enkripsi data-at-rest

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::CloudTrail::Trail`

AWS Config aturan: **`cloud-trail-encryption-enabled`**

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah CloudTrail dikonfigurasi untuk menggunakan enkripsi server-side encryption (SSE). AWS KMS key Kontrol gagal jika `KmsKeyId` tidak ditentukan.

Untuk lapisan keamanan tambahan untuk file CloudTrail log sensitif Anda, Anda harus menggunakan enkripsi sisi server dengan AWS KMS keys (SSE-KMS) untuk file CloudTrail log Anda untuk enkripsi saat istirahat. Perhatikan bahwa secara default, file log yang dikirimkan CloudTrail ke bucket Anda dienkripsi oleh enkripsi sisi server Amazon dengan kunci enkripsi yang dikelola Amazon S3 (SSE-S3).

Remediasi

Untuk mengaktifkan enkripsi SSE-KMS untuk file CloudTrail log, lihat Memperbarui jejak untuk menggunakan kunci KMS di Panduan Pengguna.AWS CloudTrail

[CloudTrail.3] Setidaknya satu CloudTrail jejak harus diaktifkan

Persyaratan terkait: PCI DSS v3.2.1/10.1, PCI DSS v3.2.1/10.2.1, PCI DSS v3.2.1/10.2.2, PCI DSS v3.2.1/10.2.3, PCI DSS v3.2.1/10.2.4, PCI DSS v3.2.1/10.2.5, PCI DSS v3.2.1/10.2.6, PCI DSS v3.2.1/10.2.7, DSS v3.2.1/10.3.1, PCI DSS v3.2.1/10.3.2, PCI DSS v3.2.1/10.3.3, PCI DSS v3.2.1/10.3.4, PCI DSS v3.2.1/10.3.5, PCI DSS v3.2.1/10.3.6

Kategori: Identifikasi > Logging

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS:::Account`

AWS Config aturan: **`cloudtrail-enabled`**

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah AWS CloudTrail jejak diaktifkan di Anda Akun AWS. Kontrol gagal jika akun Anda tidak memiliki setidaknya satu CloudTrail jejak yang diaktifkan.

Namun, beberapa AWS layanan tidak mengaktifkan pencatatan semua API dan peristiwa. Anda harus menerapkan jejak audit tambahan selain CloudTrail dan meninjau dokumentasi untuk setiap layanan di Layanan dan Integrasi yang CloudTrail Didukung.

Remediasi

Untuk memulai CloudTrail dan membuat jejak, lihat AWS CloudTrail tutorial Memulai dengan di Panduan AWS CloudTrail Pengguna.

[CloudTrail.4] validasi file CloudTrail log harus diaktifkan

Persyaratan terkait: PCI DSS v3.2.1/10.5.2, PCI DSS v3.2.1/10.5.5, Tolok Ukur Yayasan CIS v1.2.0/2.2, Tolok Ukur Yayasan CIS v1.4.0/3.2, Tolok Ukur AWS Yayasan CIS v3.0.0/3.2, NIST.800-53.R5 AU-9, NIST.800-53.r5 SI-4, NIST.800-53.r5 SI-7 (1), AWS NIST.800-53.R5 SI-7 (3), NIST.800-53.R5 AWS SI-7 (7)

Kategori: Perlindungan data > Integritas data

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::CloudTrail::Trail`

AWS Config aturan: **`cloud-trail-log-file-validation-enabled`**

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah validasi integritas file log diaktifkan pada CloudTrail jejak.

CloudTrail validasi file log membuat file digest yang ditandatangani secara digital yang berisi hash dari setiap log yang menulis ke CloudTrail Amazon S3. Anda dapat menggunakan file intisari ini untuk menentukan apakah file log diubah, dihapus, atau tidak diubah setelah CloudTrail mengirimkan log.

Security Hub merekomendasikan agar Anda mengaktifkan validasi file di semua jalur. Validasi file log memberikan pemeriksaan integritas tambahan CloudTrail log.

Remediasi

Untuk mengaktifkan validasi file CloudTrail log, lihat Mengaktifkan validasi integritas file log CloudTrail di Panduan Pengguna.AWS CloudTrail

[CloudTrail.5] CloudTrail jalur harus diintegrasikan dengan Amazon Logs CloudWatch

Persyaratan terkait: PCI DSS v3.2.1/10.5.3, Tolok Ukur Yayasan CIS v1.2.0/2.4, Tolok Ukur AWS Yayasan CIS v1.4.0/3.4, Nist.800-53.r5 AC-2 (4), Nist.800-53.r5 AC-4 (26), Nist.800-53.r5 AC-6 (9), Nist.800-53.r5 AU-10, Nist.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.R5 AU-3, Nist.800-53.r5 AU-6 (1), Nist.800-53.r5 AU-6 (3), Nist.800-53.r5 AU-6 (4), Nist.800-53.r5 AU-6 (5), NIST.800-53.R5 AU-7 (1), NIST.800-53.R5 CA-7, NIST.800-53.R5 SC-7 (9), NIST.800-53.R5 SI-20, NIST.800-53.R5 SI-3 (8), NIST.800-53.R5 SI-4 (20), NIST.800-800-800-53.R5 SI-4 (AWS 5), NIST.800-53.R5 SI-7 (8)

Kategori: Identifikasi > Logging

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::CloudTrail::Trail`

AWS Config aturan: **`cloud-trail-cloud-watch-logs-enabled`**

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah CloudTrail jejak dikonfigurasi untuk mengirim log ke CloudWatch Log. Kontrol gagal jika `CloudWatchLogsLogGroupArn` properti jejak kosong.

CloudTrail merekam panggilan AWS API yang dibuat di akun tertentu. Informasi yang direkam meliputi yang berikut:

- Identitas pemanggil API
- Waktu panggilan API
- Alamat IP sumber pemanggil API
- Parameter permintaan
- Elemen respons yang dikembalikan oleh Layanan AWS

CloudTrail menggunakan Amazon S3 untuk penyimpanan dan pengiriman file log. Anda dapat menangkap CloudTrail log dalam bucket S3 tertentu untuk analisis jangka panjang. Untuk melakukan analisis real-time, Anda dapat mengonfigurasi CloudTrail untuk mengirim log ke CloudWatch Log.

Untuk jejak yang diaktifkan di semua Wilayah dalam akun, CloudTrail kirimkan file log dari semua Wilayah tersebut ke grup CloudWatch log Log.

Security Hub merekomendasikan agar Anda mengirim CloudTrail log ke CloudWatch Log. Perhatikan bahwa rekomendasi ini dimaksudkan untuk memastikan bahwa aktivitas akun ditangkap, dipantau, dan diwaspadai dengan tepat. Anda dapat menggunakan CloudWatch Log untuk mengatur ini dengan Anda Layanan AWS. Rekomendasi ini tidak menghalangi penggunaan solusi yang berbeda.

Mengirim CloudTrail CloudWatch log ke Log memfasilitasi pencatatan aktivitas real-time dan historis berdasarkan pengguna, API, sumber daya, dan alamat IP. Anda dapat menggunakan pendekatan ini untuk membuat alarm dan pemberitahuan untuk aktivitas akun anomali atau sensitivitas.

Remediasi

Untuk mengintegrasikan CloudTrail dengan CloudWatch Log, lihat Mengirim peristiwa ke CloudWatch Log di Panduan AWS CloudTrail Pengguna.

[CloudTrail.6] Pastikan bucket S3 yang digunakan untuk menyimpan CloudTrail log tidak dapat diakses publik

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v1.2.0/2.3, Tolok Ukur Yayasan CIS v1.4.0/3.3 AWS

Kategori: Identifikasi > Logging

Tingkat keparahan: Kritis

Jenis sumber daya: `AWS::S3::Bucket`

AWS Config aturan: Tidak ada (aturan Security Hub khusus)

Jenis jadwal: Berkala dan perubahan dipicu

Parameter: Tidak ada

CloudTrail mencatat catatan setiap panggilan API yang dilakukan di akun Anda. File log ini disimpan dalam ember S3. CIS merekomendasikan agar kebijakan bucket S3, atau daftar kontrol akses (ACL), diterapkan pada bucket S3 yang CloudTrail mencatat untuk mencegah akses publik ke

log. CloudTrail Mengizinkan akses publik ke konten CloudTrail log dapat membantu musuh dalam mengidentifikasi kelemahan dalam penggunaan atau konfigurasi akun yang terpengaruh.

Untuk menjalankan pemeriksaan ini, Security Hub pertama-tama menggunakan logika kustom untuk mencari bucket S3 tempat CloudTrail log Anda disimpan. Kemudian menggunakan aturan AWS Config terkelola untuk memeriksa apakah bucket dapat diakses publik.

Jika Anda menggabungkan log Anda ke dalam satu bucket S3 terpusat, maka Security Hub hanya menjalankan pemeriksaan terhadap akun dan Wilayah tempat bucket S3 terpusat berada. Untuk akun dan Wilayah lain, status kontrolnya adalah Tidak ada data.

Jika bucket dapat diakses publik, cek akan menghasilkan temuan yang gagal.

Remediasi

Untuk memblokir akses publik ke bucket CloudTrail S3, lihat Mengonfigurasi blokir setelan akses publik untuk bucket S3 di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon. Pilih keempat Pengaturan Akses Publik Blok Amazon S3.

[CloudTrail.7] Pastikan pencatatan akses bucket S3 diaktifkan pada bucket CloudTrail S3

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v1.2.0/2.6, Tolok Ukur Yayasan CIS v1.4.0/3.6, Tolok Ukur AWS Yayasan CIS v3.0.0/3.4 AWS

Kategori: Identifikasi > Logging

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::S3::Bucket`

AWS Config aturan: Tidak ada (aturan Security Hub khusus)

Jenis jadwal: Periodik

Parameter: Tidak ada

Pencatatan akses bucket S3 menghasilkan log yang berisi catatan akses untuk setiap permintaan yang dibuat ke bucket S3 Anda. Catatan log akses berisi rincian tentang permintaan, seperti jenis permintaan, sumber daya yang ditentukan dalam permintaan berfungsi, dan waktu dan tanggal permintaan diproses.

CIS menyarankan agar Anda mengaktifkan pencatatan akses bucket pada bucket CloudTrail S3.

Dengan mengaktifkan pencatatan bucket S3 pada bucket S3 target, Anda dapat menangkap semua peristiwa yang mungkin memengaruhi objek dalam bucket target. Mengkonfigurasi log untuk ditempatkan di bucket terpisah memungkinkan akses ke informasi log, yang dapat berguna dalam alur kerja keamanan dan respons insiden.

Untuk menjalankan pemeriksaan ini, Security Hub pertama-tama menggunakan logika kustom untuk mencari bucket tempat CloudTrail log Anda disimpan dan kemudian menggunakan aturan AWS Config terkelola untuk memeriksa apakah logging diaktifkan.

Jika CloudTrail mengirimkan file log dari beberapa Akun AWS ke dalam satu bucket Amazon S3 tujuan, Security Hub mengevaluasi kontrol ini hanya terhadap bucket tujuan di Wilayah tempatnya berada. Ini merampingkan temuan Anda. Namun, Anda harus mengaktifkan CloudTrail semua akun yang mengirimkan log ke bucket tujuan. Untuk semua akun kecuali akun yang menyimpan bucket tujuan, status kontrolnya adalah Tidak ada data.

Jika bucket dapat diakses publik, cek akan menghasilkan temuan yang gagal.

Remediasi

Untuk mengaktifkan pencatatan akses server untuk bucket CloudTrail S3 Anda, lihat Mengaktifkan log akses server Amazon S3 di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

[CloudTrail.9] CloudTrail jejak harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::CloudTrail::Trail`

AWS Config aturan: `tagged-cloudtrail-trail` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya	StringList	Daftar tag yang	`No default value`

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
	yang dievaluasi. Kunci tag peka huruf besar dan kecil.		memenuhi AWS persyaratan	

Kontrol ini memeriksa apakah AWS CloudTrail jejak memiliki tag dengan kunci tertentu yang ditentukan dalam parameter`requiredTagKeys`. Kontrol gagal jika jejak tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika jejak tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke CloudTrail jejak, lihat AddTagsdi Referensi AWS CloudTrail API.

CloudWatch Kontrol Amazon

Kontrol ini terkait dengan CloudWatch sumber daya.

Kontrol ini mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[CloudWatch.1] Filter metrik log dan alarm harus ada untuk penggunaan pengguna “root”

Persyaratan terkait: PCI DSS v3.2.1/7.2.1, Tolok Ukur Yayasan CIS v1.2.0/1.1, Tolok Ukur AWS Yayasan CIS v1.2.0/3.3, Tolok Ukur Yayasan CIS v1.4.0/1.7, Tolok Ukur Yayasan CIS AWS v1.4.0/4.3 AWS AWS

Kategori: Deteksi > Layanan deteksi

Tingkat keparahan: Rendah

Jenis sumber daya:`AWS::Logs::MetricFilter`,`AWS::CloudWatch::Alarm`,`AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config aturan: Tidak ada (aturan Security Hub khusus)

Jenis jadwal: Periodik

Parameter: Tidak ada

Pengguna root memiliki akses tak terbatas ke semua layanan dan sumber daya dalam file Akun AWS. Kami sangat menyarankan Anda menghindari penggunaan pengguna root untuk tugas sehari-hari. Meminimalkan penggunaan pengguna root dan mengadopsi prinsip hak istimewa paling sedikit untuk manajemen akses mengurangi risiko perubahan yang tidak disengaja dan pengungkapan kredensyal yang sangat istimewa yang tidak diinginkan.

Sebagai praktik terbaik, gunakan kredensil pengguna root Anda hanya jika diperlukan untuk melakukan tugas manajemen akun dan layanan. Terapkan kebijakan AWS Identity and Access Management (IAM) secara langsung ke grup dan peran tetapi bukan pengguna. Untuk tutorial tentang cara mengatur administrator untuk penggunaan sehari-hari, lihat Membuat pengguna dan grup admin IAM pertama Anda di Panduan Pengguna IAM

Untuk menjalankan pemeriksaan ini, Security Hub menggunakan logika kustom untuk melakukan langkah-langkah audit yang tepat yang ditentukan untuk kontrol 1.7 di CIS AWS Foundations

Benchmark v1.4.0. Kontrol ini gagal jika filter metrik yang tepat yang ditentukan oleh CIS tidak digunakan. Bidang atau istilah tambahan tidak dapat ditambahkan ke filter metrik.

Note

Ketika Security Hub melakukan pemeriksaan untuk kontrol ini, ia mencari CloudTrail jejak yang digunakan akun saat ini. Jalur ini mungkin merupakan jalur organisasi yang dimiliki oleh akun lain. Jalur Multi-Wilayah juga mungkin berbasis di Wilayah yang berbeda.
Hasil pemeriksaan dalam `FAILED` temuan dalam kasus-kasus berikut:

- Tidak ada jejak yang dikonfigurasi.
- Jalur yang tersedia yang berada di Wilayah saat ini dan yang dimiliki oleh rekening giro tidak memenuhi persyaratan kontrol.

Hasil pemeriksaan dalam status kontrol `NO_DATA` dalam kasus berikut:

- Jejak multi-wilayah berbasis di Wilayah yang berbeda. Security Hub hanya dapat menghasilkan temuan di Wilayah tempat jejak itu berada.
- Jejak multi-wilayah milik akun yang berbeda. Security Hub hanya dapat menghasilkan temuan untuk akun yang memiliki jejak.

  Kami merekomendasikan jejak organisasi untuk mencatat peristiwa dari banyak akun dalam suatu organisasi. Jejak organisasi adalah jalur Multi-wilayah secara default dan hanya dapat dikelola oleh akun AWS Organizations manajemen atau akun administrator yang CloudTrail didelegasikan. Menggunakan jejak organisasi menghasilkan status kontrol `NO_DATA` untuk kontrol yang dievaluasi dalam akun anggota organisasi. Di akun anggota, Security Hub hanya menghasilkan temuan untuk sumber daya milik anggota. Temuan yang berkaitan dengan jejak organisasi dihasilkan di akun pemilik sumber daya. Anda dapat melihat temuan ini di akun administrator yang didelegasikan Security Hub menggunakan agregasi lintas wilayah.

Untuk alarm, akun saat ini harus memiliki topik Amazon SNS yang direferensikan, atau harus mendapatkan akses ke topik Amazon SNS dengan menelepon. `ListSubscriptionsByTopic` Jika tidak, Security Hub menghasilkan `WARNING` temuan untuk kontrol.

Remediasi

Untuk melewati kontrol ini, ikuti langkah-langkah berikut untuk membuat topik Amazon SNS, AWS CloudTrail jejak, filter metrik, dan alarm untuk filter metrik.

1. Buat topik Amazon SNS. Untuk petunjuknya, lihat Memulai Amazon SNS di Panduan Pengembang Layanan Pemberitahuan Sederhana Amazon. Buat topik yang menerima semua alarm CIS, dan buat setidaknya satu langganan ke topik tersebut.
2. Buat CloudTrail jejak yang berlaku untuk semua Wilayah AWS. Untuk petunjuk, lihat Membuat jejak di Panduan AWS CloudTrail Pengguna.

   Catat nama grup CloudWatch log Log yang Anda kaitkan dengan CloudTrail jejak. Anda membuat filter metrik untuk grup log tersebut di langkah berikutnya.
3. Membuat sebuah filter metrik. Untuk petunjuknya, lihat Membuat filter metrik untuk grup log di Panduan CloudWatch Pengguna Amazon. Gunakan nilai berikut:

Bidang	Nilai
Tentukan pola, Pola filter	`{$.userIdentity.type="Root" && $.userIdentity.invokedBy NOT EXISTS && $.eventType !="AwsServiceEvent"}`
Namespace metrik	**`LogMetrics`**
Nilai metrik	**`1`**
Nilai default	**`0`**

4. Buat alarm berdasarkan filter. Untuk petunjuknya, lihat Membuat CloudWatch alarm berdasarkan filter metrik grup log di CloudWatch Panduan Pengguna Amazon. Gunakan nilai berikut:

Bidang	Nilai
Kondisi, tipe Ambang	Statis
`your-metric-name` Kapanpun...	lebih besar/sama
dari...	**`1`**

[CloudWatch.2] Pastikan filter metrik log dan alarm ada untuk panggilan API yang tidak sah

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v1.2.0/3.1

Kategori: Deteksi > Layanan deteksi

Tingkat keparahan: Rendah

Jenis sumber daya:`AWS::Logs::MetricFilter`,`AWS::CloudWatch::Alarm`,`AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config aturan: Tidak ada (aturan Security Hub khusus)

Jenis jadwal: Periodik

Parameter: Tidak ada

Anda dapat melakukan pemantauan real-time panggilan API dengan mengarahkan CloudTrail CloudWatch log ke Log dan membuat filter dan alarm metrik yang sesuai.

CIS menyarankan agar Anda membuat filter metrik dan alarm panggilan API yang tidak sah. Memantau panggilan API yang tidak sah membantu mengungkapkan kesalahan aplikasi dan dapat mengurangi waktu untuk mendeteksi aktivitas berbahaya.

Untuk menjalankan pemeriksaan ini, Security Hub menggunakan logika khusus untuk melakukan langkah-langkah audit yang tepat yang ditentukan untuk kontrol 3.1 di CIS AWS Foundations Benchmark v1.2. Kontrol ini gagal jika filter metrik yang tepat yang ditentukan oleh CIS tidak digunakan. Bidang atau istilah tambahan tidak dapat ditambahkan ke filter metrik.

> **Note**
>
> Ketika Security Hub melakukan pemeriksaan untuk kontrol ini, ia mencari CloudTrail jejak yang digunakan akun saat ini. Jalur ini mungkin merupakan jalur organisasi yang dimiliki oleh akun lain. Jalur Multi-Wilayah juga mungkin berbasis di Wilayah yang berbeda.
> Hasil pemeriksaan dalam `FAILED` temuan dalam kasus-kasus berikut:
>
> - Tidak ada jejak yang dikonfigurasi.
> - Jalur yang tersedia yang berada di Wilayah saat ini dan yang dimiliki oleh rekening giro tidak memenuhi persyaratan kontrol.

Hasil pemeriksaan dalam status kontrol `NO_DATA` dalam kasus berikut:

- Jejak multi-wilayah berbasis di Wilayah yang berbeda. Security Hub hanya dapat menghasilkan temuan di Wilayah tempat jejak itu berada.
- Jejak multi-wilayah milik akun yang berbeda. Security Hub hanya dapat menghasilkan temuan untuk akun yang memiliki jejak.

  Kami merekomendasikan jejak organisasi untuk mencatat peristiwa dari banyak akun dalam suatu organisasi. Jejak organisasi adalah jalur Multi-wilayah secara default dan hanya dapat dikelola oleh akun AWS Organizations manajemen atau akun administrator yang CloudTrail didelegasikan. Menggunakan jejak organisasi menghasilkan status kontrol `NO_DATA` untuk kontrol yang dievaluasi dalam akun anggota organisasi. Di akun anggota, Security Hub hanya menghasilkan temuan untuk sumber daya milik anggota. Temuan yang berkaitan dengan jejak organisasi dihasilkan di akun pemilik sumber daya. Anda dapat melihat temuan ini di akun administrator yang didelegasikan Security Hub menggunakan agregasi lintas wilayah.

Untuk alarm, akun saat ini harus memiliki topik Amazon SNS yang direferensikan, atau harus mendapatkan akses ke topik Amazon SNS dengan menelepon. `ListSubscriptionsByTopic` Jika tidak, Security Hub menghasilkan `WARNING` temuan untuk kontrol.

Remediasi

Untuk melewati kontrol ini, ikuti langkah-langkah berikut untuk membuat topik Amazon SNS, AWS CloudTrail jejak, filter metrik, dan alarm untuk filter metrik.

1. Buat topik Amazon SNS. Untuk petunjuknya, lihat Memulai Amazon SNS di Panduan Pengembang Layanan Pemberitahuan Sederhana Amazon. Buat topik yang menerima semua alarm CIS, dan buat setidaknya satu langganan ke topik tersebut.
2. Buat CloudTrail jejak yang berlaku untuk semua Wilayah AWS. Untuk petunjuk, lihat Membuat jejak di Panduan AWS CloudTrail Pengguna.

   Catat nama grup CloudWatch log Log yang Anda kaitkan dengan CloudTrail jejak. Anda membuat filter metrik untuk grup log tersebut di langkah berikutnya.

3. Membuat sebuah filter metrik. Untuk petunjuknya, lihat Membuat filter metrik untuk grup log di Panduan CloudWatch Pengguna Amazon. Gunakan nilai berikut:

Bidang	Nilai
Tentukan pola, Pola filter	`{($.errorCode="*Unauthorized0peration") \|\| ($.errorCode="AccessDenied*")}`
Namespace metrik	**`LogMetrics`**
Nilai metrik	**`1`**
Nilai default	**`0`**

4. Buat alarm berdasarkan filter. Untuk petunjuknya, lihat Membuat CloudWatch alarm berdasarkan filter metrik grup log di CloudWatch Panduan Pengguna Amazon. Gunakan nilai berikut:

Bidang	Nilai
Kondisi, tipe Ambang	Statis
`your-metric-name` Kapanpun...	lebih besar/sama
dari...	**`1`**

[CloudWatch.3] Pastikan filter metrik log dan alarm ada untuk login Konsol Manajemen tanpa MFA

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v1.2.0/3.2

Kategori: Deteksi > Layanan deteksi

Tingkat keparahan: Rendah

Jenis sumber daya:`AWS::Logs::MetricFilter`,`AWS::CloudWatch::Alarm`,`AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config aturan: Tidak ada (aturan Security Hub khusus)

Jenis jadwal: Periodik

Parameter: Tidak ada

Anda dapat melakukan pemantauan real-time panggilan API dengan mengarahkan CloudTrail CloudWatch log ke Log dan membuat filter dan alarm metrik yang sesuai.

CIS merekomendasikan agar Anda membuat filter metrik dan login konsol alarm yang tidak dilindungi oleh MFA. Pemantauan untuk login konsol faktor tunggal meningkatkan visibilitas ke akun yang tidak dilindungi oleh MFA.

Untuk menjalankan pemeriksaan ini, Security Hub menggunakan logika khusus untuk melakukan langkah-langkah audit yang tepat yang ditentukan untuk kontrol 3.2 di CIS AWS Foundations Benchmark v1.2. Kontrol ini gagal jika filter metrik yang tepat yang ditentukan oleh CIS tidak digunakan. Bidang atau istilah tambahan tidak dapat ditambahkan ke filter metrik.

> **Note**
>
> Ketika Security Hub melakukan pemeriksaan untuk kontrol ini, ia mencari CloudTrail jejak yang digunakan akun saat ini. Jalur ini mungkin merupakan jalur organisasi yang dimiliki oleh akun lain. Jalur Multi-Wilayah juga mungkin berbasis di Wilayah yang berbeda.
> Hasil pemeriksaan dalam `FAILED` temuan dalam kasus-kasus berikut:
>
> - Tidak ada jejak yang dikonfigurasi.
> - Jalur yang tersedia yang berada di Wilayah saat ini dan yang dimiliki oleh rekening giro tidak memenuhi persyaratan kontrol.
>
> Hasil pemeriksaan dalam status kontrol `NO_DATA` dalam kasus berikut:
>
> - Jejak multi-wilayah berbasis di Wilayah yang berbeda. Security Hub hanya dapat menghasilkan temuan di Wilayah tempat jejak itu berada.
> - Jejak multi-wilayah milik akun yang berbeda. Security Hub hanya dapat menghasilkan temuan untuk akun yang memiliki jejak.
>
>   Kami merekomendasikan jejak organisasi untuk mencatat peristiwa dari banyak akun dalam suatu organisasi. Jejak organisasi adalah jalur Multi-wilayah secara default dan hanya dapat dikelola oleh akun AWS Organizations manajemen atau akun administrator

yang CloudTrail didelegasikan. Menggunakan jejak organisasi menghasilkan status kontrol `NO_DATA` untuk kontrol yang dievaluasi dalam akun anggota organisasi. Di akun anggota, Security Hub hanya menghasilkan temuan untuk sumber daya milik anggota. Temuan yang berkaitan dengan jejak organisasi dihasilkan di akun pemilik sumber daya. Anda dapat melihat temuan ini di akun administrator yang didelegasikan Security Hub menggunakan agregasi lintas wilayah.

Untuk alarm, akun saat ini harus memiliki topik Amazon SNS yang direferensikan, atau harus mendapatkan akses ke topik Amazon SNS dengan menelepon. `ListSubscriptionsByTopic` Jika tidak, Security Hub menghasilkan `WARNING` temuan untuk kontrol.

Remediasi

Untuk melewati kontrol ini, ikuti langkah-langkah berikut untuk membuat topik Amazon SNS, AWS CloudTrail jejak, filter metrik, dan alarm untuk filter metrik.

1. Buat topik Amazon SNS. Untuk petunjuknya, lihat Memulai Amazon SNS di Panduan Pengembang Layanan Pemberitahuan Sederhana Amazon. Buat topik yang menerima semua alarm CIS, dan buat setidaknya satu langganan ke topik tersebut.
2. Buat CloudTrail jejak yang berlaku untuk semua Wilayah AWS. Untuk petunjuk, lihat Membuat jejak di Panduan AWS CloudTrail Pengguna.

   Catat nama grup CloudWatch log Log yang Anda kaitkan dengan CloudTrail jejak. Anda membuat filter metrik untuk grup log tersebut di langkah berikutnya.
3. Membuat sebuah filter metrik. Untuk petunjuknya, lihat Membuat filter metrik untuk grup log di Panduan CloudWatch Pengguna Amazon. Gunakan nilai berikut:

Bidang	Nilai
Tentukan pola, Pola filter	`{ ($.eventName = "ConsoleLogin") && ($.additionalEventData.MFAUsed != "Yes") && ($.userIdentity.type = "IAMUser") && ($.respon`

Bidang	Nilai
	`seElements.ConsoleLogin = "Success") }`
Namespace metrik	**`LogMetrics`**
Nilai metrik	**`1`**
Nilai default	**`0`**

4. Buat alarm berdasarkan filter. Untuk petunjuknya, lihat Membuat CloudWatch alarm berdasarkan filter metrik grup log di CloudWatch Panduan Pengguna Amazon. Gunakan nilai berikut:

Bidang	Nilai
Kondisi, tipe Ambang	Statis
`your-metric-name` Kapanpun...	lebih besar/sama
dari...	**`1`**

[CloudWatch.4] Pastikan filter metrik log dan alarm ada untuk perubahan kebijakan IAM

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v1.2.0/3.4, Tolok Ukur Yayasan CIS v1.4.0/4.4 AWS

Kategori: Deteksi > Layanan deteksi

Tingkat keparahan: Rendah

Jenis sumber daya:`AWS::Logs::MetricFilter`,`AWS::CloudWatch::Alarm`,`AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config aturan: Tidak ada (aturan Security Hub khusus)

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah Anda memantau panggilan API secara real time dengan mengarahkan CloudTrail CloudWatch log ke Log dan membuat filter dan alarm metrik yang sesuai.

CIS menyarankan agar Anda membuat filter metrik dan alarm untuk perubahan yang dibuat pada kebijakan IAM. Memantau perubahan ini membantu memastikan bahwa kontrol otentikasi dan otorisasi tetap utuh.

Note

Ketika Security Hub melakukan pemeriksaan untuk kontrol ini, ia mencari CloudTrail jejak yang digunakan akun saat ini. Jalur ini mungkin merupakan jalur organisasi yang dimiliki oleh akun lain. Jalur Multi-Wilayah juga mungkin berbasis di Wilayah yang berbeda.
Hasil pemeriksaan dalam `FAILED` temuan dalam kasus-kasus berikut:

- Tidak ada jejak yang dikonfigurasi.
- Jalur yang tersedia yang berada di Wilayah saat ini dan yang dimiliki oleh rekening giro tidak memenuhi persyaratan kontrol.

Hasil pemeriksaan dalam status kontrol `NO_DATA` dalam kasus berikut:

- Jejak multi-wilayah berbasis di Wilayah yang berbeda. Security Hub hanya dapat menghasilkan temuan di Wilayah tempat jejak itu berada.
- Jejak multi-wilayah milik akun yang berbeda. Security Hub hanya dapat menghasilkan temuan untuk akun yang memiliki jejak.

  Kami merekomendasikan jejak organisasi untuk mencatat peristiwa dari banyak akun dalam suatu organisasi. Jejak organisasi adalah jalur Multi-wilayah secara default dan hanya dapat dikelola oleh akun AWS Organizations manajemen atau akun administrator yang CloudTrail didelegasikan. Menggunakan jejak organisasi menghasilkan status kontrol `NO_DATA` untuk kontrol yang dievaluasi dalam akun anggota organisasi. Di akun anggota, Security Hub hanya menghasilkan temuan untuk sumber daya milik anggota. Temuan yang berkaitan dengan jejak organisasi dihasilkan di akun pemilik sumber daya. Anda dapat melihat temuan ini di akun administrator yang didelegasikan Security Hub menggunakan agregasi lintas wilayah.

Untuk alarm, akun saat ini harus memiliki topik Amazon SNS yang direferensikan, atau harus mendapatkan akses ke topik Amazon SNS dengan menelepon.

`ListSubscriptionsByTopic` Jika tidak, Security Hub menghasilkan `WARNING` temuan untuk kontrol.

Remediasi

> **Note**
>
> Pola filter yang kami rekomendasikan dalam langkah-langkah remediasi ini berbeda dari pola filter dalam panduan CIS. Filter yang kami rekomendasikan hanya menargetkan peristiwa yang berasal dari panggilan API IAM.

Untuk melewati kontrol ini, ikuti langkah-langkah berikut untuk membuat topik Amazon SNS, AWS CloudTrail jejak, filter metrik, dan alarm untuk filter metrik.

1. Buat topik Amazon SNS. Untuk petunjuknya, lihat Memulai Amazon SNS di Panduan Pengembang Layanan Pemberitahuan Sederhana Amazon. Buat topik yang menerima semua alarm CIS, dan buat setidaknya satu langganan ke topik tersebut.
2. Buat CloudTrail jejak yang berlaku untuk semua Wilayah AWS. Untuk petunjuk, lihat Membuat jejak di Panduan AWS CloudTrail Pengguna.

   Catat nama grup CloudWatch log Log yang Anda kaitkan dengan CloudTrail jejak. Anda membuat filter metrik untuk grup log tersebut di langkah berikutnya.
3. Membuat sebuah filter metrik. Untuk petunjuknya, lihat Membuat filter metrik untuk grup log di Panduan CloudWatch Pengguna Amazon. Gunakan nilai berikut:

Bidang	Nilai
Tentukan pola, Pola filter	`{($.eventSource=iam.amazonaws.com) && (($.eventName=DeleteGroupPolicy) || ($.eventName=DeleteRolePolicy) \|\| ($.eventName=DeleteUserPolicy) || ($.eventName=PutGroupPolicy) \|\| ($.eventName=PutRolePolicy) || ($.eventName=PutUs`

Bidang	Nilai
	`erPolicy) || ($.eventName=Creat ePolicy) \|\| ($.eventName=Delet ePolicy) || ($.eventName=Creat ePolicyVersion) \|\| ($.eventN ame=DeletePolicyVersion) || ($.eventName=AttachRolePoli cy) \|\| ($.eventName=Detac hRolePolicy) || ($.eventN ame=AttachUserPolicy) \|\| ($.eventName=DetachUserPolicy) || ($.eventName=AttachGroupPol icy) \|\| ($.eventName=Detac hGroupPolicy))}`
Namespace metrik	**`LogMetrics`**
Nilai metrik	**`1`**
Nilai default	**`0`**

4. Buat alarm berdasarkan filter. Untuk petunjuknya, lihat Membuat CloudWatch alarm berdasarkan filter metrik grup log di CloudWatch Panduan Pengguna Amazon. Gunakan nilai berikut:

Bidang	Nilai
Kondisi, tipe Ambang	Statis
`your-metric-name` Kapanpun...	lebih besar/sama
dari...	**`1`**

[CloudWatch.5] Pastikan filter metrik log dan alarm ada untuk perubahan CloudTrail AWS Config urasi

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v1.2.0/3.5, Tolok Ukur Yayasan CIS v1.4.0/4.5 AWS

Kategori: Deteksi > Layanan deteksi

Tingkat keparahan: Rendah

Jenis sumber daya:`AWS::Logs::MetricFilter`,`AWS::CloudWatch::Alarm`,`AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config aturan: Tidak ada (aturan Security Hub khusus)

Jenis jadwal: Periodik

Parameter: Tidak ada

Anda dapat melakukan pemantauan real-time panggilan API dengan mengarahkan CloudTrail CloudWatch log ke Log dan membuat filter dan alarm metrik yang sesuai.

CIS merekomendasikan agar Anda membuat filter metrik dan alarm untuk perubahan pengaturan CloudTrail konfigurasi. Memantau perubahan ini membantu memastikan visibilitas berkelanjutan terhadap aktivitas di akun.

Untuk menjalankan pemeriksaan ini, Security Hub menggunakan logika kustom untuk melakukan langkah-langkah audit yang tepat yang ditentukan untuk kontrol 4.5 di CIS AWS Foundations Benchmark v1.4.0. Kontrol ini gagal jika filter metrik yang tepat yang ditentukan oleh CIS tidak digunakan. Bidang atau istilah tambahan tidak dapat ditambahkan ke filter metrik.

> **Note**
>
> Ketika Security Hub melakukan pemeriksaan untuk kontrol ini, ia mencari CloudTrail jejak yang digunakan akun saat ini. Jalur ini mungkin merupakan jalur organisasi yang dimiliki oleh akun lain. Jalur Multi-Wilayah juga mungkin berbasis di Wilayah yang berbeda.
> Hasil pemeriksaan dalam `FAILED` temuan dalam kasus-kasus berikut:
>
> - Tidak ada jejak yang dikonfigurasi.
> - Jalur yang tersedia yang berada di Wilayah saat ini dan yang dimiliki oleh rekening giro tidak memenuhi persyaratan kontrol.
>
> Hasil pemeriksaan dalam status kontrol `NO_DATA` dalam kasus berikut:
>
> - Jejak multi-wilayah berbasis di Wilayah yang berbeda. Security Hub hanya dapat menghasilkan temuan di Wilayah tempat jejak itu berada.

- Jejak multi-wilayah milik akun yang berbeda. Security Hub hanya dapat menghasilkan temuan untuk akun yang memiliki jejak.

  Kami merekomendasikan jejak organisasi untuk mencatat peristiwa dari banyak akun dalam suatu organisasi. Jejak organisasi adalah jalur Multi-wilayah secara default dan hanya dapat dikelola oleh akun AWS Organizations manajemen atau akun administrator yang CloudTrail didelegasikan. Menggunakan jejak organisasi menghasilkan status kontrol `NO_DATA` untuk kontrol yang dievaluasi dalam akun anggota organisasi. Di akun anggota, Security Hub hanya menghasilkan temuan untuk sumber daya milik anggota. Temuan yang berkaitan dengan jejak organisasi dihasilkan di akun pemilik sumber daya. Anda dapat melihat temuan ini di akun administrator yang didelegasikan Security Hub menggunakan agregasi lintas wilayah.

Untuk alarm, akun saat ini harus memiliki topik Amazon SNS yang direferensikan, atau harus mendapatkan akses ke topik Amazon SNS dengan menelepon. `ListSubscriptionsByTopic` Jika tidak, Security Hub menghasilkan `WARNING` temuan untuk kontrol.

Remediasi

Untuk melewati kontrol ini, ikuti langkah-langkah berikut untuk membuat topik Amazon SNS, AWS CloudTrail jejak, filter metrik, dan alarm untuk filter metrik.

1. Buat topik Amazon SNS. Untuk petunjuknya, lihat Memulai Amazon SNS di Panduan Pengembang Layanan Pemberitahuan Sederhana Amazon. Buat topik yang menerima semua alarm CIS, dan buat setidaknya satu langganan ke topik tersebut.
2. Buat CloudTrail jejak yang berlaku untuk semua Wilayah AWS. Untuk petunjuk, lihat Membuat jejak di Panduan AWS CloudTrail Pengguna.

   Catat nama grup CloudWatch log Log yang Anda kaitkan dengan CloudTrail jejak. Anda membuat filter metrik untuk grup log tersebut di langkah berikutnya.
3. Membuat sebuah filter metrik. Untuk petunjuknya, lihat Membuat filter metrik untuk grup log di Panduan CloudWatch Pengguna Amazon. Gunakan nilai berikut:

Bidang	Nilai
Tentukan pola, Pola filter	`{($.eventName=CreateTrail) \|\| ($.eventName=UpdateTrail) || ($.eventName=DeleteTrail) \|\| ($.eventName=StartLogging) || ($.eventName=StopLogging)}`
Namespace metrik	**`LogMetrics`**
Nilai metrik	**`1`**
Nilai default	**`0`**

4. Buat alarm berdasarkan filter. Untuk petunjuknya, lihat Membuat CloudWatch alarm berdasarkan filter metrik grup log di CloudWatch Panduan Pengguna Amazon. Gunakan nilai berikut:

Bidang	Nilai
Kondisi, tipe Ambang	Statis
`your-metric-name` Kapanpun...	lebih besar/sama
dari...	**`1`**

[CloudWatch.6] Pastikan filter metrik log dan alarm ada untuk kegagalan AWS Management Console otentikasi

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v1.2.0/3.6, Tolok Ukur Yayasan CIS v1.4.0/4.6 AWS

Kategori: Deteksi > Layanan deteksi

Tingkat keparahan: Rendah

Jenis sumber daya:`AWS::Logs::MetricFilter`,`AWS::CloudWatch::Alarm`,`AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config aturan: Tidak ada (aturan Security Hub khusus)

Jenis jadwal: Periodik

Parameter: Tidak ada

Anda dapat melakukan pemantauan real-time panggilan API dengan mengarahkan CloudTrail CloudWatch log ke Log dan membuat filter dan alarm metrik yang sesuai.

CIS menyarankan agar Anda membuat filter metrik dan alarm untuk upaya otentikasi konsol yang gagal. Memantau login konsol yang gagal dapat mengurangi waktu tunggu untuk mendeteksi upaya brute-force kredensyal, yang mungkin memberikan indikator, seperti IP sumber, yang dapat Anda gunakan dalam korelasi peristiwa lain.

Untuk menjalankan pemeriksaan ini, Security Hub menggunakan logika kustom untuk melakukan langkah-langkah audit yang tepat yang ditentukan untuk kontrol 4.6 di CIS AWS Foundations Benchmark v1.4.0. Kontrol ini gagal jika filter metrik yang tepat yang ditentukan oleh CIS tidak digunakan. Bidang atau istilah tambahan tidak dapat ditambahkan ke filter metrik.

> **Note**
>
> Ketika Security Hub melakukan pemeriksaan untuk kontrol ini, ia mencari CloudTrail jejak yang digunakan akun saat ini. Jalur ini mungkin merupakan jalur organisasi yang dimiliki oleh akun lain. Jalur Multi-Wilayah juga mungkin berbasis di Wilayah yang berbeda.
> Hasil pemeriksaan dalam `FAILED` temuan dalam kasus-kasus berikut:
>
> - Tidak ada jejak yang dikonfigurasi.
> - Jalur yang tersedia yang berada di Wilayah saat ini dan yang dimiliki oleh rekening giro tidak memenuhi persyaratan kontrol.
>
> Hasil pemeriksaan dalam status kontrol `NO_DATA` dalam kasus berikut:
>
> - Jejak multi-wilayah berbasis di Wilayah yang berbeda. Security Hub hanya dapat menghasilkan temuan di Wilayah tempat jejak itu berada.
> - Jejak multi-wilayah milik akun yang berbeda. Security Hub hanya dapat menghasilkan temuan untuk akun yang memiliki jejak.
>
>   Kami merekomendasikan jejak organisasi untuk mencatat peristiwa dari banyak akun dalam suatu organisasi. Jejak organisasi adalah jalur Multi-wilayah secara default dan

hanya dapat dikelola oleh akun AWS Organizations manajemen atau akun administrator yang CloudTrail didelegasikan. Menggunakan jejak organisasi menghasilkan status kontrol `NO_DATA` untuk kontrol yang dievaluasi dalam akun anggota organisasi. Di akun anggota, Security Hub hanya menghasilkan temuan untuk sumber daya milik anggota. Temuan yang berkaitan dengan jejak organisasi dihasilkan di akun pemilik sumber daya. Anda dapat melihat temuan ini di akun administrator yang didelegasikan Security Hub menggunakan agregasi lintas wilayah.

Untuk alarm, akun saat ini harus memiliki topik Amazon SNS yang direferensikan, atau harus mendapatkan akses ke topik Amazon SNS dengan menelepon. `ListSubscriptionsByTopic` Jika tidak, Security Hub menghasilkan `WARNING` temuan untuk kontrol.

Remediasi

Untuk melewati kontrol ini, ikuti langkah-langkah berikut untuk membuat topik Amazon SNS, AWS CloudTrail jejak, filter metrik, dan alarm untuk filter metrik.

1. Buat topik Amazon SNS. Untuk petunjuknya, lihat Memulai Amazon SNS di Panduan Pengembang Layanan Pemberitahuan Sederhana Amazon. Buat topik yang menerima semua alarm CIS, dan buat setidaknya satu langganan ke topik tersebut.
2. Buat CloudTrail jejak yang berlaku untuk semua Wilayah AWS. Untuk petunjuk, lihat Membuat jejak di Panduan AWS CloudTrail Pengguna.

   Catat nama grup CloudWatch log Log yang Anda kaitkan dengan CloudTrail jejak. Anda membuat filter metrik untuk grup log tersebut di langkah berikutnya.
3. Membuat sebuah filter metrik. Untuk petunjuknya, lihat Membuat filter metrik untuk grup log di Panduan CloudWatch Pengguna Amazon. Gunakan nilai berikut:

Bidang	Nilai
Tentukan pola, Pola filter	`{($.eventName=ConsoleLogin) && ($.errorMessage="Failed authentication")}`
Namespace metrik	**`LogMetrics`**

Bidang	Nilai
Nilai metrik	**1**
Nilai default	**0**

4. Buat alarm berdasarkan filter. Untuk petunjuknya, lihat Membuat CloudWatch alarm berdasarkan filter metrik grup log di CloudWatch Panduan Pengguna Amazon. Gunakan nilai berikut:

Bidang	Nilai
Kondisi, tipe Ambang	Statis
your-metric-name Kapanpun...	lebih besar/sama
dari...	**1**

[CloudWatch.7] Pastikan filter metrik log dan alarm ada untuk menonaktifkan atau menjadwalkan penghapusan kunci yang dikelola pelanggan

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v1.2.0/3.7, Tolok Ukur Yayasan CIS v1.4.0/4.7 AWS

Kategori: Deteksi > Layanan deteksi

Tingkat keparahan: Rendah

Jenis sumber daya:`AWS::Logs::MetricFilter`,`AWS::CloudWatch::Alarm`,`AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config aturan: Tidak ada (aturan Security Hub khusus)

Jenis jadwal: Periodik

Parameter: Tidak ada

Anda dapat melakukan pemantauan real-time panggilan API dengan mengarahkan CloudTrail CloudWatch log ke Log dan membuat filter dan alarm metrik yang sesuai.

CIS merekomendasikan agar Anda membuat filter metrik dan alarm untuk kunci terkelola pelanggan yang telah mengubah status menjadi penghapusan dinonaktifkan atau terjadwal. Data yang dienkripsi dengan kunci yang dinonaktifkan atau dihapus tidak lagi dapat diakses.

Untuk menjalankan pemeriksaan ini, Security Hub menggunakan logika kustom untuk melakukan langkah-langkah audit yang tepat yang ditentukan untuk kontrol 4.7 di CIS AWS Foundations Benchmark v1.4.0. Kontrol ini gagal jika filter metrik yang tepat yang ditentukan oleh CIS tidak digunakan. Bidang atau istilah tambahan tidak dapat ditambahkan ke filter metrik. Kontrol juga gagal jika `ExcludeManagementEventSources` berisi`kms.amazonaws.com`.

> **Note**
>
> Ketika Security Hub melakukan pemeriksaan untuk kontrol ini, ia mencari CloudTrail jejak yang digunakan akun saat ini. Jalur ini mungkin merupakan jalur organisasi yang dimiliki oleh akun lain. Jalur Multi-Wilayah juga mungkin berbasis di Wilayah yang berbeda.
> Hasil pemeriksaan dalam `FAILED` temuan dalam kasus-kasus berikut:
>
> - Tidak ada jejak yang dikonfigurasi.
> - Jalur yang tersedia yang berada di Wilayah saat ini dan yang dimiliki oleh rekening giro tidak memenuhi persyaratan kontrol.
>
> Hasil pemeriksaan dalam status kontrol `NO_DATA` dalam kasus berikut:
>
> - Jejak multi-wilayah berbasis di Wilayah yang berbeda. Security Hub hanya dapat menghasilkan temuan di Wilayah tempat jejak itu berada.
> - Jejak multi-wilayah milik akun yang berbeda. Security Hub hanya dapat menghasilkan temuan untuk akun yang memiliki jejak.
>
>   Kami merekomendasikan jejak organisasi untuk mencatat peristiwa dari banyak akun dalam suatu organisasi. Jejak organisasi adalah jalur Multi-wilayah secara default dan hanya dapat dikelola oleh akun AWS Organizations manajemen atau akun administrator yang CloudTrail didelegasikan. Menggunakan jejak organisasi menghasilkan status kontrol `NO_DATA` untuk kontrol yang dievaluasi dalam akun anggota organisasi. Di akun anggota, Security Hub hanya menghasilkan temuan untuk sumber daya milik anggota. Temuan yang berkaitan dengan jejak organisasi dihasilkan di akun pemilik sumber daya. Anda dapat melihat temuan ini di akun administrator yang didelegasikan Security Hub menggunakan agregasi lintas wilayah.

Untuk alarm, akun saat ini harus memiliki topik Amazon SNS yang direferensikan, atau harus mendapatkan akses ke topik Amazon SNS dengan menelepon. `ListSubscriptionsByTopic` Jika tidak, Security Hub menghasilkan `WARNING` temuan untuk kontrol.

Remediasi

Untuk melewati kontrol ini, ikuti langkah-langkah berikut untuk membuat topik Amazon SNS, AWS CloudTrail jejak, filter metrik, dan alarm untuk filter metrik.

1. Buat topik Amazon SNS. Untuk petunjuknya, lihat Memulai Amazon SNS di Panduan Pengembang Layanan Pemberitahuan Sederhana Amazon. Buat topik yang menerima semua alarm CIS, dan buat setidaknya satu langganan ke topik tersebut.
2. Buat CloudTrail jejak yang berlaku untuk semua Wilayah AWS. Untuk petunjuk, lihat Membuat jejak di Panduan AWS CloudTrail Pengguna.

   Catat nama grup CloudWatch log Log yang Anda kaitkan dengan CloudTrail jejak. Anda membuat filter metrik untuk grup log tersebut di langkah berikutnya.
3. Membuat sebuah filter metrik. Untuk petunjuknya, lihat Membuat filter metrik untuk grup log di Panduan CloudWatch Pengguna Amazon. Gunakan nilai berikut:

Bidang	Nilai
Tentukan pola, Pola filter	`{($.eventSource=kms.amazonaws.com) && (($.eventName=DisableKey) || ($.eventName=ScheduleKeyDeletion))}`
Namespace metrik	**`LogMetrics`**
Nilai metrik	**`1`**
Nilai default	**`0`**

4. Buat alarm berdasarkan filter. Untuk petunjuknya, lihat Membuat CloudWatch alarm berdasarkan filter metrik grup log di CloudWatch Panduan Pengguna Amazon. Gunakan nilai berikut:

Bidang	Nilai
Kondisi, tipe Ambang	Statis
your-metric-name Kapanpun...	lebih besar/sama
dari...	**1**

[CloudWatch.8] Pastikan filter metrik log dan alarm ada untuk perubahan kebijakan bucket S3

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v1.2.0/3.8, Tolok Ukur Yayasan CIS v1.4.0/4.8 AWS

Kategori: Deteksi > Layanan deteksi

Tingkat keparahan: Rendah

Jenis sumber daya:`AWS::Logs::MetricFilter`,`AWS::CloudWatch::Alarm`,`AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config aturan: Tidak ada (aturan Security Hub khusus)

Jenis jadwal: Periodik

Parameter: Tidak ada

Anda dapat melakukan pemantauan real-time panggilan API dengan mengarahkan CloudTrail CloudWatch log ke Log dan membuat filter dan alarm metrik yang sesuai.

CIS menyarankan agar Anda membuat filter metrik dan alarm untuk perubahan kebijakan bucket S3. Memantau perubahan ini dapat mengurangi waktu untuk mendeteksi dan memperbaiki kebijakan permisif pada bucket S3 yang sensitif.

Untuk menjalankan pemeriksaan ini, Security Hub menggunakan logika kustom untuk melakukan langkah-langkah audit yang tepat yang ditentukan untuk kontrol 4.8 di CIS AWS Foundations Benchmark v1.4.0. Kontrol ini gagal jika filter metrik yang tepat yang ditentukan oleh CIS tidak digunakan. Bidang atau istilah tambahan tidak dapat ditambahkan ke filter metrik.

Note

Ketika Security Hub melakukan pemeriksaan untuk kontrol ini, ia mencari CloudTrail jejak yang digunakan akun saat ini. Jalur ini mungkin merupakan jalur organisasi yang dimiliki oleh akun lain. Jalur Multi-Wilayah juga mungkin berbasis di Wilayah yang berbeda.
Hasil pemeriksaan dalam `FAILED` temuan dalam kasus-kasus berikut:

- Tidak ada jejak yang dikonfigurasi.
- Jalur yang tersedia yang berada di Wilayah saat ini dan yang dimiliki oleh rekening giro tidak memenuhi persyaratan kontrol.

Hasil pemeriksaan dalam status kontrol `NO_DATA` dalam kasus berikut:

- Jejak multi-wilayah berbasis di Wilayah yang berbeda. Security Hub hanya dapat menghasilkan temuan di Wilayah tempat jejak itu berada.
- Jejak multi-wilayah milik akun yang berbeda. Security Hub hanya dapat menghasilkan temuan untuk akun yang memiliki jejak.

  Kami merekomendasikan jejak organisasi untuk mencatat peristiwa dari banyak akun dalam suatu organisasi. Jejak organisasi adalah jalur Multi-wilayah secara default dan hanya dapat dikelola oleh akun AWS Organizations manajemen atau akun administrator yang CloudTrail didelegasikan. Menggunakan jejak organisasi menghasilkan status kontrol `NO_DATA` untuk kontrol yang dievaluasi dalam akun anggota organisasi. Di akun anggota, Security Hub hanya menghasilkan temuan untuk sumber daya milik anggota. Temuan yang berkaitan dengan jejak organisasi dihasilkan di akun pemilik sumber daya. Anda dapat melihat temuan ini di akun administrator yang didelegasikan Security Hub menggunakan agregasi lintas wilayah.

Untuk alarm, akun saat ini harus memiliki topik Amazon SNS yang direferensikan, atau harus mendapatkan akses ke topik Amazon SNS dengan menelepon. `ListSubscriptionsByTopic` Jika tidak, Security Hub menghasilkan `WARNING` temuan untuk kontrol.

Remediasi

Untuk melewati kontrol ini, ikuti langkah-langkah berikut untuk membuat topik Amazon SNS, AWS CloudTrail jejak, filter metrik, dan alarm untuk filter metrik.

1. Buat topik Amazon SNS. Untuk petunjuknya, lihat Memulai Amazon SNS di Panduan Pengembang Layanan Pemberitahuan Sederhana Amazon. Buat topik yang menerima semua alarm CIS, dan buat setidaknya satu langganan ke topik tersebut.
2. Buat CloudTrail jejak yang berlaku untuk semua Wilayah AWS. Untuk petunjuk, lihat Membuat jejak di Panduan AWS CloudTrail Pengguna.

   Catat nama grup CloudWatch log Log yang Anda kaitkan dengan CloudTrail jejak. Anda membuat filter metrik untuk grup log tersebut di langkah berikutnya.
3. Membuat sebuah filter metrik. Untuk petunjuknya, lihat Membuat filter metrik untuk grup log di Panduan CloudWatch Pengguna Amazon. Gunakan nilai berikut:

Bidang	Nilai
Tentukan pola, Pola filter	`{($.eventSource=s3.amazonaws.com) && (($.eventName=PutBucketAcl) || ($.eventName=PutBucketPolicy) \|\| ($.eventName=PutBucketCors) || ($.eventName=PutBucketLifecycle) \|\| ($.eventName=PutBucketReplication) || ($.eventName=DeleteBucketPolicy) \|\| ($.eventName=DeleteBucketCors) || ($.eventName=DeleteBucketLifecycle) \|\| ($.eventName=DeleteBucketReplication))}`
Namespace metrik	**`LogMetrics`**
Nilai metrik	**`1`**
Nilai default	**`0`**

4. Buat alarm berdasarkan filter. Untuk petunjuknya, lihat Membuat CloudWatch alarm berdasarkan filter metrik grup log di CloudWatch Panduan Pengguna Amazon. Gunakan nilai berikut:

Bidang	Nilai
Kondisi, tipe Ambang	Statis
your-metric-name Kapanpun...	lebih besar/sama
dari...	**1**

[CloudWatch.9] Pastikan filter metrik log dan alarm ada untuk perubahan AWS Config konfigurasi

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v1.2.0/3.9, Tolok Ukur Yayasan CIS v1.4.0/4.9 AWS

Kategori: Deteksi > Layanan deteksi

Tingkat keparahan: Rendah

Jenis sumber daya:`AWS::Logs::MetricFilter`,`AWS::CloudWatch::Alarm`,`AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config aturan: Tidak ada (aturan Security Hub khusus)

Jenis jadwal: Periodik

Parameter: Tidak ada

Anda dapat melakukan pemantauan real-time panggilan API dengan mengarahkan CloudTrail CloudWatch log ke Log dan membuat filter dan alarm metrik yang sesuai.

CIS merekomendasikan agar Anda membuat filter metrik dan alarm untuk perubahan pengaturan AWS Config konfigurasi. Memantau perubahan ini membantu memastikan visibilitas item konfigurasi yang berkelanjutan di akun.

Untuk menjalankan pemeriksaan ini, Security Hub menggunakan logika kustom untuk melakukan langkah-langkah audit yang tepat yang ditentukan untuk kontrol 4.9 di CIS AWS Foundations

Benchmark v1.4.0. Kontrol ini gagal jika filter metrik yang tepat yang ditentukan oleh CIS tidak digunakan. Bidang atau istilah tambahan tidak dapat ditambahkan ke filter metrik.

Note

Ketika Security Hub melakukan pemeriksaan untuk kontrol ini, ia mencari CloudTrail jejak yang digunakan akun saat ini. Jalur ini mungkin merupakan jalur organisasi yang dimiliki oleh akun lain. Jalur Multi-Wilayah juga mungkin berbasis di Wilayah yang berbeda.
Hasil pemeriksaan dalam `FAILED` temuan dalam kasus-kasus berikut:

- Tidak ada jejak yang dikonfigurasi.
- Jalur yang tersedia yang berada di Wilayah saat ini dan yang dimiliki oleh rekening giro tidak memenuhi persyaratan kontrol.

Hasil pemeriksaan dalam status kontrol `NO_DATA` dalam kasus berikut:

- Jejak multi-wilayah berbasis di Wilayah yang berbeda. Security Hub hanya dapat menghasilkan temuan di Wilayah tempat jejak itu berada.
- Jejak multi-wilayah milik akun yang berbeda. Security Hub hanya dapat menghasilkan temuan untuk akun yang memiliki jejak.

  Kami merekomendasikan jejak organisasi untuk mencatat peristiwa dari banyak akun dalam suatu organisasi. Jejak organisasi adalah jalur Multi-wilayah secara default dan hanya dapat dikelola oleh akun AWS Organizations manajemen atau akun administrator yang CloudTrail didelegasikan. Menggunakan jejak organisasi menghasilkan status kontrol `NO_DATA` untuk kontrol yang dievaluasi dalam akun anggota organisasi. Di akun anggota, Security Hub hanya menghasilkan temuan untuk sumber daya milik anggota. Temuan yang berkaitan dengan jejak organisasi dihasilkan di akun pemilik sumber daya. Anda dapat melihat temuan ini di akun administrator yang didelegasikan Security Hub menggunakan agregasi lintas wilayah.

Untuk alarm, akun saat ini harus memiliki topik Amazon SNS yang direferensikan, atau harus mendapatkan akses ke topik Amazon SNS dengan menelepon. `ListSubscriptionsByTopic` Jika tidak, Security Hub menghasilkan `WARNING` temuan untuk kontrol.

Remediasi

Untuk melewati kontrol ini, ikuti langkah-langkah berikut untuk membuat topik Amazon SNS, AWS CloudTrail jejak, filter metrik, dan alarm untuk filter metrik.

1. Buat topik Amazon SNS. Untuk petunjuknya, lihat Memulai Amazon SNS di Panduan Pengembang Layanan Pemberitahuan Sederhana Amazon. Buat topik yang menerima semua alarm CIS, dan buat setidaknya satu langganan ke topik tersebut.
2. Buat CloudTrail jejak yang berlaku untuk semua Wilayah AWS. Untuk petunjuk, lihat Membuat jejak di Panduan AWS CloudTrail Pengguna.

   Catat nama grup CloudWatch log Log yang Anda kaitkan dengan CloudTrail jejak. Anda membuat filter metrik untuk grup log tersebut di langkah berikutnya.
3. Membuat sebuah filter metrik. Untuk petunjuknya, lihat Membuat filter metrik untuk grup log di Panduan CloudWatch Pengguna Amazon. Gunakan nilai berikut:

Bidang	Nilai
Tentukan pola, Pola filter	`{($.eventSource=config.amazonaws.com) && (($.eventName=StopConfigurationRecorder) || ($.eventName=DeleteDeliveryChannel) \|\| ($.eventName=PutDeliveryChannel) || ($.eventName=PutConfigurationRecorder))}`
Namespace metrik	**`LogMetrics`**
Nilai metrik	**`1`**
Nilai default	**`0`**

4. Buat alarm berdasarkan filter. Untuk petunjuknya, lihat Membuat CloudWatch alarm berdasarkan filter metrik grup log di CloudWatch Panduan Pengguna Amazon. Gunakan nilai berikut:

Bidang	Nilai
Kondisi, tipe Ambang	Statis
your-metric-name Kapanpun...	lebih besar/sama
dari...	**1**

[CloudWatch.10] Pastikan filter metrik log dan alarm ada untuk perubahan grup keamanan

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v1.2.0/3.10, Tolok Ukur Yayasan CIS v1.4.0/4.10 AWS

Kategori: Deteksi > Layanan deteksi

Tingkat keparahan: Rendah

Jenis sumber daya:`AWS::Logs::MetricFilter`,`AWS::CloudWatch::Alarm`,`AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config aturan: Tidak ada (aturan Security Hub khusus)

Jenis jadwal: Periodik

Parameter: Tidak ada

Anda dapat melakukan pemantauan real-time panggilan API dengan mengarahkan CloudTrail CloudWatch log ke Log dan membuat filter dan alarm metrik yang sesuai. Grup keamanan adalah filter paket stateful yang mengontrol lalu lintas masuk dan keluar di VPC.

CIS merekomendasikan agar Anda membuat filter metrik dan alarm untuk perubahan pada grup keamanan. Memantau perubahan ini membantu memastikan bahwa sumber daya dan layanan tidak terekspos secara tidak sengaja.

Untuk menjalankan pemeriksaan ini, Security Hub menggunakan logika kustom untuk melakukan langkah-langkah audit yang tepat yang ditentukan untuk kontrol 4.10 di CIS AWS Foundations

Benchmark v1.4.0. Kontrol ini gagal jika filter metrik yang tepat yang ditentukan oleh CIS tidak digunakan. Bidang atau istilah tambahan tidak dapat ditambahkan ke filter metrik.

> **Note**
>
> Ketika Security Hub melakukan pemeriksaan untuk kontrol ini, ia mencari CloudTrail jejak yang digunakan akun saat ini. Jalur ini mungkin merupakan jalur organisasi yang dimiliki oleh akun lain. Jalur Multi-Wilayah juga mungkin berbasis di Wilayah yang berbeda.
> Hasil pemeriksaan dalam `FAILED` temuan dalam kasus-kasus berikut:
>
> - Tidak ada jejak yang dikonfigurasi.
> - Jalur yang tersedia yang berada di Wilayah saat ini dan yang dimiliki oleh rekening giro tidak memenuhi persyaratan kontrol.
>
> Hasil pemeriksaan dalam status kontrol `NO_DATA` dalam kasus berikut:
>
> - Jejak multi-wilayah berbasis di Wilayah yang berbeda. Security Hub hanya dapat menghasilkan temuan di Wilayah tempat jejak itu berada.
> - Jejak multi-wilayah milik akun yang berbeda. Security Hub hanya dapat menghasilkan temuan untuk akun yang memiliki jejak.
>
>   Kami merekomendasikan jejak organisasi untuk mencatat peristiwa dari banyak akun dalam suatu organisasi. Jejak organisasi adalah jalur Multi-wilayah secara default dan hanya dapat dikelola oleh akun AWS Organizations manajemen atau akun administrator yang CloudTrail didelegasikan. Menggunakan jejak organisasi menghasilkan status kontrol `NO_DATA` untuk kontrol yang dievaluasi dalam akun anggota organisasi. Di akun anggota, Security Hub hanya menghasilkan temuan untuk sumber daya milik anggota. Temuan yang berkaitan dengan jejak organisasi dihasilkan di akun pemilik sumber daya. Anda dapat melihat temuan ini di akun administrator yang didelegasikan Security Hub menggunakan agregasi lintas wilayah.
>
> Untuk alarm, akun saat ini harus memiliki topik Amazon SNS yang direferensikan, atau harus mendapatkan akses ke topik Amazon SNS dengan menelepon. `ListSubscriptionsByTopic` Jika tidak, Security Hub menghasilkan `WARNING` temuan untuk kontrol.

Remediasi

Untuk melewati kontrol ini, ikuti langkah-langkah berikut untuk membuat topik Amazon SNS, AWS CloudTrail jejak, filter metrik, dan alarm untuk filter metrik.

1. Buat topik Amazon SNS. Untuk petunjuknya, lihat Memulai Amazon SNS di Panduan Pengembang Layanan Pemberitahuan Sederhana Amazon. Buat topik yang menerima semua alarm CIS, dan buat setidaknya satu langganan ke topik tersebut.
2. Buat CloudTrail jejak yang berlaku untuk semua Wilayah AWS. Untuk petunjuk, lihat Membuat jejak di Panduan AWS CloudTrail Pengguna.

   Catat nama grup CloudWatch log Log yang Anda kaitkan dengan CloudTrail jejak. Anda membuat filter metrik untuk grup log tersebut di langkah berikutnya.
3. Membuat sebuah filter metrik. Untuk petunjuknya, lihat Membuat filter metrik untuk grup log di Panduan CloudWatch Pengguna Amazon. Gunakan nilai berikut:

Bidang	Nilai
Tentukan pola, Pola filter	`{($.eventName=AuthorizeSecurityGroupIngress) \|\| ($.eventName=AuthorizeSecurityGroupEgress) || ($.eventName=RevokeSecurityGroupIngress) \|\| ($.eventName=RevokeSecurityGroupEgress) || ($.eventName=CreateSecurityGroup) \|\| ($.eventName=DeleteSecurityGroup)}`
Namespace metrik	**`LogMetrics`**
Nilai metrik	**`1`**
Nilai default	**`0`**

4. Buat alarm berdasarkan filter. Untuk petunjuknya, lihat Membuat CloudWatch alarm berdasarkan filter metrik grup log di CloudWatch Panduan Pengguna Amazon. Gunakan nilai berikut:

Bidang	Nilai
Kondisi, tipe Ambang	Statis
your-metric-name Kapanpun...	lebih besar/sama
dari...	**1**

[CloudWatch.11] Pastikan filter metrik log dan alarm ada untuk perubahan pada Daftar Kontrol Akses Jaringan (NACL)

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v1.2.0/3.11, Tolok Ukur Yayasan CIS v1.4.0/4.11 AWS

Kategori: Deteksi > Layanan deteksi

Tingkat keparahan: Rendah

Jenis sumber daya:`AWS::Logs::MetricFilter`,`AWS::CloudWatch::Alarm`,`AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config aturan: Tidak ada (aturan Security Hub khusus)

Jenis jadwal: Periodik

Parameter: Tidak ada

Anda dapat melakukan pemantauan real-time panggilan API dengan mengarahkan CloudTrail CloudWatch log ke Log dan membuat filter dan alarm metrik yang sesuai. NACL digunakan sebagai filter paket stateless untuk mengontrol masuknya dan keluar lalu lintas untuk subnet dalam VPC.

CIS merekomendasikan agar Anda membuat filter metrik dan alarm untuk perubahan pada NACL. Memantau perubahan ini membantu memastikan bahwa AWS sumber daya dan layanan tidak terekspos secara tidak sengaja.

Untuk menjalankan pemeriksaan ini, Security Hub menggunakan logika kustom untuk melakukan langkah-langkah audit yang tepat yang ditentukan untuk kontrol 4.11 di CIS AWS Foundations

Benchmark v1.4.0. Kontrol ini gagal jika filter metrik yang tepat yang ditentukan oleh CIS tidak digunakan. Bidang atau istilah tambahan tidak dapat ditambahkan ke filter metrik.

> **Note**
>
> Ketika Security Hub melakukan pemeriksaan untuk kontrol ini, ia mencari CloudTrail jejak yang digunakan akun saat ini. Jalur ini mungkin merupakan jalur organisasi yang dimiliki oleh akun lain. Jalur Multi-Wilayah juga mungkin berbasis di Wilayah yang berbeda.
> Hasil pemeriksaan dalam `FAILED` temuan dalam kasus-kasus berikut:
>
> - Tidak ada jejak yang dikonfigurasi.
> - Jalur yang tersedia yang berada di Wilayah saat ini dan yang dimiliki oleh rekening giro tidak memenuhi persyaratan kontrol.
>
> Hasil pemeriksaan dalam status kontrol `NO_DATA` dalam kasus berikut:
>
> - Jejak multi-wilayah berbasis di Wilayah yang berbeda. Security Hub hanya dapat menghasilkan temuan di Wilayah tempat jejak itu berada.
> - Jejak multi-wilayah milik akun yang berbeda. Security Hub hanya dapat menghasilkan temuan untuk akun yang memiliki jejak.
>
>   Kami merekomendasikan jejak organisasi untuk mencatat peristiwa dari banyak akun dalam suatu organisasi. Jejak organisasi adalah jalur Multi-wilayah secara default dan hanya dapat dikelola oleh akun AWS Organizations manajemen atau akun administrator yang CloudTrail didelegasikan. Menggunakan jejak organisasi menghasilkan status kontrol `NO_DATA` untuk kontrol yang dievaluasi dalam akun anggota organisasi. Di akun anggota, Security Hub hanya menghasilkan temuan untuk sumber daya milik anggota. Temuan yang berkaitan dengan jejak organisasi dihasilkan di akun pemilik sumber daya. Anda dapat melihat temuan ini di akun administrator yang didelegasikan Security Hub menggunakan agregasi lintas wilayah.
>
> Untuk alarm, akun saat ini harus memiliki topik Amazon SNS yang direferensikan, atau harus mendapatkan akses ke topik Amazon SNS dengan menelepon. `ListSubscriptionsByTopic` Jika tidak, Security Hub menghasilkan `WARNING` temuan untuk kontrol.

Remediasi

Untuk melewati kontrol ini, ikuti langkah-langkah berikut untuk membuat topik Amazon SNS, AWS CloudTrail jejak, filter metrik, dan alarm untuk filter metrik.

1. Buat topik Amazon SNS. Untuk petunjuknya, lihat Memulai Amazon SNS di Panduan Pengembang Layanan Pemberitahuan Sederhana Amazon. Buat topik yang menerima semua alarm CIS, dan buat setidaknya satu langganan ke topik tersebut.
2. Buat CloudTrail jejak yang berlaku untuk semua Wilayah AWS. Untuk petunjuk, lihat Membuat jejak di Panduan AWS CloudTrail Pengguna.

   Catat nama grup CloudWatch log Log yang Anda kaitkan dengan CloudTrail jejak. Anda membuat filter metrik untuk grup log tersebut di langkah berikutnya.
3. Membuat sebuah filter metrik. Untuk petunjuknya, lihat Membuat filter metrik untuk grup log di Panduan CloudWatch Pengguna Amazon. Gunakan nilai berikut:

Bidang	Nilai
Tentukan pola, Pola filter	`{($.eventName=CreateNetworkAcl) \|\| ($.eventName=CreateNetworkAclEntry) || ($.eventName=DeleteNetworkAcl) \|\| ($.eventName=DeleteNetworkAclEntry) || ($.eventName=ReplaceNetworkAclEntry) \|\| ($.eventName=ReplaceNetworkAclAssociation)}`
Namespace metrik	**`LogMetrics`**
Nilai metrik	**`1`**
Nilai default	**`0`**

4. Buat alarm berdasarkan filter. Untuk petunjuknya, lihat Membuat CloudWatch alarm berdasarkan filter metrik grup log di CloudWatch Panduan Pengguna Amazon. Gunakan nilai berikut:

Bidang	Nilai
Kondisi, tipe Ambang	Statis
your-metric-name Kapanpun...	lebih besar/sama
dari...	**1**

[CloudWatch.12] Pastikan filter metrik log dan alarm ada untuk perubahan pada gateway jaringan

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v1.2.0/3.12, Tolok Ukur Yayasan CIS v1.4.0/4.12 AWS

Kategori: Deteksi > Layanan deteksi

Tingkat keparahan: Rendah

Jenis sumber daya:`AWS::Logs::MetricFilter`,`AWS::CloudWatch::Alarm`,`AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config aturan: Tidak ada (aturan Security Hub khusus)

Jenis jadwal: Periodik

Parameter: Tidak ada

Anda dapat melakukan pemantauan panggilan API secara real-time dengan mengarahkan CloudTrail CloudWatch log ke Log dan membuat filter dan alarm metrik yang sesuai. Gateway jaringan diperlukan untuk mengirim dan menerima lalu lintas ke tujuan di luar VPC.

CIS merekomendasikan agar Anda membuat filter metrik dan alarm untuk perubahan gateway jaringan. Memantau perubahan ini membantu memastikan bahwa semua lalu lintas masuk dan keluar melintasi perbatasan VPC melalui jalur yang terkendali.

Untuk menjalankan pemeriksaan ini, Security Hub menggunakan logika khusus untuk melakukan langkah-langkah audit yang tepat yang ditentukan untuk kontrol 4.12 di CIS AWS Foundations

Benchmark v1.2. Kontrol ini gagal jika filter metrik yang tepat yang ditentukan oleh CIS tidak digunakan. Bidang atau istilah tambahan tidak dapat ditambahkan ke filter metrik.

> **Note**
>
> Ketika Security Hub melakukan pemeriksaan untuk kontrol ini, ia mencari CloudTrail jejak yang digunakan akun saat ini. Jalur ini mungkin merupakan jalur organisasi yang dimiliki oleh akun lain. Jalur Multi-Wilayah juga mungkin berbasis di Wilayah yang berbeda.
> Hasil pemeriksaan dalam `FAILED` temuan dalam kasus-kasus berikut:
>
> - Tidak ada jejak yang dikonfigurasi.
> - Jalur yang tersedia yang berada di Wilayah saat ini dan yang dimiliki oleh rekening giro tidak memenuhi persyaratan kontrol.
>
> Hasil pemeriksaan dalam status kontrol `NO_DATA` dalam kasus berikut:
>
> - Jejak multi-wilayah berbasis di Wilayah yang berbeda. Security Hub hanya dapat menghasilkan temuan di Wilayah tempat jejak itu berada.
> - Jejak multi-wilayah milik akun yang berbeda. Security Hub hanya dapat menghasilkan temuan untuk akun yang memiliki jejak.
>
>   Kami merekomendasikan jejak organisasi untuk mencatat peristiwa dari banyak akun dalam suatu organisasi. Jejak organisasi adalah jalur Multi-wilayah secara default dan hanya dapat dikelola oleh akun AWS Organizations manajemen atau akun administrator yang CloudTrail didelegasikan. Menggunakan jejak organisasi menghasilkan status kontrol `NO_DATA` untuk kontrol yang dievaluasi dalam akun anggota organisasi. Di akun anggota, Security Hub hanya menghasilkan temuan untuk sumber daya milik anggota. Temuan yang berkaitan dengan jejak organisasi dihasilkan di akun pemilik sumber daya. Anda dapat melihat temuan ini di akun administrator yang didelegasikan Security Hub menggunakan agregasi lintas wilayah.
>
> Untuk alarm, akun saat ini harus memiliki topik Amazon SNS yang direferensikan, atau harus mendapatkan akses ke topik Amazon SNS dengan menelepon. `ListSubscriptionsByTopic` Jika tidak, Security Hub menghasilkan `WARNING` temuan untuk kontrol.

Remediasi

Untuk melewati kontrol ini, ikuti langkah-langkah berikut untuk membuat topik Amazon SNS, AWS CloudTrail jejak, filter metrik, dan alarm untuk filter metrik.

1. Buat topik Amazon SNS. Untuk petunjuk, lihat Memulai Amazon SNS di Panduan Pengembang Layanan Pemberitahuan Sederhana Amazon. Buat topik yang menerima semua alarm CIS, dan buat setidaknya satu langganan ke topik tersebut.
2. Buat CloudTrail jejak yang berlaku untuk semua Wilayah AWS. Untuk petunjuk, lihat Membuat jejak di Panduan AWS CloudTrail Pengguna.

   Catat nama grup CloudWatch log Log yang Anda kaitkan dengan CloudTrail jejak. Anda membuat filter metrik untuk grup log tersebut di langkah berikutnya.
3. Membuat sebuah filter metrik. Untuk petunjuknya, lihat Membuat filter metrik untuk grup log di Panduan CloudWatch Pengguna Amazon. Gunakan nilai berikut:

Bidang	Nilai
Tentukan pola, Pola filter	`{($.eventName=CreateCustomerGateway) \|\| ($.eventName=DeleteCustomerGateway) || ($.eventName=AttachInternetGateway) \|\| ($.eventName=CreateInternetGateway) || ($.eventName=DeleteInternetGateway) \|\| ($.eventName=DetachInternetGateway)}`
Ruang nama metrik	**`LogMetrics`**
Nilai metrik	**`1`**
Nilai default	**`0`**

4. Buat alarm berdasarkan filter. Untuk petunjuknya, lihat Membuat CloudWatch alarm berdasarkan filter metrik grup log di CloudWatch Panduan Pengguna Amazon. Gunakan nilai berikut:

Bidang	Nilai
Kondisi, tipe Ambang	Statis
your-metric-name Kapanpun...	Lebih Besar/Setara
dari...	**1**

[CloudWatch.13] Pastikan filter metrik log dan alarm ada untuk perubahan tabel rute

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v1.2.0/3.13, Tolok Ukur Yayasan CIS v1.4.0/4.13 AWS

Kategori: Deteksi > Layanan deteksi

Tingkat keparahan: Rendah

Jenis sumber daya:`AWS::Logs::MetricFilter`,`AWS::CloudWatch::Alarm`,`AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config aturan: Tidak ada (aturan Security Hub khusus)

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah Anda memantau panggilan API secara real time dengan mengarahkan CloudTrail CloudWatch log ke Log dan membuat filter dan alarm metrik yang sesuai. Tabel routing merutekan lalu lintas jaringan antara subnet dan ke gateway jaringan.

CIS merekomendasikan agar Anda membuat filter metrik dan alarm untuk perubahan pada tabel rute. Memantau perubahan ini membantu memastikan bahwa semua lalu lintas VPC mengalir melalui jalur yang diharapkan.

> **Note**
>
> Ketika Security Hub melakukan pemeriksaan untuk kontrol ini, ia mencari CloudTrail jejak yang digunakan akun saat ini. Jalur ini mungkin merupakan jalur organisasi yang dimiliki oleh akun lain. Jalur Multi-Wilayah juga mungkin berbasis di Wilayah yang berbeda.

Hasil pemeriksaan dalam `FAILED` temuan dalam kasus-kasus berikut:

- Tidak ada jejak yang dikonfigurasi.
- Jalur yang tersedia yang berada di Wilayah saat ini dan yang dimiliki oleh rekening giro tidak memenuhi persyaratan kontrol.

Hasil pemeriksaan dalam status kontrol `NO_DATA` dalam kasus berikut:

- Jejak multi-wilayah berbasis di Wilayah yang berbeda. Security Hub hanya dapat menghasilkan temuan di Wilayah tempat jejak itu berada.
- Jejak multi-wilayah milik akun yang berbeda. Security Hub hanya dapat menghasilkan temuan untuk akun yang memiliki jejak.

  Kami merekomendasikan jejak organisasi untuk mencatat peristiwa dari banyak akun dalam suatu organisasi. Jejak organisasi adalah jalur Multi-wilayah secara default dan hanya dapat dikelola oleh akun AWS Organizations manajemen atau akun administrator yang CloudTrail didelegasikan. Menggunakan jejak organisasi menghasilkan status kontrol `NO_DATA` untuk kontrol yang dievaluasi dalam akun anggota organisasi. Di akun anggota, Security Hub hanya menghasilkan temuan untuk sumber daya milik anggota. Temuan yang berkaitan dengan jejak organisasi dihasilkan di akun pemilik sumber daya. Anda dapat melihat temuan ini di akun administrator yang didelegasikan Security Hub menggunakan agregasi lintas wilayah.

Untuk alarm, akun saat ini harus memiliki topik Amazon SNS yang direferensikan, atau harus mendapatkan akses ke topik Amazon SNS dengan menelepon. `ListSubscriptionsByTopic` Jika tidak, Security Hub menghasilkan `WARNING` temuan untuk kontrol.

Remediasi

> **Note**
>
> Pola filter yang kami rekomendasikan dalam langkah-langkah remediasi ini berbeda dari pola filter dalam panduan CIS. Filter yang kami rekomendasikan hanya menargetkan peristiwa yang berasal dari panggilan API Amazon Elastic Compute Cloud (EC2).

Untuk melewati kontrol ini, ikuti langkah-langkah berikut untuk membuat topik Amazon SNS, AWS CloudTrail jejak, filter metrik, dan alarm untuk filter metrik.

1. Buat topik Amazon SNS. Untuk petunjuk, lihat Memulai Amazon SNS di Panduan Pengembang Layanan Pemberitahuan Sederhana Amazon. Buat topik yang menerima semua alarm CIS, dan buat setidaknya satu langganan ke topik tersebut.
2. Buat CloudTrail jejak yang berlaku untuk semua Wilayah AWS. Untuk petunjuk, lihat Membuat jejak di Panduan AWS CloudTrail Pengguna.

   Catat nama grup CloudWatch log Log yang Anda kaitkan dengan CloudTrail jejak. Anda membuat filter metrik untuk grup log tersebut di langkah berikutnya.
3. Membuat sebuah filter metrik. Untuk petunjuknya, lihat Membuat filter metrik untuk grup log di Panduan CloudWatch Pengguna Amazon. Gunakan nilai berikut:

Bidang	Nilai
Tentukan pola, Pola filter	`{($.eventSource=ec2.amazonaws.com) && (($.eventName=CreateRoute) || ($.eventName=CreateRouteTable) \|\| ($.eventName=ReplaceRoute) || ($.eventName=ReplaceRouteTableAssociation) \|\| ($.eventName=DeleteRouteTable) || ($.eventName=DeleteRoute) \|\| ($.eventName=DisassociateRouteTable))}`
Ruang nama metrik	**`LogMetrics`**
Nilai metrik	**`1`**
Nilai default	**`0`**

4. Buat alarm berdasarkan filter. Untuk petunjuknya, lihat Membuat CloudWatch alarm berdasarkan filter metrik grup log di CloudWatch Panduan Pengguna Amazon. Gunakan nilai berikut:

Bidang	Nilai
Kondisi, tipe Ambang	Statis
your-metric-name Kapanpun...	Lebih Besar/Setara
dari...	**1**

[CloudWatch.14] Pastikan filter metrik log dan alarm ada untuk perubahan VPC

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v1.2.0/3.14, Tolok Ukur Yayasan CIS v1.4.0/4.14 AWS

Kategori: Deteksi > Layanan deteksi

Tingkat keparahan: Rendah

Jenis sumber daya:`AWS::Logs::MetricFilter`,`AWS::CloudWatch::Alarm`,`AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config aturan: Tidak ada (aturan Security Hub khusus)

Jenis jadwal: Periodik

Parameter: Tidak ada

Anda dapat melakukan pemantauan panggilan API secara real-time dengan mengarahkan CloudTrail CloudWatch log ke Log dan membuat filter dan alarm metrik yang sesuai. Anda dapat memiliki lebih dari satu VPC dalam sebuah akun, dan Anda dapat membuat koneksi peer antara dua VPC, memungkinkan lalu lintas jaringan untuk rute antara VPC.

CIS merekomendasikan agar Anda membuat filter metrik dan alarm untuk perubahan pada VPC. Memantau perubahan ini membantu memastikan bahwa kontrol otentikasi dan otorisasi tetap utuh.

Untuk menjalankan pemeriksaan ini, Security Hub menggunakan logika kustom untuk melakukan langkah-langkah audit yang tepat yang ditentukan untuk kontrol 4.14 di CIS AWS Foundations Benchmark v1.4.0. Kontrol ini gagal jika filter metrik yang tepat yang ditentukan oleh CIS tidak digunakan. Bidang atau istilah tambahan tidak dapat ditambahkan ke filter metrik.

Note

Ketika Security Hub melakukan pemeriksaan untuk kontrol ini, ia mencari CloudTrail jejak yang digunakan akun saat ini. Jalur ini mungkin merupakan jalur organisasi yang dimiliki oleh akun lain. Jalur Multi-Wilayah juga mungkin berbasis di Wilayah yang berbeda.
Hasil pemeriksaan dalam `FAILED` temuan dalam kasus-kasus berikut:

- Tidak ada jejak yang dikonfigurasi.
- Jalur yang tersedia yang berada di Wilayah saat ini dan yang dimiliki oleh rekening giro tidak memenuhi persyaratan kontrol.

Hasil pemeriksaan dalam status kontrol `NO_DATA` dalam kasus berikut:

- Jejak multi-wilayah berbasis di Wilayah yang berbeda. Security Hub hanya dapat menghasilkan temuan di Wilayah tempat jejak itu berada.
- Jejak multi-wilayah milik akun yang berbeda. Security Hub hanya dapat menghasilkan temuan untuk akun yang memiliki jejak.

  Kami merekomendasikan jejak organisasi untuk mencatat peristiwa dari banyak akun dalam suatu organisasi. Jejak organisasi adalah jalur Multi-wilayah secara default dan hanya dapat dikelola oleh akun AWS Organizations manajemen atau akun administrator yang CloudTrail didelegasikan. Menggunakan jejak organisasi menghasilkan status kontrol `NO_DATA` untuk kontrol yang dievaluasi dalam akun anggota organisasi. Di akun anggota, Security Hub hanya menghasilkan temuan untuk sumber daya milik anggota. Temuan yang berkaitan dengan jejak organisasi dihasilkan di akun pemilik sumber daya. Anda dapat melihat temuan ini di akun administrator yang didelegasikan Security Hub menggunakan agregasi lintas wilayah.

Untuk alarm, akun saat ini harus memiliki topik Amazon SNS yang direferensikan, atau harus mendapatkan akses ke topik Amazon SNS dengan menelepon. `ListSubscriptionsByTopic` Jika tidak, Security Hub menghasilkan `WARNING` temuan untuk kontrol.

Remediasi

Untuk melewati kontrol ini, ikuti langkah-langkah berikut untuk membuat topik Amazon SNS, AWS CloudTrail jejak, filter metrik, dan alarm untuk filter metrik.

1. Buat topik Amazon SNS. Untuk petunjuk, lihat Memulai Amazon SNS di Panduan Pengembang Layanan Pemberitahuan Sederhana Amazon. Buat topik yang menerima semua alarm CIS, dan buat setidaknya satu langganan ke topik tersebut.
2. Buat CloudTrail jejak yang berlaku untuk semua Wilayah AWS. Untuk petunjuk, lihat Membuat jejak di Panduan AWS CloudTrail Pengguna.

   Catat nama grup CloudWatch log Log yang Anda kaitkan dengan CloudTrail jejak. Anda membuat filter metrik untuk grup log tersebut di langkah berikutnya.
3. Membuat sebuah filter metrik. Untuk petunjuknya, lihat Membuat filter metrik untuk grup log di Panduan CloudWatch Pengguna Amazon. Gunakan nilai berikut:

Bidang	Nilai
Tentukan pola, Pola filter	`{($.eventName=CreateVpc) \|\| ($.eventName=DeleteVpc) || ($.eventName=ModifyVpcAttribute) \|\| ($.eventName=AcceptVpcPeeringConnection) || ($.eventName=CreateVpcPeeringConnection) \|\| ($.eventName=DeleteVpcPeeringConnection) || ($.eventName=RejectVpcPeeringConnection) \|\| ($.eventName=AttachClassicLinkVpc) || ($.eventName=DetachClassicLinkVpc) \|\| ($.eventName=DisableVpcClassicLink) || ($.eventName=EnableVpcClassicLink)}`
Ruang nama metrik	**`LogMetrics`**

Bidang	Nilai
Nilai metrik	**1**
Nilai default	**0**

4. Buat alarm berdasarkan filter. Untuk petunjuknya, lihat Membuat CloudWatch alarm berdasarkan filter metrik grup log di CloudWatch Panduan Pengguna Amazon. Gunakan nilai berikut:

Bidang	Nilai
Kondisi, tipe Ambang	Statis
Setiap *your-metric-name* kali...	Lebih Besar/Setara
dari...	**1**

[CloudWatch.15] CloudWatch alarm harus memiliki tindakan tertentu yang dikonfigurasi

Kategori: Deteksi > Layanan deteksi

Persyaratan terkait: Nist.800-53.R5 AU-6 (1), Nist.800-53.R5 AU-6 (5), Nist.800-53.r5 CA-7, Nist.800-53.r5 IR-4 (1), Nist.800-53.r5 IR-4 (5), Nist.800-53.r5 SI-2, Nist.800-53.r5 SI-2, Nist.800-53.r5 00-53.R5 SI-20, NIST.800-53.R5 SI-4 (12), NIST.800-53.R5 SI-4 (5)

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::CloudWatch::Alarm`

AWS Config aturan: **`cloudwatch-alarm-action-check`**

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`alarmActionRequired`	Kontrol menghasilkan `PASSED` temuan jika parameter disetel ke `true` dan alarm memiliki tindakan ketika status alarm berubah menjadi`ALARM`.	Boolean	Tidak dapat disesuaikan	`true`
`insufficientDataActionRequired`	Kontrol menghasilkan `PASSED` temuan jika parameter disetel ke `true` dan alarm memiliki tindakan ketika status alarm berubah menjadi`INSUFFICIENT_DATA` .	Boolean	`true` atau `false`	`false`
`okActionRequired`	Kontrol menghasilkan `PASSED` temuan jika parameter disetel ke `true` dan alarm memiliki tindakan ketika status alarm berubah menjadi`OK`.	Boolean	`true` atau `false`	`false`

Kontrol ini memeriksa apakah CloudWatch alarm Amazon memiliki setidaknya satu tindakan yang dikonfigurasi untuk `ALARM` status tersebut. Kontrol gagal jika alarm tidak memiliki tindakan yang dikonfigurasi untuk `ALARM` status. Secara opsional, Anda dapat menyertakan nilai parameter khusus untuk juga memerlukan tindakan alarm untuk `OK` status `INSUFFICIENT_DATA` atau.

> **Note**
>
> Security Hub mengevaluasi kontrol ini berdasarkan alarm CloudWatch metrik. Alarm metrik dapat menjadi bagian dari alarm komposit yang memiliki tindakan yang ditentukan dikonfigurasi. Kontrol menghasilkan `FAILED` temuan dalam kasus-kasus berikut:
>
> - Tindakan yang ditentukan tidak dikonfigurasi untuk alarm metrik.

- Alarm metrik adalah bagian dari alarm komposit yang memiliki tindakan yang ditentukan dikonfigurasi.

Kontrol ini berfokus pada apakah CloudWatch alarm memiliki tindakan alarm yang dikonfigurasi, sedangkan CloudWatch.17 berfokus pada status aktivasi tindakan CloudWatch alarm.

Kami merekomendasikan tindakan CloudWatch alarm untuk secara otomatis mengingatkan Anda ketika metrik yang dipantau berada di luar ambang batas yang ditentukan. Memantau alarm membantu Anda mengidentifikasi aktivitas yang tidak biasa dan dengan cepat menanggapi masalah keamanan dan operasional ketika alarm masuk ke keadaan tertentu. Jenis tindakan alarm yang paling umum adalah memberi tahu satu atau beberapa pengguna dengan mengirim pesan ke topik Amazon Simple Notification Service (Amazon SNS).

Remediasi

Untuk informasi tentang tindakan yang didukung oleh CloudWatch alarm, lihat Tindakan alarm di Panduan CloudWatch Pengguna Amazon.

[CloudWatch.16] grup CloudWatch log harus dipertahankan untuk jangka waktu tertentu

Kategori: Identifikasi > Logging

Persyaratan terkait: Nist.800-53.R5 AU-10, Nist.800-53.R5 AU-11, Nist.800-53.R5 AU-6 (3), Nist.800-53.R5 AU-6 (4), Nist.800-53.R5 CA-7, Nist.800-53.R5 SI-12

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::Logs::LogGroup`

AWS Config aturan: **`cw-loggroup-retention-period-check`**

Jenis jadwal: Periodik

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub	
`minRetentionTime`	Periode retensi minimum dalam beberapa hari untuk grup CloudWatch log	Enum	`365`, `400`, `545`, `731`, `1827`, `3653`	`365`	

Kontrol ini memeriksa apakah grup CloudWatch log Amazon memiliki periode retensi setidaknya dalam jumlah hari yang ditentukan. Kontrol gagal jika periode retensi kurang dari jumlah yang ditentukan. Kecuali Anda memberikan nilai parameter khusus untuk periode retensi, Security Hub menggunakan nilai default 365 hari.

CloudWatch Log memusatkan log dari semua sistem, aplikasi, dan Layanan AWS dalam satu layanan yang sangat skalabel. Anda dapat menggunakan CloudWatch Log untuk memantau, menyimpan, dan mengakses file log dari instans Amazon Elastic Compute Cloud (EC2), Amazon Route 53 AWS CloudTrail, dan sumber lainnya. Mempertahankan log Anda setidaknya selama 1 tahun dapat membantu Anda mematuhi standar penyimpanan log.

Remediasi

Untuk mengonfigurasi setelan penyimpanan log, lihat Mengubah penyimpanan data CloudWatch log di Log di Panduan CloudWatch Pengguna Amazon.

[CloudWatch.17] tindakan CloudWatch alarm harus diaktifkan

Kategori: Deteksi > Layanan deteksi

Persyaratan terkait: Nist.800-53.R5 AU-6 (1), Nist.800-53.R5 AU-6 (5), Nist.800-53.R5 CA-7, Nist.800-53.R5 SI-2, Nist.800-53.R5 SI-4 (12)

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::CloudWatch::Alarm`

AWS Config aturan: **`cloudwatch-alarm-action-enabled-check`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah tindakan CloudWatch alarm diaktifkan (`ActionEnabled`harus disetel ke true). Kontrol gagal jika tindakan alarm untuk CloudWatch alarm dinonaktifkan.

> **Note**
>
> Security Hub mengevaluasi kontrol ini berdasarkan alarm CloudWatch metrik. Alarm metrik dapat menjadi bagian dari alarm komposit yang mengaktifkan tindakan alarm. Kontrol menghasilkan `FAILED` temuan dalam kasus-kasus berikut:
>
> - Tindakan yang ditentukan tidak dikonfigurasi untuk alarm metrik.
> - Alarm metrik adalah bagian dari alarm komposit yang mengaktifkan tindakan alarm.

Kontrol ini berfokus pada status aktivasi tindakan CloudWatch alarm, sedangkan CloudWatch.15 berfokus pada apakah `ALARM` tindakan apa pun dikonfigurasi dalam CloudWatch alarm.

Tindakan alarm secara otomatis mengingatkan Anda ketika metrik yang dipantau berada di luar ambang batas yang ditentukan. Jika tindakan alarm dinonaktifkan, tidak ada tindakan yang dijalankan saat alarm berubah status, dan Anda tidak akan diberitahu tentang perubahan dalam metrik yang dipantau. Sebaiknya aktifkan tindakan CloudWatch alarm untuk membantu Anda merespons masalah keamanan dan operasional dengan cepat.

Remediasi

Untuk mengaktifkan aksi CloudWatch alarm (konsol)

1. Buka CloudWatch konsol di https://console.aws.amazon.com/cloudwatch/.
2. Di panel navigasi, di bawah Alarm, pilih Semua alarm.
3. Pilih alarm yang ingin Anda aktifkan tindakan.
4. Untuk Tindakan, pilih Tindakan alarm — baru, lalu pilih Aktifkan.

Untuk informasi selengkapnya tentang mengaktifkan tindakan CloudWatch alarm, lihat Tindakan alarm di Panduan CloudWatch Pengguna Amazon.

AWS CodeArtifact kontrol

Kontrol ini terkait dengan CodeArtifact sumber daya.

Kontrol ini mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[CodeArtifact.1] CodeArtifact repositori harus diberi tag

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::CodeArtifact::Repository`

AWS Config aturan: `tagged-codeartifact-repository` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList	Daftar tag yang memenuhi AWS persyaratan	Tidak ada nilai default

Kontrol ini memeriksa apakah AWS CodeArtifact repositori memiliki tag dengan kunci tertentu yang ditentukan dalam parameter. `requiredTagKeys` Kontrol gagal jika repositori tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter. `requiredTagKeys` Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika repositori tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik,

lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke CodeArtifact repositori, lihat Tag repositori CodeArtifact di Panduan Pengguna.AWS CodeArtifact

AWS CodeBuild kontrol

Kontrol ini terkait dengan CodeBuild sumber daya.

Kontrol ini mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[CodeBuild.1] URL repositori sumber CodeBuild Bitbucket tidak boleh berisi kredensyal sensitif

Persyaratan terkait: PCI DSS v3.2.1/8.2.1, NIST.800-53.R5 SA-3

Kategori: Lindungi > Pengembangan aman

Tingkat keparahan: Kritis

Jenis sumber daya: `AWS::CodeBuild::Project`

AWS Config aturan: **`codebuild-project-source-repo-url-check`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah URL repositori sumber Bitbucket AWS CodeBuild proyek berisi token akses pribadi atau nama pengguna dan kata sandi. Kontrol gagal jika URL repositori sumber Bitbucket berisi token akses pribadi atau nama pengguna dan kata sandi.

> **Note**
>
> Kontrol ini mengevaluasi sumber primer dan sumber sekunder dari proyek CodeBuild pembangunan. Untuk informasi selengkapnya tentang sumber proyek, lihat Beberapa sumber input dan sampel artefak keluaran di Panduan AWS CodeBuild Pengguna.

Kredensi login tidak boleh disimpan atau ditransmisikan dalam teks yang jelas atau muncul di URL repositori sumber. Alih-alih token akses pribadi atau kredensyal masuk, Anda harus mengakses penyedia sumber Anda CodeBuild, dan mengubah URL repositori sumber Anda agar hanya berisi jalur ke lokasi repositori Bitbucket. Menggunakan token akses pribadi atau kredensyal masuk dapat mengakibatkan paparan data yang tidak diinginkan atau akses yang tidak sah.

Remediasi

Anda dapat memperbarui CodeBuild proyek Anda untuk menggunakan OAuth.

Untuk menghapus otentikasi dasar/(GitHub) Token Akses Pribadi dari sumber CodeBuild proyek

1. Buka CodeBuild konsol di https://console.aws.amazon.com/codebuild/.
2. Pilih proyek build yang berisi token akses pribadi atau nama pengguna dan kata sandi.
3. Dari Edit, pilih Sumber.
4. Pilih Putuskan sambungan GitHub dari/Bitbucket.
5. Pilih Connect menggunakan OAuth, lalu pilih Connect to GitHub/Bitbucket.
6. Saat diminta, pilih otorisasi yang sesuai.
7. Konfigurasikan ulang URL repositori Anda dan pengaturan konfigurasi tambahan, sesuai kebutuhan.

8. Pilih Perbarui sumber.

Untuk informasi selengkapnya, lihat CodeBuild menggunakan sampel berbasis kasus di AWS CodeBuild Panduan Pengguna.

[CodeBuild.2] variabel lingkungan CodeBuild proyek tidak boleh berisi kredensil teks yang jelas

Persyaratan terkait: PCI DSS v3.2.1/8.2.1, NIST.800-53.R5 IA-5 (7), NIST.800-53.R5 SA-3

Kategori: Lindungi > Pengembangan aman

Tingkat keparahan: Kritis

Jenis sumber daya: `AWS::CodeBuild::Project`

AWS Config aturan: **`codebuild-project-envvar-awscred-check`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah proyek berisi variabel lingkungan `AWS_ACCESS_KEY_ID` dan`AWS_SECRET_ACCESS_KEY`.

Kredensyal otentikasi `AWS_ACCESS_KEY_ID` dan tidak `AWS_SECRET_ACCESS_KEY` boleh disimpan dalam teks yang jelas, karena ini dapat menyebabkan paparan data yang tidak diinginkan dan akses yang tidak sah.

Remediasi

Untuk menghapus variabel lingkungan dari CodeBuild proyek, lihat Mengubah setelan proyek build AWS CodeBuild di Panduan AWS CodeBuild Pengguna. Pastikan tidak ada yang dipilih untuk variabel Lingkungan.

Anda dapat menyimpan variabel lingkungan dengan nilai sensitif di AWS Systems Manager Parameter Store atau AWS Secrets Manager kemudian mengambilnya dari spesifikasi build Anda. Untuk petunjuk, lihat kotak berlabel Penting di bagian Lingkungan di Panduan AWS CodeBuild Pengguna.

[CodeBuild.3] Log CodeBuild S3 harus dienkripsi

Persyaratan terkait: Nist.800-53.R5 CA-9 (1), Nist.800-53.R5 CM-3 (6), Nist.800-53.r5 SC-13, Nist.800-53.r5 SC-28, Nist.800-53.r5 SC-28 (1), Nist.800-53.r5 SI-7 (6)

Kategori: Lindungi > Perlindungan Data > Enkripsi data-at-rest

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::CodeBuild::Project`

AWS Config aturan: **`codebuild-project-s3-logs-encrypted`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah log Amazon S3 untuk AWS CodeBuild proyek dienkripsi. Kontrol gagal jika enkripsi dinonaktifkan untuk log S3 untuk sebuah CodeBuild proyek.

Enkripsi data saat istirahat adalah praktik terbaik yang disarankan untuk menambahkan lapisan manajemen akses di sekitar data Anda. Mengenkripsi log saat istirahat mengurangi risiko bahwa pengguna yang tidak diautentikasi oleh AWS akan mengakses data yang disimpan pada disk. Ini menambahkan satu set kontrol akses untuk membatasi kemampuan pengguna yang tidak sah untuk mengakses data.

Remediasi

Untuk mengubah setelan enkripsi log S3 CodeBuild proyek, lihat Mengubah setelan proyek build AWS CodeBuild di Panduan AWS CodeBuild Pengguna.

[CodeBuild.4] lingkungan CodeBuild proyek harus memiliki urasi logging AWS Config

Persyaratan terkait: Nist.800-53.r5 AC-2 (12), Nist.800-53.r5 AC-2 (4), Nist.800-53.r5 AC-4 (26), Nist.800-53.r5 AC-6 (9), Nist.800-53.r5 AU-10, Nist.800-53.r5 AU-12, Nist.800-800-53.r5 AU-2, NIST.800-53.R5 AU-3, NIST.800-53.R5 AU-6 (3), Nist.800-53.r5 AU-6 (4), Nist.800-53.r5 AU-9 (7), Nist.800-53.r5 CA-7, Nist.800-53.r5 SC-7 (9), Nist.800-53.r5 SC-7 (9), Nist.800-53.r5 ST.800-53.R5 SI-3 (8), NIST.800-53.R5 SI-4, NIST.800-53.R5 SI-4 (20), NIST.800-53.R5 SI-7 (8)

Kategori: Identifikasi > Logging

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::CodeBuild::Project`

AWS Config aturan: **`codebuild-project-logging-enabled`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah lingkungan CodeBuild proyek memiliki setidaknya satu opsi log, baik untuk S3 atau CloudWatch log diaktifkan. Kontrol ini gagal jika lingkungan CodeBuild proyek tidak memiliki setidaknya satu opsi log diaktifkan.

Dari perspektif keamanan, logging adalah fitur penting untuk memungkinkan upaya forensik masa depan dalam kasus insiden keamanan apa pun. Mengkorelasikan anomali dalam CodeBuild proyek dengan deteksi ancaman dapat meningkatkan kepercayaan pada keakuratan deteksi ancaman tersebut.

Remediasi

Untuk informasi selengkapnya tentang cara mengonfigurasi setelan log CodeBuild proyek, lihat Membuat proyek build (konsol) di Panduan CodeBuild Pengguna.

[CodeBuild.5] lingkungan CodeBuild proyek seharusnya tidak mengaktifkan mode istimewa

> **Important**
>
> Security Hub menghentikan kontrol ini pada April 2024. Untuk informasi selengkapnya, lihat Ubah log untuk kontrol Security Hub.

Persyaratan terkait: Nist.800-53.r5 AC-2 (1), Nist.800-53.r5 AC-3, Nist.800-53.r5 AC-3 (15), Nist.800-53.r5 AC-3 (7), Nist.800-53.r5 AC-5, Nist.800-53.r5 AC-6, Nist.800-800-53.r5 AC-6 (10), NIST.800-53.R5 AC-6 (2)

Kategori: Lindungi > Manajemen Akses Aman

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::CodeBuild::Project`

AWS Config aturan: **`codebuild-project-environment-privileged-check`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah lingkungan AWS CodeBuild proyek memiliki mode istimewa yang diaktifkan atau dinonaktifkan. Kontrol gagal jika lingkungan CodeBuild proyek memiliki mode istimewa yang diaktifkan.

Secara default, kontainer Docker tidak mengizinkan akses ke perangkat apa pun. Mode istimewa memberikan akses container Docker proyek build ke semua perangkat. Pengaturan `privilegedMode` dengan nilai `true` memungkinkan daemon Docker berjalan di dalam wadah Docker. Daemon Docker mendengarkan permintaan API Docker dan mengelola objek Docker seperti gambar, wadah, jaringan, dan volume. Parameter ini hanya boleh disetel ke true jika proyek build digunakan untuk membangun image Docker. Jika tidak, pengaturan ini harus dinonaktifkan untuk mencegah akses yang tidak diinginkan ke API Docker serta perangkat keras yang mendasarinya. Pengaturan `privilegedMode` untuk `false` membantu melindungi sumber daya penting dari gangguan dan penghapusan.

Remediasi

Untuk mengonfigurasi pengaturan lingkungan CodeBuild proyek, lihat Membuat proyek build (konsol) di Panduan CodeBuild Pengguna. Di bagian Lingkungan, jangan pilih pengaturan Privileged.

AWS Config kontrol

Kontrol ini terkait dengan AWS Config sumber daya.

Kontrol ini mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[Config.1] AWS Config harus diaktifkan dan menggunakan peran terkait layanan untuk perekaman sumber daya

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v1.2.0/2.5, Tolok Ukur Yayasan CIS v1.4.0/3.5, Tolok Ukur AWS Yayasan CIS v3.0.0/3.3, NIST.800-53.R5 CM-3, NIST.800-53.r5 AWS CM-6 (1), NIST.800-53.R5 CM-8 (2), PCI DSS v3.2.1/10.5.2, PCI DSS v3.2.1/11.5

Kategori: Identifikasi > Persediaan

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::::Account`

AWS Config aturan: Tidak ada (aturan Security Hub khusus)

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah AWS Config diaktifkan di akun Anda saat ini Wilayah AWS, mencatat semua sumber daya yang sesuai dengan kontrol yang diaktifkan di Wilayah saat ini, dan menggunakan peran terkait layanan AWS Config. Jika Anda tidak menggunakan peran terkait layanan, kontrol gagal karena peran lain mungkin tidak memiliki izin yang diperlukan AWS Config untuk merekam sumber daya Anda secara akurat.

AWS Config Layanan ini melakukan manajemen konfigurasi AWS sumber daya yang didukung di akun Anda dan mengirimkan file log kepada Anda. Informasi yang direkam mencakup item konfigurasi (AWS sumber daya), hubungan antara item konfigurasi, dan perubahan konfigurasi apa pun dalam sumber daya. Sumber daya global adalah sumber daya yang tersedia di Wilayah mana pun.

Kontrol dievaluasi sebagai berikut:

- Jika Wilayah saat ini ditetapkan sebagai Wilayah agregasi Anda, kontrol menghasilkan `PASSED` temuan hanya jika sumber daya global AWS Identity and Access Management (IAM) direkam (jika Anda telah mengaktifkan kontrol yang memerlukannya).
- Jika Wilayah saat ini ditetapkan sebagai Wilayah tertaut, kontrol tidak mengevaluasi apakah sumber daya global IAM dicatat.
- Jika Wilayah saat ini tidak ada dalam agregator Anda, atau jika agregasi lintas wilayah tidak diatur di akun Anda, kontrol akan menghasilkan `PASSED` temuan hanya jika sumber daya global IAM direkam (jika Anda telah mengaktifkan kontrol yang memerlukannya).

Hasil kontrol tidak terpengaruh oleh apakah Anda memilih pencatatan harian atau terus menerus dari perubahan status sumber daya di AWS Config. Namun, hasil kontrol ini dapat berubah ketika kontrol baru dirilis jika Anda telah mengonfigurasi pengaktifan otomatis kontrol baru atau memiliki kebijakan konfigurasi pusat yang secara otomatis mengaktifkan kontrol baru. Dalam kasus ini, jika Anda tidak

merekam semua sumber daya, Anda harus mengonfigurasi rekaman untuk sumber daya yang terkait dengan kontrol baru untuk menerima `PASSED` temuan.

Pemeriksaan keamanan Security Hub berfungsi sebagaimana dimaksud hanya jika Anda mengaktifkan AWS Config di semua Wilayah dan mengonfigurasi perekaman sumber daya untuk kontrol yang memerlukannya.

> **Note**
>
> Config.1 mengharuskan itu AWS Config diaktifkan di semua Wilayah tempat Anda menggunakan Security Hub.
> Karena Security Hub adalah layanan Regional, pemeriksaan yang dilakukan untuk kontrol ini hanya mengevaluasi Wilayah saat ini untuk akun tersebut.
> Untuk mengizinkan pemeriksaan keamanan terhadap sumber daya global IAM di suatu Wilayah, Anda harus mencatat sumber daya global IAM di Wilayah tersebut. Wilayah yang tidak memiliki sumber daya global IAM yang direkam akan menerima `PASSED` temuan default untuk kontrol yang memeriksa sumber daya global IAM. Karena sumber daya global IAM identik Wilayah AWS, kami sarankan Anda merekam sumber daya global IAM hanya di Wilayah asal (jika agregasi lintas wilayah diaktifkan di akun Anda). Sumber daya IAM hanya akan direkam di Wilayah di mana perekaman sumber daya global dihidupkan.
> Jenis sumber daya yang direkam secara global IAM yang AWS Config mendukung adalah pengguna IAM, grup, peran, dan kebijakan yang dikelola pelanggan. Anda dapat mempertimbangkan untuk menonaktifkan kontrol Security Hub yang memeriksa jenis sumber daya ini di Wilayah tempat perekaman sumber daya global dinonaktifkan. Untuk informasi selengkapnya, lihat Kontrol Security Hub yang mungkin ingin Anda nonaktifkan.

Remediasi

Untuk daftar sumber daya mana yang harus direkam untuk setiap kontrol, lihatAWS Config sumber daya yang dibutuhkan untuk menghasilkan temuan kontrol.

Di Wilayah dan Wilayah asal yang bukan merupakan bagian dari agregator, catat semua sumber daya yang diperlukan untuk kontrol yang diaktifkan di Wilayah saat ini, termasuk sumber daya global IAM jika Anda telah mengaktifkan kontrol yang memerlukan sumber daya global IAM.

Di Wilayah tertaut, Anda dapat menggunakan mode AWS Config perekaman apa pun, selama Anda merekam semua sumber daya yang sesuai dengan kontrol yang diaktifkan di Wilayah saat ini. Di

Wilayah tertaut, jika Anda mengaktifkan kontrol yang memerlukan perekaman sumber daya global IAM, Anda tidak akan menerima `FAILED` temuan (rekaman sumber daya lainnya sudah cukup).

Untuk mengaktifkan AWS Config dan mengonfigurasinya untuk merekam sumber daya, lihat Menyiapkan AWS Config dengan konsol di Panduan AWS Config Pengembang. Anda juga dapat menggunakan AWS CloudFormation template untuk mengotomatiskan proses ini. Untuk informasi selengkapnya, lihat AWS CloudFormation StackSets contoh templat di Panduan AWS CloudFormation Pengguna.

Kontrol Firehose Data Amazon

Kontrol ini terkait dengan sumber daya Amazon Data Firehose.

Kontrol ini mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[DataFirehose.1] Aliran pengiriman Firehose harus dienkripsi saat istirahat

Persyaratan terkait: Nist.800-53.r5 AC-3, Nist.800-53.R5 AU-3, Nist.800-53.R5 SC-12, Nist.800-53.r5 SC-13, Nist.800-53.r5 SC-28

Kategori: Lindungi > Perlindungan Data > Enkripsi data-at-rest

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::KinesisFirehose::DeliveryStream`

AWS Config aturan: **`kinesis-firehose-delivery-stream-encrypted`**

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah aliran pengiriman Amazon Data Firehose dienkripsi saat istirahat dengan enkripsi sisi server. Kontrol ini gagal jika aliran pengiriman Firehose tidak dienkripsi saat istirahat dengan enkripsi sisi server.

Enkripsi sisi server adalah fitur dalam aliran pengiriman Amazon Data Firehose yang secara otomatis mengenkripsi data sebelum diam dengan menggunakan kunci yang dibuat di (). AWS Key Management Service AWS KMS Data dienkripsi sebelum ditulis ke lapisan penyimpanan aliran Firehose Data, dan didekripsi setelah diambil dari penyimpanan. Ini memungkinkan Anda untuk mematuhi persyaratan peraturan dan meningkatkan keamanan data Anda.

Remediasi

Untuk mengaktifkan enkripsi sisi server pada aliran pengiriman Firehose, lihat Perlindungan Data di Amazon Data Firehose di Panduan Pengembang Amazon Data Firehose.

Kontrol Detektif Amazon

Kontrol ini terkait dengan sumber daya Detektif.

Kontrol ini mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[Detective.1] Grafik perilaku detektif harus diberi tag

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::Detective::Graph`

AWS Config aturan: `tagged-detective-graph` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList	Daftar tag yang memenuhi AWS persyaratan	`No default value`

Kontrol ini memeriksa apakah grafik perilaku Detektif Amazon memiliki tag dengan kunci tertentu yang ditentukan dalam parameter. `requiredTagKeys` Kontrol gagal jika grafik perilaku tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya

memeriksa keberadaan kunci tag dan gagal jika grafik perilaku tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke grafik perilaku Detektif, lihat Menambahkan tag ke grafik perilaku di Panduan Administrasi Detektif Amazon.

AWS Database Migration Service kontrol

Kontrol ini terkait dengan AWS DMS sumber daya.

Kontrol ini mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[DMS.1] Instans replikasi Layanan Migrasi Database tidak boleh bersifat publik

Persyaratan terkait: PCI DSS v3.2.1/1.2.1, PCI DSS v3.2.1/1.3.1, PCI DSS v3.2.1/1.3.4, PCI DSS v3.2.1/1.3.2, PCI DSS v3.2.1/1.3.6, Nist.800-53.R5 AC-21, Nist.800-53.r5 AC-3, Nist.800-53.r5 5 AC-3 (7), NIST.800-53.R5 AC-4, NIST.800-53.R5 AC-4 (21), Nist.800-53.r5 AC-6, Nist.800-53.r5

SC-7, Nist.800-53.r5 SC-7 (11), Nist.800-53.r5 SC-7 (16), Nist.800-53.r5 SC-7 (20), NIST.800-53.R5 SC-7 (21), Nist.800-53.r5 SC-7 (3), Nist.800-53.r5 SC-7 (4), Nist.800-53.r5 SC-7 (9)

Kategori: Lindungi > Konfigurasi jaringan aman

Tingkat keparahan: Kritis

Jenis sumber daya: `AWS::DMS::ReplicationInstance`

AWS Config aturan: **`dms-replication-not-public`**

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah instance AWS DMS replikasi bersifat publik. Untuk melakukan ini, ia memeriksa nilai `PubliclyAccessible` bidang.

Instance replikasi pribadi memiliki alamat IP pribadi yang tidak dapat Anda akses di luar jaringan replikasi. Sebuah contoh replikasi harus memiliki alamat IP pribadi ketika database sumber dan target berada dalam jaringan yang sama. Jaringan juga harus terhubung ke VPC instance replikasi menggunakan VPN AWS Direct Connect,, atau VPC peering. Untuk mempelajari lebih lanjut tentang instans replikasi publik dan pribadi, lihat Instans replikasi publik dan pribadi di Panduan Pengguna.AWS Database Migration Service

Anda juga harus memastikan bahwa akses ke konfigurasi AWS DMS instans terbatas hanya untuk pengguna yang berwenang. Untuk melakukan ini, batasi izin IAM pengguna untuk mengubah AWS DMS pengaturan dan sumber daya.

Remediasi

Anda tidak dapat mengubah pengaturan akses publik untuk instance replikasi DMS setelah membuatnya. Untuk mengubah setelan akses publik, hapus instans Anda saat ini, lalu buat ulang. Jangan pilih opsi yang dapat diakses publik.

[DMS.2] Sertifikat DMS harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::DMS::Certificate`

AWS Config aturan: `tagged-dms-certificate` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList	Daftar tag yang memenuhi AWS persyaratan	`No default value`

Kontrol ini memeriksa apakah AWS DMS sertifikat memiliki tag dengan kunci spesifik yang ditentukan dalam parameter`requiredTagKeys`. Kontrol gagal jika sertifikat tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika sertifikat tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS

Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke sertifikat DMS, lihat Menandai sumber daya AWS Database Migration Service di AWS Database Migration Service Panduan Pengguna.

[DMS.3] Langganan acara DMS harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::DMS::EventSubscription`

AWS Config aturan: `tagged-dms-eventsubscription` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList	Daftar tag yang memenuhi AWS persyaratan	`No default value`

Kontrol ini memeriksa apakah langganan AWS DMS acara memiliki tag dengan kunci tertentu yang ditentukan dalam parameter`requiredTagKeys`. Kontrol gagal jika langganan acara tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika langganan acara tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke langganan acara DMS, lihat Menandai sumber daya AWS Database Migration Service di AWS Database Migration Service Panduan Pengguna.

[DMS.4] Contoh replikasi DMS harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::DMS::ReplicationInstance`

AWS Config aturan: `tagged-dms-replicationinstance` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList	Daftar tag yang memenuhi AWS persyaratan	`No default value`

Kontrol ini memeriksa apakah instance AWS DMS replikasi memiliki tag dengan kunci spesifik yang ditentukan dalam parameter`requiredTagKeys`. Kontrol gagal jika instance replikasi tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika instance replikasi tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke instance replikasi DMS, lihat Menandai sumber daya AWS Database Migration Service di Panduan Pengguna.AWS Database Migration Service

[DMS.5] Grup subnet replikasi DMS harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::DMS::ReplicationSubnetGroup`

AWS Config aturan: `tagged-dms-replicationsubnetgroup` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList	Daftar tag yang memenuhi AWS persyaratan	`No default value`

Kontrol ini memeriksa apakah grup subnet AWS DMS replikasi memiliki tag dengan kunci tertentu yang ditentukan dalam parameter. `requiredTagKeys` Kontrol gagal jika grup subnet replikasi tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter. `requiredTagKeys` Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika grup subnet replikasi tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik,

lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke grup subnet replikasi DMS, lihat Menandai sumber daya AWS Database Migration Service di Panduan Pengguna.AWS Database Migration Service

[DMS.6] Instans replikasi DMS harus mengaktifkan peningkatan versi minor otomatis

Persyaratan terkait: NIST.800-53.R5 SI-2, NIST.800-53.R5 SI-2 (2), NIST.800-53.R5 SI-2 (4), Nist.800-53.R5 SI-2 (5)

Kategori: Identifikasi > Kerentanan, tambalan, dan manajemen versi

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::DMS::ReplicationInstance`

AWS Config aturan: **`dms-auto-minor-version-upgrade-check`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah upgrade versi minor otomatis diaktifkan untuk instance AWS DMS replikasi. Kontrol gagal jika upgrade versi minor otomatis tidak diaktifkan untuk instance replikasi DMS.

DMS menyediakan upgrade versi minor otomatis ke setiap mesin replikasi yang didukung sehingga Anda dapat menyimpan instance replikasi Anda. up-to-date Versi minor dapat memperkenalkan fitur perangkat lunak baru, perbaikan bug, patch keamanan, dan peningkatan kinerja. Dengan mengaktifkan pemutakhiran versi minor otomatis pada instance replikasi DMS, peningkatan kecil diterapkan secara otomatis selama jendela pemeliharaan atau segera jika opsi Terapkan segera berubah dipilih.

Remediasi

Untuk mengaktifkan upgrade versi minor otomatis pada instance replikasi DMS, lihat Memodifikasi instance replikasi di Panduan Pengguna.AWS Database Migration Service

[DMS.7] Tugas replikasi DMS untuk database target seharusnya mengaktifkan logging

Persyaratan terkait: Nist.800-53.r5 AC-2 (4), Nist.800-53.r5 AC-4 (26), Nist.800-53.r5 AC-6 (9), Nist.800-53.r5 AU-10, Nist.800-53.r5 AU-12, Nist.800-53.r5 AU-2, Nist.800-53.r5 5 AU-3, NIST.800-53.R5 AU-6 (3), NIST.800-53.R5 AU-6 (4), NIST.800-53.R5 CA-7, NIST.800-53.R5 SC-7 (9), NIST.800-53.R5 SI-4 (20), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-4 (20), nistST.800-53.R5 SI-7 (8)

Kategori: Identifikasi > Logging

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::DMS::ReplicationTask`

AWS Config aturan: **`dms-replication-task-targetdb-logging`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah logging diaktifkan dengan tingkat keparahan minimum `LOGGER_SEVERITY_DEFAULT` untuk tugas `TARGET_APPLY` replikasi DMS dan. `TARGET_LOAD` Kontrol gagal jika logging tidak diaktifkan untuk tugas-tugas ini atau jika tingkat keparahan minimum kurang dari`LOGGER_SEVERITY_DEFAULT`.

DMS menggunakan Amazon CloudWatch untuk mencatat informasi selama proses migrasi. Menggunakan pengaturan tugas logging, Anda dapat menentukan aktivitas komponen mana yang dicatat dan berapa banyak informasi yang dicatat. Anda harus menentukan pencatatan untuk tugas-tugas berikut:

- `TARGET_APPLY`— Pernyataan bahasa definisi data dan data (DDL) diterapkan ke database target.
- `TARGET_LOAD`— Data dimuat ke dalam database target.

Logging memainkan peran penting dalam tugas replikasi DMS dengan memungkinkan pemantauan, pemecahan masalah, audit, analisis kinerja, deteksi kesalahan, dan pemulihan, serta analisis historis dan pelaporan. Ini membantu memastikan keberhasilan replikasi data antar database sambil menjaga integritas data dan kepatuhan terhadap persyaratan peraturan. Level logging selain `DEFAULT` jarang diperlukan untuk komponen ini selama pemecahan masalah. Kami merekomendasikan untuk menjaga tingkat logging seperti `DEFAULT` untuk komponen ini kecuali secara khusus diminta untuk mengubahnya AWS Support. Tingkat logging minimal `DEFAULT` memastikan bahwa pesan informasi, peringatan, dan pesan kesalahan ditulis ke log. Kontrol ini memeriksa apakah tingkat logging setidaknya salah satu dari yang berikut untuk tugas replikasi sebelumnya:`LOGGER_SEVERITY_DEFAULT`,, `LOGGER_SEVERITY_DEBUG` atau. `LOGGER_SEVERITY_DETAILED_DEBUG`

Remediasi

Untuk mengaktifkan pencatatan tugas replikasi DMS basis data target, lihat Melihat dan mengelola log AWS DMS tugas di AWS Database Migration Service Panduan Pengguna.

[DMS.8] Tugas replikasi DMS untuk database sumber seharusnya mengaktifkan logging

Persyaratan terkait: Nist.800-53.r5 AC-2 (4), Nist.800-53.r5 AC-4 (26), Nist.800-53.r5 AC-6 (9), Nist.800-53.r5 AU-10, Nist.800-53.r5 AU-12, Nist.800-53.r5 AU-2, Nist.800-53.r5 5 AU-3, NIST.800-53.R5 AU-6 (3), NIST.800-53.R5 AU-6 (4), NIST.800-53.R5 CA-7, NIST.800-53.R5 SC-7 (9), NIST.800-53.R5 SI-4 (20), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-4 (20), nistST.800-53.R5 SI-7 (8)

Kategori: Identifikasi > Logging

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::DMS::ReplicationTask`

AWS Config aturan: **`dms-replication-task-sourcedb-logging`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah logging diaktifkan dengan tingkat keparahan minimum `LOGGER_SEVERITY_DEFAULT` untuk tugas `SOURCE_CAPTURE` replikasi DMS dan. `SOURCE_UNLOAD` Kontrol gagal jika logging tidak diaktifkan untuk tugas-tugas ini atau jika tingkat keparahan minimum kurang dari`LOGGER_SEVERITY_DEFAULT`.

DMS menggunakan Amazon CloudWatch untuk mencatat informasi selama proses migrasi. Menggunakan pengaturan tugas logging, Anda dapat menentukan aktivitas komponen mana yang dicatat dan berapa banyak informasi yang dicatat. Anda harus menentukan pencatatan untuk tugas-tugas berikut:

- `SOURCE_CAPTURE`Data replikasi atau perubahan data capture (CDC) yang sedang berlangsung diambil dari database sumber atau layanan, dan diteruskan ke komponen `SORTER` layanan.
- `SOURCE_UNLOAD`— Data diturunkan dari database sumber atau layanan selama pemuatan penuh.

Logging memainkan peran penting dalam tugas replikasi DMS dengan memungkinkan pemantauan, pemecahan masalah, audit, analisis kinerja, deteksi kesalahan, dan pemulihan, serta analisis historis dan pelaporan. Ini membantu memastikan keberhasilan replikasi data antar database sambil menjaga integritas data dan kepatuhan terhadap persyaratan peraturan. Level logging selain `DEFAULT` jarang diperlukan untuk komponen ini selama pemecahan masalah. Kami merekomendasikan untuk menjaga tingkat logging seperti `DEFAULT` untuk komponen ini kecuali secara khusus diminta untuk mengubahnya AWS Support. Tingkat logging minimal `DEFAULT` memastikan bahwa pesan informasi, peringatan, dan pesan kesalahan ditulis ke log. Kontrol ini memeriksa apakah tingkat logging setidaknya salah satu dari yang berikut untuk tugas replikasi sebelumnya:`LOGGER_SEVERITY_DEFAULT`,, `LOGGER_SEVERITY_DEBUG` atau. `LOGGER_SEVERITY_DETAILED_DEBUG`

Remediasi

Untuk mengaktifkan pencatatan tugas replikasi DMS basis data sumber, lihat Melihat dan mengelola log AWS DMS tugas di AWS Database Migration Service Panduan Pengguna.

[DMS.9] Titik akhir DMS harus menggunakan SSL

Persyaratan terkait: Nist.800-53.r5 AC-4, Nist.800-53.r5 SC-13, Nist.800-53.r5 SC-23, Nist.800-53.r5 SC-23 (3), Nist.800-53.r5 SC-7 (4), Nist.800-53.r5 SC-8, Nist.800-53.r5 R5 SC-8 (1), NIST.800-53.R5 SC-8 (2)

Kategori: Lindungi > Perlindungan Data > Enkripsi data-in-transit

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::DMS::Endpoint`

AWS Config aturan: **`dms-endpoint-ssl-configured`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah AWS DMS titik akhir menggunakan koneksi SSL. Kontrol gagal jika titik akhir tidak menggunakan SSL.

Koneksi SSL/TLS menyediakan lapisan keamanan dengan mengenkripsi koneksi antara instance replikasi DMS dan database Anda. Menggunakan sertifikat memberikan lapisan keamanan tambahan dengan memvalidasi bahwa koneksi sedang dibuat ke database yang diharapkan. Ia melakukannya dengan memeriksa sertifikat server yang secara otomatis diinstal pada semua instance database yang Anda berikan. Dengan mengaktifkan koneksi SSL pada titik akhir DMS Anda, Anda melindungi kerahasiaan data selama migrasi.

Remediasi

Untuk menambahkan koneksi SSL ke titik akhir DMS baru atau yang sudah ada, lihat Menggunakan SSL dengan AWS Database Migration Service di Panduan Pengguna.AWS Database Migration Service

[DMS.10] Titik akhir DMS untuk database Neptunus harus mengaktifkan otorisasi IAM

Persyaratan terkait: Nist.800-53.r5 AC-2, Nist.800-53.r5 AC-3, Nist.800-53.r5 AC-6, Nist.800-53.r5 AC-17, Nist.800-53.r5 IA-2, Nist.800-53.r5 IA-5

Kategori: Lindungi > Manajemen akses aman > Otentikasi tanpa kata sandi

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::DMS::Endpoint`

AWS Config aturan: **`dms-neptune-iam-authorization-enabled`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah AWS DMS titik akhir untuk database Amazon Neptunus dikonfigurasi dengan otorisasi IAM. Kontrol gagal jika titik akhir DMS tidak mengaktifkan otorisasi IAM.

AWS Identity and Access Management (IAM) menyediakan kontrol akses berbutir halus di seluruh. AWS Dengan IAM, Anda dapat menentukan siapa yang dapat mengakses layanan dan sumber daya mana, dan dalam kondisi apa. Dengan kebijakan IAM, Anda mengelola izin untuk tenaga kerja dan sistem Anda untuk memastikan izin hak istimewa paling sedikit. Dengan mengaktifkan otorisasi IAM pada AWS DMS titik akhir untuk database Neptunus, Anda dapat memberikan hak otorisasi kepada pengguna IAM dengan menggunakan peran layanan yang ditentukan oleh parameter. `ServiceAccessRoleARN`

Remediasi

Untuk mengaktifkan otorisasi IAM pada titik akhir DMS untuk database Neptunus, lihat Menggunakan Amazon Neptunus sebagai target dalam Panduan Pengguna. AWS Database Migration ServiceAWS Database Migration Service

[DMS.11] Titik akhir DMS untuk MongoDB harus mengaktifkan mekanisme otentikasi

Persyaratan terkait: Nist.800-53.r5 AC-3, Nist.800-53.r5 AC-6, Nist.800-53.r5 IA-2, Nist.800-53.r5 IA-5

Kategori: Lindungi > Manajemen akses aman > Otentikasi tanpa kata sandi

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::DMS::Endpoint`

AWS Config aturan: **`dms-mongo-db-authentication-enabled`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah AWS DMS titik akhir untuk MongoDB dikonfigurasi dengan mekanisme otentikasi. Kontrol gagal jika jenis otentikasi tidak disetel untuk titik akhir.

AWS Database Migration Service mendukung dua metode otentikasi untuk MongoDB- MONGODB-CR untuk MongoDB versi 2.x, dan SCRAM-SHA-1 untuk MongoDB versi 3.x atau yang lebih baru. Metode otentikasi ini digunakan untuk mengautentikasi dan mengenkripsi kata sandi MongoDB jika pengguna ingin menggunakan kata sandi untuk mengakses database. Otentikasi pada AWS DMS titik akhir memastikan bahwa hanya pengguna yang berwenang yang dapat mengakses dan memodifikasi data yang sedang dimigrasi antar database. Tanpa autentikasi yang tepat, pengguna yang tidak sah dapat memperoleh akses ke data sensitif selama proses migrasi. Hal ini dapat mengakibatkan pelanggaran data, kehilangan data, atau insiden keamanan lainnya.

Remediasi

Untuk mengaktifkan mekanisme otentikasi pada titik akhir DMS untuk MongoDB, lihat Menggunakan MongoDB sebagai sumber di Panduan Pengguna. AWS DMSAWS Database Migration Service

[DMS.12] Titik akhir DMS untuk Redis harus mengaktifkan TLS

Persyaratan terkait: Nist.800-53.r5 SC-8, Nist.800-53.R5 SC-13

Kategori: Lindungi > Perlindungan Data > Enkripsi data-in-transit

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::DMS::Endpoint`

AWS Config aturan: **`dms-redis-tls-enabled`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah AWS DMS titik akhir untuk Redis dikonfigurasi dengan koneksi TLS. Kontrol gagal jika titik akhir tidak mengaktifkan TLS.

TLS memberikan end-to-end keamanan ketika data dikirim antara aplikasi atau database melalui internet. Saat Anda mengonfigurasi enkripsi SSL untuk titik akhir DMS Anda, ini memungkinkan komunikasi terenkripsi antara basis data sumber dan target selama proses migrasi. Ini membantu

mencegah penyadapan dan intersepsi data sensitif oleh aktor jahat. Tanpa enkripsi SSL, data sensitif dapat diakses, mengakibatkan pelanggaran data, kehilangan data, atau insiden keamanan lainnya.

Remediasi

Untuk mengaktifkan koneksi TLS pada titik akhir DMS untuk Redis, lihat Menggunakan Redis sebagai target dalam Panduan Pengguna. AWS Database Migration ServiceAWS Database Migration Service

Kontrol Amazon DocumentDB

Kontrol ini terkait dengan sumber daya Amazon DocumentDB.

Kontrol ini mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[DocumentDB.1] Cluster Amazon DocumentDB harus dienkripsi saat istirahat

Persyaratan terkait: Nist.800-53.r5 CA-9 (1), NIST.800-53.R5 CM-3 (6), Nist.800-53.r5 SC-13, Nist.800-53.r5 SC-28, Nist.800-53.r5 SC-28 (1), Nist.800-53.r5 SC-7 (10), Nist.800-53.r5 SC-7 (10), Nist.800-53.r5 SC-7 (10), Nist.800-53.r5 SC-7 (10), Nist.800-53.r5 SC-7 (10), Nist.800-53.r5 SC-7 (10), Nist.800-53.r5 SC-7 (10), ST.800-53.R5 SI-7 (6)

Kategori: Lindungi > Perlindungan Data > Enkripsi data-at-rest

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::RDS::DBCluster`

AWS Config aturan: **`docdb-cluster-encrypted`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah cluster Amazon DocumentDB dienkripsi saat istirahat. Kontrol gagal jika cluster Amazon DocumentDB tidak dienkripsi saat istirahat.

Data saat istirahat mengacu pada data apa pun yang disimpan dalam penyimpanan persisten dan tidak mudah menguap untuk durasi berapa pun. Enkripsi membantu Anda melindungi kerahasiaan data tersebut, mengurangi risiko bahwa pengguna yang tidak sah mendapatkan akses ke sana. Data di cluster Amazon DocumentDB harus dienkripsi saat istirahat untuk lapisan keamanan tambahan. Amazon DocumentDB menggunakan Advanced Encryption Standard 256-bit (AES-256) untuk

mengenkripsi data Anda menggunakan kunci enkripsi yang disimpan dalam AWS Key Management Service (AWS KMS).

Remediasi

Anda dapat mengaktifkan enkripsi saat istirahat saat membuat cluster Amazon DocumentDB. Anda tidak dapat mengubah pengaturan enkripsi setelah membuat cluster. Untuk informasi selengkapnya, lihat Mengaktifkan enkripsi saat istirahat untuk klaster Amazon DocumentDB di Panduan Pengembang Amazon DocumentDB.

[DocumentDB.2] Cluster Amazon DocumentDB harus memiliki periode retensi cadangan yang memadai

Persyaratan terkait: NIST.800-53.R5 SI-12

Kategori: Pulih> Ketahanan > Cadangan diaktifkan

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::RDS::DBCluster`

AWS Config aturan: **`docdb-cluster-backup-retention-check`**

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub	
`minimumBackupRetentionPeriod`	Periode retensi cadangan minimum dalam beberapa hari	Bilangan Bulat	7 untuk 35	7	

Kontrol ini memeriksa apakah klaster Amazon DocumentDB memiliki periode retensi cadangan yang lebih besar dari atau sama dengan kerangka waktu yang ditentukan. Kontrol gagal jika periode retensi cadangan kurang dari kerangka waktu yang ditentukan. Kecuali Anda memberikan nilai

parameter khusus untuk periode penyimpanan cadangan, Security Hub menggunakan nilai default 7 hari.

Pencadangan membantu Anda pulih lebih cepat dari insiden keamanan dan memperkuat ketahanan sistem Anda. Dengan mengotomatiskan backup untuk cluster Amazon DocumentDB Anda, Anda akan dapat memulihkan sistem Anda ke titik waktu tertentu dan meminimalkan waktu henti dan kehilangan data. Di Amazon DocumentDB, cluster memiliki periode retensi cadangan default 1 hari. Ini harus ditingkatkan menjadi nilai antara 7 dan 35 hari untuk melewati kontrol ini.

Remediasi

Untuk mengubah periode retensi cadangan untuk klaster Amazon DocumentDB Anda, lihat Memodifikasi klaster Amazon DocumentDB di Panduan Pengembang Amazon DocumentDB. Untuk Backup, pilih periode retensi cadangan.

[DocumentDB.3] Cuplikan cluster manual Amazon DocumentDB seharusnya tidak bersifat publik

Persyaratan terkait: Nist.800-53.r5 AC-21, Nist.800-53.r5 AC-3, Nist.800-53.r5 AC-3 (7), Nist.800-53.r5 AC-4, Nist.800-53.r5 AC-4 (21), Nist.800-53.r5 AC-6, Nist.800-53.r5 R5 SC-7, Nist.800-53.r5 SC-7 (11), NIST.800-53.R5 SC-7 (16), Nist.800-53.r5 SC-7 (20), Nist.800-53.r5 SC-7 (21), Nist.800-53.r5 SC-7 (3), Nist.800-53.r5 5 SC-7 (4), NIST.800-53.R5 SC-7 (9)

Kategori: Lindungi > Konfigurasi jaringan aman

Tingkat keparahan: Kritis

Jenis sumber daya:`AWS::RDS::DBClusterSnapshot`, `AWS::RDS:DBSnapshot`

AWS Config aturan: **`docdb-cluster-snapshot-public-prohibited`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah snapshot kluster manual Amazon DocumentDB bersifat publik. Kontrol gagal jika snapshot cluster manual bersifat publik.

Snapshot kluster manual Amazon DocumentDB tidak boleh bersifat publik kecuali dimaksudkan. Jika Anda membagikan snapshot manual yang tidak terenkripsi sebagai publik, snapshot tersedia untuk semua. Akun AWS Cuplikan publik dapat mengakibatkan eksposur data yang tidak diinginkan.

> **Note**
>
> Kontrol ini mengevaluasi snapshot cluster manual. Anda tidak dapat membagikan snapshot klaster otomatis Amazon DocumentDB. Namun, Anda dapat membuat snapshot manual dengan menyalin snapshot otomatis, lalu membagikan salinannya.

Remediasi

Untuk menghapus akses publik untuk snapshot kluster manual Amazon DocumentDB, lihat Berbagi snapshot di Panduan Pengembang Amazon DocumentDB. Secara terprogram, Anda dapat menggunakan operasi Amazon DocumentDB. `modify-db-snapshot-attribute` Tetapkan `attribute-name` sebagai `restore` dan `values-to-remove` sebagai`all`.

[DocumentDB.4] Cluster Amazon DocumentDB harus mempublikasikan log audit ke Log CloudWatch

Persyaratan terkait: Nist.800-53.r5 AC-2 (4), Nist.800-53.r5 AC-4 (26), Nist.800-53.r5 AC-6 (9), Nist.800-53.r5 AU-10, Nist.800-53.r5 AU-12, Nist.800-53.r5 AU-2, Nist.800-53.r5 5 AU-3, NIST.800-53.R5 AU-6 (3), NIST.800-53.R5 AU-6 (4), NIST.800-53.R5 CA-7, NIST.800-53.R5 SC-7 (9), NIST.800-53.R5 SI-4 (20), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-4 (20), nistST.800-53.R5 SI-7 (8)

Kategori: Identifikasi > Logging

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::RDS::DBCluster`

AWS Config aturan: **`docdb-cluster-audit-logging-enabled`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah klaster Amazon DocumentDB menerbitkan log audit ke Amazon Logs. CloudWatch Kontrol gagal jika klaster tidak mempublikasikan log audit ke CloudWatch Log.

Amazon DocumentDB (dengan kompatibilitas MongoDB) memungkinkan Anda mengaudit peristiwa yang dilakukan di cluster Anda. Contoh log acara termasuk upaya autentikasi yang berhasil

dan gagal, membuang koleksi dalam basis data, atau membuat indeks. Secara default, audit dinonaktifkan di Amazon DocumentDB dan mengharuskan Anda mengambil tindakan untuk mengaktifkannya.

Remediasi

Untuk mempublikasikan log audit Amazon DocumentDB CloudWatch ke Log, lihat Mengaktifkan audit di Panduan Pengembang Amazon DocumentDB.

[DocumentDB.5] Cluster Amazon DocumentDB harus mengaktifkan perlindungan penghapusan

Persyaratan terkait: Nist.800-53.r5 CA-9 (1), Nist.800-53.R5 CM-2, Nist.800-53.R5 CM-2 (2), Nist.800-53.r5 CM-3, Nist.800-53.r5 SC-5 (2)

Kategori: Lindungi > Perlindungan data > Perlindungan penghapusan data

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::RDS::DBCluster`

AWS Config aturan: **`docdb-cluster-deletion-protection-enabled`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah klaster Amazon DocumentDB mengaktifkan perlindungan penghapusan. Kontrol gagal jika klaster tidak mengaktifkan perlindungan penghapusan.

Mengaktifkan perlindungan penghapusan klaster menawarkan lapisan perlindungan tambahan terhadap penghapusan atau penghapusan database yang tidak disengaja oleh pengguna yang tidak sah. Cluster Amazon DocumentDB tidak dapat dihapus saat perlindungan penghapusan diaktifkan. Anda harus menonaktifkan perlindungan penghapusan terlebih dahulu sebelum permintaan penghapusan berhasil. Perlindungan penghapusan diaktifkan secara default saat Anda membuat klaster di konsol Amazon DocumentDB.

Remediasi

Untuk mengaktifkan perlindungan penghapusan klaster Amazon DocumentDB yang ada, lihat Memodifikasi klaster Amazon DocumentDB di Panduan Pengembang Amazon DocumentDB. Di bagian Modify Cluster, pilih Enable for Deletion protection.

Kontrol Amazon DynamoDB

Kontrol ini terkait dengan sumber daya DynamoDB.

Kontrol ini mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[DynamoDB.1] Tabel DynamoDB harus secara otomatis menskalakan kapasitas sesuai permintaan

Persyaratan terkait: Nist.800-53.r5 CP-10, Nist.800-53.r5 CP-2 (2), Nist.800-53.R5 CP-6 (2), Nist.800-53.r5 SC-36, Nist.800-53.r5 SC-5 (2), Nist.800-53.r5 SI-13 (5)

Kategori: Pulihkan > Ketahanan > Ketersediaan tinggi

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::DynamoDB::Table`

AWS Config aturan: **`dynamodb-autoscaling-enabled`**

Jenis jadwal: Periodik

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang valid	Nilai default Security Hub
`minProvisionedReadCapacity`	Jumlah minimum unit kapasitas baca yang disediakan untuk penskalaan otomatis DynamoDB	Bilangan Bulat	1 untuk `40000`	Tidak ada nilai default
`targetReadUtilization`	Target persentase pemanfaatan untuk kapasitas baca	Bilangan Bulat	`20` untuk `90`	Tidak ada nilai default
`minProvisionedWriteCapacity`	Jumlah minimum unit kapasitas tulis yang disediakan untuk penskalaan otomatis DynamoDB	Bilangan Bulat	1 untuk `40000`	Tidak ada nilai default

Parameter	Deskripsi	Jenis	Nilai kustom yang valid	Nilai default Security Hub
`targetWriteUtilization`	Target persentase pemanfaatan untuk kapasitas tulis	Bilangan Bulat	`20` untuk `90`	Tidak ada nilai default

Kontrol ini memeriksa apakah tabel Amazon DynamoDB dapat menskalakan kapasitas baca dan tulisnya sesuai kebutuhan. Kontrol gagal jika tabel tidak menggunakan mode kapasitas sesuai permintaan atau mode yang disediakan dengan penskalaan otomatis yang dikonfigurasi. Secara default, kontrol ini hanya mengharuskan salah satu mode ini dikonfigurasi, tanpa memperhatikan tingkat kapasitas baca atau tulis tertentu. Secara opsional, Anda dapat memberikan nilai parameter khusus untuk memerlukan tingkat kapasitas baca dan tulis tertentu atau pemanfaatan target.

Kapasitas penskalaan dengan permintaan menghindari pengecualian pembatasan, yang membantu menjaga ketersediaan aplikasi Anda. Tabel DynamoDB dalam mode kapasitas sesuai permintaan hanya dibatasi oleh kuota tabel default throughput DynamoDB. Untuk meningkatkan kuota ini, Anda dapat mengajukan tiket dukungan dengan AWS Support tabel.DynamoDB dalam mode yang disediakan dengan penskalaan otomatis menyesuaikan kapasitas throughput yang disediakan secara dinamis sebagai respons terhadap pola lalu lintas. Untuk informasi selengkapnya tentang pembatasan permintaan DynamoDB, lihat Meminta pelambatan dan kapasitas burst di Panduan Pengembang Amazon DynamoDB.

Remediasi

Untuk mengaktifkan penskalaan otomatis DynamoDB pada tabel yang ada dalam mode kapasitas, lihat Mengaktifkan penskalaan otomatis DynamoDB pada tabel yang ada di Panduan Pengembang Amazon DynamoDB.

[DynamoDB.2] Tabel DynamoDB harus mengaktifkan pemulihan point-in-time

Persyaratan terkait: NIST.800-53.R5 CP-10, Nist.800-53.R5 CP-6 (2), Nist.800-53.R5 CP-9, Nist.800-53.R5 SC-5 (2), Nist.800-53.r5 SI-12, NIST.800-53.R5 SI-13 (5)

Kategori: Pulih> Ketahanan > Cadangan diaktifkan

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::DynamoDB::Table`

AWS Config aturan: **`dynamodb-pitr-enabled`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah point-in-time pemulihan (PITR) diaktifkan untuk tabel Amazon DynamoDB.

Cadangan membantu Anda pulih lebih cepat dari insiden keamanan. Mereka juga memperkuat ketahanan sistem Anda. DynamoDB recovery point-in-time mengotomatiskan backup untuk tabel DynamoDB. Ini mengurangi waktu untuk memulihkan dari menghapus atau menulis operasi yang tidak disengaja. Tabel DynamoDB yang mengaktifkan PITR dapat dikembalikan ke titik waktu mana pun dalam 35 hari terakhir.

Remediasi

Untuk mengembalikan tabel DynamoDB ke titik waktu, lihat Memulihkan tabel DynamoDB ke titik waktu dalam Panduan Pengembang Amazon DynamoDB.

[DynamoDB.3] Cluster DynamoDB Accelerator (DAX) harus dienkripsi saat istirahat

Persyaratan terkait: Nist.800-53.r5 CA-9 (1), NIST.800-53.R5 CM-3 (6), Nist.800-53.r5 SC-13, Nist.800-53.r5 SC-28, Nist.800-53.r5 SC-28 (1), Nist.800-53.r5 SC-7 (10), Nist.800-53.r5 SC-7 (10), Nist.800-53.r5 SC-7 (10), Nist.800-53.r5 SC-7 (10), Nist.800-53.r5 SC-7 (10), Nist.800-53.r5 SC-7 (10), Nist.800-53.r5 SC-7 (10), ST.800-53.R5 SI-7 (6)

Kategori: Lindungi > Perlindungan Data > Enkripsi data-at-rest

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::DAX::Cluster`

AWS Config aturan: **`dax-encryption-enabled`**

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah klaster Amazon DynamoDB Accelerator (DAX) dienkripsi saat istirahat. Kontrol gagal jika cluster DAX tidak dienkripsi saat istirahat.

Mengenkripsi data saat istirahat mengurangi risiko data yang disimpan pada disk diakses oleh pengguna yang tidak diautentikasi. AWS Enkripsi menambahkan satu set kontrol akses lain untuk membatasi kemampuan pengguna yang tidak sah untuk mengakses data. Misalnya, izin API diperlukan untuk mendekripsi data sebelum dapat dibaca.

Remediasi

Anda tidak dapat mengaktifkan atau menonaktifkan enkripsi saat istirahat setelah cluster dibuat. Anda harus membuat ulang cluster untuk mengaktifkan enkripsi saat istirahat. Untuk petunjuk terperinci tentang cara membuat klaster DAX dengan enkripsi saat istirahat diaktifkan, lihat Mengaktifkan enkripsi saat istirahat menggunakan Panduan Pengembang Amazon DynamoDB AWS Management Console di Amazon DynamoDB.

[DynamoDB.4] Tabel DynamoDB harus ada dalam rencana cadangan

Persyaratan terkait: Nist.800-53.r5 CP-10, Nist.800-53.r5 CP-6, Nist.800-53.R5 CP-6 (1), Nist.800-53.r5 CP-6 (2), Nist.800-53.r5 CP-9, Nist.800-53.r5 SC-5 (2), Nist.800-53.r5 SC-5 (2), Nist.800-53.r5 00-53.R5 SI-12, NIST.800-53.R5 SI-13 (5)

Kategori: Pulih> Ketahanan > Cadangan diaktifkan

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::DynamoDB::Table`

AWS Config aturan: **`dynamodb-resources-protected-by-backup-plan`**

Jenis jadwal: Periodik

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`backupVaultLockCheck`	Kontrol menghasilkan `PASSED` temuan jika parameter disetel ke `true` dan sumber daya menggunakan AWS Backup Vault Lock.	Boolean	`true` atau `false`	Tidak ada nilai default

Kontrol ini mengevaluasi apakah `ACTIVE` tabel Amazon DynamoDB dalam status dicakup oleh rencana cadangan. Kontrol gagal jika tabel DynamoDB tidak dicakup oleh rencana cadangan. Jika Anda menyetel `backupVaultLockCheck` parameter sama dengan`true`, kontrol hanya akan diteruskan jika tabel DynamoDB dicadangkan di AWS Backup vault terkunci.

AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya yang membantu Anda memusatkan dan mengotomatiskan pencadangan data di seluruh. Layanan AWS Dengan AWS Backup, Anda dapat membuat rencana cadangan yang menentukan persyaratan pencadangan Anda, seperti seberapa sering mencadangkan data Anda dan berapa lama untuk menyimpan cadangan tersebut. Menyertakan tabel DynamoDB dalam paket cadangan membantu Anda melindungi data dari kehilangan atau penghapusan yang tidak diinginkan.

Remediasi

Untuk menambahkan tabel DynamoDB ke AWS Backup paket cadangan, lihat Menetapkan sumber daya ke paket cadangan di Panduan Pengembang.AWS Backup

[DynamoDB.5] Tabel DynamoDB harus diberi tag

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::DynamoDB::Table`

AWS Config aturan: `tagged-dynamodb-table` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList	Daftar tag yang memenuhi	`No default value`

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
			AWS persyaratan	

Kontrol ini memeriksa apakah tabel Amazon DynamoDB memiliki tag dengan kunci tertentu yang ditentukan dalam parameter. `requiredTagKeys` Kontrol gagal jika tabel tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika tabel tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke tabel DynamoDB, lihat Menandai sumber daya di DynamoDB di Panduan Pengembang Amazon DynamoDB.

[DynamoDB.6] Tabel DynamoDB harus mengaktifkan perlindungan penghapusan

Persyaratan terkait: Nist.800-53.r5 CA-9 (1), Nist.800-53.R5 CM-2, Nist.800-53.R5 CM-2 (2), Nist.800-53.r5 CM-3, Nist.800-53.r5 SC-5 (2)

Kategori: Lindungi > Perlindungan data > Perlindungan penghapusan data

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::DynamoDB::Table`

AWS Config aturan: **`dynamodb-table-deletion-protection-enabled`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah tabel Amazon DynamoDB memiliki perlindungan penghapusan yang diaktifkan. Kontrol gagal jika tabel DynamoDB tidak mengaktifkan proteksi penghapusan.

Anda dapat melindungi tabel DynamoDB dari penghapusan yang tidak disengaja dengan properti perlindungan penghapusan. Mengaktifkan properti ini untuk tabel membantu memastikan bahwa tabel tidak terhapus secara tidak sengaja selama operasi manajemen tabel reguler oleh administrator Anda. Ini membantu mencegah gangguan pada operasi bisnis normal Anda.

Remediasi

Untuk mengaktifkan perlindungan penghapusan untuk tabel DynamoDB, lihat Menggunakan perlindungan penghapusan di Panduan Pengembang Amazon DynamoDB.

[DynamoDB.7] Cluster DynamoDB Accelerator harus dienkripsi saat transit

Persyaratan terkait: Nist.800-53.r5 AC-17, Nist.800-53.r5 SC-8, Nist.800-53.R5 SC-13, Nist.800-53.r5 SC-23

Kategori: Lindungi > Perlindungan Data > Enkripsi data-in-transit

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::DynamoDB::Table`

AWS Config aturan: **`dax-tls-endpoint-encryption`**

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah klaster Amazon DynamoDB Accelerator (DAX) dienkripsi saat transit, dengan jenis enkripsi endpoint disetel ke TLS. Kontrol gagal jika klaster DAX tidak dienkripsi saat transit.

HTTPS (TLS) dapat digunakan untuk membantu mencegah penyerang potensial menggunakan person-in-the-middle atau serangan serupa untuk menguping atau memanipulasi lalu lintas jaringan. Anda hanya boleh mengizinkan koneksi terenkripsi melalui TLS untuk mengakses kluster DAX. Namun, mengenkripsi data dalam perjalanan dapat memengaruhi kinerja. Anda harus menguji aplikasi Anda dengan enkripsi diaktifkan untuk memahami profil kinerja dan dampak TLS.

Remediasi

Anda tidak dapat mengubah setelan enkripsi TLS setelah membuat cluster DAX. Untuk mengenkripsi klaster DAX yang ada, buat klaster baru dengan enkripsi saat transit diaktifkan, geser lalu lintas aplikasi Anda ke klaster tersebut, lalu hapus klaster lama. Untuk informasi selengkapnya, lihat Menggunakan perlindungan penghapusan di Panduan Pengembang Amazon DynamoDB.

Kontrol Registri Kontainer Elastis Amazon

Kontrol ini terkait dengan sumber daya Amazon ECR.

Kontrol ini mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[ECR.1] Repositori pribadi ECR harus memiliki pemindaian gambar yang dikonfigurasi

Persyaratan terkait: Nist.800-53.r5 RA-5

Kategori: Identifikasi > Kerentanan, tambalan, dan manajemen versi

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::ECR::Repository`

AWS Config aturan: **`ecr-private-image-scanning-enabled`**

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah repositori Amazon ECR pribadi memiliki pemindaian gambar yang dikonfigurasi. Kontrol gagal jika repositori ECR pribadi tidak dikonfigurasi untuk pemindaian saat push atau pemindaian berkelanjutan.

Pemindaian gambar ECR membantu mengidentifikasi kerentanan perangkat lunak dalam gambar kontainer Anda. Mengkonfigurasi pemindaian gambar pada repositori ECR menambahkan lapisan verifikasi untuk integritas dan keamanan gambar yang disimpan.

Remediasi

Untuk mengonfigurasi pemindaian gambar untuk repositori ECR, lihat Pemindaian gambar di Panduan Pengguna Amazon Elastic Container Registry.

[ECR.2] Repositori pribadi ECR harus memiliki kekekalan tag yang dikonfigurasi

Persyaratan terkait: NIST.800-53.R5 CA-9 (1), Nist.800-53.R5 CM-2, Nist.800-53.R5 CM-8 (1)

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::ECR::Repository`

AWS Config aturan: **`ecr-private-tag-immutability-enabled`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah repositori ECR pribadi memiliki kekekalan tag yang diaktifkan. Kontrol ini gagal jika repositori ECR pribadi menonaktifkan kekekalan tag. Aturan ini berlaku jika kekekalan tag diaktifkan dan memiliki nilai. `IMMUTABLE`

Amazon ECR Tag Immutability memungkinkan pelanggan untuk mengandalkan tag deskriptif gambar sebagai mekanisme yang andal untuk melacak dan mengidentifikasi gambar secara unik. Tag yang tidak dapat diubah bersifat statis, yang berarti setiap tag mengacu pada gambar yang unik. Ini meningkatkan keandalan dan skalabilitas karena penggunaan tag statis akan selalu menghasilkan

gambar yang sama yang digunakan. Saat dikonfigurasi, kekekalan tag mencegah tag diganti, yang mengurangi permukaan serangan.

Remediasi

Untuk membuat repositori dengan tag yang tidak dapat diubah yang dikonfigurasi atau memperbarui setelan mutabilitas tag gambar untuk repositori yang ada, lihat Mutabilitas tag gambar di Panduan Pengguna Registri Amazon Elastic Container.

[ECR.3] Repositori ECR harus memiliki setidaknya satu kebijakan siklus hidup yang dikonfigurasi

Persyaratan terkait: NIST.800-53.R5 CA-9 (1), Nist.800-53.R5 CM-2, Nist.800-53.R5 CM-2 (2)

Kategori: Identifikasi > Konfigurasi sumber daya

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::ECR::Repository`

AWS Config aturan: **`ecr-private-lifecycle-policy-configured`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah repositori Amazon ECR memiliki setidaknya satu kebijakan siklus hidup yang dikonfigurasi. Kontrol ini gagal jika repositori ECR tidak memiliki kebijakan siklus hidup yang dikonfigurasi.

Kebijakan siklus hidup Amazon ECR memungkinkan Anda untuk menentukan manajemen siklus hidup citra dalam repositori. Dengan mengonfigurasi kebijakan siklus hidup, Anda dapat mengotomatiskan pembersihan gambar yang tidak digunakan dan kedaluwarsa gambar berdasarkan usia atau hitungan. Mengotomatiskan tugas-tugas ini dapat membantu Anda menghindari penggunaan gambar usang secara tidak sengaja di repositori Anda.

Remediasi

Untuk mengonfigurasi kebijakan siklus hidup, lihat Membuat pratinjau kebijakan siklus hidup di Panduan Pengguna Amazon Elastic Container Registry.

[ECR.4] Repositori publik ECR harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::ECR::PublicRepository`

AWS Config aturan: `tagged-ecr-publicrepository` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList	Daftar tag yang memenuhi AWS persyaratan	Tidak ada nilai default

Kontrol ini memeriksa apakah repositori publik Amazon ECR memiliki tag dengan kunci tertentu yang ditentukan dalam parameter. `requiredTagKeys` Kontrol gagal jika repositori publik tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter. `requiredTagKeys` Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika repositori publik tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke

AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke repositori publik ECR, lihat Menandai repositori publik Amazon ECR di Panduan Pengguna Registri Amazon Elastic Container.

Kontrol Amazon ECS

Kontrol ini terkait dengan sumber daya Amazon ECS.

Kontrol ini mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[ECS.1] Definisi tugas Amazon ECS harus memiliki mode jaringan yang aman dan definisi pengguna.

Persyaratan terkait: Nist.800-53.r5 AC-2 (1), Nist.800-53.r5 AC-3, Nist.800-53.r5 AC-3 (15), Nist.800-53.r5 AC-3 (7), Nist.800-53.r5 AC-5, Nist.800-53.r5 AC-6

Kategori: Lindungi > Manajemen akses yang aman

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::ECS::TaskDefinition`

AWS Config aturan: **`ecs-task-definition-user-for-host-mode-check`**

Jenis jadwal: Perubahan dipicu

Parameter:

- `SkipInactiveTaskDefinitions`: `true` (tidak dapat disesuaikan)

Kontrol ini memeriksa apakah definisi tugas Amazon ECS aktif dengan mode jaringan host memiliki `privileged` atau definisi `user` kontainer. Kontrol gagal untuk definisi tugas yang memiliki mode jaringan host dan definisi wadah`privileged=false`, kosong dan`user=root`, atau kosong.

Kontrol ini hanya mengevaluasi revisi aktif terbaru dari definisi tugas Amazon ECS.

Tujuan dari kontrol ini adalah untuk memastikan bahwa akses didefinisikan dengan sengaja ketika Anda menjalankan tugas yang menggunakan mode jaringan host. Jika definisi tugas memiliki hak istimewa yang tinggi, itu karena Anda telah memilih konfigurasi itu. Kontrol ini memeriksa eskalasi hak istimewa yang tidak terduga ketika definisi tugas mengaktifkan jaringan host, dan Anda tidak memilih hak istimewa yang ditinggikan.

Remediasi

Untuk informasi tentang cara memperbarui definisi tugas, lihat Memperbarui definisi tugas di Panduan Pengembang Layanan Amazon Elastic Container.

Saat Anda memperbarui definisi tugas, itu tidak memperbarui tugas yang sedang berjalan yang diluncurkan dari definisi tugas sebelumnya. Untuk memperbarui tugas yang sedang berjalan, Anda harus menerapkan ulang tugas dengan definisi tugas baru.

[ECS.2] Layanan ECS seharusnya tidak memiliki alamat IP publik yang ditetapkan kepadanya secara otomatis

Persyaratan terkait: Nist.800-53.r5 AC-21, Nist.800-53.r5 AC-3, Nist.800-53.r5 AC-3 (7), Nist.800-53.r5 AC-4, Nist.800-53.r5 AC-4 (21), Nist.800-53.r5 AC-6, Nist.800-53.r5 R5 SC-7, Nist.800-53.r5 SC-7 (11), NIST.800-53.R5 SC-7 (16), Nist.800-53.r5 SC-7 (20), Nist.800-53.r5 SC-7 (21), Nist.800-53.r5 SC-7 (3), Nist.800-53.r5 5 SC-7 (4), NIST.800-53.R5 SC-7 (9)

Kategori: Lindungi > Konfigurasi jaringan aman > Sumber daya tidak dapat diakses publik

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::ECS::Service`

AWS Config aturan: `ecs-service-assign-public-ip-disabled` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

- `exemptEcsServiceArns`(tidak dapat disesuaikan). Security Hub tidak mengisi parameter ini. Daftar ARN layanan Amazon ECS yang dipisahkan koma yang dikecualikan dari aturan ini.

  Aturan ini adalah `COMPLIANT` jika layanan Amazon ECS telah `AssignPublicIP` disetel ke `ENABLED` dan ditentukan dalam daftar parameter ini.

  Aturan ini adalah `NON_COMPLIANT` jika layanan Amazon ECS telah `AssignPublicIP` disetel ke `ENABLED` dan tidak ditentukan dalam daftar parameter ini.

Kontrol ini memeriksa apakah layanan Amazon ECS dikonfigurasi untuk secara otomatis menetapkan alamat IP publik. Kontrol ini gagal jika `AssignPublicIP` ada`ENABLED`. Kontrol ini lolos jika `AssignPublicIP` ada`DISABLED`.

Alamat IP publik adalah alamat IP yang dapat dijangkau dari internet. Jika Anda meluncurkan instans Amazon ECS Anda dengan alamat IP publik, maka instans Amazon ECS Anda dapat dijangkau dari internet. Layanan Amazon ECS tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke server aplikasi kontainer Anda.

Remediasi

Untuk menonaktifkan penetapan IP publik otomatis, lihat Untuk mengonfigurasi pengaturan VPC dan grup keamanan untuk layanan Anda di Panduan Pengembang Layanan Amazon Elastic Container.

[ECS.3] Definisi tugas ECS tidak boleh membagikan namespace proses host

Persyaratan terkait: NIST.800-53.R5 CA-9 (1), NIST.800-53.R5 CM-2

Kategori: Identifikasi > Konfigurasi sumber daya

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::ECS::TaskDefinition`

AWS Config aturan: ecs-task-definition-pid-mode-check

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah definisi tugas Amazon ECS dikonfigurasi untuk berbagi namespace proses host dengan kontainernya. Kontrol gagal jika definisi tugas membagikan namespace proses host dengan wadah yang berjalan di atasnya. Kontrol ini hanya mengevaluasi revisi aktif terbaru dari definisi tugas Amazon ECS.

Namespace ID proses (PID) menyediakan pemisahan antar proses. Ini mencegah proses sistem agar tidak terlihat, dan memungkinkan PID untuk digunakan kembali, termasuk PID 1. Jika namespace PID host dibagikan dengan kontainer, itu akan memungkinkan kontainer untuk melihat semua proses pada sistem host. Ini mengurangi manfaat isolasi tingkat proses antara host dan wadah. Keadaan ini dapat menyebabkan akses tidak sah ke proses pada host itu sendiri, termasuk kemampuan untuk memanipulasi dan menghentikannya. Pelanggan tidak boleh membagikan namespace proses host dengan wadah yang berjalan di atasnya.

Remediasi

Untuk mengonfigurasi definisi tugas, lihat Parameter definisi tugas di Panduan Pengembang Layanan Amazon Elastic Container. `pidMode`

[ECS.4] Kontainer ECS harus berjalan sebagai non-hak istimewa

Persyaratan terkait: Nist.800-53.r5 AC-2 (1), Nist.800-53.r5 AC-3, Nist.800-53.r5 AC-3 (15), Nist.800-53.r5 AC-3 (7), Nist.800-53.r5 AC-5, Nist.800-53.r5 AC-6

Kategori: Lindungi > Manajemen akses aman > Pembatasan akses pengguna root

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::ECS::TaskDefinition`

AWS Config aturan: ecs-containers-nonprivileged

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah `privileged` parameter dalam definisi penampung Definisi Tugas Amazon ECS disetel ke`true`. Kontrol gagal jika parameter ini sama dengan`true`. Kontrol ini hanya mengevaluasi revisi aktif terbaru dari definisi tugas Amazon ECS.

Kami menyarankan Anda menghapus hak istimewa yang ditinggikan dari definisi tugas ECS Anda. Ketika parameter privilege adalah`true`, wadah diberikan hak istimewa yang ditinggikan pada instance wadah host (mirip dengan pengguna root).

Remediasi

Untuk mengonfigurasi `privileged` parameter pada definisi tugas, lihat Parameter definisi kontainer lanjutan di Panduan Pengembang Layanan Kontainer Elastis Amazon.

[ECS.5] Wadah ECS harus dibatasi pada akses hanya-baca ke sistem file root

Persyaratan terkait: Nist.800-53.r5 AC-2 (1), Nist.800-53.r5 AC-3, Nist.800-53.r5 AC-3 (15), Nist.800-53.r5 AC-3 (7), Nist.800-53.r5 AC-5, Nist.800-53.r5 AC-6

Kategori: Lindungi > Manajemen akses yang aman

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::ECS::TaskDefinition`

AWS Config aturan: ecs-containers-readonly-access

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah kontainer Amazon ECS terbatas pada akses hanya-baca ke sistem file root yang dipasang. Kontrol gagal jika `readonlyRootFilesystem` parameter disetel ke `false` atau jika parameter tidak ada dalam definisi wadah dalam definisi tugas. Kontrol ini hanya mengevaluasi revisi aktif terbaru dari definisi tugas Amazon ECS.

Mengaktifkan opsi ini mengurangi vektor serangan keamanan karena sistem file instance kontainer tidak dapat dirusak atau ditulis kecuali jika memiliki izin baca-tulis eksplisit pada folder dan direktori sistem file. Kontrol ini juga menganut prinsip hak istimewa paling sedikit.

Remediasi

Membatasi definisi kontainer untuk akses hanya-baca ke sistem file root

1. Buka konsol klasik Amazon ECS di https://console.aws.amazon.com/ecs/.
2. Di panel navigasi kiri, pilih Definisi tugas.
3. Pilih definisi tugas yang memiliki definisi wadah yang perlu diperbarui. Untuk masing-masing, selesaikan langkah-langkah berikut:
   - Dari drop-down, pilih Buat revisi baru dengan JSON.

- Tambahkan `readonlyRootFilesystem` parameter, dan atur ke `true` dalam definisi wadah dalam definisi tugas.
- Pilih Buat.

[ECS.8] Rahasia tidak boleh diteruskan sebagai variabel lingkungan kontainer

Persyaratan terkait: NIST.800-53.R5 CA-9 (1), NIST.800-53.R5 CM-2

Kategori: Lindungi > Pengembangan aman > Kredensyal tidak dikodekan dengan keras

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::ECS::TaskDefinition`

AWS Config aturan: ecs-no-environment-secrets

Jenis jadwal: Perubahan dipicu

Parameter:

- secretKeys =`AWS_ACCESS_KEY_ID`,`AWS_SECRET_ACCESS_KEY`, `ECS_ENGINE_AUTH_DATA` (tidak dapat disesuaikan)

Kontrol ini memeriksa apakah nilai kunci dari setiap variabel dalam `environment` parameter definisi kontainer termasuk`AWS_ACCESS_KEY_ID`,`AWS_SECRET_ACCESS_KEY`, atau`ECS_ENGINE_AUTH_DATA`. Kontrol ini gagal jika variabel lingkungan tunggal dalam definisi kontainer sama`AWS_ACCESS_KEY_ID`,`AWS_SECRET_ACCESS_KEY`, atau`ECS_ENGINE_AUTH_DATA`. Kontrol ini tidak mencakup variabel lingkungan yang diteruskan dari lokasi lain seperti Amazon S3. Kontrol ini hanya mengevaluasi revisi aktif terbaru dari definisi tugas Amazon ECS.

AWS Systems Manager Parameter Store dapat membantu Anda meningkatkan postur keamanan organisasi Anda. Sebaiknya gunakan Parameter Store untuk menyimpan rahasia dan kredensil alih-alih langsung meneruskannya ke instance container Anda atau hard coding ke dalam kode Anda.

Remediasi

Untuk membuat parameter menggunakan SSM, lihat Membuat parameter Systems Manager di Panduan AWS Systems Manager Pengguna. Untuk informasi selengkapnya tentang membuat definisi tugas yang menentukan rahasia, lihat Menentukan data sensitif menggunakan Secrets Manager di Panduan Pengembang Layanan Amazon Elastic Container.

[ECS.9] Definisi tugas ECS harus memiliki konfigurasi logging

Persyaratan terkait: Nist.800-53.r5 AC-4 (26), Nist.800-53.R5 AU-10, Nist.800-53.R5 AU-12, Nist.800-53.r5 AU-2, Nist.800-53.r5 AU-3, Nist.800-53.r5 AU-6 (3), Nist.800-53.r5 AU-6 (4), NIST.800-53.R5 CA-7, NIST.800-53.R5 SC-7 (9), NIST.800-53.R5 SI-7 (8)

Kategori: Identifikasi > Logging

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::ECS::TaskDefinition`

AWS Config aturan: ecs-task-definition-log -konfigurasi

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah definisi tugas Amazon ECS aktif terbaru memiliki konfigurasi logging yang ditentukan. Kontrol gagal jika definisi tugas tidak memiliki `logConfiguration` properti yang ditentukan atau jika nilai untuk `logDriver` adalah nol dalam setidaknya satu definisi kontainer.

Logging membantu Anda menjaga keandalan, ketersediaan, dan kinerja Amazon ECS. Mengumpulkan data dari definisi tugas memberikan visibilitas, yang dapat membantu Anda men-debug proses dan menemukan akar penyebab kesalahan. Jika Anda menggunakan solusi logging yang tidak harus didefinisikan dalam definisi tugas ECS (seperti solusi logging pihak ketiga), Anda dapat menonaktifkan kontrol ini setelah memastikan bahwa log Anda ditangkap dan dikirim dengan benar.

Remediasi

Untuk menentukan konfigurasi log untuk definisi tugas Amazon ECS Anda, lihat Menentukan konfigurasi log dalam definisi tugas Anda di Panduan Pengembang Layanan Amazon Elastic Container.

[ECS.10] Layanan ECS Fargate harus berjalan pada versi platform Fargate terbaru

Persyaratan terkait: NIST.800-53.R5 SI-2, NIST.800-53.R5 SI-2 (2), NIST.800-53.R5 SI-2 (4), Nist.800-53.R5 SI-2 (5)

Kategori: Identifikasi > Kerentanan, tambalan, dan manajemen versi

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::ECS::Service`

AWS Config aturan: **`ecs-fargate-latest-platform-version`**

Jenis jadwal: Perubahan dipicu

Parameter:

- `latestLinuxVersion: 1.4.0`(tidak dapat disesuaikan)
- `latestWindowsVersion: 1.0.0`(tidak dapat disesuaikan)

Kontrol ini memeriksa apakah layanan Amazon ECS Fargate menjalankan versi platform Fargate terbaru. Kontrol ini gagal jika versi platform bukan yang terbaru.

AWS Fargate Versi platform mengacu pada lingkungan runtime tertentu untuk infrastruktur tugas Fargate, yang merupakan kombinasi dari versi runtime kernel dan container. Versi platform baru dirilis saat lingkungan runtime berkembang. Misalnya, versi baru dapat dirilis untuk pembaruan kernel atau sistem operasi, fitur baru, perbaikan bug, atau pembaruan keamanan. Pembaruan dan tambalan keamanan diterapkan secara otomatis untuk tugas Fargate Anda. Jika ditemukan masalah keamanan yang memengaruhi versi platform, AWS tambal versi platform.

Remediasi

Untuk memperbarui layanan yang ada, termasuk versi platformnya, lihat Memperbarui layanan di Panduan Pengembang Layanan Amazon Elastic Container.

[ECS.12] Cluster ECS harus menggunakan Wawasan Kontainer

Persyaratan terkait: Nist.800-53.R5 AU-6 (3), Nist.800-53.R5 AU-6 (4), Nist.800-53.R5 CA-7, Nist.800-53.R5 SI-2

Kategori: Identifikasi > Logging

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::ECS::Cluster`

AWS Config aturan: **`ecs-container-insights-enabled`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah cluster ECS menggunakan Wawasan Kontainer. Kontrol ini gagal jika Wawasan Kontainer tidak disiapkan untuk klaster.

Pemantauan adalah bagian penting dalam menjaga keandalan, ketersediaan, dan kinerja klaster Amazon ECS. Gunakan CloudWatch Wawasan Kontainer untuk mengumpulkan, menggabungkan, dan meringkas metrik dan log dari aplikasi dan layanan mikro dalam kontainer Anda. CloudWatch Secara otomatis mengumpulkan metrik untuk banyak sumber daya, seperti CPU, memori, disk, dan jaringan. Wawasan Kontainer juga akan menyediakan informasi diagnostik, seperti kegagalan mengulang kembali kontainer, untuk membantu Anda melakukan isolasi atas masalah dan mengatasi masalah itu dengan cepat. Anda juga dapat menyetel CloudWatch alarm pada metrik yang dikumpulkan Container Insights.

Remediasi

Untuk menggunakan Wawasan Penampung, lihat Memperbarui layanan di Panduan CloudWatch Pengguna Amazon.

[ECS.13] Layanan ECS harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::ECS::Service`

AWS Config aturan: `tagged-ecs-service` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya	StringList	Daftar tag yang memenuhi	Tidak ada nilai default

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
	yang dievaluasi. Kunci tag peka huruf besar dan kecil.		AWS persyaratan	

Kontrol ini memeriksa apakah layanan Amazon ECS memiliki tag dengan kunci spesifik yang ditentukan dalam parameter`requiredTagKeys`. Kontrol gagal jika layanan tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika layanan tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke layanan ECS, lihat Menandai resource Amazon ECS Anda di Panduan Pengembang Layanan Kontainer Elastis Amazon.

[ECS.14] Cluster ECS harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::ECS::Cluster`

AWS Config aturan: `tagged-ecs-cluster` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList	Daftar tag yang memenuhi AWS persyaratan	Tidak ada nilai default

Kontrol ini memeriksa apakah klaster Amazon ECS memiliki tag dengan kunci spesifik yang ditentukan dalam parameter`requiredTagKeys`. Kontrol gagal jika cluster tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika cluster tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan

terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke cluster ECS, lihat Menandai resource Amazon ECS Anda di Panduan Pengembang Layanan Amazon Elastic Container.

[ECS.15] Definisi tugas ECS harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::ECS::TaskDefinition`

AWS Config aturan: `tagged-ecs-taskdefinition` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList	Daftar tag yang memenuhi AWS persyaratan	Tidak ada nilai default

Kontrol ini memeriksa apakah definisi tugas Amazon ECS memiliki tag dengan kunci tertentu yang ditentukan dalam parameter`requiredTagKeys`. Kontrol gagal jika definisi tugas tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika definisi tugas tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke definisi tugas ECS, lihat Menandai resource Amazon ECS Anda di Panduan Pengembang Layanan Amazon Elastic Container.

Kontrol Amazon Elastic Compute Cloud

Kontrol ini terkait dengan sumber daya Amazon EC2.

Kontrol ini mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[EC2.1] Snapshot Amazon EBS tidak boleh dipulihkan secara publik

Persyaratan terkait: PCI DSS v3.2.1/1.2.1, PCI DSS v3.2.1/1.3.1, PCI DSS v3.2.1/1.3.4, PCI DSS v3.2.1/7.2.1, Nist.800-53.r5 AC-21, Nist.800-53.r5 AC-3, Nist.800-53.r5 AC-3 (7), Nist.800-53.r5 AC-3 (7), Nist.800-53.r5 00-53.r5 AC-4, Nist.800-53.r5 AC-4 (21), Nist.800-53.r5 AC-6, Nist.800-53.r5 SC-7, Nist.800-53.r5 SC-7 (11), Nist.800-53.r5 SC-7 (16), Nist.800-53.r5 SC-7 (20), NIST.800-53.R5 SC-7 (21), NIST.800-53.R5 SC-7 (3), NIST.800-53.R5 SC-7 (4), NIST.800-53.R5 SC-7 (9)

Kategori: Lindungi > Konfigurasi jaringan aman

Tingkat keparahan: Kritis

Jenis sumber daya: `AWS::::Account`

AWS Config aturan: **`ebs-snapshot-public-restorable-check`**

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah snapshot Amazon Elastic Block Store tidak bersifat publik. Kontrol gagal jika snapshot Amazon EBS dapat dipulihkan oleh siapa pun.

Snapshot EBS digunakan untuk mencadangkan data pada volume EBS Anda ke Amazon S3 pada titik waktu tertentu. Anda dapat menggunakan snapshot untuk memulihkan status volume EBS sebelumnya. Jarang dapat diterima untuk berbagi snapshot dengan publik. Biasanya keputusan untuk membagikan snapshot secara publik dibuat karena kesalahan atau tanpa pemahaman lengkap tentang implikasinya. Pemeriksaan ini membantu memastikan bahwa semua pembagian tersebut sepenuhnya direncanakan dan disengaja.

Untuk menjadikan snapshot EBS publik menjadi pribadi, lihat Membagikan snapshot di Panduan Pengguna Amazon EC2. Untuk Tindakan, Ubah izin, pilih Pribadi.

[EC2.2] Grup keamanan default VPC tidak boleh mengizinkan lalu lintas masuk atau keluar

Persyaratan terkait: PCI DSS v3.2.1/1.2.1, PCI DSS v3.2.1/1.3.4, PCI DSS v3.2.1/2.1, Tolok Ukur Yayasan CIS v1.2.0/4.3, Tolok Ukur Yayasan CIS v1.4.0/5.3, Tolok Ukur AWS Yayasan CIS v3.0.0/5.4, Nist.800-53.r5 AC-4, Nist.800-53.r5 AC-4 4 (21), NIST.800-53.R5 SC-7, NIST.800-53.R5 SC-7 (11), Nist.800-53.r5 SC-7 (16), Nist.800-53.r5 AWS SC-7 (21), Nist.800-53.r5 SC-7 (4), Nist.800-53.r5 SC-7 (5) AWS

Kategori: Lindungi > Konfigurasi jaringan aman

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::EC2::SecurityGroup`

AWS Config aturan: **`vpc-default-security-group-closed`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah grup keamanan default VPC memungkinkan lalu lintas masuk atau keluar. Kontrol gagal jika grup keamanan mengizinkan lalu lintas masuk atau keluar.

Aturan untuk grup keamanan default memungkinkan semua lalu lintas keluar dan masuk dari antarmuka jaringan (dan instance terkait) yang ditetapkan ke grup keamanan yang sama. Kami menyarankan Anda untuk tidak menggunakan grup keamanan default. Karena grup keamanan default tidak dapat dihapus, Anda harus mengubah pengaturan aturan grup keamanan default untuk membatasi lalu lintas masuk dan keluar. Ini mencegah lalu lintas yang tidak diinginkan jika grup keamanan default secara tidak sengaja dikonfigurasi untuk sumber daya seperti instans EC2.

Remediasi

Untuk mengatasi masalah ini, mulailah dengan membuat grup keamanan paling tidak memiliki hak istimewa baru. Untuk petunjuknya, lihat Membuat grup keamanan di Panduan Pengguna Amazon VPC. Kemudian, tetapkan grup keamanan baru ke instans EC2 Anda. Untuk petunjuknya, lihat Mengubah grup keamanan instans di Panduan Pengguna Amazon EC2.

Setelah Anda menetapkan grup keamanan baru ke sumber daya Anda, hapus semua aturan masuk dan keluar dari grup keamanan default. Untuk petunjuknya, lihat Menghapus aturan grup keamanan di Panduan Pengguna Amazon VPC.

[EC2.3] Volume Amazon EBS yang terpasang harus dienkripsi saat istirahat

Persyaratan terkait: Nist.800-53.r5 CA-9 (1), NIST.800-53.R5 CM-3 (6), Nist.800-53.r5 SC-13, Nist.800-53.r5 SC-28, Nist.800-53.r5 SC-28 (1), Nist.800-53.r5 SC-7 (10), Nist.800-53.r5 SC-7 (10), Nist.800-53.r5 SC-7 (10), Nist.800-53.r5 SC-7 (10), Nist.800-53.r5 SC-7 (10), Nist.800-53.r5 SC-7 (10), Nist.800-53.r5 SC-7 (10), ST.800-53.R5 SI-7 (6)

Kategori: Lindungi > Perlindungan Data > Enkripsi data-at-rest

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::EC2::Volume`

AWS Config aturan: **`encrypted-volumes`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah volume EBS yang berada dalam keadaan terlampir dienkripsi. Untuk lulus pemeriksaan ini, volume EBS harus digunakan dan dienkripsi. Jika volume EBS tidak terpasang, maka tidak tunduk pada pemeriksaan ini.

Untuk lapisan keamanan tambahan data sensitif Anda dalam volume EBS, Anda harus mengaktifkan enkripsi EBS saat istirahat. Enkripsi Amazon EBS menawarkan solusi enkripsi langsung untuk sumber daya EBS Anda yang tidak mengharuskan Anda membangun, memelihara, dan mengamankan infrastruktur manajemen kunci Anda sendiri. Ini menggunakan kunci KMS saat membuat volume dan snapshot terenkripsi.

Untuk mempelajari lebih lanjut tentang enkripsi Amazon EBS, lihat enkripsi Amazon EBS di Panduan Pengguna Amazon EC2.

Remediasi

Tidak ada cara langsung untuk mengenkripsi volume atau snapshot yang tidak terenkripsi yang ada. Anda hanya dapat mengenkripsi volume atau snapshot baru saat Anda membuatnya.

Jika Anda mengaktifkan enkripsi secara default, Amazon EBS mengenkripsi volume atau snapshot baru yang dihasilkan menggunakan kunci default untuk enkripsi Amazon EBS. Meskipun Anda belum mengaktifkan enkripsi secara default, Anda dapat mengaktifkan enkripsi saat Anda membuat volume atau snapshot individu. Dalam kedua kasus tersebut, Anda dapat mengganti kunci default untuk enkripsi Amazon EBS dan memilih kunci terkelola pelanggan simetris.

Untuk informasi selengkapnya, lihat Membuat volume Amazon EBS dan Menyalin snapshot Amazon EBS di Panduan Pengguna Amazon EC2.

[EC2.4] Instans EC2 yang dihentikan harus dihapus setelah periode waktu tertentu

Persyaratan terkait: NIST.800-53.R5 CA-9 (1), Nist.800-53.R5 CM-2, Nist.800-53.R5 CM-2 (2)

Kategori: Identifikasi > Persediaan

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::EC2::Instance`

AWS Config aturan: **`ec2-stopped-instance`**

Jenis jadwal: Periodik

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`AllowedDays`	Jumlah hari instans EC2 diizinkan berada dalam keadaan berhenti sebelum menghasilkan temuan yang gagal.	Bilangan Bulat	1 untuk 365	`30`

Kontrol ini memeriksa apakah instans Amazon EC2 telah dihentikan lebih lama dari jumlah hari yang diizinkan. Kontrol gagal jika instans EC2 dihentikan lebih lama dari periode waktu maksimum yang diizinkan. Kecuali Anda memberikan nilai parameter khusus untuk jangka waktu maksimum yang diizinkan, Security Hub menggunakan nilai default 30 hari.

Ketika instans EC2 tidak berjalan untuk jangka waktu yang signifikan, itu menciptakan risiko keamanan karena instans tidak dipelihara secara aktif (dianalisis, ditambal, diperbarui). Jika kemudian diluncurkan, kurangnya perawatan yang tepat dapat mengakibatkan masalah tak terduga di AWS lingkungan Anda. Untuk mempertahankan instans EC2 dengan aman dari waktu ke waktu dalam keadaan tidak aktif, mulailah secara berkala untuk pemeliharaan dan kemudian hentikan setelah pemeliharaan. Idealnya, ini harus menjadi proses otomatis.

Remediasi

Untuk menghentikan instans EC2 yang tidak aktif, lihat Mengakhiri instance di Panduan Pengguna Amazon EC2.

[EC2.6] Pencatatan aliran VPC harus diaktifkan di semua VPC

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v1.2.0/2.9, Tolok Ukur Yayasan CIS v1.4.0/3.9, Tolok Ukur AWS Yayasan CIS v3.0.0/3.7, PCI DSS v3.2.1/10.3.3, PCI DSS v3.2.1/10.3.4, PCI DSS v3.2.1/10.3.5, PCI DSS v3.2.1/10.3.6, Nist.800-53.R5 AC-4 (26), NIST.800-53.R5 AU-12, NIST.800-53.R5 AU-2, NIST.800-53.R5 AU-3, NIST.800-53.R5 AU-6 (3), NIST.800-53.R5 AU-6 (4), NIST.800-53.R5 AWS CA-7, NIST.800-53.R5 SI-7 (8)

Kategori: Identifikasi > Logging

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::EC2::VPC`

AWS Config aturan: **`vpc-flow-logs-enabled`**

Jenis jadwal: Periodik

Parameter:

- `trafficType`: `REJECT` (tidak dapat disesuaikan)

Kontrol ini memeriksa apakah Amazon VPC Flow Logs ditemukan dan diaktifkan untuk VPC. Jenis lalu lintas diatur ke`Reject`.

Dengan fitur VPC Flow Logs, Anda dapat menangkap informasi tentang lalu lintas alamat IP yang menuju dan dari antarmuka jaringan di VPC Anda. Setelah membuat log aliran, Anda dapat melihat dan mengambil datanya di CloudWatch Log. Untuk mengurangi biaya, Anda juga dapat mengirim log aliran Anda ke Amazon S3.

Security Hub merekomendasikan agar Anda mengaktifkan flow logging untuk penolakan paket untuk VPC. Flow log memberikan visibilitas ke lalu lintas jaringan yang melintasi VPC dan dapat mendeteksi lalu lintas anomali atau memberikan wawasan selama alur kerja keamanan.

Secara default, catatan menyertakan nilai untuk berbagai komponen aliran alamat IP, termasuk sumber, tujuan, dan protokol. Untuk informasi selengkapnya dan deskripsi bidang log, lihat Log Aliran VPC di Panduan Pengguna Amazon VPC.

Remediasi

Untuk membuat Log Aliran VPC, lihat Membuat Log Aliran di Panduan Pengguna Amazon VPC. Setelah Anda membuka konsol VPC Amazon, pilih VPC Anda. Untuk Filter, pilih Tolak atau Semua.

[EC2.7] Enkripsi default EBS harus diaktifkan

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v1.4.0/2.2.1, Tolok Ukur Yayasan CIS v3.0.0/2.2.1, Nist.800-53.r5 CA-9 (1), Nist.800-53.r5 AWS CM-3 (6), Nist.800-53.r5 SC-13, Nist.800-53.r5 SC-28, Nist.800-53.r5 SC-28, Nist.800-53.r5 SC-28, Nist.800-53.r5 SC-28 -28 (1), NIST.800-53.R5 SC-7 (10), NIST.800-53.R5 SI-7 (6)

Kategori: Lindungi > Perlindungan Data > Enkripsi data-at-rest

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::::Account`

AWS Config aturan: **`ec2-ebs-encryption-by-default`**

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah enkripsi tingkat akun diaktifkan secara default untuk Amazon Elastic Block Store (Amazon EBS). Kontrol gagal jika enkripsi tingkat akun tidak diaktifkan.

Saat enkripsi diaktifkan untuk akun Anda, volume Amazon EBS dan salinan snapshot dienkripsi saat istirahat. Ini menambahkan lapisan perlindungan tambahan untuk data Anda. Untuk informasi selengkapnya, lihat Enkripsi secara default di Panduan Pengguna Amazon EC2.

Perhatikan bahwa jenis instance berikut tidak mendukung enkripsi: R1, C1, dan M1.

Remediasi

Untuk mengonfigurasi enkripsi default untuk volume Amazon EBS, lihat Enkripsi secara default di Panduan Pengguna Amazon EC2.

[EC2.8] Instans EC2 harus menggunakan Layanan Metadata Instance Versi 2 (IMDSv2)

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v3.0.0/5.6, Nist.800-53.r5 AC-3, Nist.800-53.r5 AC-3 (15), Nist.800-53.r5 AC-3 (7), Nist.800-53.r5 AC-6

Kategori: Lindungi > Keamanan Jaringan

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::EC2::Instance`

AWS Config aturan: **`ec2-imdsv2-check`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah versi metadata instans EC2 Anda dikonfigurasi dengan Instance Metadata Service Version 2 (IMDSv2). Kontrol lolos jika `HttpTokens` disetel ke required untuk IMDSv2. Kontrol gagal jika `HttpTokens` disetel ke`optional`.

Anda menggunakan metadata instance untuk mengonfigurasi atau mengelola instance yang sedang berjalan. IMDS menyediakan akses ke kredensyal sementara yang sering diputar. Kredensyal ini menghapus kebutuhan untuk kode keras atau mendistribusikan kredensyal sensitif ke instance secara manual atau terprogram. IMDS dilampirkan secara lokal ke setiap instans EC2. Ini berjalan pada alamat IP “link lokal” khusus 169.254.169.254. Alamat IP ini hanya dapat diakses oleh perangkat lunak yang berjalan pada instance.

Versi 2 IMDS menambahkan perlindungan baru untuk jenis kerentanan berikut. Kerentanan ini dapat digunakan untuk mencoba mengakses IMDS.

- Buka firewall aplikasi situs web
- Buka proxy terbalik
- Kerentanan pemalsuan permintaan sisi server (SSRF)
- Buka firewall Layer 3 dan terjemahan alamat jaringan (NAT)

Security Hub merekomendasikan agar Anda mengonfigurasi instans EC2 Anda dengan IMDSv2.

Remediasi

Untuk mengonfigurasi instans EC2 dengan IMDSv2, lihat Jalur yang disarankan untuk mewajibkan IMDSv2 di Panduan Pengguna Amazon EC2.

[EC2.9] Instans Amazon EC2 seharusnya tidak memiliki alamat IPv4 publik

Persyaratan terkait: Nist.800-53.r5 AC-21, Nist.800-53.r5 AC-3, Nist.800-53.r5 AC-3 (7), Nist.800-53.r5 AC-4, Nist.800-53.r5 AC-4 (21), Nist.800-53.r5 AC-6, Nist.800-53.r5 R5 SC-7, Nist.800-53.r5 SC-7 (11), NIST.800-53.R5 SC-7 (16), Nist.800-53.r5 SC-7 (20), Nist.800-53.r5 SC-7 (21), Nist.800-53.r5 SC-7 (3), Nist.800-53.r5 5 SC-7 (4), NIST.800-53.R5 SC-7 (9)

Kategori: Lindungi > Konfigurasi jaringan aman > Sumber daya tidak dapat diakses publik

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::EC2::Instance`

AWS Config aturan: **`ec2-instance-no-public-ip`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah instans EC2 memiliki alamat IP publik. Kontrol gagal jika `publicIp` bidang hadir dalam item konfigurasi instans EC2. Kontrol ini hanya berlaku untuk alamat IPv4.

Alamat IPv4 publik adalah alamat IP yang dapat dijangkau dari internet. Jika Anda meluncurkan instans Anda dengan alamat IP publik, maka instans EC2 Anda dapat dijangkau dari internet. Alamat IPv4 pribadi adalah alamat IP yang tidak dapat dijangkau dari internet. Anda dapat menggunakan alamat IPv4 pribadi untuk komunikasi antara instans EC2 di VPC yang sama atau di jaringan pribadi Anda yang terhubung.

Alamat IPv6 unik secara global, dan karenanya dapat dijangkau dari internet. Namun, secara default semua subnet memiliki atribut pengalamatan IPv6 disetel ke false. Untuk informasi selengkapnya tentang IPv6, lihat Pengalamatan IP di VPC Anda di Panduan Pengguna Amazon VPC.

Jika Anda memiliki kasus penggunaan yang sah untuk mempertahankan instans EC2 dengan alamat IP publik, maka Anda dapat menekan temuan dari kontrol ini. Untuk informasi selengkapnya tentang opsi arsitektur front-end, lihat Blog AWS Arsitektur atau seri This Is My Architecture.

Remediasi

Gunakan VPC non-default sehingga instans Anda tidak diberi alamat IP publik secara default.

Ketika Anda meluncurkan instans EC2 ke VPC default, itu diberikan alamat IP publik. Saat Anda meluncurkan instans EC2 ke VPC non-default, konfigurasi subnet menentukan apakah ia menerima alamat IP publik. Subnet memiliki atribut untuk menentukan apakah instans EC2 baru di subnet menerima alamat IP publik dari kumpulan alamat IPv4 publik.

Anda tidak dapat secara manual mengaitkan atau memisahkan alamat IP publik yang ditetapkan secara otomatis dari instans EC2 Anda. Untuk mengontrol apakah instans EC2 Anda menerima alamat IP publik, lakukan salah satu hal berikut:

- Ubah atribut pengalamatan IP publik dari subnet Anda. Untuk informasi selengkapnya, lihat Memodifikasi atribut pengalamatan IPv4 publik untuk subnet Anda dalam Panduan Pengguna Amazon VPC.
- Aktifkan atau nonaktifkan fitur pengalamatan IP publik selama peluncuran. Ini mengesampingkan atribut pengalamatan IP publik subnet. Untuk informasi selengkapnya, lihat Menetapkan alamat IPv4 publik selama peluncuran instans di Panduan Pengguna Amazon EC2.

Untuk informasi selengkapnya, lihat Alamat IPv4 publik dan nama host DNS eksternal di Panduan Pengguna Amazon EC2.

Jika instans EC2 Anda dikaitkan dengan alamat IP Elastis, maka instans EC2 Anda dapat dijangkau dari internet. : Untuk melepaskan pengaitan alamat IP Elastis dari instans atau antarmuka jaringan. Untuk memisahkan alamat IP Elastis, lihat Memutuskan alamat IP Elastis di Panduan Pengguna Amazon EC2.

[EC2.10] Amazon EC2 harus dikonfigurasi untuk menggunakan titik akhir VPC yang dibuat untuk layanan Amazon EC2

Persyaratan terkait: Nist.800-53.r5 AC-21, Nist.800-53.r5 AC-3, Nist.800-53.r5 AC-3 (7), Nist.800-53.r5 AC-4, Nist.800-53.r5 AC-4 (21), Nist.800-53.r5 AC-6, Nist.800-53.r5 R5 SC-7, Nist.800-53.r5 SC-7 (11), NIST.800-53.R5 SC-7 (16), Nist.800-53.r5 SC-7 (20), Nist.800-53.r5 SC-7 (21), Nist.800-53.r5 SC-7 (3), Nist.800-53.r5 5 SC-7 (4)

Kategori: Lindungi > Konfigurasi jaringan aman > Akses pribadi API

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::EC2::VPC`

AWS Config aturan: **`service-vpc-endpoint-enabled`**

Jenis jadwal: Periodik

Parameter:

- `serviceName`: `ec2` (tidak dapat disesuaikan)

Kontrol ini memeriksa apakah titik akhir layanan untuk Amazon EC2 dibuat untuk setiap VPC. Kontrol gagal jika VPC tidak memiliki titik akhir VPC yang dibuat untuk layanan Amazon EC2.

Kontrol ini mengevaluasi sumber daya dalam satu akun. Itu tidak dapat menggambarkan sumber daya yang berada di luar akun. Karena AWS Config Security Hub tidak melakukan pemeriksaan lintas akun, Anda akan melihat `FAILED` temuan untuk VPC yang dibagikan di seluruh akun. Security Hub merekomendasikan agar Anda menekan `FAILED` temuan ini.

Untuk meningkatkan postur keamanan VPC Anda, Anda dapat mengonfigurasi Amazon EC2 untuk menggunakan titik akhir VPC antarmuka. Endpoint antarmuka didukung oleh AWS PrivateLink, teknologi yang memungkinkan Anda mengakses operasi Amazon EC2 API secara pribadi. Ini membatasi semua lalu lintas jaringan antara VPC Anda dan Amazon EC2 ke jaringan Amazon. Karena titik akhir hanya didukung dalam Wilayah yang sama, Anda tidak dapat membuat titik akhir antara VPC dan layanan di Wilayah yang berbeda. Ini mencegah panggilan API Amazon EC2 yang tidak diinginkan ke Wilayah lain.

Untuk mempelajari selengkapnya tentang membuat titik akhir VPC untuk Amazon EC2, lihat Amazon EC2 dan titik akhir VPC antarmuka di Panduan Pengguna Amazon EC2.

Remediasi

Untuk membuat titik akhir antarmuka ke Amazon EC2 dari konsol VPC Amazon, lihat Membuat titik akhir VPC di Panduan.AWS PrivateLink Untuk nama Layanan, pilih com.amazonaws. ***wilayah*** .ec2.

Anda juga dapat membuat dan melampirkan kebijakan titik akhir ke titik akhir VPC Anda untuk mengontrol akses ke Amazon EC2 API. Untuk petunjuk cara membuat kebijakan titik akhir VPC, lihat Membuat kebijakan titik akhir di Panduan Pengguna Amazon EC2.

[EC2.12] EIP Amazon EC2 yang tidak digunakan harus dihapus

Persyaratan terkait: PCI DSS v3.2.1/2.4, Nist.800-53.r5 CM-8 (1)

Kategori: Lindungi > Konfigurasi jaringan aman

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::EC2::EIP`

AWS Config aturan: **`eip-attached`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah alamat Elastic IP (EIP) yang dialokasikan ke VPC dilampirkan ke instans EC2 atau antarmuka jaringan elastis (ENI) yang sedang digunakan.

Temuan yang gagal menunjukkan Anda mungkin memiliki EC2 EIP yang tidak digunakan.

Ini akan membantu Anda mempertahankan inventaris aset EIP yang akurat di lingkungan data pemegang kartu (CDE) Anda.

Untuk merilis EIP yang tidak digunakan, lihat Melepaskan alamat IP Elastis di Panduan Pengguna Amazon EC2.

[EC2.13] Grup keamanan tidak boleh mengizinkan masuknya dari 0.0.0.0/0 atau: :/0 ke port 22

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v1.2.0/4.1, PCI DSS v3.2.1/1.2.1, PCI DSS v3.2.1/1.3.1, PCI DSS v3.2.1/2.2.2, Nist.800-53.r5 AC-4, NIST.800-53.R5 AC-4 (21), Nist.800-53.r5 CM-7, NIST.800-500-500-553.R5 SC-7, NIST.800-53.R5 SC-7 (11), NIST.800-53.R5 SC-7 (16), Nist.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (4), Nist.800-53.r5 SC-7 (5)

Kategori: Lindungi > Konfigurasi jaringan aman

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::EC2::SecurityGroup`

AWS Config aturan: **`restricted-ssh`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah grup keamanan Amazon EC2 mengizinkan masuknya dari 0.0.0.0/0 atau: :/0 ke port 22. Kontrol gagal jika grup keamanan mengizinkan masuknya dari 0.0.0.0/0 atau: :/0 ke port 22.

Grup keamanan menyediakan penyaringan stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Kami menyarankan agar tidak ada grup keamanan yang mengizinkan akses masuk tanpa batas ke port 22. Menghapus konektivitas tanpa batas ke layanan konsol jarak jauh, seperti SSH, mengurangi eksposur server terhadap risiko.

Remediasi

Untuk melarang masuknya ke port 22, hapus aturan yang memungkinkan akses tersebut untuk setiap grup keamanan yang terkait dengan VPC. Untuk petunjuknya, lihat Memperbarui aturan grup

keamanan di Panduan Pengguna Amazon EC2. Setelah memilih grup keamanan di konsol Amazon EC2, pilih Tindakan, Edit aturan masuk. Hapus aturan yang memungkinkan akses ke port 22.

[EC2.14] Grup keamanan tidak boleh mengizinkan masuknya dari 0.0.0.0/0 atau: :/0 ke port 3389

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v1.2.0/4.2

Kategori: Lindungi > Konfigurasi jaringan aman

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::EC2::SecurityGroup`

AWS Config aturan: **`restricted-common-ports`**(aturan yang dibuat adalah`restricted-rdp`)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah grup keamanan Amazon EC2 mengizinkan masuknya dari 0.0.0.0/0 atau: :/0 ke port 3389. Kontrol gagal jika grup keamanan mengizinkan masuknya dari 0.0.0.0/0 atau: :/0 ke port 3389.

Grup keamanan menyediakan penyaringan stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Kami menyarankan agar tidak ada grup keamanan yang mengizinkan akses masuk tanpa batas ke port 3389. Menghapus konektivitas tanpa batas ke layanan konsol jarak jauh, seperti RDP, mengurangi eksposur server terhadap risiko.

Remediasi

Untuk melarang masuknya ke port 3389, hapus aturan yang memungkinkan akses tersebut untuk setiap grup keamanan yang terkait dengan VPC. Untuk petunjuknya, lihat Memperbarui aturan grup keamanan di Panduan Pengguna Amazon VPC. Setelah memilih grup keamanan di Konsol VPC Amazon, pilih Tindakan, Edit aturan masuk. Hapus aturan yang memungkinkan akses ke port 3389.

[EC2.15] Subnet Amazon EC2 seharusnya tidak secara otomatis menetapkan alamat IP publik

Persyaratan terkait: Nist.800-53.r5 AC-21, Nist.800-53.r5 AC-3, Nist.800-53.r5 AC-3 (7), Nist.800-53.r5 AC-4, Nist.800-53.r5 AC-4 (21), Nist.800-53.r5 AC-6, Nist.800-53.r5 R5 SC-7,

Nist.800-53.r5 SC-7 (11), NIST.800-53.R5 SC-7 (16), Nist.800-53.r5 SC-7 (20), Nist.800-53.r5 SC-7 (21), Nist.800-53.r5 SC-7 (3), Nist.800-53.r5 5 SC-7 (4), NIST.800-53.R5 SC-7 (9)

Kategori: Lindungi > Keamanan Jaringan

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::EC2::Subnet`

AWS Config aturan: **`subnet-auto-assign-public-ip-disabled`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah penetapan IP publik di subnet Amazon Virtual Private Cloud (Amazon VPC) telah disetel ke. `MapPublicIpOnLaunch` `FALSE` Kontrol lolos jika bendera disetel ke`FALSE`.

Semua subnet memiliki atribut yang menentukan apakah antarmuka jaringan yang dibuat di subnet secara otomatis menerima alamat IPv4 publik. Instance yang diluncurkan ke subnet yang memiliki atribut ini diaktifkan memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utama mereka.

Remediasi

Untuk mengonfigurasi subnet agar tidak menetapkan alamat IP publik, lihat Memodifikasi atribut pengalamatan IPv4 publik untuk subnet Anda di Panduan Pengguna Amazon VPC. Kosongkan kotak centang untuk Aktifkan alamat IPv4 publik yang ditetapkan secara otomatis.

[EC2.16] Daftar Kontrol Akses Jaringan yang Tidak Digunakan harus dihapus

Persyaratan terkait: Nist.800-53.r5 CM-8 (1)

Kategori: Lindungi > Keamanan Jaringan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::EC2::NetworkAcl`

AWS Config aturan: **`vpc-network-acl-unused-check`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah ada daftar kontrol akses jaringan (ACL jaringan) yang tidak digunakan di cloud pribadi virtual (VPC) Anda. Kontrol gagal jika ACL jaringan tidak terkait dengan subnet. Kontrol tidak menghasilkan temuan untuk ACL jaringan default yang tidak digunakan.

Kontrol memeriksa konfigurasi item sumber daya `AWS::EC2::NetworkAcl` dan menentukan hubungan ACL jaringan.

Jika satu-satunya hubungan adalah VPC jaringan ACL, kontrol gagal.

Jika hubungan lain terdaftar, maka kontrol berlalu.

Remediasi

Untuk petunjuk cara menghapus ACL jaringan yang tidak digunakan, lihat Menghapus ACL jaringan di Panduan Pengguna Amazon VPC. Anda tidak dapat menghapus ACL jaringan default atau ACL yang terkait dengan subnet.

[EC2.17] Instans Amazon EC2 tidak boleh menggunakan beberapa ENI

Persyaratan terkait: Nist.800-53.r5 AC-4 (21)

Kategori: Lindungi > Keamanan Jaringan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::EC2::Instance`

AWS Config aturan: **`ec2-instance-multiple-eni-check`**

Jenis jadwal: Perubahan dipicu

Parameter:

- `Adapterids`— Daftar ID antarmuka jaringan yang dilampirkan ke instans EC2 (tidak dapat disesuaikan)

Kontrol ini memeriksa apakah instans EC2 menggunakan beberapa Elastic Network Interfaces (ENIs) atau Elastic Fabric Adapters (EFA). Kontrol ini lolos jika adaptor jaringan tunggal digunakan. Kontrol mencakup daftar parameter opsional untuk mengidentifikasi ENI yang diizinkan. Kontrol ini juga gagal

jika instans EC2 milik kluster Amazon EKS menggunakan lebih dari satu ENI. Jika instans EC2 Anda perlu memiliki beberapa ENI sebagai bagian dari kluster Amazon EKS, Anda dapat menekan temuan kontrol tersebut.

Beberapa ENI dapat menyebabkan instance dual-homed, yang berarti instance yang memiliki beberapa subnet. Ini dapat menambah kompleksitas keamanan jaringan dan memperkenalkan jalur dan akses jaringan yang tidak diinginkan.

Remediasi

Untuk melepaskan antarmuka jaringan dari instans EC2, lihat Melepaskan antarmuka jaringan dari instans di Panduan Pengguna Amazon EC2.

[EC2.18] Grup keamanan seharusnya hanya mengizinkan lalu lintas masuk yang tidak terbatas untuk port resmi

Persyaratan terkait: Nist.800-53.r5 AC-4, NIST.800-53.R5 AC-4 (21), Nist.800-53.r5 SC-7, Nist.800-53.r5 SC-7 (11), Nist.800-53.r5 SC-7 (16), Nist.800-53.r5 SC-7 (21), Nist.800-53.r5 SC-7 (21), Nist.800-53.r5 SC-7 (21), Nist.800-53.r5 SC-7 (21), Nist.800-53.r5 SC-7 (21), Nist.800-53.r5 SC-7 (21), Nist.800-53.r5 SC-7 (21), ST.800-53.R5 SC-7 (4), NIST.800-53.R5 SC-7 (5)

Kategori: Lindungi > Konfigurasi jaringan aman > Konfigurasi grup keamanan

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::EC2::SecurityGroup`

AWS Config aturan: **`vpc-sg-open-only-to-authorized-ports`**

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`authorizedTcpPorts`	Daftar port TCP resmi	IntegerList (maksimal 32 item)	1 untuk 65535	`[80,443]`

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`authorizedUdpPorts`	Daftar port UDP resmi	IntegerList (maksimal 32 item)	1 untuk 65535	Tidak ada nilai default

Kontrol ini memeriksa apakah grup keamanan Amazon EC2 mengizinkan lalu lintas masuk yang tidak dibatasi dari port yang tidak sah. Status kontrol ditentukan sebagai berikut:

- Jika Anda menggunakan nilai default untuk`authorizedTcpPorts`, kontrol gagal jika grup keamanan mengizinkan lalu lintas masuk yang tidak dibatasi dari port selain port 80 dan 443.
- Jika Anda memberikan nilai khusus untuk `authorizedTcpPorts` atau`authorizedUdpPorts`, kontrol gagal jika grup keamanan mengizinkan lalu lintas masuk yang tidak dibatasi dari port yang tidak terdaftar.
- Jika tidak ada parameter yang digunakan, kontrol gagal untuk grup keamanan mana pun yang memiliki aturan lalu lintas masuk yang tidak dibatasi.

Grup keamanan menyediakan penyaringan stateful dari lalu lintas jaringan masuk dan keluar ke. AWS Aturan grup keamanan harus mengikuti prinsip akses yang paling tidak memiliki hak istimewa. Akses tidak terbatas (alamat IP dengan akhiran /0) meningkatkan peluang aktivitas berbahaya seperti peretasan, denial-of-service serangan, dan kehilangan data. Kecuali port diizinkan secara khusus, port harus menolak akses tidak terbatas.

Remediasi

Untuk mengubah grup keamanan, lihat Bekerja dengan grup keamanan di Panduan Pengguna Amazon VPC.

[EC2.19] Grup keamanan tidak boleh mengizinkan akses tidak terbatas ke port dengan risiko tinggi

Persyaratan terkait: Nist.800-53.r5 AC-4, Nist.800-53.r5 AC-4 (21), Nist.800-53.r5 CA-9 (1), Nist.800-53.r5 CM-2, Nist.800-53.r5 CM-2 (2), Nist.800-53.r5 CM-7, Nist.800-53.r5 CM-7, Nist.800-53.r5 00-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), Nist.800-53.r5 SC-7 (16), Nist.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (5)

Kategori: Lindungi > Akses jaringan terbatas

Tingkat keparahan: Kritis

Jenis sumber daya: `AWS::EC2::SecurityGroup`

AWS Config aturan: **`restricted-common-ports`**(aturan yang dibuat adalah`vpc-sg-restricted-common-ports`)

Jenis jadwal: Perubahan dipicu

Parameter: `"blockedPorts": "20,21,22,23,25,110,135,143,445,1433,1434,3000,3306,3389,4333,5000,5432,5500,560` (tidak dapat disesuaikan)

Kontrol ini memeriksa apakah lalu lintas masuk yang tidak dibatasi untuk grup keamanan Amazon EC2 dapat diakses ke port tertentu yang dianggap berisiko tinggi. Kontrol ini gagal jika salah satu aturan dalam grup keamanan mengizinkan lalu lintas masuk dari '0.0.0.0/0' atau ': :/0' ke port tersebut.

Grup keamanan menyediakan penyaringan stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Akses tidak terbatas (0.0.0.0/0) meningkatkan peluang untuk aktivitas berbahaya, seperti peretasan, denial-of-service serangan, dan kehilangan data. Tidak ada grup keamanan yang mengizinkan akses masuk tanpa batas ke port berikut:

- 20, 21 (FTP)
- 22 (SSH)
- 23 (Telnet)
- 25 (SMTP)
- 110 (POP3)
- 135 (RPC)
- 143 (IMAP)
- 445 (CIFS)
- 1433, 1434 (MSSQL)
- 3000 (kerangka kerja pengembangan web Go, Node.js, dan Ruby)
- 3306 (MySQL)
- 3389 (RDP)

- 4333 (ahsp)
- 5000 (Kerangka pengembangan web Python)
- 5432 (Postgresql)
- 5500 (fcp-addr-srvr1)
- 5601 (Dasbor) OpenSearch
- 8080 (proksi)
- 8088 (port HTTP lama)
- 8888 (port HTTP alternatif)
- 9200 atau 9300 () OpenSearch

Remediasi

Untuk menghapus aturan dari grup keamanan, lihat Menghapus aturan dari grup keamanan di Panduan Pengguna Amazon EC2.

[EC2.20] Kedua terowongan VPN untuk koneksi VPN Site-to-Site harus AWS aktif

Persyaratan terkait: Nist.800-53.r5 CP-10, Nist.800-53.R5 CP-6 (2), Nist.800-53.R5 SC-36, Nist.800-53.R5 SC-5 (2), Nist.800-53.r5 SI-13 (5)

Kategori: Pulihkan > Ketahanan > Ketersediaan tinggi

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::EC2::VPNConnection`

AWS Config aturan: **`vpc-vpn-2-tunnels-up`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Terowongan VPN adalah tautan terenkripsi tempat data dapat diteruskan dari jaringan pelanggan ke atau dari AWS dalam koneksi VPN AWS Site-to-Site. Setiap koneksi VPN mencakup dua terowongan VPN yang dapat Anda gunakan secara bersamaan untuk ketersediaan tinggi. Memastikan bahwa kedua terowongan VPN siap untuk koneksi VPN penting untuk mengonfirmasi koneksi yang aman dan sangat tersedia antara AWS VPC dan jaringan jarak jauh Anda.

Kontrol ini memeriksa apakah kedua terowongan VPN yang disediakan oleh AWS Site-to-Site VPN berada dalam status UP. Kontrol gagal jika salah satu atau kedua terowongan berada dalam status DOWN.

Remediasi

Untuk mengubah opsi terowongan VPN, lihat Memodifikasi opsi terowongan VPN Site-to-Site di Panduan Pengguna VPN Site-to-Site. AWS

[EC2.21] ACL jaringan seharusnya tidak mengizinkan masuknya dari 0.0.0.0/0 ke port 22 atau port 3389

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v1.4.0/5.1, Tolok Ukur Yayasan CIS v3.0.0/5.1, Nist.800-53.r5 AC-4 (21), Nist.800-53.r5 AWS CA-9 (1), Nist.800-53.r5 CM-2, Nist.800-53.r5 CM-2 (2), Nist.800-53.r5 CM-7, NIST.800-53.R5 SC-7, NIST.800-53.R5 SC-7 (21), NIST.800-53.R5 SC-7 (5)

Kategori: Lindungi > Konfigurasi Jaringan Aman

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::EC2::NetworkAcl`

AWS Config aturan: **`nacl-no-unrestricted-ssh-rdp`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah daftar kontrol akses jaringan (ACL jaringan) memungkinkan akses tidak terbatas ke port TCP default untuk lalu lintas masuk SSH/RDP. Kontrol gagal jika entri masuk ACL jaringan memungkinkan blok CIDR sumber '0.0.0.0/0' atau ': :/0' untuk port TCP 22 atau 3389. Kontrol tidak menghasilkan temuan untuk ACL jaringan default.

Akses ke port administrasi server jarak jauh, seperti port 22 (SSH) dan port 3389 (RDP), tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke sumber daya dalam VPC Anda.

Remediasi

Untuk mengedit aturan lalu lintas ACL jaringan, lihat Bekerja dengan ACL jaringan di Panduan Pengguna Amazon VPC.

[EC2.22] Grup keamanan Amazon EC2 yang tidak digunakan harus dihapus

> **Important**
>
> PENSIUN DARI STANDAR KHUSUS - Security Hub menghapus kontrol ini pada 20 September 2023 dari standar Praktik Terbaik Keamanan AWS Dasar dan NIST SP 800-53 Rev. 5. Kontrol ini masih merupakan bagian dari Standar yang Dikelola Layanan:. AWS Control Tower Kontrol ini menghasilkan temuan yang diteruskan jika grup keamanan dilampirkan ke instans EC2 atau ke elastic network interface. Namun, untuk kasus penggunaan tertentu, kelompok keamanan yang tidak terikat tidak menimbulkan risiko keamanan. Anda dapat menggunakan kontrol EC2 lainnya—seperti EC2.2, EC2.13, EC2.14, EC2.18, dan EC2.19—untuk memantau grup keamanan Anda.

Kategori: Identifikasi > Persediaan

Tingkat keparahan: Sedang

Jenis sumber daya:`AWS::EC2::NetworkInterface`, `AWS::EC2::SecurityGroup`

AWS Config aturan: **`ec2-security-group-attached-to-eni-periodic`**

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah grup keamanan dilampirkan ke instans Amazon Elastic Compute Cloud (Amazon EC2) atau ke antarmuka elastic network. Kontrol gagal jika grup keamanan tidak terkait dengan instans Amazon EC2 atau elastic network interface.

Remediasi

Untuk membuat, menetapkan, dan menghapus grup keamanan, lihat Grup keamanan di panduan pengguna Amazon EC2.

[EC2.23] Amazon EC2 Transit Gateways seharusnya tidak secara otomatis menerima permintaan lampiran VPC

Persyaratan terkait: Nist.800-53.r5 AC-4 (21), NIST.800-53.R5 CA-9 (1), Nist.800-53.r5 CM-2

Kategori: Lindungi > Konfigurasi jaringan aman

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::EC2::TransitGateway`

AWS Config aturan: **`ec2-transit-gateway-auto-vpc-attach-disabled`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah gateway transit EC2 secara otomatis menerima lampiran VPC bersama. Kontrol ini gagal untuk gateway transit yang secara otomatis menerima permintaan lampiran VPC bersama.

Menghidupkan `AutoAcceptSharedAttachments` mengonfigurasi gateway transit untuk secara otomatis menerima permintaan lampiran VPC lintas akun apa pun tanpa memverifikasi permintaan atau akun tempat lampiran berasal. Untuk mengikuti praktik otorisasi dan otentikasi terbaik, kami sarankan untuk mematikan fitur ini untuk memastikan bahwa hanya permintaan lampiran VPC resmi yang diterima.

Remediasi

Untuk mengubah gateway transit, lihat Memodifikasi gateway transit di Panduan Pengembang Amazon VPC.

[EC2.24] Jenis instans paravirtual Amazon EC2 tidak boleh digunakan

Persyaratan terkait: Nist.800-53.r5 CM-2, Nist.800-53.r5 CM-2 (2)

Kategori: Identifikasi > Kerentanan, tambalan, dan manajemen versi

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::EC2::Instance`

AWS Config aturan: **`ec2-paravirtual-instance-check`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah jenis virtualisasi dari instans EC2 adalah paravirtual. Kontrol gagal jika instans EC2 diatur ke`paravirtual`. `virtualizationType`

Linux Amazon Machine Images (AMI) menggunakan salah satu dari dua jenis virtualisasi: paravirtual (PV) atau hardware virtual machine (HVM). Perbedaan utama antara AMI PV dan HVM adalah caranya melakukan boot dan apakah keduanya dapat memanfaatkan ekstensi perangkat keras khusus (CPU, jaringan, dan penyimpanan) untuk performa yang lebih baik.

Secara historis, tamu PV biasanya memiliki performa yang lebih baik dibandingkan tamu HVM, tetapi karena peningkatan virtualisasi HVM dan ketersediaan driver PV untuk HVM HMI, ini tidak lagi benar. Untuk informasi selengkapnya, lihat jenis virtualisasi AMI Linux di Panduan Pengguna Amazon EC2.

Remediasi

Untuk memperbarui instans EC2 ke jenis instans baru, lihat Mengubah jenis instans di Panduan Pengguna Amazon EC2.

[EC2.25] Templat peluncuran Amazon EC2 tidak boleh menetapkan IP publik ke antarmuka jaringan

Persyaratan terkait: Nist.800-53.r5 AC-21, Nist.800-53.r5 AC-3, Nist.800-53.r5 AC-3 (7), Nist.800-53.r5 AC-4, Nist.800-53.r5 AC-4 (21), Nist.800-53.r5 AC-6, Nist.800-53.r5 R5 SC-7, Nist.800-53.r5 SC-7 (11), NIST.800-53.R5 SC-7 (16), Nist.800-53.r5 SC-7 (20), Nist.800-53.r5 SC-7 (21), Nist.800-53.r5 SC-7 (3), Nist.800-53.r5 5 SC-7 (4), NIST.800-53.R5 SC-7 (9)

Kategori: Lindungi > Konfigurasi jaringan aman > Sumber daya tidak dapat diakses publik

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::EC2::LaunchTemplate`

AWS Config aturan: **`ec2-launch-template-public-ip-disabled`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah templat peluncuran Amazon EC2 dikonfigurasi untuk menetapkan alamat IP publik ke antarmuka jaringan saat diluncurkan. Kontrol gagal jika template peluncuran EC2 dikonfigurasi untuk menetapkan alamat IP publik ke antarmuka jaringan atau jika ada setidaknya satu antarmuka jaringan yang memiliki alamat IP publik.

Alamat IP publik adalah alamat yang dapat dijangkau dari internet. Jika Anda mengonfigurasi antarmuka jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan antarmuka jaringan tersebut dapat dijangkau dari internet. Sumber daya EC2 tidak boleh diakses publik karena ini memungkinkan akses yang tidak diinginkan ke beban kerja Anda.

Remediasi

Untuk memperbarui template peluncuran EC2, lihat Mengubah setelan antarmuka jaringan default di Panduan Pengguna Auto Scaling Amazon EC2.

[EC2.28] Volume EBS harus dicakup oleh rencana cadangan

Kategori: Pulih> Ketahanan > Cadangan diaktifkan

Persyaratan terkait: Nist.800-53.r5 CP-10, Nist.800-53.r5 CP-6, Nist.800-53.R5 CP-6 (1), Nist.800-53.r5 CP-6 (2), Nist.800-53.r5 CP-9, Nist.800-53.r5 SC-5 (2), Nist.800-53.r5 SC-5 (2), Nist.800-53.r5 00-53.R5 SI-12, NIST.800-53.R5 SI-13 (5)

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::EC2::Volume`

AWS Config aturan: **`ebs-resources-protected-by-backup-plan`**

Jenis jadwal: Periodik

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`backupVaultLockCheck`	Kontrol menghasilkan `PASSED` temuan jika parameter disetel ke `true` dan sumber daya menggunakan AWS Backup Vault Lock.	Boolean	`true` atau `false`	Tidak ada nilai default

Kontrol ini mengevaluasi jika volume Amazon EBS dalam `in-use` status dicakup oleh paket cadangan. Kontrol gagal jika volume EBS tidak tercakup oleh paket cadangan. Jika Anda menyetel

`backupVaultLockCheck` parameter sama dengan`true`, kontrol hanya akan diteruskan jika volume EBS dicadangkan di brankas yang AWS Backup terkunci.

Cadangan membantu Anda pulih lebih cepat dari insiden keamanan. Mereka juga memperkuat ketahanan sistem Anda. Menyertakan volume Amazon EBS dalam paket cadangan membantu Anda melindungi data dari kehilangan atau penghapusan yang tidak diinginkan.

Remediasi

Untuk menambahkan volume Amazon EBS ke paket AWS Backup cadangan, lihat Menetapkan sumber daya ke paket cadangan di Panduan AWS Backup Pengembang.

[EC2.33] Lampiran gateway transit EC2 harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::EC2::TransitGatewayAttachment`

AWS Config aturan: `tagged-ec2-transitgatewayattachment` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList	Daftar tag yang memenuhi AWS persyaratan	Tidak ada nilai default

Kontrol ini memeriksa apakah lampiran gateway transit Amazon EC2 memiliki tag dengan kunci spesifik yang ditentukan dalam parameter. `requiredTagKeys` Kontrol gagal jika lampiran

gateway transit tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika lampiran gateway transit tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke lampiran gateway transit EC2, lihat Menandai sumber daya Amazon EC2 Anda di Panduan Pengguna Amazon EC2.

[EC2.34] Tabel rute gateway transit EC2 harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::EC2::TransitGatewayRouteTable`

AWS Config aturan: `tagged-ec2-transitgatewayroutetable` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList	Daftar tag yang memenuhi AWS persyaratan	Tidak ada nilai default

Kontrol ini memeriksa apakah tabel rute gateway transit Amazon EC2 memiliki tag dengan kunci tertentu yang ditentukan dalam parameter. `requiredTagKeys` Kontrol gagal jika tabel rute gateway transit tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika tabel rute gateway transit tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS

Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke tabel rute gateway transit EC2, lihat Menandai sumber daya Amazon EC2 Anda di Panduan Pengguna Amazon EC2.

[EC2.35] Antarmuka jaringan EC2 harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::EC2::NetworkInterface`

AWS Config aturan: `tagged-ec2-networkinterface` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList	Daftar tag yang memenuhi AWS persyaratan	Tidak ada nilai default

Kontrol ini memeriksa apakah antarmuka jaringan Amazon EC2 memiliki tag dengan kunci tertentu yang ditentukan dalam parameter. `requiredTagKeys` Kontrol gagal jika antarmuka jaringan tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika antarmuka jaringan tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke antarmuka jaringan EC2, lihat Menandai sumber daya Amazon EC2 Anda di Panduan Pengguna Amazon EC2.

[EC2.36] Gateway pelanggan EC2 harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::EC2::CustomerGateway`

AWS Config aturan: `tagged-ec2-customergateway` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList	Daftar tag yang memenuhi AWS persyaratan	Tidak ada nilai default

Kontrol ini memeriksa apakah gateway pelanggan Amazon EC2 memiliki tag dengan kunci spesifik yang ditentukan dalam parameter. `requiredTagKeys` Kontrol gagal jika gateway pelanggan tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika gateway pelanggan tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke gateway pelanggan EC2, lihat Menandai sumber daya Amazon EC2 Anda di Panduan Pengguna Amazon EC2.

[EC2.37] Alamat IP Elastis EC2 harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::EC2::EIP`

AWS Config aturan: `tagged-ec2-eip` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList	Daftar tag yang memenuhi AWS persyaratan	Tidak ada nilai default

Kontrol ini memeriksa apakah alamat IP Elastis Amazon EC2 memiliki tag dengan kunci spesifik yang ditentukan dalam parameter. `requiredTagKeys` Kontrol gagal jika alamat IP Elastis tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika alamat IP Elastis tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang

bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke alamat IP Elastis EC2, lihat Menandai sumber daya Amazon EC2 Anda di Panduan Pengguna Amazon EC2.

[EC2.38] Instans EC2 harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::EC2::Instance`

AWS Config aturan: `tagged-ec2-instance` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya	StringList	Daftar tag yang	Tidak ada nilai default

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
	yang dievaluasi. Kunci tag peka huruf besar dan kecil.		memenuhi AWS persyaratan	

Kontrol ini memeriksa apakah instans Amazon EC2 memiliki tag dengan kunci tertentu yang ditentukan dalam parameter. `requiredTagKeys` Kontrol gagal jika instance tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika instance tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke instans EC2, lihat Menandai sumber daya Amazon EC2 Anda di Panduan Pengguna Amazon EC2.

[EC2.39] Gerbang internet EC2 harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::EC2::InternetGateway`

AWS Config aturan: `tagged-ec2-internetgateway` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList	Daftar tag yang memenuhi AWS persyaratan	Tidak ada nilai default

Kontrol ini memeriksa apakah gateway internet Amazon EC2 memiliki tag dengan kunci spesifik yang ditentukan dalam parameter. `requiredTagKeys` Kontrol gagal jika gateway internet tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika gateway internet tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang

bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke gateway internet EC2, lihat Menandai sumber daya Amazon EC2 Anda di Panduan Pengguna Amazon EC2.

[EC2.40] Gerbang EC2 NAT harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::EC2::NatGateway`

AWS Config aturan: `tagged-ec2-natgateway` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya	StringList	Daftar tag yang	Tidak ada nilai default

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
	yang dievaluasi. Kunci tag peka huruf besar dan kecil.		memenuhi AWS persyaratan	

Kontrol ini memeriksa apakah gateway terjemahan alamat jaringan (NAT) Amazon EC2 memiliki tag dengan kunci tertentu yang ditentukan dalam parameter. `requiredTagKeys` Kontrol gagal jika gateway NAT tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika gateway NAT tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke gateway EC2 NAT, lihat Menandai sumber daya Amazon EC2 Anda di Panduan Pengguna Amazon EC2.

[EC2.41] ACL jaringan EC2 harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::EC2::NetworkAcl`

AWS Config aturan: `tagged-ec2-networkacl` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList	Daftar tag yang memenuhi AWS persyaratan	Tidak ada nilai default

Kontrol ini memeriksa apakah daftar kontrol akses jaringan Amazon EC2 (ACL jaringan) memiliki tag dengan kunci tertentu yang ditentukan dalam parameter. `requiredTagKeys` Kontrol gagal jika ACL jaringan tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika ACL jaringan tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang

bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke ACL jaringan EC2, lihat Menandai sumber daya Amazon EC2 Anda di Panduan Pengguna Amazon EC2.

[EC2.42] Tabel rute EC2 harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::EC2::RouteTable`

AWS Config aturan: `tagged-ec2-routetable` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya	StringList	Daftar tag yang	Tidak ada nilai default

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
	yang dievaluasi. Kunci tag peka huruf besar dan kecil.		memenuhi AWS persyaratan	

Kontrol ini memeriksa apakah tabel rute Amazon EC2 memiliki tag dengan kunci tertentu yang ditentukan dalam parameter. `requiredTagKeys` Kontrol gagal jika tabel rute tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika tabel rute tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke tabel rute EC2, lihat Menandai sumber daya Amazon EC2 Anda di Panduan Pengguna Amazon EC2.

[EC2.43] Grup keamanan EC2 harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::EC2::SecurityGroup`

AWS Config aturan: `tagged-ec2-securitygroup` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList	Daftar tag yang memenuhi AWS persyaratan	Tidak ada nilai default

Kontrol ini memeriksa apakah grup keamanan Amazon EC2 memiliki tag dengan kunci tertentu yang ditentukan dalam parameter. `requiredTagKeys` Kontrol gagal jika grup keamanan tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika grup keamanan tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang

bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke grup keamanan EC2, lihat Menandai sumber daya Amazon EC2 Anda di Panduan Pengguna Amazon EC2.

[EC2.44] Subnet EC2 harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::EC2::Subnet`

AWS Config aturan: `tagged-ec2-subnet` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya	StringList	Daftar tag yang	Tidak ada nilai default

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
	yang dievaluasi. Kunci tag peka huruf besar dan kecil.		memenuhi AWS persyaratan	

Kontrol ini memeriksa apakah subnet Amazon EC2 memiliki tag dengan kunci tertentu yang ditentukan dalam parameter. `requiredTagKeys` Kontrol gagal jika subnet tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika subnet tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke subnet EC2, lihat Menandai sumber daya Amazon EC2 Anda di Panduan Pengguna Amazon EC2.

[EC2.45] Volume EC2 harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::EC2::Volume`

AWS Config aturan: `tagged-ec2-subnet` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList	Daftar tag yang memenuhi AWS persyaratan	Tidak ada nilai default

Kontrol ini memeriksa apakah volume Amazon EC2 memiliki tag dengan kunci tertentu yang ditentukan dalam parameter. `requiredTagKeys` Kontrol gagal jika volume tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika volume tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang

bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke volume EC2, lihat Menandai sumber daya Amazon EC2 Anda di Panduan Pengguna Amazon EC2.

[EC2.46] VPC Amazon harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::EC2::VPC`

AWS Config aturan: `tagged-ec2-vpc` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya	StringList	Daftar tag yang	Tidak ada nilai default

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
	yang dievaluasi. Kunci tag peka huruf besar dan kecil.		memenuhi AWS persyaratan	

Kontrol ini memeriksa apakah Amazon Virtual Private Cloud (Amazon VPC) memiliki tag dengan kunci spesifik yang ditentukan dalam parameter. `requiredTagKeys` Kontrol gagal jika VPC Amazon tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter. `requiredTagKeys` Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika VPC Amazon tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke VPC, lihat Menandai sumber daya Amazon EC2 Anda di Panduan Pengguna Amazon EC2.

[EC2.47] Layanan titik akhir Amazon VPC harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::EC2::VPCEndpointService`

AWS Config aturan: `tagged-ec2-vpcendpointservice` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList	Daftar tag yang memenuhi AWS persyaratan	Tidak ada nilai default

Kontrol ini memeriksa apakah layanan titik akhir VPC Amazon memiliki tag dengan kunci spesifik yang ditentukan dalam parameter. `requiredTagKeys` Kontrol gagal jika layanan endpoint tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika layanan titik akhir tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang

bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke layanan titik akhir Amazon VPC, lihat Mengelola Tag di bagian Mengonfigurasi layanan titik akhir dari Panduan.AWS PrivateLink

[EC2.48] Log aliran VPC Amazon harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::EC2::FlowLog`

AWS Config aturan: `tagged-ec2-flowlog` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya	StringList	Daftar tag yang	Tidak ada nilai default

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
	yang dievaluasi. Kunci tag peka huruf besar dan kecil.		memenuhi AWS persyaratan	

Kontrol ini memeriksa apakah log aliran VPC Amazon memiliki tag dengan kunci tertentu yang ditentukan dalam parameter. `requiredTagKeys` Kontrol gagal jika log aliran tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika log aliran tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke log aliran VPC Amazon, lihat Menandai log alur di Panduan Pengguna Amazon VPC.

[EC2.49] Koneksi peering VPC Amazon harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::EC2::VPCPeeringConnection`

AWS Config aturan: `tagged-ec2-vpcpeeringconnection` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList	Daftar tag yang memenuhi AWS persyaratan	Tidak ada nilai default

Kontrol ini memeriksa apakah koneksi peering VPC Amazon memiliki tag dengan kunci spesifik yang ditentukan dalam parameter. `requiredTagKeys` Kontrol gagal jika koneksi peering tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika koneksi peering tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang

bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke koneksi peering VPC Amazon, lihat Menandai sumber daya Amazon EC2 Anda di Panduan Pengguna Amazon EC2.

[EC2.50] Gateway EC2 VPN harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::EC2::VPNGateway`

AWS Config aturan: `tagged-ec2-vpngateway` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya	StringList	Daftar tag yang	Tidak ada nilai default

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
	yang dievaluasi. Kunci tag peka huruf besar dan kecil.		memenuhi AWS persyaratan	

Kontrol ini memeriksa apakah gateway Amazon EC2 VPN memiliki tag dengan kunci spesifik yang ditentukan dalam parameter. `requiredTagKeys` Kontrol gagal jika gateway VPN tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika gateway VPN tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke gateway VPN EC2, lihat Menandai sumber daya Amazon EC2 Anda di Panduan Pengguna Amazon EC2.

[EC2.51] Titik akhir EC2 Client VPN harus mengaktifkan pencatatan koneksi klien

Persyaratan terkait: Nist.800-53.r5 AC-2 (12), Nist.800-53.r5 AC-2 (4), Nist.800-53.r5 AC-4 (26), Nist.800-53.r5 AC-6 (9), Nist.800-53.r5 AU-10, Nist.800-53.r5 AU-12, Nist.800-800-53.r5 AU-2, NIST.800-53.R5 AU-3, NIST.800-53.R5 AU-6 (3), Nist.800-53.r5 AU-6 (4), Nist.800-53.r5 AU-9 (7), Nist.800-53.r5 CA-7, Nist.800-53.r5 SC-7 (9), Nist.800-53.r5 SC-7 (9), Nist.800-53.r5 ST.800-53.R5 SI-3 (8), NIST.800-53.R5 SI-4, NIST.800-53.R5 SI-4 (20), NIST.800-53.R5 SI-7 (8)

Kategori: Identifikasi > Logging

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::EC2::ClientVpnEndpoint`

AWS Config aturan: **`ec2-client-vpn-connection-log-enabled`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah AWS Client VPN titik akhir mengaktifkan pencatatan koneksi klien. Kontrol gagal jika titik akhir tidak mengaktifkan pencatatan koneksi klien.

Titik akhir Client VPN memungkinkan klien jarak jauh untuk terhubung dengan aman ke sumber daya di Virtual Private Cloud (VPC) di. AWS Log koneksi memungkinkan Anda melacak aktivitas pengguna di titik akhir VPN dan memberikan visibilitas. Bila Anda mengaktifkan logging koneksi, Anda dapat menentukan nama pengaliran log dalam grup log. Jika Anda tidak menentukan aliran log, layanan Client VPN membuatnya untuk Anda.

Remediasi

Untuk mengaktifkan pencatatan koneksi, lihat Mengaktifkan pencatatan koneksi untuk titik akhir Client VPN yang ada di Panduan AWS Client VPN Administrator.

[EC2.52] Gerbang transit EC2 harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::EC2::TransitGateway`

AWS Config aturan: `tagged-ec2-transitgateway` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList	Daftar tag yang memenuhi AWS persyaratan	`No default value`

Kontrol ini memeriksa apakah gateway transit Amazon EC2 memiliki tag dengan kunci spesifik yang ditentukan dalam parameter. `requiredTagKeys` Kontrol gagal jika gateway transit tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika gateway transit tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke gateway transit EC2, lihat Menandai sumber daya Amazon EC2 Anda di Panduan Pengguna Amazon EC2.

[EC2.53] Grup keamanan EC2 tidak boleh mengizinkan masuknya dari 0.0.0.0/0 ke port administrasi server jarak jauh

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v3.0.0/5.2

Kategori: Lindungi > Konfigurasi jaringan aman > Konfigurasi grup keamanan

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::EC2::SecurityGroup`

AWS Config aturan: **`vpc-sg-port-restriction-check`**

Jenis jadwal: Periodik

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`ipType`	Versi IP	String	Tidak dapat disesuaikan	`IPv4`
`restrictPorts`	Daftar port yang harus menolak lalu lintas masuk	IntegerList	Tidak dapat disesuaikan	`22,3389`

Kontrol ini memeriksa apakah grup keamanan Amazon EC2 memungkinkan masuknya dari 0.0.0.0/0 ke port administrasi server jarak jauh (port 22 dan 3389). Kontrol gagal jika grup keamanan mengizinkan masuknya dari 0.0.0.0/0 ke port 22 atau 3389.

Grup keamanan menyediakan penyaringan stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Kami menyarankan agar tidak ada grup keamanan yang mengizinkan akses masuk tanpa batas ke port administrasi server jarak jauh, seperti SSH ke port 22 dan RDP ke port 3389, menggunakan protokol TDP (6), UDP (17), atau ALL (-1). Memungkinkan akses publik ke port ini meningkatkan permukaan serangan sumber daya dan risiko kompromi sumber daya.

Remediasi

Untuk memperbarui aturan grup keamanan EC2 untuk melarang lalu lintas masuk ke port yang ditentukan, lihat Memperbarui aturan grup keamanan di Panduan Pengguna Amazon EC2. Setelah memilih grup keamanan di konsol Amazon EC2, pilih Tindakan, Edit aturan masuk. Hapus aturan yang memungkinkan akses ke port 22 atau port 3389.

[EC2.54] Grup keamanan EC2 tidak boleh mengizinkan masuknya dari: :/0 ke port administrasi server jarak jauh

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v3.0.0/5.3

Kategori: Lindungi > Konfigurasi jaringan aman > Konfigurasi grup keamanan

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::EC2::SecurityGroup`

AWS Config aturan: **`vpc-sg-port-restriction-check`**

Jenis jadwal: Periodik

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`ipType`	Versi IP	String	Tidak dapat disesuaikan	`IPv6`

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`restrictPorts`	Daftar port yang harus menolak lalu lintas masuk	IntegerList	Tidak dapat disesuaikan	`22,3389`

Kontrol ini memeriksa apakah grup keamanan Amazon EC2 memungkinkan masuknya dari: :/0 ke port administrasi server jarak jauh (port 22 dan 3389). Kontrol gagal jika grup keamanan mengizinkan masuknya dari: :/0 ke port 22 atau 3389.

Grup keamanan menyediakan penyaringan stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Kami menyarankan agar tidak ada grup keamanan yang mengizinkan akses masuk tanpa batas ke port administrasi server jarak jauh, seperti SSH ke port 22 dan RDP ke port 3389, menggunakan protokol TDP (6), UDP (17), atau ALL (-1). Memungkinkan akses publik ke port ini meningkatkan permukaan serangan sumber daya dan risiko kompromi sumber daya.

Remediasi

Untuk memperbarui aturan grup keamanan EC2 untuk melarang lalu lintas masuk ke port yang ditentukan, lihat Memperbarui aturan grup keamanan di Panduan Pengguna Amazon EC2. Setelah memilih grup keamanan di konsol Amazon EC2, pilih Tindakan, Edit aturan masuk. Hapus aturan yang memungkinkan akses ke port 22 atau port 3389.

Kontrol Auto Scaling Amazon EC2

Kontrol ini terkait dengan sumber daya Auto Scaling Amazon EC2.

Kontrol ini mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[AutoScaling.1] Grup Auto Scaling yang terkait dengan penyeimbang beban harus menggunakan pemeriksaan kesehatan ELB

Persyaratan terkait: PCI DSS v3.2.1/2.2, Nist.800-53.R5 CA-7, Nist.800-53.R5 CP-2 (2), Nist.800-53.R5 SI-2

Kategori: Identifikasi > Persediaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::AutoScaling::AutoScalingGroup`

AWS Config aturan: **`autoscaling-group-elb-healthcheck-required`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah grup Auto Scaling Amazon EC2 yang terkait dengan penyeimbang beban menggunakan pemeriksaan kesehatan Elastic Load Balancing (ELB). Kontrol gagal jika grup Auto Scaling tidak menggunakan pemeriksaan kesehatan ELB.

Pemeriksaan kesehatan ELB membantu memastikan bahwa grup Auto Scaling dapat menentukan kesehatan instans berdasarkan tes tambahan yang disediakan oleh penyeimbang beban. Menggunakan pemeriksaan kesehatan Elastic Load Balancing juga membantu mendukung ketersediaan aplikasi yang menggunakan grup EC2 Auto Scaling.

Remediasi

Untuk menambahkan pemeriksaan kesehatan Elastic Load Balancing, lihat Menambahkan pemeriksaan kesehatan Menambahkan Elastic Load Balancing di Panduan Pengguna Auto Scaling Amazon EC2.

[AutoScaling.2] Grup Auto Scaling Amazon EC2 harus mencakup beberapa Availability Zone

Persyaratan terkait: Nist.800-53.r5 CP-10, Nist.800-53.r5 CP-2 (2), Nist.800-53.R5 CP-6 (2), Nist.800-53.r5 SC-36, Nist.800-53.r5 SC-5 (2), Nist.800-53.r5 SI-13 (5)

Kategori: Pulihkan > Ketahanan > Ketersediaan tinggi

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::AutoScaling::AutoScalingGroup`

AWS Config aturan: **`autoscaling-multiple-az`**

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub	
`minAvailabilityZones`	Jumlah minimum Availability Zone	Enum	`2, 3, 4, 5, 6`	`2`	

Kontrol ini memeriksa apakah grup Auto Scaling Amazon EC2 mencakup setidaknya jumlah Availability Zone (AZ) yang ditentukan. Kontrol gagal jika grup Auto Scaling tidak menjangkau setidaknya jumlah AZ yang ditentukan. Kecuali Anda memberikan nilai parameter khusus untuk jumlah minimum AZ, Security Hub menggunakan nilai default dua AZ.

Grup Auto Scaling yang tidak menjangkau beberapa AZ tidak dapat meluncurkan instance di AZ lain untuk mengkompensasi jika AZ tunggal yang dikonfigurasi menjadi tidak tersedia. Namun, grup Auto Scaling dengan satu Availability Zone mungkin lebih disukai dalam beberapa kasus penggunaan, seperti pekerjaan batch atau ketika biaya transfer antar-AZ harus dijaga seminimal mungkin. Dalam kasus seperti itu, Anda dapat menonaktifkan kontrol ini atau menekan temuannya.

Remediasi

Untuk menambahkan AZ ke grup Auto Scaling yang ada, lihat Menambahkan dan menghapus Availability Zone di Panduan Pengguna Auto Scaling Amazon EC2.

[AutoScaling.3] Konfigurasi peluncuran grup Auto Scaling harus mengonfigurasi instans EC2 agar memerlukan Layanan Metadata Instans Versi 2 (IMDSv2)

Persyaratan terkait: Nist.800-53.r5 AC-3, Nist.800-53.r5 AC-3 (15), Nist.800-53.r5 AC-3 (7), Nist.800-53.r5 AC-6, Nist.800-53.r5 CA-9 (1), Nist.800-53.r5 CM-2

Kategori: Lindungi > Konfigurasi jaringan aman

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::AutoScaling::LaunchConfiguration`

AWS Config aturan: **`autoscaling-launchconfig-requires-imdsv2`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah IMDSv2 diaktifkan pada semua instans yang diluncurkan oleh grup Auto Scaling Amazon EC2. Kontrol gagal jika versi Instance Metadata Service (IMDS) tidak disertakan dalam konfigurasi peluncuran atau jika IMDSv1 dan IMDSv2 diaktifkan.

IMDS menyediakan data tentang instans yang dapat Anda gunakan untuk mengonfigurasi atau mengelola instance yang sedang berjalan.

IMDS versi 2 menambahkan perlindungan baru yang tidak tersedia di IMDSv1 untuk lebih melindungi instans EC2 Anda.

Remediasi

Grup Auto Scaling dikaitkan dengan satu konfigurasi peluncuran pada satu waktu. Anda tidak dapat mengubah konfigurasi peluncuran setelah Anda membuatnya. Untuk mengubah konfigurasi peluncuran untuk grup Auto Scaling, gunakan konfigurasi peluncuran yang ada sebagai dasar untuk konfigurasi peluncuran baru dengan IMDSv2 diaktifkan. Untuk informasi selengkapnya, lihat Mengonfigurasi opsi metadata instans untuk instans baru di Panduan Pengguna Amazon EC2.

[AutoScaling.4] Konfigurasi peluncuran grup Auto Scaling seharusnya tidak memiliki batas hop respons metadata yang lebih besar dari 1

> **Important**
>
> Security Hub menghentikan kontrol ini pada April 2024. Untuk informasi selengkapnya, lihat Ubah log untuk kontrol Security Hub.

Persyaratan terkait: NIST.800-53.R5 CA-9 (1), Nist.800-53.R5 CM-2, Nist.800-53.R5 CM-2 (2)

Kategori: Lindungi > Konfigurasi jaringan aman

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::AutoScaling::LaunchConfiguration`

AWS Config aturan: **`autoscaling-launch-config-hop-limit`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa jumlah hop jaringan yang dapat ditempuh oleh token metadata. Kontrol gagal jika batas hop respons metadata lebih besar dari. 1

Layanan Metadata Instans (IMDS) menyediakan informasi metadata tentang instans Amazon EC2 dan berguna untuk konfigurasi aplikasi. Membatasi PUT respons HTTP untuk layanan metadata hanya untuk instans EC2 melindungi IMDS dari penggunaan yang tidak sah.

Bidang Time To Live (TTL) dalam paket IP dikurangi satu pada setiap hop. Pengurangan ini dapat digunakan untuk memastikan bahwa paket tidak bergerak di luar EC2. IMDSv2 melindungi instans EC2 yang mungkin salah dikonfigurasi sebagai router terbuka, firewall lapisan 3, VPN, terowongan, atau perangkat NAT, yang mencegah pengguna yang tidak sah mengambil metadata. Dengan ImDSv2, PUT respons yang berisi token rahasia tidak dapat berjalan di luar instance karena batas hop respons metadata default disetel ke. 1 Namun, jika nilai ini lebih besar dari1, token dapat meninggalkan instans EC2.

Remediasi

Untuk mengubah batas hop respons metadata untuk konfigurasi peluncuran yang ada, lihat Memodifikasi opsi metadata instans untuk instans yang ada di Panduan Pengguna Amazon EC2.

[Autoscaling.5] Instans Amazon EC2 yang diluncurkan menggunakan konfigurasi peluncuran grup Auto Scaling seharusnya tidak memiliki alamat IP Publik

Persyaratan terkait: Nist.800-53.r5 AC-21, Nist.800-53.r5 AC-3, Nist.800-53.r5 AC-3 (7), Nist.800-53.r5 AC-4, Nist.800-53.r5 AC-4 (21), Nist.800-53.r5 AC-6, Nist.800-53.r5 R5 SC-7, Nist.800-53.r5 SC-7 (11), NIST.800-53.R5 SC-7 (16), Nist.800-53.r5 SC-7 (20), Nist.800-53.r5 SC-7 (21), Nist.800-53.r5 SC-7 (3), Nist.800-53.r5 5 SC-7 (4), NIST.800-53.R5 SC-7 (9)

Kategori: Lindungi > Konfigurasi jaringan aman > Sumber daya tidak dapat diakses publik

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::AutoScaling::LaunchConfiguration`

AWS Config aturan: **`autoscaling-launch-config-public-ip-disabled`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah konfigurasi peluncuran terkait grup Auto Scaling menetapkan alamat IP publik ke instans grup. Kontrol gagal jika konfigurasi peluncuran terkait menetapkan alamat IP publik.

Instans Amazon EC2 dalam konfigurasi peluncuran grup Auto Scaling tidak boleh memiliki alamat IP publik terkait, kecuali dalam kasus edge terbatas. Instans Amazon EC2 seharusnya hanya dapat diakses dari belakang penyeimbang beban alih-alih langsung terpapar ke internet.

Remediasi

Grup Auto Scaling dikaitkan dengan satu konfigurasi peluncuran pada satu waktu. Anda tidak dapat mengubah konfigurasi peluncuran setelah Anda membuatnya. Untuk mengubah konfigurasi peluncuran untuk grup Auto Scaling, gunakan konfigurasi peluncuran yang ada sebagai dasar untuk konfigurasi peluncuran baru. Lalu, perbarui grup Auto Scaling Anda untuk menggunakan konfigurasi peluncuran baru. Untuk step-by-step petunjuknya, lihat Mengubah konfigurasi peluncuran untuk grup Auto Scaling di Panduan Pengguna Auto Scaling Amazon EC2. Saat membuat konfigurasi peluncuran baru, di bawah Konfigurasi tambahan, untuk detail lanjutan, jenis alamat IP, pilih Jangan tetapkan alamat IP publik ke instance apa pun.

Setelah Anda mengubah konfigurasi peluncuran, Auto Scaling meluncurkan instance baru dengan opsi konfigurasi baru. Instance yang ada tidak terpengaruh. Untuk memperbarui instans yang ada, kami sarankan Anda menyegarkan instans Anda, atau mengizinkan penskalaan otomatis untuk secara bertahap mengganti instans lama dengan instans yang lebih baru berdasarkan kebijakan penghentian Anda. Untuk informasi selengkapnya tentang memperbarui instans Auto Scaling, lihat Memperbarui instans Auto Scaling di Panduan Pengguna Auto Scaling Amazon EC2.

[AutoScaling.6] Grup Auto Scaling harus menggunakan beberapa jenis instance di beberapa Availability Zone

Persyaratan terkait: Nist.800-53.r5 CP-10, Nist.800-53.r5 CP-2 (2), Nist.800-53.R5 CP-6 (2), Nist.800-53.r5 SC-36, Nist.800-53.r5 SC-5 (2), Nist.800-53.r5 SI-13 (5)

Kategori: Pulihkan > Ketahanan > Ketersediaan tinggi

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::AutoScaling::AutoScalingGroup`

AWS Config aturan: **`autoscaling-multiple-instance-types`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah grup Auto Scaling Amazon EC2 menggunakan beberapa jenis instans. Kontrol gagal jika grup Auto Scaling hanya memiliki satu jenis instance yang ditentukan.

Anda dapat meningkatkan ketersediaan dengan menerapkan aplikasi Anda di beberapa jenis instance yang berjalan di beberapa Availability Zone. Security Hub merekomendasikan penggunaan beberapa jenis instans agar grup Auto Scaling dapat meluncurkan tipe instans lain jika kapasitas instans tidak mencukupi di Availability Zone yang Anda pilih.

Remediasi

Untuk membuat grup Auto Scaling dengan beberapa jenis instans, lihat grup Auto Scaling dengan beberapa jenis instans dan opsi pembelian di Panduan Pengguna Auto Scaling Amazon EC2.

[AutoScaling.9] Grup Auto Scaling Amazon EC2 harus menggunakan templat peluncuran Amazon EC2

Persyaratan terkait: NIST.800-53.R5 CA-9 (1), Nist.800-53.R5 CM-2, Nist.800-53.R5 CM-2 (2)

Kategori: Identifikasi > Konfigurasi Sumber Daya

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::AutoScaling::AutoScalingGroup`

AWS Config aturan: **`autoscaling-launch-template`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah grup Auto Scaling Amazon EC2 dibuat dari templat peluncuran EC2. Kontrol ini gagal jika grup Auto Scaling Amazon EC2 tidak dibuat dengan templat peluncuran atau jika templat peluncuran tidak ditentukan dalam kebijakan instance campuran.

Grup EC2 Auto Scaling dapat dibuat dari templat peluncuran EC2 atau konfigurasi peluncuran. Namun, menggunakan template peluncuran untuk membuat grup Auto Scaling memastikan bahwa Anda memiliki akses ke fitur dan peningkatan terbaru.

Remediasi

Untuk membuat grup Auto Scaling dengan template peluncuran EC2, lihat Membuat grup Auto Scaling menggunakan template peluncuran di Panduan Pengguna Auto Scaling Amazon EC2. Untuk informasi tentang cara mengganti konfigurasi peluncuran dengan templat peluncuran, lihat Mengganti konfigurasi peluncuran dengan templat peluncuran di Panduan Pengguna Amazon EC2.

[AutoScaling.10] Grup Penskalaan Otomatis EC2 harus diberi tag

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::AutoScaling::AutoScalingGroup`

AWS Config aturan: `tagged-autoscaling-autoscalinggroup` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList	Daftar tag yang memenuhi AWS persyaratan	Tidak ada nilai default

Kontrol ini memeriksa apakah grup Auto Scaling Amazon EC2 memiliki tag dengan kunci tertentu yang ditentukan dalam parameter. `requiredTagKeys` Kontrol gagal jika grup Auto Scaling tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter. `requiredTagKeys` Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika grup Auto Scaling tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik,

lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke grup Auto Scaling, lihat Menandai grup dan instans Auto Scaling di Panduan Pengguna Auto Scaling Amazon EC2.

Kontrol Manajer Sistem Amazon EC2

Kontrol ini terkait dengan instans Amazon EC2 yang dikelola oleh. AWS Systems Manager

Kontrol ini mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[SSM.1] Instans Amazon EC2 harus dikelola oleh AWS Systems Manager

Persyaratan terkait: PCI DSS v3.2.1/2.4, Nist.800-53.R5 CA-9 (1), Nist.800-53.R5 CM-2, Nist.800-53.r5 CM-2 (2), Nist.800-53.r5 CM-8, Nist.800-53.r5 CM-8 (1), Nist.800-53.r5 R5 CM-8 (2), NIST.800-53.R5 CM-8 (3), NIST.800-53.R5 SA-15 (2), NIST.800-53.R5 SA-15 (8), NIST.800-53.R5 SA-3, NIST.800-53.R5 SI-2 (3)

Kategori: Identifikasi > Persediaan

Tingkat keparahan: Sedang

Sumber daya yang dievaluasi: `AWS::EC2::Instance`

Sumber daya AWS Config perekaman yang diperlukan:`AWS::EC2::Instance`, `AWS::SSM::ManagedInstanceInventory`

AWS Config aturan: **`ec2-instance-managed-by-systems-manager`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah instans EC2 yang berhenti dan berjalan di akun Anda dikelola oleh. AWS Systems Manager Systems Manager adalah Layanan AWS yang dapat Anda gunakan untuk melihat dan mengontrol AWS infrastruktur Anda.

Untuk membantu Anda menjaga keamanan dan kepatuhan, Systems Manager memindai instans terkelola yang berhenti dan berjalan. Sebuah instance terkelola adalah mesin yang dikonfigurasi untuk digunakan dengan Systems Manager. Systems Manager kemudian melaporkan atau mengambil tindakan korektif atas setiap pelanggaran kebijakan yang terdeteksi. Systems Manager juga membantu Anda mengonfigurasi dan memelihara instans terkelola.

Untuk mempelajari lebih lanjut, lihat Panduan AWS Systems Manager Pengguna.

Remediasi

Untuk mengelola instans EC2 dengan Systems Manager, lihat Manajemen host Amazon EC2 di AWS Systems Manager Panduan Pengguna. Di bagian Opsi konfigurasi, Anda dapat menyimpan pilihan default atau mengubahnya seperlunya untuk konfigurasi pilihan Anda.

[SSM.2] Instans Amazon EC2 yang dikelola oleh Systems Manager harus memiliki status kepatuhan patch COMPLIANT setelah instalasi patch

Persyaratan terkait: PCI DSS v3.2.1/6.2, NIST.800-53.R5 CM-8 (3), Nist.800-53.R5 SI-2, Nist.800-53.R5 SI-2 (2), Nist.800-53.R5 SI-2 (3), Nist.800-53.R5 SI-2 (4), NIST.800-53.R5 R5 SI-2 (5)

Kategori: Deteksi > Layanan deteksi

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::SSM::PatchCompliance`

AWS Config aturan: **`ec2-managedinstance-patch-compliance-status-check`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah status kepatuhan kepatuhan patch Systems Manager `COMPLIANT` atau `NON_COMPLIANT` setelah instalasi patch pada instance. Kontrol gagal jika status kepatuhan`NON_COMPLIANT`. Kontrol hanya memeriksa instance yang dikelola oleh Systems Manager Patch Manager.

Menambal instans EC2 Anda seperti yang dipersyaratkan oleh organisasi Anda mengurangi permukaan serangan Anda. Akun AWS

Remediasi

Systems Manager merekomendasikan penggunaan kebijakan tambalan untuk mengonfigurasi patching untuk instance terkelola Anda. Anda juga dapat menggunakan dokumen Systems Manager, seperti yang dijelaskan dalam prosedur berikut, untuk menambal instance.

Untuk memulihkan tambalan yang tidak sesuai

1. Buka AWS Systems Manager konsol di https://console.aws.amazon.com/systems-manager/.
2. Untuk Node Management, pilih Run Command, dan kemudian pilih Run command.
3. Pilih opsi untuk AWS- RunPatchBaseline.
4. Ubah Operasi untuk Menginstal.
5. Pilih instans secara manual, lalu pilih instans yang tidak sesuai.
6. Pilih Jalankan.
7. Setelah perintah selesai, untuk memantau status kepatuhan baru dari instance yang ditambal, pilih Kepatuhan di panel navigasi.

[SSM.3] Instans Amazon EC2 yang dikelola oleh Systems Manager harus memiliki status kepatuhan asosiasi COMPLIANT

Persyaratan terkait: PCI DSS v3.2.1/2.4, Nist.800-53.R5 CA-9 (1), Nist.800-53.R5 CM-2, Nist.800-53.r5 CM-2 (2), Nist.800-53.r5 CM-8, Nist.800-53.r5 CM-8 (1), Nist.800-53.r5 R5 CM-8 (3), NIST.800-53.R5 SI-2 (3)

Kategori: Deteksi > Layanan deteksi

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::SSM::AssociationCompliance`

AWS Config aturan: **`ec2-managedinstance-association-compliance-status-check`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah status kepatuhan AWS Systems Manager asosiasi `COMPLIANT` atau `NON_COMPLIANT` setelah asosiasi dijalankan pada sebuah instance. Kontrol gagal jika status kepatuhan asosiasi`NON_COMPLIANT`.

Asosiasi State Manager adalah konfigurasi yang ditetapkan untuk instans terkelola Anda. Konfigurasi mendefinisikan status yang ingin Anda pertahankan pada instans Anda. Misalnya, asosiasi dapat menentukan bahwa perangkat lunak antivirus harus diinstal dan berjalan pada instance Anda atau port tertentu harus ditutup.

Setelah Anda membuat satu atau beberapa asosiasi Manajer Negara, informasi status kepatuhan segera tersedia untuk Anda. Anda dapat melihat status kepatuhan di konsol atau sebagai respons terhadap AWS CLI perintah atau tindakan API Systems Manager terkait. Untuk asosiasi, Kepatuhan Konfigurasi menunjukkan status kepatuhan (`Compliant`atau`Non-compliant`). Ini juga menunjukkan tingkat keparahan yang ditetapkan untuk asosiasi, seperti `Critical` atau`Medium`.

Untuk mempelajari lebih lanjut tentang kepatuhan asosiasi Manajer Negara, lihat Tentang kepatuhan asosiasi Manajer Negara di Panduan AWS Systems Manager Pengguna.

Remediasi

Asosiasi yang gagal dapat dikaitkan dengan hal-hal yang berbeda, termasuk target dan nama dokumen SSM. Untuk mengatasi masalah ini, Anda harus terlebih dahulu mengidentifikasi dan menyelidiki asosiasi dengan melihat riwayat asosiasi. Untuk petunjuk tentang melihat riwayat asosiasi, lihat Melihat riwayat asosiasi di Panduan AWS Systems Manager Pengguna.

Setelah menyelidiki, Anda dapat mengedit asosiasi untuk memperbaiki masalah yang diidentifikasi. Anda dapat mengedit asosiasi untuk menentukan nama, jadwal, tingkat keparahan, atau target baru. Setelah Anda mengedit asosiasi, AWS Systems Manager buat versi baru. Untuk petunjuk tentang mengedit asosiasi, lihat Mengedit dan membuat versi baru asosiasi di Panduan AWS Systems Manager Pengguna.

[SSM.4] Dokumen SSM seharusnya tidak bersifat publik

Persyaratan terkait: Nist.800-53.r5 AC-21, Nist.800-53.r5 AC-3, Nist.800-53.r5 AC-3 (7), Nist.800-53.r5 AC-4, Nist.800-53.r5 AC-4 (21), Nist.800-53.r5 AC-6, Nist.800-53.r5 R5 SC-7, Nist.800-53.r5 SC-7 (11), NIST.800-53.R5 SC-7 (16), Nist.800-53.r5 SC-7 (20), Nist.800-53.r5 SC-7 (21), Nist.800-53.r5 SC-7 (3), Nist.800-53.r5 5 SC-7 (4), NIST.800-53.R5 SC-7 (9)

Kategori: Lindungi > Konfigurasi jaringan aman > Sumber daya tidak dapat diakses publik

Tingkat keparahan: Kritis

Jenis sumber daya: `AWS::SSM::Document`

AWS Config aturan: **`ssm-document-not-public`**

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah AWS Systems Manager dokumen yang dimiliki oleh akun bersifat publik. Kontrol ini gagal jika dokumen SSM dengan pemiliknya `Self` bersifat publik.

Dokumen SSM yang bersifat publik mungkin memungkinkan akses yang tidak diinginkan ke dokumen Anda. Dokumen SSM publik dapat mengekspos informasi berharga tentang akun, sumber daya, dan proses internal Anda.

Kecuali kasus penggunaan Anda memerlukan berbagi publik, sebaiknya Anda memblokir pengaturan berbagi publik untuk dokumen Systems Manager yang dimiliki oleh`Self`.

Remediasi

Untuk memblokir berbagi publik untuk dokumen SSM, lihat Memblokir berbagi publik untuk dokumen SSM di AWS Systems Manager Panduan Pengguna.

Kontrol Amazon Elastic File System

Kontrol ini terkait dengan sumber daya Amazon EFS.

Kontrol ini mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[EFS.1] Sistem File Elastis harus dikonfigurasi untuk mengenkripsi data file saat istirahat menggunakan AWS KMS

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v3.0.0/2.4.1, Nist.800-53.r5 CA-9 (1), Nist.800-53.R5 CM-3 (6), Nist.800-53.r5 SC-13, Nist.800-53.r5 SC-28, Nist.800-53.r5 SC-28 (1), NIST.800-800-53.R5 SC-7 (10), NIST.800-53.R5 SI-7 (6)

Kategori: Lindungi > Perlindungan Data > Enkripsi data-at-rest

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::EFS::FileSystem`

AWS Config aturan: **`efs-encrypted-check`**

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah Amazon Elastic File System dikonfigurasi untuk mengenkripsi data file yang digunakan AWS KMS. Pemeriksaan gagal dalam kasus-kasus berikut.

- `Encrypted`diatur ke `false` dalam `DescribeFileSystems`respons.
- `KmsKeyId`Kunci dalam `DescribeFileSystems`respons tidak cocok dengan `KmsKeyId` parameter untuk `efs-encrypted-check`.

Perhatikan bahwa kontrol ini tidak menggunakan `KmsKeyId` parameter untuk `efs-encrypted-check`. Itu hanya memeriksa nilai`Encrypted`.

Untuk lapisan keamanan tambahan untuk data sensitif Anda di Amazon EFS, Anda harus membuat sistem file terenkripsi. Amazon EFS mendukung enkripsi untuk sistem file saat istirahat. Anda dapat mengaktifkan enkripsi data saat istirahat saat Anda membuat sistem file Amazon EFS. Untuk mempelajari lebih lanjut tentang enkripsi Amazon EFS, lihat Enkripsi data di Amazon EFS di Panduan Pengguna Amazon Elastic File System.

Remediasi

Untuk detail tentang cara mengenkripsi sistem file Amazon EFS baru, lihat Mengenkripsi data saat istirahat di Panduan Pengguna Amazon Elastic File System.

[EFS.2] Volume Amazon EFS harus dalam rencana cadangan

Persyaratan terkait: Nist.800-53.r5 CP-10, Nist.800-53.r5 CP-6, Nist.800-53.R5 CP-6 (1), Nist.800-53.r5 CP-6 (2), Nist.800-53.r5 CP-9, Nist.800-53.r5 SC-5 (2), Nist.800-53.r5 SC-5 (2), Nist.800-53.r5 00-53.R5 SI-12, NIST.800-53.R5 SI-13 (5)

Kategori: Pulihkan > Ketahanan > Cadangan

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::EFS::FileSystem`

AWS Config aturan: **`efs-in-backup-plan`**

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah sistem file Amazon Elastic File System (Amazon EFS) ditambahkan ke paket cadangan AWS Backup. Kontrol gagal jika sistem file Amazon EFS tidak disertakan dalam paket cadangan.

Menyertakan sistem file EFS dalam paket cadangan membantu Anda melindungi data dari penghapusan dan kehilangan data.

Remediasi

Untuk mengaktifkan pencadangan otomatis untuk sistem file Amazon EFS yang ada, lihat Memulai 4: Membuat cadangan otomatis Amazon EFS di Panduan Pengembang.AWS Backup

[EFS.3] Titik akses EFS harus menegakkan direktori root

Persyaratan terkait: Nist.800-53.r5 AC-6 (10)

Kategori: Lindungi > Manajemen akses yang aman

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::EFS::AccessPoint`

AWS Config aturan: **`efs-access-point-enforce-root-directory`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah titik akses Amazon EFS dikonfigurasi untuk menerapkan direktori root. Kontrol gagal jika nilai `Path` diatur ke `/` (direktori root default dari sistem file).

Saat Anda menerapkan direktori root, klien NFS yang menggunakan titik akses menggunakan direktori root yang dikonfigurasi pada titik akses alih-alih direktori root sistem file. Menegakkan direktori root untuk titik akses membantu membatasi akses data dengan memastikan bahwa pengguna titik akses hanya dapat menjangkau file dari subdirektori yang ditentukan.

Remediasi

Untuk petunjuk tentang cara menerapkan direktori root untuk jalur akses Amazon EFS, lihat Menerapkan direktori root dengan titik akses di Panduan Pengguna Amazon Elastic File System.

[EFS.4] Titik akses EFS harus menegakkan identitas pengguna

Persyaratan terkait: Nist.800-53.r5 AC-6 (2)

Kategori: Lindungi > Manajemen akses yang aman

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::EFS::AccessPoint`

AWS Config aturan: **`efs-access-point-enforce-user-identity`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah titik akses Amazon EFS dikonfigurasi untuk menegakkan identitas pengguna. Kontrol ini gagal jika identitas pengguna POSIX tidak ditentukan saat membuat titik akses EFS.

Titik akses Amazon EFS adalah titik masuk khusus aplikasi ke dalam sistem file EFS yang memudahkan pengelolaan akses aplikasi ke kumpulan data bersama. Titik akses dapat menerapkan identitas pengguna, termasuk grup POSIX pengguna, pada semua permintaan sistem file yang dibuat melalui titik akses. Titik akses juga dapat menerapkan direktori asal yang berbeda untuk sistem file sehingga klien hanya dapat mengakses data dalam direktori tertentu atau subdirektorinya.

Remediasi

Untuk menerapkan identitas pengguna untuk jalur akses Amazon EFS, lihat Menerapkan identitas pengguna menggunakan titik akses di Panduan Pengguna Amazon Elastic File System.

[EFS.5] Titik akses EFS harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::EFS::AccessPoint`

AWS Config aturan: `tagged-efs-accesspoint` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList	Daftar tag yang memenuhi AWS persyaratan	Tidak ada nilai default

Kontrol ini memeriksa apakah titik akses Amazon EFS memiliki tag dengan kunci tertentu yang ditentukan dalam parameter`requiredTagKeys`. Kontrol gagal jika titik akses tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika titik akses tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke

AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke titik akses EFS, lihat Menandai resource Amazon EFS di Panduan Pengguna Amazon Elastic File System.

[EFS.6] Target pemasangan EFS tidak boleh dikaitkan dengan subnet publik

Kategori: Lindungi > Konfigurasi jaringan aman > Sumber daya tidak dapat diakses publik

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::EFS::FileSystem`

AWS Config aturan: **`efs-mount-target-public-accessible`**

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah target pemasangan Amazon EFS dikaitkan dengan subnet pribadi. Kontrol gagal jika target pemasangan dikaitkan dengan subnet publik.

Secara default, sistem file hanya dapat diakses dari virtual private cloud (VPC) tempat Anda membuatnya. Kami merekomendasikan untuk membuat target pemasangan EFS di subnet pribadi yang tidak dapat diakses dari internet. Ini membantu memastikan bahwa sistem file Anda hanya dapat diakses oleh pengguna yang berwenang dan tidak rentan terhadap akses atau serangan yang tidak sah.

Remediasi

Anda tidak dapat mengubah asosiasi antara target pemasangan EFS dan subnet setelah membuat target pemasangan. Untuk mengaitkan target mount yang ada dengan subnet yang berbeda, Anda harus membuat target mount baru di subnet pribadi dan kemudian menghapus target mount lama. Untuk informasi tentang mengelola target mount, lihat Membuat dan mengelola target mount dan grup keamanan di Panduan Pengguna Amazon Elastic File System.

Kontrol Layanan Amazon Elastic Kubernetes

Kontrol ini terkait dengan sumber daya Amazon EKS.

Kontrol ini mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[EKS.1] Titik akhir klaster EKS seharusnya tidak dapat diakses publik

Persyaratan terkait: Nist.800-53.r5 AC-21, Nist.800-53.r5 AC-3, Nist.800-53.r5 AC-3 (7), Nist.800-53.r5 AC-4, Nist.800-53.r5 AC-4 (21), Nist.800-53.r5 AC-6, Nist.800-53.r5 R5 SC-7, Nist.800-53.r5 SC-7 (11), NIST.800-53.R5 SC-7 (16), Nist.800-53.r5 SC-7 (20), Nist.800-53.r5 SC-7 (21), Nist.800-53.r5 SC-7 (3), Nist.800-53.r5 5 SC-7 (4), NIST.800-53.R5 SC-7 (9)

Kategori: Lindungi > Konfigurasi jaringan aman > Sumber daya tidak dapat diakses publik

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::EKS::Cluster`

AWS Config aturan: **`eks-endpoint-no-public-access`**

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah titik akhir kluster Amazon EKS dapat diakses publik. Kontrol gagal jika kluster EKS memiliki titik akhir yang dapat diakses publik.

Saat Anda membuat klaster baru, Amazon EKS membuat endpoint untuk server API Kubernetes terkelola yang Anda gunakan untuk berkomunikasi dengan klaster Anda. Secara default, titik akhir server API ini tersedia untuk umum di internet. Akses ke server API diamankan menggunakan kombinasi AWS Identity and Access Management (IAM) dan Kubernetes Role Based Access Control

(RBAC) asli. Dengan menghapus akses publik ke titik akhir, Anda dapat menghindari eksposur yang tidak disengaja dan akses ke cluster Anda.

Remediasi

Untuk mengubah akses titik akhir untuk kluster EKS yang ada, lihat Memodifikasi akses titik akhir klaster di Panduan Pengguna Amazon EKS. Anda dapat mengatur akses titik akhir untuk kluster EKS baru saat membuatnya. Untuk petunjuk cara membuat kluster Amazon EKS baru, lihat Membuat klaster Amazon EKS di Panduan Pengguna Amazon EKS.

[EKS.2] Kluster EKS harus berjalan pada versi Kubernetes yang didukung

Persyaratan terkait: NIST.800-53.R5 CA-9 (1), NIST.800-53.R5 CM-2, NIST.800-53.R5 SI-2, NIST.800-53.R5 SI-2 (2), NIST.800-53.R5 SI-2 (4), NIST.800-53.R5 SI-2 (5)

Kategori: Identifikasi > Kerentanan, tambalan, dan manajemen versi

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::EKS::Cluster`

AWS Config aturan: **`eks-cluster-supported-version`**

Jenis jadwal: Perubahan dipicu

Parameter:

- `oldestVersionSupported`: `1.26` (tidak dapat disesuaikan)

Kontrol ini memeriksa apakah Amazon Elastic Kubernetes Service (klaster Amazon EKS berjalan pada versi Kubernetes yang didukung. Kontrol gagal jika kluster EKS berjalan pada versi yang tidak didukung.

Jika aplikasi Anda tidak memerlukan versi Kubernetes tertentu, kami sarankan Anda menggunakan versi Kubernetes terbaru yang tersedia yang didukung oleh EKS untuk cluster Anda. Untuk informasi selengkapnya, lihat Kalender rilis Amazon EKS Kubernetes dan dukungan versi Amazon EKS serta FAQ di Panduan Pengguna Amazon EKS.

Remediasi

Untuk memperbarui kluster EKS, Memperbarui versi Kubernetes kluster Amazon EKS di Panduan Pengguna Amazon EKS.

[EKS.3] Kluster EKS harus menggunakan rahasia Kubernetes terenkripsi

Persyaratan terkait: Nist.800-53.R5 SC-8, Nist.800-53.R5 SC-12, Nist.800-53.R5 SC-13, Nist.800-53.R5 SI-28

Kategori: Lindungi > Perlindungan Data > Enkripsi data-at-rest

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::EKS::Cluster`

AWS Config aturan: **`eks-secrets-encrypted`**

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah klaster Amazon EKS menggunakan rahasia Kubernetes terenkripsi. Kontrol gagal jika rahasia Kubernetes cluster tidak dienkripsi.

Saat Anda mengenkripsi rahasia, Anda dapat menggunakan kunci AWS Key Management Service (AWS KMS) untuk menyediakan enkripsi amplop rahasia Kubernetes yang disimpan di etcd untuk klaster Anda. Enkripsi ini merupakan tambahan dari enkripsi volume EBS yang diaktifkan secara default untuk semua data (termasuk rahasia) yang disimpan dalam etcd sebagai bagian dari cluster EKS. Menggunakan enkripsi rahasia untuk kluster EKS Anda memungkinkan Anda untuk menerapkan strategi pertahanan secara mendalam untuk aplikasi Kubernetes dengan mengenkripsi rahasia Kubernetes dengan kunci KMS yang Anda tentukan dan kelola.

Remediasi

Untuk mengaktifkan enkripsi rahasia pada kluster EKS, lihat Mengaktifkan enkripsi rahasia pada klaster yang ada di Panduan Pengguna Amazon EKS.

[EKS.6] Kluster EKS harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::EKS::Cluster`

AWS Config aturan: `tagged-eks-cluster` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList	Daftar tag yang memenuhi AWS persyaratan	Tidak ada nilai default

Kontrol ini memeriksa apakah klaster Amazon EKS memiliki tag dengan kunci spesifik yang ditentukan dalam parameter`requiredTagKeys`. Kontrol gagal jika cluster tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika cluster tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS

Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke kluster EKS, lihat Menandai resource Amazon EKS Anda di Panduan Pengguna Amazon EKS.

[EKS.7] Konfigurasi penyedia identitas EKS harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::EKS::IdentityProviderConfig`

AWS Config aturan: `tagged-eks-identityproviderconfig` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList	Daftar tag yang memenuhi AWS persyaratan	Tidak ada nilai default

Kontrol ini memeriksa apakah konfigurasi penyedia identitas Amazon EKS memiliki tag dengan kunci spesifik yang ditentukan dalam parameter`requiredTagKeys`. Kontrol gagal jika konfigurasi tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika konfigurasi tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke konfigurasi penyedia identitas EKS, lihat Menandai resource Amazon EKS Anda di Panduan Pengguna Amazon EKS.

[EKS.8] Kluster EKS harus mengaktifkan pencatatan audit

Persyaratan terkait: Nist.800-53.r5 AC-2 (12), Nist.800-53.r5 AC-2 (4), Nist.800-53.r5 AC-4 (26), Nist.800-53.r5 AC-6 (9), Nist.800-53.r5 AU-10, Nist.800-53.r5 AU-12, Nist.800-800-53.r5 AU-2, NIST.800-53.R5 AU-3, NIST.800-53.R5 AU-6 (3), Nist.800-53.r5 AU-6 (4), Nist.800-53.r5 AU-9 (7), Nist.800-53.r5 CA-7, Nist.800-53.r5 SC-7 (9), Nist.800-53.r5 SC-7 (9), Nist.800-53.r5 ST.800-53.R5 SI-3 (8), NIST.800-53.R5 SI-4, NIST.800-53.R5 SI-4 (20), NIST.800-53.R5 SI-7 (8)

Kategori: Identifikasi > Logging

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::EKS::Cluster`

AWS Config aturan: **`eks-cluster-logging-enabled`**

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah klaster Amazon EKS mengaktifkan pencatatan audit. Kontrol gagal jika pencatatan audit tidak diaktifkan untuk klaster.

Pencatatan pesawat kontrol EKS menyediakan log audit dan diagnostik langsung dari bidang kontrol EKS ke Amazon CloudWatch Logs di akun Anda. Anda dapat memilih jenis log yang Anda butuhkan, dan log dikirim sebagai aliran log ke grup untuk setiap kluster EKS. CloudWatch Logging memberikan visibilitas ke dalam akses dan kinerja kluster EKS. Dengan mengirimkan log pesawat kontrol EKS untuk kluster EKS Anda ke CloudWatch Log, Anda dapat merekam operasi untuk tujuan audit dan diagnostik di lokasi pusat.

Remediasi

Untuk mengaktifkan log audit untuk kluster EKS Anda, lihat Mengaktifkan dan menonaktifkan log bidang kontrol di Panduan Pengguna Amazon EKS.

ElastiCache Kontrol Amazon

Kontrol ini terkait dengan ElastiCache sumber daya.

Kontrol ini mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[ElastiCache.1] Cluster ElastiCache Redis harus mengaktifkan pencadangan otomatis

Persyaratan terkait: Nist.800-53.r5 CP-10, Nist.800-53.r5 CP-6, Nist.800-53.R5 CP-6 (1), Nist.800-53.r5 CP-6 (2), Nist.800-53.r5 CP-9, Nist.800-53.r5 SC-5 (2), Nist.800-53.r5 SC-5 (2), Nist.800-53.r5 00-53.R5 SI-12, NIST.800-53.R5 SI-13 (5)

Kategori: Pulih> Ketahanan > Cadangan diaktifkan

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::ElastiCache::CacheCluster`

AWS Config aturan: **`elasticache-redis-cluster-automatic-backup-check`**

Jenis jadwal: Periodik

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`snapshotRetentionPeriod`	Periode retensi snapshot minimum dalam beberapa hari	Bilangan Bulat	1 untuk 35	1

Kontrol ini mengevaluasi jika klaster Amazon ElastiCache untuk Redis memiliki pencadangan otomatis yang dijadwalkan. Kontrol gagal jika `SnapshotRetentionLimit` untuk cluster Redis kurang dari periode waktu yang ditentukan. Kecuali Anda memberikan nilai parameter khusus untuk periode retensi snapshot, Security Hub menggunakan nilai default 1 hari.

Amazon ElastiCache untuk kluster Redis dapat mencadangkan data mereka. Anda dapat menggunakan backup untuk memulihkan klaster atau menyemai klaster baru. Backup terdiri dari metadata klaster, beserta semua data di dalam klaster. Semua cadangan ditulis ke Amazon Simple Storage Service (Amazon S3), yang menyediakan penyimpanan durabel. Anda dapat memulihkan data Anda dengan membuat cluster Redis baru dan mengisinya dengan data dari cadangan. Anda dapat mengelola backup menggunakan AWS Management Console, the AWS Command Line Interface (AWS CLI), dan API. ElastiCache

Remediasi

Untuk menjadwalkan pencadangan otomatis pada klaster Redis, lihat Menjadwalkan pencadangan otomatis di Panduan Pengguna Amazon. ElastiCache ElastiCache

[ElastiCache.2] ElastiCache untuk kluster cache Redis harus mengaktifkan peningkatan versi minor otomatis

Persyaratan terkait: NIST.800-53.R5 SI-2, NIST.800-53.R5 SI-2 (2), NIST.800-53.R5 SI-2 (4), Nist.800-53.R5 SI-2 (5)

Kategori: Identifikasi > Kerentanan, tambalan, dan manajemen versi

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::ElastiCache::CacheCluster`

AWS Config aturan: **`elasticache-auto-minor-version-upgrade-check`**

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini mengevaluasi apakah ElastiCache untuk Redis secara otomatis menerapkan upgrade versi minor ke cluster cache. Kontrol ini gagal jika ElastiCache untuk Redis cache cluster tidak memiliki upgrade versi minor otomatis diterapkan.

`AutoMinorVersionUpgrade`adalah fitur yang dapat Anda aktifkan ElastiCache untuk Redis agar cluster cache Anda ditingkatkan secara otomatis ketika versi mesin cache kecil baru tersedia. Upgrade ini mungkin termasuk patch keamanan dan perbaikan bug. Tetap up-to-date dengan instalasi patch adalah langkah penting dalam mengamankan sistem.

Remediasi

Untuk menerapkan upgrade versi minor otomatis ke cluster cache Redis ElastiCache yang sudah ada, lihat Memutakhirkan versi engine di Panduan Pengguna Amazon ElastiCache .

[ElastiCache.3] ElastiCache untuk grup replikasi Redis harus mengaktifkan failover otomatis

Persyaratan terkait: Nist.800-53.R5 CP-10, Nist.800-53.R5 SC-36, Nist.800-53.R5 SC-5 (2), Nist.800-53.R5 SI-13 (5)

Kategori: Pulihkan > Ketahanan > Ketersediaan tinggi

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::ElastiCache::ReplicationGroup`

AWS Config aturan: **`elasticache-repl-grp-auto-failover-enabled`**

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah ElastiCache grup replikasi Redis mengaktifkan failover otomatis. Kontrol ini gagal jika failover otomatis tidak diaktifkan untuk grup replikasi Redis.

Ketika failover otomatis diaktifkan untuk grup replikasi, peran node utama akan secara otomatis gagal ke salah satu replika baca. Promosi failover dan replika ini memastikan bahwa Anda dapat melanjutkan penulisan ke primer baru setelah promosi selesai, yang mengurangi waktu henti secara keseluruhan jika terjadi kegagalan.

Remediasi

Untuk mengaktifkan failover otomatis untuk grup replikasi Redis yang ada ElastiCache , lihat Memodifikasi klaster ElastiCache di Panduan Pengguna Amazon. ElastiCache Jika Anda menggunakan ElastiCache konsol, setel Auto failover ke diaktifkan.

[ElastiCache.4] ElastiCache untuk grup replikasi Redis harus dienkripsi saat istirahat

Persyaratan terkait: Nist.800-53.r5 CA-9 (1), NIST.800-53.R5 CM-3 (6), Nist.800-53.r5 SC-13, Nist.800-53.r5 SC-28, Nist.800-53.r5 SC-28 (1), Nist.800-53.r5 SC-7 (10), Nist.800-53.r5 SC-7 (10), Nist.800-53.r5 SC-7 (10), Nist.800-53.r5 SC-7 (10), Nist.800-53.r5 SC-7 (10), Nist.800-53.r5 SC-7 (10), ST.800-53.R5 SI-7 (6)

Kategori: Lindungi > Perlindungan Data > Enkripsi data-at-rest

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::ElastiCache::ReplicationGroup`

AWS Config aturan: **`elasticache-repl-grp-encrypted-at-rest`**

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah ElastiCache grup replikasi Redis dienkripsi saat istirahat. Kontrol ini gagal jika grup replikasi ElastiCache for Redis tidak dienkripsi saat istirahat.

Mengenkripsi data saat istirahat mengurangi risiko bahwa pengguna yang tidak diautentikasi mendapatkan akses ke data yang disimpan pada disk. ElastiCache untuk grup replikasi Redis harus dienkripsi saat istirahat untuk lapisan keamanan tambahan.

Remediasi

Untuk mengonfigurasi enkripsi saat istirahat pada grup replikasi Redis ElastiCache untuk Redis, lihat Mengaktifkan enkripsi saat istirahat di Panduan Pengguna Amazon. ElastiCache

[ElastiCache.5] ElastiCache untuk grup replikasi Redis harus dienkripsi saat transit

Persyaratan terkait: Nist.800-53.r5 AC-17 (2), Nist.800-53.r5 AC-4, Nist.800-53.r5 IA-5 (1), Nist.800-53.r5 SC-12 (3), Nist.800-53.r5 SC-13, Nist.800-53.r5 SC-23, Nist.800-53.r5 SC-23, Nist.800-53.r5 00-53.r5 SC-23 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.R5 SC-8, Nist.800-53.r5 SC-8 (1), NIST.800-53.r5 SC-8 (2), NIST.800-53.r5 SI-7 (6)

Kategori: Lindungi > Perlindungan Data > Enkripsi data-in-transit

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::ElastiCache::ReplicationGroup`

AWS Config aturan: **`elasticache-repl-grp-encrypted-in-transit`**

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah ElastiCache grup replikasi Redis dienkripsi dalam perjalanan. Kontrol ini gagal jika grup replikasi ElastiCache for Redis tidak dienkripsi dalam perjalanan.

Mengenkripsi data dalam perjalanan mengurangi risiko bahwa pengguna yang tidak sah dapat menguping lalu lintas jaringan. Mengaktifkan enkripsi saat transit pada grup replikasi ElastiCache for Redis mengenkripsi data Anda setiap kali data berpindah dari satu tempat ke tempat lain, seperti antar node di cluster Anda atau antara cluster Anda dan aplikasi Anda.

Remediasi

Untuk mengonfigurasi enkripsi dalam transit pada grup replikasi Redis ElastiCache untuk Redis, lihat Mengaktifkan enkripsi dalam transit di Panduan Pengguna Amazon. ElastiCache

[ElastiCache.6] ElastiCache untuk grup replikasi Redis sebelum versi 6.0 harus menggunakan Redis AUTH

Persyaratan terkait: Nist.800-53.r5 AC-2 (1), Nist.800-53.r5 AC-3, Nist.800-53.r5 AC-3 (15), Nist.800-53.r5 AC-3 (7), Nist.800-53.r5 AC-6

Kategori: Lindungi > Manajemen akses yang aman

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::ElastiCache::ReplicationGroup`

AWS Config aturan: **`elasticache-repl-grp-redis-auth-enabled`**

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah ElastiCache untuk grup replikasi Redis mengaktifkan Redis AUTH. Kontrol gagal untuk grup replikasi ElastiCache for Redis jika versi Redis dari node-nya di bawah 6.0 dan `AuthToken` tidak digunakan.

Saat Anda menggunakan token otentikasi Redis, atau kata sandi, Redis memerlukan kata sandi sebelum mengizinkan klien menjalankan perintah, yang meningkatkan keamanan data. Untuk Redis 6.0 dan versi yang lebih baru, sebaiknya gunakan Role-Based Access Control (RBAC). Karena RBAC tidak didukung untuk versi Redis lebih awal dari 6.0, kontrol ini hanya mengevaluasi versi yang tidak dapat menggunakan fitur RBAC.

Remediasi

Untuk menggunakan Redis AUTH pada grup replikasi ElastiCache for Redis, lihat Memodifikasi token AUTH pada klaster ElastiCache Redis yang sudah ada di Panduan Pengguna Amazon. ElastiCache

[ElastiCache.7] ElastiCache cluster tidak boleh menggunakan grup subnet default

Persyaratan terkait: Nist.800-53.r5 AC-4, NIST.800-53.R5 AC-4 (21), Nist.800-53.r5 SC-7, Nist.800-53.r5 SC-7 (11), Nist.800-53.r5 SC-7 (16), Nist.800-53.r5 SC-7 (21), Nist.800-53.r5 SC-7 (21), Nist.800-53.r5 SC-7 (21), Nist.800-53.r5 SC-7 (21), Nist.800-53.r5 SC-7 (21), Nist.800-53.r5 SC-7 (21), ST.800-53.R5 SC-7 (4), NIST.800-53.R5 SC-7 (5)

Kategori: Lindungi > Konfigurasi jaringan aman

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::ElastiCache::CacheCluster`

AWS Config aturan: **`elasticache-subnet-group-check`**

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah ElastiCache cluster dikonfigurasi dengan grup subnet kustom. Kontrol gagal untuk ElastiCache cluster jika `CacheSubnetGroupName` memiliki nilai`default`.

Saat meluncurkan ElastiCache cluster, grup subnet default dibuat jika belum ada. Grup default menggunakan subnet dari Virtual Private Cloud (VPC) default. Sebaiknya gunakan grup subnet khusus yang lebih membatasi subnet tempat cluster berada, dan jaringan yang diwarisi cluster dari subnet.

Remediasi

Untuk membuat grup subnet baru untuk ElastiCache klaster, lihat Membuat grup subnet di ElastiCache Panduan Pengguna Amazon.

AWS Elastic Beanstalk kontrol

Kontrol ini terkait dengan sumber daya Elastic Beanstalk.

Kontrol ini mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[ElasticBeanstalk.1] Lingkungan Elastic Beanstalk seharusnya mengaktifkan pelaporan kesehatan yang ditingkatkan

Persyaratan terkait: NIST.800-53.R5 CA-7, NIST.800-53.R5 SI-2

Kategori: Deteksi > Layanan deteksi > Pemantauan aplikasi

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::ElasticBeanstalk::Environment`

AWS Config aturan: **`beanstalk-enhanced-health-reporting-enabled`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah pelaporan kesehatan yang ditingkatkan diaktifkan untuk AWS Elastic Beanstalk lingkungan Anda.

Pelaporan kesehatan yang ditingkatkan Elastic Beanstalk memungkinkan respons yang lebih cepat terhadap perubahan kesehatan infrastruktur yang mendasarinya. Perubahan ini dapat mengakibatkan kurangnya ketersediaan aplikasi.

Pelaporan kesehatan yang ditingkatkan Elastic Beanstalk menyediakan deskriptor status untuk mengukur tingkat keparahan masalah yang diidentifikasi dan mengidentifikasi kemungkinan penyebab untuk diselidiki. Agen kesehatan Elastic Beanstalk, termasuk dalam Amazon Machine Images (AMI) yang didukung, mengevaluasi log dan metrik instans EC2 lingkungan.

Untuk informasi tambahan, lihat Pelaporan dan pemantauan kesehatan yang ditingkatkan di Panduan AWS Elastic Beanstalk Pengembang.

Remediasi

Untuk petunjuk tentang cara mengaktifkan pelaporan kesehatan yang disempurnakan, lihat Mengaktifkan pelaporan kesehatan yang disempurnakan menggunakan konsol Elastic Beanstalk di Panduan Pengembang.AWS Elastic Beanstalk

[ElasticBeanstalk.2] Pembaruan platform yang dikelola Elastic Beanstalk harus diaktifkan

Persyaratan terkait: NIST.800-53.R5 SI-2, NIST.800-53.R5 SI-2 (2), NIST.800-53.R5 SI-2 (4), Nist.800-53.R5 SI-2 (5)

Kategori: Identifikasi > Kerentanan, tambalan, dan manajemen versi

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::ElasticBeanstalk::Environment`

AWS Config aturan: **`elastic-beanstalk-managed-updates-enabled`**

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`UpdateLevel`	Tingkat pembaruan versi	Enum	`minor`, `patch`	Tidak ada nilai default

Kontrol ini memeriksa apakah pembaruan platform terkelola diaktifkan untuk lingkungan Elastic Beanstalk. Kontrol gagal jika tidak ada pembaruan platform terkelola yang diaktifkan. Secara default, kontrol lolos jika semua jenis pembaruan platform diaktifkan. Secara opsional, Anda dapat memberikan nilai parameter khusus untuk memerlukan tingkat pembaruan tertentu.

Mengaktifkan pembaruan platform terkelola memastikan bahwa perbaikan, pembaruan, dan fitur platform terbaru yang tersedia untuk lingkungan diinstal. Tetap up to date dengan instalasi patch adalah langkah penting dalam mengamankan sistem.

Remediasi

Untuk mengaktifkan pembaruan platform terkelola, lihat Untuk mengonfigurasi pembaruan platform terkelola di bawah Pembaruan platform terkelola di Panduan AWS Elastic Beanstalk Pengembang.

[ElasticBeanstalk.3] Elastic Beanstalk harus mengalirkan log ke CloudWatch

Kategori: Identifikasi > Logging

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::ElasticBeanstalk::Environment`

AWS Config aturan: **`elastic-beanstalk-logs-to-cloudwatch`**

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`RetentionInDays`	Jumlah hari untuk menyimpan peristiwa log sebelum kedaluwarsa	Enum	`1`, `3`, `5`, `7`, `14`, `30`, `60`, `90`, `120`, `150`, `180`, `365` , `400`, `545`, `731`, `1827`, `3653`	Tidak ada nilai default

Kontrol ini memeriksa apakah lingkungan Elastic Beanstalk dikonfigurasi untuk mengirim log ke Log. CloudWatch Kontrol gagal jika lingkungan Elastic Beanstalk tidak dikonfigurasi untuk mengirim log ke Log. CloudWatch Secara opsional, Anda dapat memberikan nilai kustom untuk `RetentionInDays` parameter jika Anda ingin kontrol lulus hanya jika log dipertahankan untuk jumlah hari yang ditentukan sebelum kedaluwarsa.

CloudWatch membantu Anda mengumpulkan dan memantau berbagai metrik untuk aplikasi dan sumber daya infrastruktur Anda. Anda juga dapat menggunakan CloudWatch untuk mengonfigurasi tindakan alarm berdasarkan metrik tertentu. Sebaiknya integrasikan Elastic Beanstalk dengan

Elastic CloudWatch Beanstalk untuk meningkatkan visibilitas ke lingkungan Elastic Beanstalk Anda. Log Elastic Beanstalk mencakup eb-activity.log, log akses dari server proxy nginx atau Apache lingkungan, dan log yang khusus untuk lingkungan.

Remediasi

Untuk mengintegrasikan Elastic CloudWatch Beanstalk dengan Log, lihat Streaming CloudWatch log instance ke Log di Panduan Pengembang.AWS Elastic Beanstalk

Kontrol Elastic Load Balancing

Kontrol ini terkait dengan sumber daya Elastic Load Balancing.

Kontrol ini mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[ELB.1] Application Load Balancer harus dikonfigurasi untuk mengalihkan semua permintaan HTTP ke HTTPS

Persyaratan terkait: PCI DSS v3.2.1/2.3, PCI DSS v3.2.1/4.1, Nist.800-53.r5 AC-17 (2), Nist.800-53.r5 AC-4, Nist.800-53.r5 IA-5 (1), Nist.800-53.r5 SC-12 (3), Nist.800-53.r5 SC-12 (3), Nist.800-53.r5 SC-12 -13, Nist.800-53.r5 SC-23, NIST.800-53.r5 SC-23 (3), Nist.800-53.r5 SC-7 (4), Nist.800-53.r5 SC-8, Nist.800-53.r5 SC-8 (1), Nist.800-53.r5 SC-8 (2), Nist.800-53.r5 SC-8 (2), Nist.800-53.r5 SC-8 (2), Nist.800-53.r5 ST.800-53.R5 SI-7 (6)

Kategori: Deteksi > Layanan deteksi

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::ElasticLoadBalancingV2::LoadBalancer`

AWS Config aturan: **`alb-http-to-https-redirection-check`**

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah pengalihan HTTP ke HTTPS dikonfigurasi pada semua pendengar HTTP Application Load Balancers. Kontrol gagal jika salah satu pendengar HTTP dari Application Load Balancers tidak memiliki pengalihan HTTP ke HTTPS yang dikonfigurasi.

Sebelum Anda mulai menggunakan Application Load Balancer, Anda harus menambahkan satu atau lebih pendengar. Listener adalah proses yang menggunakan protokol dan port yang dikonfigurasi

untuk memeriksa permintaan koneksi. Pendengar mendukung protokol HTTP dan HTTPS. Anda dapat menggunakan pendengar HTTPS untuk menurunkan pekerjaan enkripsi dan dekripsi ke penyeimbang beban Anda. Untuk menerapkan enkripsi dalam perjalanan, Anda harus menggunakan tindakan pengalihan dengan Application Load Balancers untuk mengarahkan permintaan HTTP klien ke permintaan HTTPS pada port 443.

Untuk mempelajari lebih lanjut, lihat Pendengar untuk Penyeimbang Beban Aplikasi Anda di Panduan Pengguna untuk Penyeimbang Beban Aplikasi.

Remediasi

Untuk mengarahkan permintaan HTTP ke HTTPS, Anda harus menambahkan aturan pendengar Application Load Balancer atau mengedit aturan yang ada.

Untuk petunjuk tentang menambahkan aturan baru, lihat Menambahkan aturan di Panduan Pengguna untuk Penyeimbang Beban Aplikasi. Untuk Protokol: Port, pilih HTTP, lalu masukkan**80**. Untuk Add action, Redirect ke, pilih HTTPS, lalu masukkan**443**.

Untuk petunjuk cara mengedit aturan yang ada, lihat Mengedit aturan di Panduan Pengguna untuk Penyeimbang Beban Aplikasi. Untuk Protokol: Port, pilih HTTP, lalu masukkan**80**. Untuk Add action, Redirect ke, pilih HTTPS, lalu masukkan**443**.

[ELB.2] Classic Load Balancer dengan pendengar SSL/HTTPS harus menggunakan sertifikat yang disediakan oleh AWS Certificate Manager

Persyaratan terkait: Nist.800-53.r5 AC-17 (2), Nist.800-53.r5 AC-4, Nist.800-53.r5 IA-5 (1), Nist.800-53.r5 SC-12 (3), Nist.800-53.r5 SC-13, Nist.800-53.r5 SC-23, Nist.800-53.r5 SC-23, Nist.800-53.r5 00-53.r5 SC-23 (5), NIST.800-53.r5 SC-7 (4), NIST.800-53.R5 SC-8, Nist.800-53.r5 SC-8 (1), NIST.800-53.r5 SC-8 (2), NIST.800-53.r5 SI-7 (6)

Kategori: Lindungi > Perlindungan Data > Enkripsi data-in-transit

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::ElasticLoadBalancing::LoadBalancer`

AWS Config aturan: **`elb-acm-certificate-required`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah Classic Load Balancer menggunakan sertifikat HTTPS/SSL yang disediakan oleh (ACM). AWS Certificate Manager Kontrol gagal jika Classic Load Balancer yang dikonfigurasi dengan HTTPS/SSL listener tidak menggunakan sertifikat yang disediakan oleh ACM.

Untuk membuat sertifikat, Anda dapat menggunakan ACM atau alat yang mendukung protokol SSL dan TLS, seperti OpenSSL. Security Hub merekomendasikan agar Anda menggunakan ACM untuk membuat atau mengimpor sertifikat penyeimbang beban Anda.

ACM terintegrasi dengan Classic Load Balancers sehingga Anda dapat menyebarkan sertifikat pada penyeimbang beban Anda. Anda juga harus memperbarui sertifikat ini secara otomatis.

Remediasi

Untuk informasi tentang cara mengaitkan sertifikat ACM SSL/TLS dengan Classic Load Balancer, lihat artikel Pusat AWS Pengetahuan Bagaimana cara mengaitkan sertifikat ACM SSL/TLS dengan Classic, Application, atau Network Load Balancer?

[ELB.3] Pendengar Classic Load Balancer harus dikonfigurasi dengan penghentian HTTPS atau TLS

Persyaratan terkait: Nist.800-53.r5 AC-17 (2), Nist.800-53.r5 AC-4, Nist.800-53.r5 IA-5 (1), Nist.800-53.r5 SC-12 (3), Nist.800-53.r5 SC-13, Nist.800-53.r5 SC-23, Nist.800-53.r5 SC-23, Nist.800-53.r5 00-53.r5 SC-23 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.R5 SC-8, Nist.800-53.r5 SC-8 (1), NIST.800-53.r5 SC-8 (2), NIST.800-53.r5 SI-7 (6)

Kategori: Lindungi > Perlindungan Data > Enkripsi data-in-transit

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::ElasticLoadBalancing::LoadBalancer`

AWS Config aturan: **`elb-tls-https-listeners-only`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah pendengar Classic Load Balancer Anda dikonfigurasi dengan protokol HTTPS atau TLS untuk koneksi front-end (client to load balancer). Kontrol ini berlaku jika Classic Load Balancer memiliki pendengar. Jika Classic Load Balancer Anda tidak memiliki listener yang dikonfigurasi, kontrol tidak melaporkan temuan apa pun.

Kontrol akan diteruskan jika pendengar Classic Load Balancer dikonfigurasi dengan TLS atau HTTPS untuk koneksi front-end.

Kontrol gagal jika pendengar tidak dikonfigurasi dengan TLS atau HTTPS untuk koneksi front-end.

Sebelum Anda mulai menggunakan penyeimbang beban, Anda harus menambahkan satu atau lebih pendengar. Listener adalah proses yang menggunakan protokol dan port yang dikonfigurasi untuk memeriksa permintaan koneksi. Pendengar dapat mendukung protokol HTTP dan HTTPS/TLS. Anda harus selalu menggunakan pendengar HTTPS atau TLS, sehingga penyeimbang beban melakukan pekerjaan enkripsi dan dekripsi dalam perjalanan.

Remediasi

Untuk mengatasi masalah ini, perbarui pendengar Anda untuk menggunakan protokol TLS atau HTTPS.

Untuk mengubah semua pendengar yang tidak patuh menjadi pendengar TLS/HTTPS

1. Buka konsol Amazon EC2 di https://console.aws.amazon.com/ec2/.
2. Pada panel navigasi, di bawah Penyeimbangan Beban, pilih Penyeimbang Beban.
3. Pilih Classic Load Balancer Anda.
4. Pada tab Listeners, pilih Edit.
5. Untuk semua pendengar yang Protokol Load Balancer tidak disetel ke HTTPS atau SSL, ubah pengaturan ke HTTPS atau SSL.
6. Untuk semua pendengar yang dimodifikasi, pada tab Sertifikat, pilih Ubah default.
7. Untuk sertifikat ACM dan IAM, pilih sertifikat.
8. Pilih Simpan sebagai default.
9. Setelah Anda memperbarui semua pendengar, pilih Simpan.

[ELB.4] Application Load Balancer harus dikonfigurasi untuk menjatuhkan header http

Persyaratan terkait: Nist.800-53.r5 SC-7 (4), Nist.800-53.R5 SC-8 (2)

Kategori: Lindungi > Keamanan Jaringan

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::ElasticLoadBalancingV2::LoadBalancer`

AWS Config aturan: **`alb-http-drop-invalid-header-enabled`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini mengevaluasi AWS Application Load Balancers untuk memastikan mereka dikonfigurasi untuk menjatuhkan header HTTP yang tidak valid. Kontrol gagal jika nilai `routing.http.drop_invalid_header_fields.enabled` disetel `kefalse`.

Secara default, Application Load Balancers tidak dikonfigurasi untuk menjatuhkan nilai header HTTP yang tidak valid. Menghapus nilai header ini mencegah serangan desync HTTP.

Perhatikan bahwa Anda dapat menonaktifkan kontrol ini jika ELB.12 diaktifkan.

Remediasi

Untuk mengatasi masalah ini, konfigurasikan penyeimbang beban Anda untuk menghapus bidang header yang tidak valid.

Untuk mengonfigurasi penyeimbang beban untuk menjatuhkan bidang header yang tidak valid

1. Buka konsol Amazon EC2 di https://console.aws.amazon.com/ec2/.
2. Di panel navigasi, pilih Load balancer.
3. Pilih Application Load Balancer.
4. Dari Tindakan, pilih Edit atribut.
5. Di bawah Jatuhkan Bidang Header Tidak Valid, pilih Aktifkan.
6. Pilih Simpan.

[ELB.5] Pencatatan aplikasi dan Classic Load Balancer harus diaktifkan

Persyaratan terkait: Nist.800-53.r5 AC-4 (26), Nist.800-53.R5 AU-10, Nist.800-53.R5 AU-12, Nist.800-53.r5 AU-2, Nist.800-53.r5 AU-3, Nist.800-53.r5 AU-6 (3), Nist.800-53.r5 AU-6 (4), NIST.800-53.R5 CA-7, NIST.800-53.R5 SC-7 (9), NIST.800-53.R5 SI-7 (8)

Kategori: Identifikasi > Logging

Tingkat keparahan: Sedang

Jenis sumber daya:`AWS::ElasticLoadBalancing::LoadBalancer`, `AWS::ElasticLoadBalancingV2::LoadBalancer`

AWS Config aturan: **`elb-logging-enabled`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah Application Load Balancer dan Classic Load Balancer telah mengaktifkan logging. Kontrol gagal jika `access_logs.s3.enabled` ada`false`.

Elastic Load Balancing memberikan log akses yang mengambil informasi mendetail tentang permintaan yang dikirim ke penyeimbang beban Anda. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server. Anda dapat menggunakan log akses ini untuk menganalisis pola lalu lintas dan untuk memecahkan masalah.

Untuk mempelajari selengkapnya, lihat Akses log untuk Classic Load Balancer di Panduan Pengguna untuk Penyeimbang Beban Klasik.

Remediasi

Untuk mengaktifkan log akses, lihat Langkah 3: Mengkonfigurasi log akses di Panduan Pengguna untuk Penyeimbang Beban Aplikasi.

[ELB.6] Aplikasi, Gateway, dan Network Load Balancer harus mengaktifkan perlindungan penghapusan

Persyaratan terkait: Nist.800-53.r5 CA-9 (1), Nist.800-53.R5 CM-2, Nist.800-53.R5 CM-2 (2), Nist.800-53.r5 CM-3, Nist.800-53.r5 SC-5 (2)

Kategori: Pulihkan > Ketahanan > Ketersediaan tinggi

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::ElasticLoadBalancingV2::LoadBalancer`

AWS Config aturan: **`elb-deletion-protection-enabled`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah Application, Gateway, atau Network Load Balancer telah mengaktifkan perlindungan penghapusan. Kontrol gagal jika perlindungan penghapusan dinonaktifkan.

Aktifkan perlindungan penghapusan untuk melindungi Aplikasi, Gateway, atau Network Load Balancer Anda dari penghapusan.

Remediasi

Untuk mencegah penyeimbang beban terhapus secara tidak sengaja, Anda dapat mengaktifkan perlindungan penghapusan. Secara default, perlindungan penghapusan dinonaktifkan untuk penyeimbang beban Anda.

Jika Anda mengaktifkan perlindungan penghapusan untuk penyeimbang beban, Anda harus menonaktifkan proteksi penghapusan sebelum dapat menghapus penyeimbang beban.

Untuk mengaktifkan perlindungan penghapusan untuk Application Load Balancer, lihat Perlindungan penghapusan di Panduan Pengguna untuk Penyeimbang Beban Aplikasi. Untuk mengaktifkan perlindungan penghapusan untuk Load Balancer Gateway, lihat Perlindungan penghapusan di Panduan Pengguna untuk Penyeimbang Beban Gateway. Untuk mengaktifkan perlindungan penghapusan Network Load Balancer, lihat Perlindungan penghapusan di Panduan Pengguna untuk Network Load Balancer.

[ELB.7] Classic Load Balancers harus mengaktifkan pengurasan koneksi

Persyaratan terkait: NIST.800-53.R5 CA-9 (1), NIST.800-53.R5 CM-2

Kategori: Memulihkan > Ketahanan

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::ElasticLoadBalancing::LoadBalancer`

AWS Config aturan: `elb-connection-draining-enabled` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah Classic Load Balancer mengaktifkan pengurasan koneksi.

Mengaktifkan pengurasan koneksi pada Classic Load Balancer memastikan bahwa penyeimbang beban berhenti mengirim permintaan ke instans yang tidak terdaftar atau tidak sehat. Itu membuat koneksi yang ada tetap terbuka. Ini sangat berguna untuk instance di grup Auto Scaling, untuk memastikan bahwa koneksi tidak terputus secara tiba-tiba.

Remediasi

Untuk mengaktifkan pengurasan koneksi pada Classic Load Balancer, lihat Mengonfigurasi pengurasan koneksi untuk Classic Load Balancer Anda di Panduan Pengguna untuk Penyeimbang Beban Klasik.

[ELB.8] Classic Load Balancer dengan pendengar SSL harus menggunakan kebijakan keamanan yang telah ditentukan sebelumnya yang memiliki urasi yang kuat AWS Config

Persyaratan terkait: Nist.800-53.r5 AC-17 (2), Nist.800-53.r5 AC-4, Nist.800-53.r5 IA-5 (1), Nist.800-53.r5 SC-12 (3), Nist.800-53.r5 SC-13, Nist.800-53.r5 SC-23, Nist.800-53.r5 SC-23, Nist.800-53.r5 00-53.r5 SC-23 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.R5 SC-8, Nist.800-53.r5 SC-8 (1), NIST.800-53.r5 SC-8 (2), NIST.800-53.r5 SI-7 (6)

Kategori: Lindungi > Perlindungan Data > Enkripsi data-in-transit

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::ElasticLoadBalancing::LoadBalancer`

AWS Config aturan: **`elb-predefined-security-policy-ssl-check`**

Jenis jadwal: Perubahan dipicu

Parameter:

- `predefinedPolicyName`: `ELBSecurityPolicy-TLS-1-2-2017-01` (tidak dapat disesuaikan)

Kontrol ini memeriksa apakah pendengar Classic Load Balancer HTTPS/SSL Anda menggunakan kebijakan yang telah ditentukan sebelumnya. `ELBSecurityPolicy-TLS-1-2-2017-01` Kontrol gagal jika Classic Load Balancer HTTPS/SSL pendengar tidak menggunakan. `ELBSecurityPolicy-TLS-1-2-2017-01`

Kebijakan keamanan adalah kombinasi dari protokol SSL, cipher, dan opsi Preferensi Pesanan Server. Kebijakan yang telah ditetapkan mengontrol cipher, protokol, dan perintah preferensi untuk mendukung selama negosiasi SSL antara klien dan penyeimbang beban.

Menggunakan `ELBSecurityPolicy-TLS-1-2-2017-01` dapat membantu Anda memenuhi standar kepatuhan dan keamanan yang mengharuskan Anda menonaktifkan versi SSL dan TLS tertentu. Untuk informasi selengkapnya, lihat Kebijakan keamanan SSL yang telah ditentukan

sebelumnya untuk Penyeimbang Beban Klasik di Panduan Pengguna untuk Penyeimbang Beban Klasik.

Remediasi

Untuk informasi tentang cara menggunakan kebijakan keamanan yang telah ditentukan sebelumnya `ELBSecurityPolicy-TLS-1-2-2017-01` dengan Classic Load Balancer, lihat Mengonfigurasi setelan keamanan di Panduan Pengguna untuk Penyeimbang Beban Klasik.

[ELB.9] Classic Load Balancer harus mengaktifkan penyeimbangan beban lintas zona

Persyaratan terkait: Nist.800-53.r5 CP-10, Nist.800-53.R5 CP-6 (2), Nist.800-53.R5 SC-36, Nist.800-53.R5 SC-5 (2), Nist.800-53.r5 SI-13 (5)

Kategori: Pulihkan > Ketahanan > Ketersediaan tinggi

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::ElasticLoadBalancing::LoadBalancer`

AWS Config aturan: **`elb-cross-zone-load-balancing-enabled`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah penyeimbangan beban lintas zona diaktifkan untuk Classic Load Balancers (CLB). Kontrol gagal jika penyeimbangan beban lintas zona tidak diaktifkan untuk CLB.

Node penyeimbang beban mendistribusikan lalu lintas hanya di seluruh target yang terdaftar di Availability Zone. Ketika load balancing lintas zona dinonaktifkan, setiap node Load Balancer mendistribusikan lalu lintas hanya di target yang telah terdaftar di Availability Zonenya. Jika jumlah target yang terdaftar tidak sama di seluruh Availability Zone, lalu lintas tidak akan didistribusikan secara merata dan contoh di satu zona mungkin berakhir lebih digunakan dibandingkan dengan contoh di zona lain. Dengan penyeimbangan beban lintas zona diaktifkan, setiap node penyeimbang beban untuk Classic Load Balancer Anda mendistribusikan permintaan secara merata di seluruh instans terdaftar di semua Availability Zone yang diaktifkan. Untuk detailnya lihat Penyeimbangan beban lintas zona di Panduan Pengguna Elastic Load Balancing.

Remediasi

Untuk mengaktifkan penyeimbangan beban lintas zona di Classic Load Balancer, lihat Mengaktifkan penyeimbangan beban lintas zona dalam Panduan Pengguna untuk Penyeimbang Beban Klasik.

[ELB.10] Classic Load Balancer harus menjangkau beberapa Availability Zone

Persyaratan terkait: Nist.800-53.r5 CP-10, Nist.800-53.R5 CP-6 (2), Nist.800-53.R5 SC-36, Nist.800-53.R5 SC-5 (2), Nist.800-53.r5 SI-13 (5)

Kategori: Pulihkan > Ketahanan > Ketersediaan tinggi

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::ElasticLoadBalancing::LoadBalancer`

AWS Config aturan: **`clb-multiple-az`**

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`minAvailabilityZones`	Jumlah minimum Availability Zone	Enum	`2, 3, 4, 5, 6`	`2`

Kontrol ini memeriksa apakah Classic Load Balancer telah dikonfigurasi untuk menjangkau setidaknya jumlah Availability Zone (AZ) yang ditentukan. Kontrol gagal jika Classic Load Balancer tidak mencakup setidaknya jumlah AZ yang ditentukan. Kecuali Anda memberikan nilai parameter khusus untuk jumlah minimum AZ, Security Hub menggunakan nilai default dua AZ.

Classic Load Balancer dapat disiapkan untuk mendistribusikan permintaan masuk di seluruh instans Amazon EC2 dalam satu Availability Zone atau beberapa Availability Zone. Classic Load Balancer yang tidak menjangkau beberapa Availability Zone tidak dapat mengarahkan lalu lintas ke target di Availability Zone lain jika Availability Zone yang dikonfigurasi menjadi tidak tersedia.

Remediasi

Untuk menambahkan Availability Zone ke Classic Load Balancer, lihat Menambahkan atau menghapus subnet untuk Classic Load Balancer Anda di Panduan Pengguna untuk Penyeimbang Beban Klasik.

[ELB.12] Application Load Balancer harus dikonfigurasi dengan mode mitigasi desync defensif atau paling ketat

Persyaratan terkait: Nist.800-53.r5 AC-4 (21), NIST.800-53.R5 CA-9 (1), Nist.800-53.r5 CM-2

Kategori: Lindungi > Perlindungan data > Integritas data

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::ElasticLoadBalancingV2::LoadBalancer`

AWS Config aturan: **`alb-desync-mode-check`**

Jenis jadwal: Perubahan dipicu

Parameter:

- `desyncMode`: `defensive, strictest` (tidak dapat disesuaikan)

Kontrol ini memeriksa apakah Application Load Balancer dikonfigurasi dengan modus mitigasi desync defensif atau paling ketat. Kontrol gagal jika Application Load Balancer tidak dikonfigurasi dengan modus mitigasi desync defensif atau paling ketat.

Masalah HTTP Desync dapat menyebabkan penyelundupan permintaan dan membuat aplikasi rentan terhadap antrian permintaan atau keracunan cache. Pada gilirannya, kerentanan ini dapat menyebabkan isian kredensyal atau eksekusi perintah yang tidak sah. Application Load Balancer yang dikonfigurasi dengan mode mitigasi desync defensif atau paling ketat melindungi aplikasi Anda dari masalah keamanan yang mungkin disebabkan oleh HTTP Desync.

Remediasi

Untuk memperbarui mode mitigasi desync dari Application Load Balancer, lihat Mode mitigasi desync di Panduan Pengguna untuk Application Load Balancers.

[ELB.13] Penyeimbang Beban Aplikasi, Jaringan, dan Gateway harus mencakup beberapa Availability Zone

Persyaratan terkait: Nist.800-53.r5 CP-10, Nist.800-53.R5 CP-6 (2), Nist.800-53.R5 SC-36, Nist.800-53.R5 SC-5 (2), Nist.800-53.r5 SI-13 (5)

Kategori: Pulihkan > Ketahanan > Ketersediaan tinggi

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::ElasticLoadBalancingV2::LoadBalancer`

AWS Config aturan: **`elbv2-multiple-az`**

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`minAvailabilityZones`	Jumlah minimum Availability Zone	Enum	`2, 3, 4, 5, 6`	2

Kontrol ini memeriksa apakah Elastic Load Balancer V2 (Application, Network, atau Gateway Load Balancer) telah mendaftarkan instans dari setidaknya jumlah Availability Zone (AZ) yang ditentukan. Kontrol gagal jika Elastic Load Balancer V2 tidak memiliki instance yang terdaftar setidaknya dalam jumlah AZ yang ditentukan. Kecuali Anda memberikan nilai parameter khusus untuk jumlah minimum AZ, Security Hub menggunakan nilai default dua AZ.

Elastic Load Balancing secara otomatis mendistribusikan lalu lintas aplikasi masuk di beberapa target, seperti instans EC2, wadah, dan IP addresses, dalam satu atau lebih Zona Ketersediaan. Elastic Load Balancing menskalakan load balancer Anda saat lalu lintas masuk Anda berubah seiring waktu. Disarankan untuk mengonfigurasi setidaknya dua zona ketersediaan untuk memastikan ketersediaan layanan, karena Elastic Load Balancer akan dapat mengarahkan lalu lintas ke zona ketersediaan lain jika salah satu tidak tersedia. Memiliki beberapa zona ketersediaan yang dikonfigurasi akan membantu menghilangkan satu titik kegagalan untuk aplikasi.

Remediasi

Untuk menambahkan Availability Zone ke Application Load Balancer, lihat Availability Zone untuk Application Load Balancer di Panduan Pengguna untuk Application Load Balancer. Untuk menambahkan Availability Zone ke Network Load Balancer, lihat Network Load Balancers di Panduan Pengguna untuk Network Load Balancer. Untuk menambahkan Availability Zone ke

Load Balancer Gateway, lihat Membuat Load Balancer Gateway di Panduan Pengguna untuk Penyeimbang Beban Gateway.

[ELB.14] Classic Load Balancer harus dikonfigurasi dengan mode mitigasi desync defensif atau paling ketat

Persyaratan terkait: Nist.800-53.r5 AC-4 (21), NIST.800-53.R5 CA-9 (1), Nist.800-53.r5 CM-2

Kategori: Lindungi > Perlindungan data > Integritas data

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::ElasticLoadBalancing::LoadBalancer`

AWS Config aturan: **`clb-desync-mode-check`**

Jenis jadwal: Perubahan dipicu

Parameter:

- `desyncMode`: `defensive, strictest` (tidak dapat disesuaikan)

Kontrol ini memeriksa apakah Classic Load Balancer dikonfigurasi dengan mode mitigasi desync defensif atau paling ketat. Kontrol gagal jika Classic Load Balancer tidak dikonfigurasi dengan mode mitigasi desync defensif atau paling ketat.

Masalah HTTP Desync dapat menyebabkan penyelundupan permintaan dan membuat aplikasi rentan terhadap antrian permintaan atau keracunan cache. Pada gilirannya, kerentanan ini dapat menyebabkan pembajakan kredenal atau eksekusi perintah yang tidak sah. Classic Load Balancer yang dikonfigurasi dengan mode mitigasi desync defensif atau paling ketat melindungi aplikasi Anda dari masalah keamanan yang mungkin disebabkan oleh HTTP Desync.

Remediasi

Untuk memperbarui mode mitigasi desync pada Classic Load Balancer, lihat Memodifikasi mode mitigasi desync di Panduan Pengguna untuk Penyeimbang Beban Klasik.

[ELB.16] Application Load Balancers harus dikaitkan dengan ACL web AWS WAF

Persyaratan terkait: Nist.800-53.r5 AC-4 (21)

Kategori: Lindungi > Layanan pelindung

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::ElasticLoadBalancingV2::LoadBalancer`

AWS Config aturan: **`alb-waf-enabled`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah Application Load Balancer dikaitkan dengan daftar kontrol akses AWS WAF Classic atau AWS WAF web (web ACL). Kontrol gagal jika `Enabled` bidang untuk AWS WAF konfigurasi diatur ke`false`.

AWS WAF adalah firewall aplikasi web yang membantu melindungi aplikasi web dan API dari serangan. Dengan AWS WAF, Anda dapat mengonfigurasi ACL web, yang merupakan seperangkat aturan yang mengizinkan, memblokir, atau menghitung permintaan web berdasarkan aturan dan ketentuan keamanan web yang dapat disesuaikan yang Anda tentukan. Sebaiknya kaitkan Application Load Balancer Anda dengan AWS WAF ACL web untuk membantu melindunginya dari serangan berbahaya.

Remediasi

Untuk mengaitkan Application Load Balancer dengan ACL web, lihat Mengaitkan atau memisahkan ACL web dengan sumber daya di Panduan Pengembang. AWS AWS WAF

Kontrol EMR Amazon

Kontrol ini terkait dengan sumber daya EMR Amazon.

Kontrol ini mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[EMR.1] Node primer cluster EMR Amazon seharusnya tidak memiliki alamat IP publik

Persyaratan terkait: PCI DSS v3.2.1/1.2.1, PCI DSS v3.2.1/1.3.1, PCI DSS v3.2.1/1.3.2, PCI DSS v3.2.1/1.3.4, PCI DSS v3.2.1/1.3.6, Nist.800-53.R5 AC-21, Nist.800-53.r5 AC-3, Nist.800-53.r5 5 AC-3 (7), NIST.800-53.R5 AC-4, NIST.800-53.R5 AC-4 (21), Nist.800-53.r5 AC-6, Nist.800-53.r5 SC-7, Nist.800-53.r5 SC-7 (11), Nist.800-53.r5 SC-7 (16), Nist.800-53.r5 SC-7 (20), NIST.800-53.R5 SC-7 (21), Nist.800-53.r5 SC-7 (3), Nist.800-53.r5 SC-7 (4), Nist.800-53.r5 SC-7 (9)

Kategori: Lindungi > Konfigurasi jaringan aman

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::EMR::Cluster`

AWS Config aturan: **`emr-master-no-public-ip`**

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah node master di klaster EMR Amazon memiliki alamat IP publik. Kontrol gagal jika alamat IP publik dikaitkan dengan salah satu instance node master.

Alamat IP publik ditunjuk di `PublicIp` bidang `NetworkInterfaces` konfigurasi untuk instance. Kontrol ini hanya memeriksa kluster EMR Amazon yang berada dalam status atau`RUNNING`. `WAITING`

Remediasi

Selama peluncuran, Anda dapat mengontrol apakah instance Anda di subnet default atau nondefault diberi alamat IPv4 publik. Secara default, subnet default memiliki atribut ini disetel k`true`. Subnet nondefault memiliki atribut pengalamatan publik IPv4 yang disetel k`false`, kecuali jika dibuat oleh wizard instans peluncuran Amazon EC2. Dalam hal ini, atribut diatur k`true`.

Setelah diluncurkan, Anda tidak dapat secara manual memisahkan alamat IPv4 publik dari instans Anda.

Untuk memulihkan temuan yang gagal, Anda harus meluncurkan cluster baru di VPC dengan subnet pribadi yang memiliki atribut pengalamatan publik IPv4 yang disetel ke. `false` Untuk petunjuknya, lihat Meluncurkan cluster ke dalam VPC di Panduan Manajemen EMR Amazon.

[EMR.2] Pengaturan akses publik blok EMR Amazon harus diaktifkan

Persyaratan terkait: Nist.800-53.r5 AC-21, Nist.800-53.r5 AC-3, Nist.800-53.r5 AC-3 (7), Nist.800-53.r5 AC-4, Nist.800-53.r5 AC-4 (21), Nist.800-53.r5 AC-6, Nist.800-53.r5 R5 SC-7, Nist.800-53.r5 SC-7 (11), NIST.800-53.R5 SC-7 (16), Nist.800-53.r5 SC-7 (20), Nist.800-53.r5 SC-7 (21), Nist.800-53.r5 SC-7 (3), Nist.800-53.r5 5 SC-7 (4), NIST.800-53.R5 SC-7 (9)

Kategori: Lindungi > Manajemen akses aman > Sumber daya tidak dapat diakses publik

Tingkat keparahan: Kritis

Jenis sumber daya: `AWS::::Account`

AWS Config aturan: **`emr-block-public-access`**

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah akun Anda dikonfigurasi dengan Amazon EMR memblokir akses publik. Kontrol gagal jika pengaturan blokir akses publik tidak diaktifkan atau jika port apa pun selain port 22 diizinkan.

Amazon EMR memblokir akses publik mencegah Anda meluncurkan cluster di subnet publik jika cluster memiliki konfigurasi keamanan yang memungkinkan lalu lintas masuk dari alamat IP publik pada port. Saat pengguna dari Anda Akun AWS meluncurkan kluster, Amazon EMR memeriksa aturan port di grup keamanan untuk klaster dan membandingkannya dengan aturan lalu lintas masuk Anda. Jika grup keamanan memiliki aturan masuk yang membuka port ke alamat IP publik IPv4 0.0.0.0/0 atau IPv6: :/0, dan port tersebut tidak ditentukan sebagai pengecualian untuk akun Anda, Amazon EMR tidak mengizinkan pengguna membuat cluster.

> **Note**
>
> Blokir akses publik diaktifkan secara default. Untuk meningkatkan perlindungan akun, kami sarankan Anda tetap mengaktifkannya.

Remediasi

Untuk mengonfigurasi blokir akses publik untuk Amazon EMR, lihat Menggunakan Amazon EMR memblokir akses publik di Panduan Manajemen EMR Amazon.

Kontrol Elasticsearch

Kontrol ini terkait dengan sumber daya Elasticsearch.

Kontrol ini mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[ES.1] Domain Elasticsearch harus mengaktifkan enkripsi saat istirahat

Persyaratan terkait: PCI DSS v3.2.1/3.4, Nist.800-53.R5 CA-9 (1), Nist.800-53.R5 CM-3 (6), Nist.800-53.r5 SC-13, Nist.800-53.r5 SC-28, Nist.800-53.r5 SC-28 (1), Nist.800-500-53.r5 3.R5 SC-7 (10), NIST.800-53.R5 SI-7 (6)

Kategori: Lindungi > Perlindungan Data > Enkripsi data-at-rest

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::Elasticsearch::Domain`

AWS Config aturan: **`elasticsearch-encrypted-at-rest`**

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah domain Elasticsearch memiliki enkripsi saat konfigurasi istirahat diaktifkan. Pemeriksaan gagal jika enkripsi saat istirahat tidak diaktifkan.

Untuk lapisan keamanan tambahan untuk data sensitif Anda OpenSearch, Anda harus mengonfigurasi Anda OpenSearch untuk dienkripsi saat istirahat. Domain Elasticsearch menawarkan enkripsi data saat istirahat. Fitur ini digunakan AWS KMS untuk menyimpan dan mengelola kunci enkripsi Anda. Untuk melakukan enkripsi, ia menggunakan algoritma Advanced Encryption Standard dengan kunci 256-bit (AES-256).

Untuk mempelajari lebih lanjut tentang OpenSearch enkripsi saat istirahat, lihat Enkripsi data saat istirahat untuk OpenSearch Layanan Amazon di Panduan Pengembang OpenSearch Layanan Amazon.

Jenis instans tertentu, seperti `t.small` dan`t.medium`, tidak mendukung enkripsi data saat istirahat. Untuk detailnya, lihat Jenis instans yang didukung di Panduan Pengembang OpenSearch Layanan Amazon.

Remediasi

Untuk mengaktifkan enkripsi saat istirahat untuk domain Elasticsearch baru dan yang sudah ada, lihat Mengaktifkan enkripsi data saat istirahat di Panduan Pengembang Layanan Amazon OpenSearch .

[ES.2] Domain Elasticsearch tidak boleh diakses publik

Persyaratan terkait: PCI DSS v3.2.1/1.2.1, PCI DSS v3.2.1/1.3.1, PCI DSS v3.2.1/1.3.2, PCI DSS v3.2.1/1.3.4, PCI DSS v3.2.1/1.3.6, Nist.800-53.R5 AC-21, Nist.800-53.r5 AC-3, Nist.800-53.r5 5 AC-3 (7), NIST.800-53.R5 AC-4, NIST.800-53.R5 AC-4 (21), Nist.800-53.r5 AC-6, Nist.800-53.r5 SC-7, Nist.800-53.r5 SC-7 (11), Nist.800-53.r5 SC-7 (16), Nist.800-53.r5 SC-7 (20), NIST.800-53.R5 SC-7 (21), Nist.800-53.r5 SC-7 (3), Nist.800-53.r5 SC-7 (4), Nist.800-53.r5 SC-7 (9)

Kategori: Lindungi > Konfigurasi jaringan aman> Sumber daya dalam VPC

Tingkat keparahan: Kritis

Jenis sumber daya: `AWS::Elasticsearch::Domain`

AWS Config aturan: **`elasticsearch-in-vpc-only`**

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah domain Elasticsearch ada di VPC. Itu tidak mengevaluasi konfigurasi perutean subnet VPC untuk menentukan akses publik. Anda harus memastikan bahwa domain Elasticsearch tidak dilampirkan ke subnet publik. Lihat Kebijakan berbasis sumber daya di Panduan Pengembang Layanan Amazon OpenSearch . Anda juga harus memastikan bahwa VPC Anda dikonfigurasi sesuai dengan praktik terbaik yang disarankan. Lihat Praktik terbaik keamanan untuk VPC Anda di Panduan Pengguna Amazon VPC.

Domain Elasticsearch yang digunakan dalam VPC dapat berkomunikasi dengan sumber daya VPC melalui jaringan AWS pribadi, tanpa perlu melintasi internet publik. Konfigurasi ini meningkatkan postur keamanan dengan membatasi akses ke data dalam perjalanan. VPC menyediakan sejumlah kontrol jaringan untuk mengamankan akses ke domain Elasticsearch, termasuk ACL jaringan dan grup keamanan. Security Hub merekomendasikan agar Anda memigrasikan domain Elasticsearch publik ke VPC untuk memanfaatkan kontrol ini.

Remediasi

Jika Anda membuat domain dengan titik akhir publik, Anda tidak dapat menempatkannya di dalam VPC nanti. Sebagai gantinya, Anda harus membuat domain baru dan memigrasi data Anda. Begitu juga sebaliknya. Jika Anda membuat domain dalam VPC, domain tersebut tidak dapat memiliki titik akhir publik. Sebagai gantinya, Anda harus membuat domain lain atau menonaktifkan kontrol ini.

Lihat Meluncurkan domain OpenSearch Layanan Amazon Anda dalam VPC di Panduan Pengembang Layanan OpenSearch Amazon.

[ES.3] Domain Elasticsearch harus mengenkripsi data yang dikirim antar node

Persyaratan terkait: Nist.800-53.r5 AC-4, Nist.800-53.r5 SC-13, Nist.800-53.r5 SC-23, Nist.800-53.r5 SC-23 (3), Nist.800-53.r5 SC-7 (4), Nist.800-53.r5 SC-8, Nist.800-53.r5 R5 SC-8 (1), NIST.800-53.R5 SC-8 (2)

Kategori: Lindungi > Perlindungan Data > Enkripsi data-in-transit

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::Elasticsearch::Domain`

AWS Config aturan: **`elasticsearch-node-to-node-encryption-check`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah domain Elasticsearch telah mengaktifkan node-to-node enkripsi. Kontrol gagal jika domain Elasticsearch tidak mengaktifkan node-to-node enkripsi. Kontrol juga menghasilkan temuan yang gagal jika versi Elasticsearch tidak mendukung pemeriksaan node-to-node enkripsi.

HTTPS (TLS) dapat digunakan untuk membantu mencegah penyerang potensial menguping atau memanipulasi lalu lintas jaringan menggunakan atau serangan serupa. person-in-the-middle Hanya koneksi terenkripsi melalui HTTPS (TLS) yang diizinkan. Mengaktifkan node-to-node enkripsi untuk domain Elasticsearch memastikan bahwa komunikasi intra-cluster dienkripsi dalam perjalanan.

Mungkin ada penalti kinerja yang terkait dengan konfigurasi ini. Anda harus mengetahui dan menguji trade-off kinerja sebelum mengaktifkan opsi ini.

Remediasi

Untuk informasi tentang mengaktifkan node-to-node enkripsi pada domain baru dan yang sudah ada, lihat Mengaktifkan node-to-node enkripsi di Panduan Pengembang OpenSearch Layanan Amazon.

[ES.4] Kesalahan domain Elasticsearch yang masuk ke CloudWatch Log harus diaktifkan

Persyaratan terkait: Nist.800-53.r5 AC-2 (4), Nist.800-53.r5 AC-4 (26), Nist.800-53.r5 AC-6 (9), Nist.800-53.r5 AU-10, Nist.800-53.r5 AU-12, Nist.800-53.r5 AU-2, Nist.800-53.r5 5 AU-3, NIST.800-53.R5 AU-6 (3), NIST.800-53.R5 AU-6 (4), NIST.800-53.R5 CA-7, NIST.800-53.R5 SC-7 (9), NIST.800-53.R5 SI-4 (20), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-4 (20), nistST.800-53.R5 SI-7 (8)

Kategori: Identifikasi - Logging

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::Elasticsearch::Domain`

AWS Config aturan: **`elasticsearch-logs-to-cloudwatch`**

Jenis jadwal: Perubahan dipicu

Parameter:

- `logtype = 'error'`(tidak dapat disesuaikan)

Kontrol ini memeriksa apakah domain Elasticsearch dikonfigurasi untuk mengirim log kesalahan ke Log. CloudWatch

Anda harus mengaktifkan log kesalahan untuk domain Elasticsearch dan mengirim log tersebut ke CloudWatch Log untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.

Remediasi

Untuk informasi tentang cara mengaktifkan penerbitan log, lihat Mengaktifkan penerbitan log (konsol) di Panduan Pengembang OpenSearch Layanan Amazon.

[ES.5] Domain Elasticsearch harus mengaktifkan pencatatan audit

Persyaratan terkait: Nist.800-53.r5 AC-2 (4), Nist.800-53.r5 AC-4 (26), Nist.800-53.r5 AC-6 (9), Nist.800-53.r5 AU-10, Nist.800-53.r5 AU-12, Nist.800-53.r5 AU-2, Nist.800-53.r5 5 AU-3, NIST.800-53.R5 AU-6 (3), NIST.800-53.R5 AU-6 (4), NIST.800-53.R5 CA-7, NIST.800-53.R5 SC-7 (9), NIST.800-53.R5 SI-4 (20), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-4 (20), nistST.800-53.R5 SI-7 (8)

Kategori: Identifikasi > Logging

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::Elasticsearch::Domain`

AWS Config aturan: `elasticsearch-audit-logging-enabled` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

- `cloudWatchLogsLogGroupArnList`(tidak dapat disesuaikan). Security Hub tidak mengisi parameter ini. Daftar grup CloudWatch log Log yang dipisahkan koma yang harus dikonfigurasi untuk log audit.

  Aturan ini adalah `NON_COMPLIANT` jika grup CloudWatch log Log dari domain Elasticsearch tidak ditentukan dalam daftar parameter ini.

Kontrol ini memeriksa apakah domain Elasticsearch mengaktifkan pencatatan audit. Kontrol ini gagal jika domain Elasticsearch tidak mengaktifkan pencatatan audit.

Log audit sangat dapat disesuaikan. Mereka memungkinkan Anda melacak aktivitas pengguna di cluster Elasticsearch Anda, termasuk keberhasilan dan kegagalan otentikasi, permintaan, perubahan indeks OpenSearch, dan kueri penelusuran yang masuk.

Remediasi

Untuk petunjuk mendetail tentang mengaktifkan log audit, lihat Mengaktifkan log audit di Panduan Pengembang OpenSearch Layanan Amazon.

[ES.6] Domain Elasticsearch harus memiliki setidaknya tiga node data

Persyaratan terkait: Nist.800-53.r5 CP-10, Nist.800-53.R5 CP-6 (2), Nist.800-53.R5 SC-36, Nist.800-53.R5 SC-5 (2), Nist.800-53.r5 SI-13 (5)

Kategori: Pulihkan > Ketahanan > Ketersediaan tinggi

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::Elasticsearch::Domain`

AWS Config aturan: `elasticsearch-data-node-fault-tolerance` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah domain Elasticsearch dikonfigurasi dengan setidaknya tiga node data dan is. `zoneAwarenessEnabled` `true`

Domain Elasticsearch membutuhkan setidaknya tiga node data untuk ketersediaan tinggi dan toleransi kesalahan. Menerapkan domain Elasticsearch dengan setidaknya tiga node data memastikan operasi cluster jika node gagal.

Remediasi

Untuk mengubah jumlah node data dalam domain Elasticsearch

1. Buka konsol OpenSearch Layanan Amazon di https://console.aws.amazon.com/aos/.
2. Di bawah Domain, pilih nama domain yang ingin Anda edit.
3. Pilih Edit domain.
4. Di bawah Node data, atur Jumlah node ke angka yang lebih besar dari atau sama dengan`3`.

   Untuk tiga penerapan Availability Zone, atur ke kelipatan tiga untuk memastikan distribusi yang sama di seluruh Availability Zone.
5. Pilih Kirim.

[ES.7] Domain Elasticsearch harus dikonfigurasi dengan setidaknya tiga node master khusus

Persyaratan terkait: Nist.800-53.r5 CP-10, Nist.800-53.R5 CP-6 (2), Nist.800-53.R5 SC-36, Nist.800-53.R5 SC-5 (2), Nist.800-53.r5 SI-13 (5)

Kategori: Pulihkan > Ketahanan > Ketersediaan tinggi

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::Elasticsearch::Domain`

AWS Config aturan: `elasticsearch-primary-node-fault-tolerance` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah domain Elasticsearch dikonfigurasi dengan setidaknya tiga node primer khusus. Kontrol ini gagal jika domain tidak menggunakan node primer khusus. Kontrol ini lolos jika domain Elasticsearch memiliki lima node primer khusus. Namun, menggunakan lebih dari tiga node

primer mungkin tidak diperlukan untuk mengurangi risiko ketersediaan, dan akan menghasilkan biaya tambahan.

Domain Elasticsearch membutuhkan setidaknya tiga node primer khusus untuk ketersediaan tinggi dan toleransi kesalahan. Sumber daya node primer khusus dapat tegang selama penerapan biru/hijau simpul data karena ada node tambahan untuk dikelola. Menerapkan domain Elasticsearch dengan setidaknya tiga node primer khusus memastikan kapasitas sumber daya node primer dan operasi cluster yang memadai jika sebuah node gagal.

Remediasi

Untuk memodifikasi jumlah node utama khusus dalam OpenSearch domain

1. Buka konsol OpenSearch Layanan Amazon di https://console.aws.amazon.com/aos/.
2. Di bawah Domain, pilih nama domain yang ingin Anda edit.
3. Pilih Edit domain.
4. Di bawah Node master khusus, setel tipe Instance ke tipe instans yang diinginkan.
5. Mengatur Jumlah node master sama dengan tiga atau lebih besar.
6. Pilih Kirim.

[ES.8] Koneksi ke domain Elasticsearch harus dienkripsi menggunakan kebijakan keamanan TLS terbaru

Persyaratan terkait: Nist.800-53.r5 AC-17 (2), Nist.800-53.r5 AC-4, Nist.800-53.r5 IA-5 (1), Nist.800-53.r5 SC-12 (3), Nist.800-53.r5 SC-13, Nist.800-53.r5 SC-23, Nist.800-53.r5 SC-23, Nist.800-53.r5 00-53.r5 SC-23 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.R5 SC-8, Nist.800-53.r5 SC-8 (1), NIST.800-53.r5 SC-8 (2), NIST.800-53.r5 SI-7 (6)

Kategori: Lindungi > Perlindungan Data > Enkripsi data-in-transit

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::Elasticsearch::Domain`

AWS Config aturan: `elasticsearch-https-required` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah titik akhir domain Elasticsearch dikonfigurasi untuk menggunakan kebijakan keamanan TLS terbaru. Kontrol gagal jika titik akhir domain Elasticsearch tidak dikonfigurasi untuk menggunakan kebijakan terbaru yang didukung atau jika HTTPS tidak diaktifkan. Kebijakan keamanan TLS terbaru yang didukung saat ini adalah`Policy-Min-TLS-1-2-PFS-2023-10`.

HTTPS (TLS) dapat digunakan untuk membantu mencegah penyerang potensial menggunakan person-in-the-middle atau serangan serupa untuk menguping atau memanipulasi lalu lintas jaringan. Hanya koneksi terenkripsi melalui HTTPS (TLS) yang diizinkan. Mengenkripsi data dalam perjalanan dapat memengaruhi kinerja. Anda harus menguji aplikasi Anda dengan fitur ini untuk memahami profil kinerja dan dampak TLS. TLS 1.2 menyediakan beberapa peningkatan keamanan dibandingkan versi TLS sebelumnya.

Remediasi

Untuk mengaktifkan enkripsi TLS, gunakan operasi UpdateDomainConfigAPI untuk mengkonfigurasi DomainEndpointOptionsobjek. Ini menetapkan`TLSSecurityPolicy`.

[ES.9] Domain Elasticsearch harus diberi tag

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::Elasticsearch::Domain`

AWS Config aturan: `tagged-elasticsearch-domain` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList	Daftar tag yang memenuhi	`No default value`

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
			AWS persyaratan	

Kontrol ini memeriksa apakah domain Elasticsearch memiliki tag dengan kunci spesifik yang ditentukan dalam parameter. `requiredTagKeys` Kontrol gagal jika domain tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika domain tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke domain Elasticsearch, lihat Bekerja dengan tag di Panduan Pengembang OpenSearch Layanan Amazon.

EventBridge Kontrol Amazon

Kontrol ini terkait dengan EventBridge sumber daya.

Kontrol ini mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[EventBridge.2] bus EventBridge acara harus diberi tag

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::Events::EventBus`

AWS Config aturan: `tagged-events-eventbus` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList	Daftar tag yang memenuhi AWS persyaratan	Tidak ada nilai default

Kontrol ini memeriksa apakah bus EventBridge acara Amazon memiliki tag dengan kunci tertentu yang ditentukan dalam parameter`requiredTagKeys`. Kontrol gagal jika bus acara tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika bus acara tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik,

lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke bus EventBridge acara, lihat EventBridge Tag Amazon di Panduan EventBridge Pengguna Amazon.

[EventBridge.3] bus acara EventBridge khusus harus memiliki kebijakan berbasis sumber daya terlampir

Persyaratan terkait: Nist.800-53.r5 AC-2, Nist.800-53.r5 AC-2 (1), Nist.800-53.r5 AC-3, Nist.800-53.r5 AC-3 (15), Nist.800-53.r5 AC-3 (7), Nist.800-53.r5 AC-5, Nist.800-53.r5 AC-5, Nist.800-500-53.r5 3.R5 AC-6, NIST.800-53.R5 AC-6 (3)

Kategori: Lindungi > Manajemen akses aman > Sumber daya tidak dapat diakses publik

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::Events::EventBus`

AWS Config aturan: **`custom-schema-registry-policy-attached`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah bus acara EventBridge khusus Amazon memiliki kebijakan berbasis sumber daya yang dilampirkan. Kontrol ini gagal jika bus acara khusus tidak memiliki kebijakan berbasis sumber daya.

Secara default, bus acara EventBridge khusus tidak memiliki kebijakan berbasis sumber daya yang dilampirkan. Hal ini memungkinkan kepala sekolah di akun untuk mengakses bus acara. Dengan melampirkan kebijakan berbasis sumber daya ke bus acara, Anda dapat membatasi akses ke bus acara ke akun tertentu, serta dengan sengaja memberikan akses ke entitas di akun lain.

Remediasi

Untuk melampirkan kebijakan berbasis sumber daya ke bus acara EventBridge khusus, lihat Mengelola izin bus acara di Panduan Pengguna Amazon. EventBridge

[EventBridge.4] titik akhir EventBridge global harus mengaktifkan replikasi acara

Persyaratan terkait: Nist.800-53.r5 CP-10, Nist.800-53.R5 CP-6 (2), Nist.800-53.R5 SC-36, Nist.800-53.R5 SC-5 (2), Nist.800-53.r5 SI-13 (5)

Kategori: Pulihkan > Ketahanan > Ketersediaan tinggi

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::Events::Endpoint`

AWS Config aturan: **`global-endpoint-event-replication-enabled`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah replikasi peristiwa diaktifkan untuk titik akhir EventBridge global Amazon. Kontrol gagal jika replikasi peristiwa tidak diaktifkan untuk titik akhir global.

Titik akhir global membantu membuat aplikasi Anda toleran terhadap kesalahan regional. Untuk memulai, Anda menetapkan pemeriksaan kesehatan Amazon Route 53 ke titik akhir. Ketika failover dimulai, pemeriksaan kesehatan melaporkan keadaan “tidak sehat”. Dalam beberapa menit setelah inisiasi failover, semua acara khusus diarahkan ke bus acara di Wilayah sekunder dan diproses oleh bus acara tersebut. Saat Anda menggunakan titik akhir global, Anda dapat mengaktifkan replikasi

peristiwa. Replikasi acara mengirimkan semua peristiwa khusus ke bus acara di Wilayah primer dan sekunder menggunakan aturan terkelola. Sebaiknya aktifkan replikasi peristiwa saat menyiapkan titik akhir global. Replikasi acara membantu Anda memverifikasi bahwa titik akhir global Anda dikonfigurasi dengan benar. Replikasi peristiwa diperlukan untuk memulihkan secara otomatis dari peristiwa failover. Jika replikasi acara tidak diaktifkan, Anda harus mengatur ulang pemeriksaan kesehatan Route 53 secara manual ke “sehat” sebelum acara dialihkan kembali ke Wilayah utama.

> **Note**
>
> Jika Anda menggunakan bus acara khusus, Anda memerlukan bus genap khusus di setiap Wilayah dengan nama yang sama dan di akun yang sama agar failover berfungsi dengan baik. Mengaktifkan replikasi acara dapat meningkatkan biaya bulanan Anda. Untuk informasi tentang harga, lihat EventBridge harga Amazon.

Remediasi

Untuk mengaktifkan replikasi peristiwa untuk titik akhir EventBridge global, lihat Membuat titik akhir global di Panduan Pengguna Amazon EventBridge . Untuk replikasi Acara, pilih Replikasi acara diaktifkan.

Kontrol Amazon FSx

Kontrol ini terkait dengan sumber daya Amazon FSx.

Kontrol ini mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[FSX.1] FSx untuk sistem file OpenZFS harus dikonfigurasi untuk menyalin tag ke cadangan dan volume

Persyaratan terkait: NIST.800-53.R5 CA-9 (1), Nist.800-53.R5 CM-2, Nist.800-53.R5 CM-2 (2)

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::FSx::FileSystem`

AWS Config aturan: **`fsx-openzfs-copy-tags-enabled`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah sistem file Amazon FSx untuk OpenZFS dikonfigurasi untuk menyalin tag ke cadangan dan volume. Kontrol gagal jika sistem file OpenZFS tidak dikonfigurasi untuk menyalin tag ke backup dan volume.

Identifikasi dan inventaris aset TI Anda merupakan aspek penting dari tata kelola dan keamanan. Tag membantu Anda mengkategorikan AWS sumber daya Anda dengan cara yang berbeda, misalnya, berdasarkan tujuan, pemilik, atau lingkungan. Ini berguna ketika Anda memiliki banyak sumber daya dari jenis yang sama karena Anda dapat dengan cepat mengidentifikasi sumber daya tertentu berdasarkan tag yang Anda tetapkan padanya.

Remediasi

Untuk mengonfigurasi sistem file FSx untuk OpenZFS untuk menyalin tag ke cadangan dan volume, lihat Memperbarui sistem file di Panduan Pengguna Amazon FSx OpenZFS.

[FSX.2] Sistem file FSx for Lustre harus dikonfigurasi untuk menyalin tag ke cadangan

Persyaratan terkait: Nist.800-53.r5 CP-9, Nist.800-53.r5 CM-8

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::FSx::FileSystem`

AWS Config aturan: **`fsx-lustre-copy-tags-to-backups`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah sistem file Amazon FSx for Lustre dikonfigurasi untuk menyalin tag ke backup dan volume. Kontrol gagal jika sistem file Lustre tidak dikonfigurasi untuk menyalin tag ke backup dan volume.

Identifikasi dan inventaris aset TI Anda merupakan aspek penting dari tata kelola dan keamanan. Tag membantu Anda mengkategorikan AWS sumber daya Anda dengan cara yang berbeda, misalnya,

berdasarkan tujuan, pemilik, atau lingkungan. Ini berguna ketika Anda memiliki banyak sumber daya dari jenis yang sama karena Anda dapat dengan cepat mengidentifikasi sumber daya tertentu berdasarkan tag yang Anda tetapkan padanya.

Remediasi

Untuk mengonfigurasi sistem file FSx for Lustre untuk menyalin tag ke cadangan, lihat Memperbarui sistem file di Panduan Pengguna Amazon FSx OpenZFS.

AWS Global Accelerator kontrol

Kontrol ini terkait dengan sumber daya Global Accelerator.

Kontrol ini mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[GlobalAccelerator.1] Akselerator Akselerator Global harus diberi tag

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::GlobalAccelerator::Accelerator`

AWS Config aturan: `tagged-globalaccelerator-accelerator` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList	Daftar tag yang memenuhi AWS persyaratan	`No default value`

Kontrol ini memeriksa apakah AWS Global Accelerator akselerator memiliki tag dengan kunci spesifik yang ditentukan dalam parameter`requiredTagKeys`. Kontrol gagal jika akselerator tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika akselerator tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke akselerator global Akselerator Global, lihat Menandai AWS Global Accelerator di Panduan PengembangAWS Global Accelerator .

AWS Glue kontrol

Kontrol ini terkait dengan AWS Glue sumber daya.

Kontrol ini mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

AWS Glue Pekerjaan [Glue.1] harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::Glue::Job`

AWS Config aturan: `tagged-glue-job` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList	Daftar tag yang memenuhi AWS persyaratan	Tidak ada nilai default

Kontrol ini memeriksa apakah AWS Glue pekerjaan memiliki tag dengan kunci tertentu yang ditentukan dalam parameter`requiredTagKeys`. Kontrol gagal jika pekerjaan tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika pekerjaan tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan

terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke AWS Glue pekerjaan, lihat AWS tag AWS Glue di Panduan AWS Glue Pengguna.

GuardDuty Kontrol Amazon

Kontrol ini terkait dengan GuardDuty sumber daya.

Kontrol ini mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[GuardDuty.1] GuardDuty harus diaktifkan

Persyaratan terkait: PCI DSS v3.2.1/11.4, Nist.800-53.r5 AC-2 (12), Nist.800-53.r5 AU-6 (1), Nist.800-53.r5 AU-6 (5), Nist.800-53.r5 CA-7, Nist.800-53.r5 CM-8 (3), NIST.800-500-53.R5 3.R5 RA-3 (4), NIST.800-53.R5 SA-11 (1), NIST.800-53.R5 SA-11 (6), NIST.800-53.R5 SA-15 (2), NIST.800-53.r5 SA-15 (8), NIST.800-53.r5 SA-8 (19), NIST.800-53.r5 SA-8 (21), NIST.800-53.R5 SA-8 (25), NIST.800-53.R5 SC-5, NIST.800-53.R5 SC-5 (1), NIST.800-53.R5 SC-5 (3), NIST.800-53.r5 SI-3 (8), NIST.800-53.r5 SI-3 (8), ST.800-53.R5 SI-4, NIST.800-53.R5 SI-4 (1), NIST.800-53.R5 SI-4 (13), NIST.800-53 .r5 SI-4 (2), NIST.800-53.R5 SI-4 (22), NIST.800-53.R5 SI-4 (25), NIST.800-53.R5 SI-4 (4), NIST.800-53.R5 SI-4 (5)

Kategori: Deteksi > Layanan deteksi

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS:::Account`

AWS Config aturan: **`guardduty-enabled-centralized`**

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah Amazon GuardDuty diaktifkan di GuardDuty akun dan Wilayah Anda.

Sangat disarankan agar Anda mengaktifkan GuardDuty di semua AWS Wilayah yang didukung. Melakukannya 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 CloudTrail peristiwa untuk global Layanan AWS seperti IAM.

Remediasi

Untuk mengatasi masalah ini, Anda mengaktifkan GuardDuty.

Untuk detail tentang cara mengaktifkan GuardDuty, termasuk cara menggunakan AWS Organizations untuk mengelola beberapa akun, lihat Memulai GuardDuty di Panduan GuardDuty Pengguna Amazon.

[GuardDuty.2] GuardDuty filter harus diberi tag

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::GuardDuty::Filter`

AWS Config aturan: `tagged-guardduty-filter` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya	StringList	Daftar tag yang	`No default value`

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
	yang dievaluasi. Kunci tag peka huruf besar dan kecil.		memenuhi AWS persyaratan	

Kontrol ini memeriksa apakah GuardDuty filter Amazon memiliki tag dengan kunci tertentu yang ditentukan dalam parameter`requiredTagKeys`. Kontrol gagal jika filter tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika filter tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke GuardDuty filter, lihat TagResourcedi Referensi Amazon GuardDuty API.

[GuardDuty.3] GuardDuty IPset harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::GuardDuty::IPSet`

AWS Config aturan: `tagged-guardduty-ipset` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList	Daftar tag yang memenuhi AWS persyaratan	`No default value`

Kontrol ini memeriksa apakah Amazon GuardDuty IPSet memiliki tag dengan kunci tertentu yang ditentukan dalam parameter`requiredTagKeys`. Kontrol gagal jika IPSet tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika IPSet tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke

AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke GuardDuty IPSet, lihat TagResourcedi Referensi Amazon GuardDuty API.

[GuardDuty.4] GuardDuty detektor harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::GuardDuty::Detector`

AWS Config aturan: `tagged-guardduty-detector` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList	Daftar tag yang memenuhi	`No default value`

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
			AWS persyaratan	

Kontrol ini memeriksa apakah GuardDuty detektor Amazon memiliki tag dengan kunci tertentu yang ditentukan dalam parameter`requiredTagKeys`. Kontrol gagal jika detektor tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika detektor tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke GuardDuty detektor, lihat TagResourcedi Referensi Amazon GuardDuty API.

AWS Identity and Access Management kontrol

Kontrol ini terkait dengan sumber daya IAM.

Kontrol ini mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[IAM.1] Kebijakan IAM seharusnya tidak mengizinkan hak administratif "*" penuh

Persyaratan terkait: PCI DSS v3.2.1/7.2.1, Tolok Ukur Yayasan CIS v1.2.0/1.22, Tolok Ukur AWS Yayasan CIS v1.4.0/1.16, Nist.800-53.r5 AC-2, Nist.800-53.r5 AC-2 (1), Nist.800-53.r5 AC-3, Nist.800-53.r5 AC-3 (15), Nist.800-53.r5 AC-3 (15), Nist.800-53.r5 AC-3 (15), Nist.800-53.r5 .800-53.r5 AC-3 (7), Nist.800-53.r5 AC-5, Nist.800-53.r5 AC-6, Nist.800-53.r5 AC-6 (10), Nist.800-53.r5 AC-6 (2), Nist.800-53.r5 AC-6 (3) AWS

Kategori: Lindungi > Manajemen akses yang aman

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::IAM::Policy`

AWS Config aturan: **`iam-policy-no-statements-with-admin-access`**

Jenis jadwal: Perubahan dipicu

Parameter:

- `excludePermissionBoundaryPolicy: true`(tidak dapat disesuaikan)

Kontrol ini memeriksa apakah versi default kebijakan IAM (juga dikenal sebagai kebijakan yang dikelola pelanggan) memiliki akses administrator dengan menyertakan pernyataan dengan `"Effect": "Allow"` with `"Action": "*"` over`"Resource": "*"`. Kontrol gagal jika Anda memiliki kebijakan IAM dengan pernyataan seperti itu.

Kontrol hanya memeriksa kebijakan terkelola pelanggan yang Anda buat. Itu tidak memeriksa kebijakan sebaris dan AWS terkelola.

Kebijakan IAM mendefinisikan serangkaian hak istimewa yang diberikan kepada pengguna, grup, atau peran. Mengikuti saran keamanan standar, AWS merekomendasikan agar Anda memberikan hak istimewa paling sedikit, yang berarti hanya memberikan izin yang diperlukan untuk melakukan

tugas. Bila Anda memberikan hak administratif penuh alih-alih set izin minimum yang dibutuhkan pengguna, Anda mengekspos sumber daya ke tindakan yang mungkin tidak diinginkan.

Alih-alih mengizinkan hak administratif penuh, tentukan apa yang perlu dilakukan pengguna dan kemudian buat kebijakan yang memungkinkan pengguna hanya melakukan tugas-tugas tersebut. Lebih aman untuk memulai dengan set izin minimum dan memberikan izin tambahan seperlunya. Jangan mulai dengan izin yang terlalu lunak dan kemudian coba kencangkan nanti.

Anda harus menghapus kebijakan IAM yang memiliki pernyataan dengan `"Effect": "Allow"` with `"Action": "*"` over`"Resource": "*"`.

> **Note**
>
> AWS Config harus diaktifkan di semua Wilayah tempat Anda menggunakan Security Hub. Namun, perekaman sumber daya global dapat diaktifkan dalam satu Wilayah. Jika Anda hanya merekam sumber daya global dalam satu Wilayah, maka Anda dapat menonaktifkan kontrol ini di semua Wilayah kecuali Wilayah tempat Anda merekam sumber daya global.

Remediasi

Untuk mengubah kebijakan IAM Anda sehingga tidak mengizinkan hak administratif “*” penuh, lihat Mengedit kebijakan IAM di Panduan Pengguna IAM.

[IAM.2] Pengguna IAM seharusnya tidak memiliki kebijakan IAM yang dilampirkan

Persyaratan terkait: PCI DSS v3.2.1/7.2.1, Tolok Ukur Yayasan CIS v3.0.0/1.15, Tolok Ukur AWS Yayasan CIS v1.2.0/1.16, Nist.800-53.r5 AC-2, Nist.800-53.r5 AC-2 (1), Nist.800-53.r5 AC-3, Nist.800-53.r5 AC-3 (15), Nist.ST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-6, NIST.800-53.r5 AC-6 (3) AWS

Kategori: Lindungi > Manajemen akses yang aman

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::IAM::User`

AWS Config aturan: **`iam-user-no-policies-check`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah pengguna IAM Anda memiliki kebijakan yang dilampirkan. Kontrol gagal jika pengguna IAM Anda memiliki kebijakan yang dilampirkan. Sebagai gantinya, pengguna IAM harus mewarisi izin dari grup IAM atau mengambil peran.

Secara default, pengguna IAM, grup, dan peran tidak memiliki akses ke AWS sumber daya. Kebijakan IAM memberikan hak istimewa kepada pengguna, grup, atau peran. Kami menyarankan Anda menerapkan kebijakan IAM secara langsung ke grup dan peran tetapi tidak untuk pengguna. Menetapkan hak istimewa di grup atau tingkat peran mengurangi kompleksitas manajemen akses seiring bertambahnya jumlah pengguna. Mengurangi kompleksitas manajemen akses pada gilirannya dapat mengurangi kesempatan bagi kepala sekolah untuk secara tidak sengaja menerima atau mempertahankan hak istimewa yang berlebihan.

> **Note**
>
> Pengguna IAM yang dibuat oleh Amazon Simple Email Service secara otomatis dibuat menggunakan kebijakan inline. Security Hub secara otomatis membebaskan pengguna ini dari kontrol ini.
> AWS Config harus diaktifkan di semua Wilayah tempat Anda menggunakan Security Hub. Namun, perekaman sumber daya global dapat diaktifkan dalam satu Wilayah. Jika Anda hanya merekam sumber daya global dalam satu Wilayah, maka Anda dapat menonaktifkan kontrol ini di semua Wilayah kecuali Wilayah tempat Anda merekam sumber daya global.

Remediasi

Untuk mengatasi masalah ini, buat grup IAM, dan lampirkan kebijakan ke grup. Kemudian, tambahkan pengguna ke grup. Kebijakan ini diterapkan untuk setiap pengguna dalam grup. Untuk menghapus kebijakan yang dilampirkan langsung ke pengguna, lihat Menambahkan dan menghapus izin identitas IAM di Panduan Pengguna IAM.

[IAM.3] Kunci akses pengguna IAM harus diputar setiap 90 hari atau kurang

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v3.0.0/1.14, Tolok Ukur Yayasan CIS v1.4.0/1.14, Tolok Ukur AWS Yayasan CIS v1.2.0/1.4, Nist.800-53.r5 AC-2 (1), Nist.800-53.r5 AWS AC-2 (3), Nist.800-53.r5 AC-3 (15)

Kategori: Lindungi > Manajemen akses yang aman

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::IAM::User`

AWS Config aturan: **`access-keys-rotated`**

Jenis jadwal: Periodik

Parameter:

- `maxAccessKeyAge`: `90` (tidak dapat disesuaikan)

Kontrol ini memeriksa apakah kunci akses aktif diputar dalam 90 hari.

Kami sangat menyarankan agar Anda tidak membuat dan menghapus semua kunci akses di akun Anda. Sebaliknya, praktik terbaik yang disarankan adalah membuat satu atau lebih peran IAM atau menggunakan federasi melalui AWS IAM Identity Center. Anda dapat menggunakan metode ini untuk memungkinkan pengguna Anda mengakses AWS Management Console dan AWS CLI.

Setiap pendekatan memiliki kasus penggunaannya. Federasi umumnya lebih baik untuk perusahaan yang memiliki direktori pusat yang ada atau berencana untuk membutuhkan lebih dari batas saat ini pada pengguna IAM. Aplikasi yang berjalan di luar AWS lingkungan membutuhkan kunci akses untuk akses terprogram ke AWS sumber daya.

Namun, jika sumber daya yang membutuhkan akses terprogram berjalan di dalam AWS, praktik terbaik adalah menggunakan peran IAM. Peran memungkinkan Anda untuk memberikan akses sumber daya tanpa hardcoding ID kunci akses dan kunci akses rahasia ke dalam konfigurasi.

Untuk mempelajari selengkapnya tentang melindungi kunci akses dan akun Anda, lihat Praktik terbaik untuk mengelola kunci AWS akses di Referensi Umum AWS. Lihat juga pedoman posting blog untuk melindungi Anda Akun AWS saat menggunakan akses terprogram.

Jika Anda sudah memiliki kunci akses, Security Hub merekomendasikan agar Anda memutar kunci akses setiap 90 hari. Memutar kunci akses mengurangi kemungkinan kunci akses yang terkait dengan akun yang disusupi atau dihentikan digunakan. Ini juga memastikan bahwa data tidak dapat diakses dengan kunci lama yang mungkin telah hilang, retak, atau dicuri. Selalu perbarui aplikasi Anda setelah Anda memutar tombol akses.

Kunci akses terdiri dari ID kunci akses dan kunci akses rahasia. Mereka digunakan untuk menandatangani permintaan terprogram yang Anda buat. AWS Pengguna memerlukan kunci akses

mereka sendiri untuk melakukan panggilan terprogram AWS dari AWS CLI, Alat untuk Windows PowerShell, AWS SDK, atau panggilan HTTP langsung menggunakan operasi API untuk individu. Layanan AWS

Jika organisasi Anda menggunakan AWS IAM Identity Center (Pusat Identitas IAM), pengguna Anda dapat masuk ke Active Directory, direktori Pusat Identitas IAM bawaan, atau penyedia identitas lain (iDP) yang terhubung ke Pusat Identitas IAM. Mereka kemudian dapat dipetakan ke peran IAM yang memungkinkan mereka menjalankan AWS CLI perintah atau memanggil operasi AWS API tanpa perlu kunci akses. Untuk mempelajari lebih lanjut, lihat Mengonfigurasi AWS CLI yang akan digunakan AWS IAM Identity Center dalam Panduan AWS Command Line Interface Pengguna.

> **Note**
>
> AWS Config harus diaktifkan di semua Wilayah tempat Anda menggunakan Security Hub. Namun, perekaman sumber daya global dapat diaktifkan dalam satu Wilayah. Jika Anda hanya merekam sumber daya global dalam satu Wilayah, maka Anda dapat menonaktifkan kontrol ini di semua Wilayah kecuali Wilayah tempat Anda merekam sumber daya global.

Remediasi

Untuk memutar tombol akses yang lebih tua dari 90 hari, lihat Memutar kunci akses di Panduan Pengguna IAM. Ikuti petunjuk untuk setiap pengguna dengan usia kunci Access lebih dari 90 hari.

[IAM.4] Kunci akses pengguna root IAM seharusnya tidak ada

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v3.0.0/1.4, Tolok Ukur Yayasan CIS v1.4.0/1.4, Tolok Ukur AWS Yayasan CIS v1.2.0/1.12, PCI DSS v3.2.1/2.1, PCI DSS v3.2.1/2.2, PCI DSS v3.2.1/7.2.1, Nist.800-53.r5 AC-2 (1), Nist.800-53.r5 AC-3 (15), Nist.800-53.r5 AC-3 (7), Nist.800-53.r5 AC-6, Nist.800-53.r5 AC-6 (10), Nist.800-53.r5 AC-6 (2) AWS

Kategori: Lindungi > Manajemen akses yang aman

Tingkat keparahan: Kritis

Jenis sumber daya: `AWS::::Account`

AWS Config aturan: **`iam-root-access-key-check`**

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah kunci akses pengguna root ada.

Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. AWS kunci akses menyediakan akses terprogram ke akun tertentu.

Security Hub merekomendasikan agar Anda menghapus semua kunci akses yang terkait dengan pengguna root. Ini membatasi vektor yang dapat digunakan untuk membahayakan akun Anda. Ini juga mendorong pembuatan dan penggunaan akun berbasis peran yang paling tidak memiliki hak istimewa.

Remediasi

Untuk menghapus kunci akses pengguna root, lihat Menghapus kunci akses untuk pengguna root di Panduan Pengguna IAM. Untuk menghapus kunci akses pengguna root dari Akun AWS dalam AWS GovCloud (US), lihat Menghapus kunci akses pengguna root AWS GovCloud (US) akun saya di Panduan AWS GovCloud (US) Pengguna.

[IAM.5] MFA harus diaktifkan untuk semua pengguna IAM yang memiliki kata sandi konsol

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v3.0.0/1.10, Tolok Ukur Yayasan CIS v1.4.0/1.10, Tolok Ukur AWS Yayasan CIS v1.2.0/1.2, Nist.800-53.r5 AC-2 (1), Nist.800-53.r5 AC-3 (15), Nist.800-53.r5 AWS IA-2 (1), Nist.800-53.r5 IA-2 (1), Nist.800-53.r5 IA-2 (2), NIST.800-53.R5 IA-2 (6), NIST.800-53.R5 IA-2 (8)

Kategori: Lindungi > Manajemen akses yang aman

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::IAM::User`

AWS Config aturan: **`mfa-enabled-for-iam-console-access`**

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah otentikasi AWS multi-faktor (MFA) diaktifkan untuk semua pengguna IAM yang menggunakan kata sandi konsol.

Otentikasi multi-faktor (MFA) menambahkan lapisan perlindungan tambahan di atas nama pengguna dan kata sandi. Dengan MFA diaktifkan, ketika pengguna masuk ke AWS situs web, mereka diminta untuk nama pengguna dan kata sandi mereka. Selain itu, mereka diminta untuk kode otentikasi dari perangkat MFA AWS mereka.

Kami menyarankan Anda mengaktifkan MFA untuk semua akun yang memiliki kata sandi konsol. MFA dirancang untuk memberikan peningkatan keamanan untuk akses konsol. Prinsipal otentikasi harus memiliki perangkat yang memancarkan kunci sensitif waktu dan harus memiliki pengetahuan tentang kredensi.

> **Note**
>
> AWS Config harus diaktifkan di semua Wilayah tempat Anda menggunakan Security Hub. Namun, perekaman sumber daya global dapat diaktifkan dalam satu Wilayah. Jika Anda hanya merekam sumber daya global dalam satu Wilayah, maka Anda dapat menonaktifkan kontrol ini di semua Wilayah kecuali Wilayah tempat Anda merekam sumber daya global.

Remediasi

Untuk menambahkan MFA bagi pengguna IAM, lihat Menggunakan otentikasi multi-faktor (MFA) di Panduan Pengguna IAM. AWS

Kami menawarkan kunci keamanan MFA gratis untuk pelanggan yang memenuhi syarat. Lihat apakah Anda memenuhi syarat, dan pesan kunci gratis Anda.

[IAM.6] MFA perangkat keras harus diaktifkan untuk pengguna root

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v3.0.0/1.6, Tolok Ukur Yayasan CIS v1.4.0/1.6, Tolok Ukur AWS Yayasan CIS v1.2.0/1.14, PCI DSS v3.2.1/8.3.1, Nist.800-53.r5 AC-2 (1), Nist.800-53.r5 AC-3 (15), Nist.800-53.r5 IA-2 (1), Nist.800-53.r5 IA-2 (1), Nist.800-53.r5 ST.800-53.r5 IA-2 (2), NIST.800-53.r5 IA-2 (6), NIST.800-53.R5 IA-2 (8) AWS

Kategori: Lindungi > Manajemen akses yang aman

Tingkat keparahan: Kritis

Jenis sumber daya: `AWS::::Account`

AWS Config aturan: **`root-account-hardware-mfa-enabled`**

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah Anda Akun AWS diaktifkan untuk menggunakan perangkat autentikasi multi-faktor perangkat keras (MFA) untuk masuk dengan kredensyal pengguna root. Kontrol gagal jika MFA tidak diaktifkan atau jika ada perangkat MFA virtual yang diizinkan untuk masuk dengan kredensyal pengguna root.

MFA virtual mungkin tidak memberikan tingkat keamanan yang sama dengan perangkat MFA perangkat keras. Kami menyarankan Anda hanya menggunakan perangkat MFA virtual saat Anda menunggu persetujuan pembelian perangkat keras atau perangkat keras Anda tiba. Untuk mempelajari lebih lanjut, lihat Mengaktifkan perangkat virtual multi-faktor otentikasi (MFA) (konsol) di Panduan Pengguna IAM.

Baik token kata sandi satu kali berbasis waktu (TOTP) dan Universal 2nd Factor (U2F) dapat digunakan sebagai opsi MFA perangkat keras.

Remediasi

Untuk menambahkan perangkat MFA perangkat keras untuk pengguna root, lihat Mengaktifkan perangkat MFA perangkat keras untuk pengguna Akun AWS root (konsol) di Panduan Pengguna IAM.

Kami menawarkan kunci keamanan MFA gratis untuk pelanggan yang memenuhi syarat. Lihat apakah Anda memenuhi syarat, dan pesan kunci gratis Anda.

[IAM.7] Kebijakan kata sandi untuk pengguna IAM harus memiliki konfigurasi yang kuat

Persyaratan terkait: Nist.800-53.r5 AC-2 (1), Nist.800-53.r5 AC-2 (3), Nist.800-53.r5 AC-3 (15), Nist.800-53.r5 IA-5 (1)

Kategori: Lindungi > Manajemen akses yang aman

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::::Account`

AWS Config aturan: **`iam-password-policy`**

Jenis jadwal: Periodik

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`RequireUppercaseCharacters`	Memerlukan setidaknya satu karakter huruf besar dalam kata sandi	Boolean	`true` atau `false`	`true`
`RequireLowercaseCharacters`	Memerlukan setidaknya satu karakter huruf kecil dalam kata sandi	Boolean	`true` atau `false`	`true`
`RequireSymbols`	Memerlukan setidaknya satu simbol dalam kata sandi	Boolean	`true` atau `false`	`true`
`RequireNumbers`	Memerlukan setidaknya satu nomor dalam kata sandi	Boolean	`true` atau `false`	`true`
`MinimumPasswordLength`	Jumlah minimum karakter dalam kata sandi	Bilangan Bulat	8 untuk 128	8
`PasswordReusePrevention`	Jumlah rotasi kata sandi sebelum kata sandi lama dapat digunakan kembali	Bilangan Bulat	12 untuk 24	Tidak ada nilai default
`MaxPasswordAge`	Jumlah hari sebelum kedaluwarsa kata sandi	Bilangan Bulat	1 untuk 90	Tidak ada nilai default

Kontrol ini memeriksa apakah kebijakan kata sandi akun untuk pengguna IAM menggunakan konfigurasi yang kuat. Kontrol gagal jika kebijakan kata sandi tidak menggunakan konfigurasi yang kuat. Kecuali Anda memberikan nilai parameter kustom, Security Hub menggunakan nilai default yang disebutkan dalam tabel sebelumnya. `MaxPasswordAge`Parameter `PasswordReusePrevention` dan tidak memiliki nilai default, jadi jika Anda mengecualikan parameter ini, Security Hub mengabaikan jumlah rotasi kata sandi dan usia kata sandi saat mengevaluasi kontrol ini.

Untuk mengakses AWS Management Console, pengguna IAM memerlukan kata sandi. Sebagai praktik terbaik, Security Hub sangat merekomendasikan bahwa alih-alih membuat pengguna IAM, Anda menggunakan federasi. Federasi memungkinkan pengguna untuk menggunakan kredensyal perusahaan mereka yang ada untuk masuk ke. AWS Management Console Gunakan AWS IAM Identity Center (IAM Identity Center) untuk membuat atau menyatukan pengguna, dan kemudian mengambil peran IAM ke dalam akun.

Untuk mempelajari lebih lanjut tentang penyedia identitas dan federasi, lihat Penyedia identitas dan federasi di Panduan Pengguna IAM. Untuk mempelajari selengkapnya tentang Pusat Identitas IAM, lihat Panduan AWS IAM Identity Center Pengguna.

Jika Anda perlu menggunakan pengguna IAM, Security Hub merekomendasikan agar Anda menerapkan pembuatan kata sandi pengguna yang kuat. Anda dapat menetapkan kebijakan kata sandi Akun AWS untuk menentukan persyaratan kompleksitas dan periode rotasi wajib untuk kata sandi. Saat Anda membuat atau mengubah kebijakan kata sandi, sebagian besar pengaturan kebijakan kata sandi diberlakukan saat pengguna mengubah kata sandi mereka berikutnya. Beberapa pengaturan diberlakukan segera.

Remediasi

Untuk memperbarui kebijakan kata sandi, lihat Menyetel kebijakan kata sandi akun untuk pengguna IAM di Panduan Pengguna IAM.

[IAM.8] Kredensyal pengguna IAM yang tidak digunakan harus dihapus

Persyaratan terkait: PCI DSS v3.2.1/8.1.4, Tolok Ukur AWS Yayasan CIS v1.2.0/1.3, Nist.800-53.r5 AC-2, Nist.800-53.r5 AC-2 (1), Nist.800-53.r5 AC-2 (3), Nist.800-53.r5 AC-3, Nist.800-53.r5 AC-3 (15), Nist.800-53.r5 AC-3 (7), NIST.800-53.R5 AC-6

Kategori: Lindungi > Manajemen akses yang aman

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::IAM::User`

AWS Config aturan: **`iam-user-unused-credentials-check`**

Jenis jadwal: Periodik

Parameter:

- `maxCredentialUsageAge`: `90` (tidak dapat disesuaikan)

Kontrol ini memeriksa apakah pengguna IAM Anda memiliki kata sandi atau kunci akses aktif yang belum digunakan selama 90 hari.

Pengguna IAM dapat mengakses AWS sumber daya menggunakan berbagai jenis kredensyal, seperti kata sandi atau kunci akses.

Security Hub menyarankan agar Anda menghapus atau menonaktifkan semua kredensi yang tidak digunakan selama 90 hari atau lebih. Menonaktifkan atau menghapus kredensyal yang tidak perlu mengurangi jendela peluang untuk kredensyal yang terkait dengan akun yang disusupi atau ditinggalkan untuk digunakan.

> **Note**
>
> AWS Config harus diaktifkan di semua Wilayah tempat Anda menggunakan Security Hub. Namun, perekaman sumber daya global dapat diaktifkan dalam satu Wilayah. Jika Anda hanya merekam sumber daya global dalam satu Wilayah, maka Anda dapat menonaktifkan kontrol ini di semua Wilayah kecuali Wilayah tempat Anda merekam sumber daya global.

Remediasi

Saat Anda melihat informasi pengguna di konsol IAM, ada kolom untuk usia kunci Access, Usia kata sandi, dan Aktivitas terakhir. Jika nilai di salah satu kolom ini lebih besar dari 90 hari, buat kredensil untuk pengguna tersebut tidak aktif.

Anda juga dapat menggunakan laporan kredensi untuk memantau pengguna dan mengidentifikasi mereka yang tidak memiliki aktivitas selama 90 hari atau lebih. Anda dapat mengunduh laporan kredensi dalam `.csv` format dari konsol IAM.

Setelah Anda mengidentifikasi akun yang tidak aktif atau kredensi yang tidak digunakan, nonaktifkan akun tersebut. Untuk petunjuk, lihat Membuat, mengubah, atau menghapus kata sandi pengguna (konsol) IAM di Panduan Pengguna IAM.

[IAM.9] MFA harus diaktifkan untuk pengguna root

Persyaratan terkait: PCI DSS v3.2.1/8.3.1, Tolok Ukur Yayasan CIS v3.0.0/1.5, Tolok Ukur Yayasan CIS v1.4.0/1.5, Tolok Ukur AWS Yayasan CIS v1.2.0/1.13, Nist.800-53.r5 AC-2 (1), Nist.800-53.r5

AC-3 (15), Nist.800-53.r5 IA-2 (1), Nist.800-53.r5 AWS IA-2 (1), Nist.800-53.r5 ST.800-53.r5 IA-2 (2), NIST.800-53.r5 IA-2 (6), NIST.800-53.R5 IA-2 (8) AWS

Kategori: Lindungi > Manajemen akses yang aman

Tingkat keparahan: Kritis

Jenis sumber daya: `AWS::::Account`

AWS Config aturan: **`root-account-mfa-enabled`**

Jenis jadwal: Periodik

Parameter: Tidak ada

Pengguna root memiliki akses lengkap ke semua layanan dan sumber daya dalam file Akun AWS. MFA menambahkan lapisan perlindungan tambahan di atas nama pengguna dan kata sandi. Dengan MFA diaktifkan, ketika pengguna masuk ke AWS Management Console, mereka diminta untuk nama pengguna dan kata sandi mereka dan untuk kode otentikasi dari perangkat MFA mereka. AWS

Ketika Anda menggunakan MFA virtual untuk pengguna root, CIS merekomendasikan bahwa perangkat yang digunakan bukan perangkat pribadi. Sebagai gantinya, gunakan perangkat seluler khusus (tablet atau ponsel) yang Anda kelola untuk tetap terisi daya dan diamankan terlepas dari perangkat pribadi individu mana pun. Ini mengurangi risiko kehilangan akses ke MFA karena kehilangan perangkat, pertukaran perangkat, atau jika individu yang memiliki perangkat tidak lagi dipekerjakan di perusahaan.

Remediasi

Untuk mengaktifkan MFA bagi pengguna root, lihat Aktifkan MFA pada pengguna Akun AWS root di Panduan Referensi Manajemen AWS Akun.

[IAM.10] Kebijakan kata sandi untuk pengguna IAM harus memiliki urasi yang kuat AWS Config

Persyaratan terkait: PCI DSS v3.2.1/8.1.4, PCI DSS v3.2.1/8.2.3, PCI DSS v3.2.1/8.2.4, PCI DSS v3.2.1/8.2.5

Kategori: Lindungi > Manajemen akses yang aman

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::::Account`

AWS Config aturan: **`iam-password-policy`**

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah kebijakan kata sandi akun untuk pengguna IAM menggunakan konfigurasi DSS PCI minimum berikut.

- `RequireUppercaseCharacters`— Memerlukan setidaknya satu karakter huruf besar dalam kata sandi. (Default = `true`)
- `RequireLowercaseCharacters`— Memerlukan setidaknya satu karakter huruf kecil dalam kata sandi. (Default = `true`)
- `RequireNumbers`— Memerlukan setidaknya satu nomor dalam kata sandi. (Default = `true`)
- `MinimumPasswordLength`— Panjang minimum kata sandi. (Default = 7 atau lebih)
- `PasswordReusePrevention`— Jumlah kata sandi sebelum mengizinkan penggunaan kembali. (Default = 4)
- MaxPasswordAge — Jumlah hari sebelum kedaluwarsa kata sandi. (Default = 90)

Remediasi

Untuk memperbarui kebijakan kata sandi agar menggunakan konfigurasi yang disarankan, lihat Menyetel kebijakan kata sandi akun untuk pengguna IAM di Panduan Pengguna IAM.

[IAM.11] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu huruf besar

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v1.2.0/1.5

Kategori: Lindungi > Manajemen akses yang aman

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::::Account`

AWS Config aturan: **`iam-password-policy`**

Jenis jadwal: Periodik

Parameter: Tidak ada

Kebijakan kata sandi, sebagian, menegakkan persyaratan kompleksitas kata sandi. Gunakan kebijakan kata sandi IAM untuk memastikan bahwa kata sandi menggunakan kumpulan karakter yang berbeda.

CIS merekomendasikan bahwa kebijakan kata sandi memerlukan setidaknya satu huruf besar. Menyetel kebijakan kompleksitas kata sandi meningkatkan ketahanan akun terhadap upaya login brute force.

Remediasi

Untuk mengubah kebijakan kata sandi, lihat Menyetel kebijakan kata sandi akun untuk pengguna IAM di Panduan Pengguna IAM. Untuk kekuatan Kata Sandi, pilih Memerlukan setidaknya satu huruf besar dari alfabet Latin (A—Z).

[IAM.12] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu huruf kecil

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v1.2.0/1.6

Kategori: Lindungi > Manajemen akses yang aman

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::::Account`

AWS Config aturan: **`iam-password-policy`**

Jenis jadwal: Periodik

Parameter: Tidak ada

Kebijakan kata sandi, sebagian, menegakkan persyaratan kompleksitas kata sandi. Gunakan kebijakan kata sandi IAM untuk memastikan bahwa kata sandi menggunakan kumpulan karakter yang berbeda. CIS merekomendasikan bahwa kebijakan kata sandi memerlukan setidaknya satu huruf kecil. Menyetel kebijakan kompleksitas kata sandi meningkatkan ketahanan akun terhadap upaya login brute force.

Remediasi

Untuk mengubah kebijakan kata sandi, lihat Menyetel kebijakan kata sandi akun untuk pengguna IAM di Panduan Pengguna IAM. Untuk kekuatan Kata Sandi, pilih Memerlukan setidaknya satu huruf kecil dari alfabet Latin (A—Z).

[IAM.13] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu simbol

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v1.2.0/1.7

Kategori: Lindungi > Manajemen akses yang aman

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::::Account`

AWS Config aturan: **`iam-password-policy`**

Jenis jadwal: Periodik

Parameter: Tidak ada

Kebijakan kata sandi, sebagian, menegakkan persyaratan kompleksitas kata sandi. Gunakan kebijakan kata sandi IAM untuk memastikan bahwa kata sandi menggunakan kumpulan karakter yang berbeda.

CIS merekomendasikan bahwa kebijakan kata sandi memerlukan setidaknya satu simbol. Menyetel kebijakan kompleksitas kata sandi meningkatkan ketahanan akun terhadap upaya login brute force.

Remediasi

Untuk mengubah kebijakan kata sandi, lihat Menyetel kebijakan kata sandi akun untuk pengguna IAM di Panduan Pengguna IAM. Untuk kekuatan Password, pilih Memerlukan setidaknya satu karakter nonalfanumerik.

[IAM.14] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu nomor

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v1.2.0/1.8

Kategori: Lindungi > Manajemen akses yang aman

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::::Account`

AWS Config aturan: **`iam-password-policy`**

Jenis jadwal: Periodik

Parameter: Tidak ada

Kebijakan kata sandi, sebagian, menegakkan persyaratan kompleksitas kata sandi. Gunakan kebijakan kata sandi IAM untuk memastikan bahwa kata sandi menggunakan kumpulan karakter yang berbeda.

CIS merekomendasikan bahwa kebijakan kata sandi memerlukan setidaknya satu nomor. Menyetel kebijakan kompleksitas kata sandi meningkatkan ketahanan akun terhadap upaya login brute force.

Remediasi

Untuk mengubah kebijakan kata sandi, lihat Menyetel kebijakan kata sandi akun untuk pengguna IAM di Panduan Pengguna IAM. Untuk kekuatan Kata Sandi, pilih Memerlukan setidaknya satu nomor.

[IAM.15] Pastikan kebijakan kata sandi IAM membutuhkan panjang kata sandi minimum 14 atau lebih

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v3.0.0/1.8, Tolok Ukur Yayasan CIS v1.4.0/1.8, Tolok Ukur AWS Yayasan CIS v1.2.0/1.9 AWS

Kategori: Lindungi > Manajemen akses yang aman

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::::Account`

AWS Config aturan: **`iam-password-policy`**

Jenis jadwal: Periodik

Parameter: Tidak ada

Kebijakan kata sandi, sebagian, menegakkan persyaratan kompleksitas kata sandi. Gunakan kebijakan kata sandi IAM untuk memastikan bahwa kata sandi setidaknya memiliki panjang tertentu.

CIS merekomendasikan bahwa kebijakan kata sandi memerlukan panjang kata sandi minimum 14 karakter. Menyetel kebijakan kompleksitas kata sandi meningkatkan ketahanan akun terhadap upaya login brute force.

Remediasi

Untuk mengubah kebijakan kata sandi, lihat Menyetel kebijakan kata sandi akun untuk pengguna IAM di Panduan Pengguna IAM. Untuk panjang minimum Kata Sandi, masukkan **14** atau nomor yang lebih besar.

[IAM.16] Pastikan kebijakan kata sandi IAM mencegah penggunaan kembali kata sandi

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v3.0.0/1.9, Tolok Ukur Yayasan CIS v1.4.0/1.9, Tolok Ukur Yayasan CIS AWS v1.2.0/1.10 AWS

Kategori: Lindungi > Manajemen akses yang aman

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::::Account`

AWS Config aturan: **`iam-password-policy`**

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah jumlah kata sandi yang harus diingat diatur ke 24. Kontrol gagal jika nilainya tidak 24.

Kebijakan kata sandi IAM dapat mencegah penggunaan kembali kata sandi yang diberikan oleh pengguna yang sama.

CIS merekomendasikan agar kebijakan kata sandi mencegah penggunaan kembali kata sandi. Mencegah penggunaan kembali kata sandi meningkatkan ketahanan akun terhadap upaya login brute force.

Remediasi

Untuk mengubah kebijakan kata sandi, lihat Menyetel kebijakan kata sandi akun untuk pengguna IAM di Panduan Pengguna IAM. Untuk Mencegah penggunaan kembali kata sandi, masukkan**24**.

[IAM.17] Pastikan kebijakan kata sandi IAM kedaluwarsa kata sandi dalam waktu 90 hari atau kurang

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v1.2.0/1.11

Kategori: Lindungi > Manajemen akses yang aman

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::::Account`

AWS Config aturan: **`iam-password-policy`**

Jenis jadwal: Periodik

Parameter: Tidak ada

Kebijakan kata sandi IAM dapat mengharuskan kata sandi diputar atau kedaluwarsa setelah beberapa hari tertentu.

CIS merekomendasikan agar kebijakan kata sandi kedaluwarsa kata sandi setelah 90 hari atau kurang. Mengurangi masa pakai kata sandi meningkatkan ketahanan akun terhadap upaya login brute force. Memerlukan perubahan kata sandi reguler juga membantu dalam skenario berikut:

- Kata sandi dapat dicuri atau dikompromikan tanpa sepengetahuan Anda. Ini dapat terjadi melalui kompromi sistem, kerentanan perangkat lunak, atau ancaman internal.
- Filter web perusahaan dan pemerintah tertentu atau server proxy dapat mencegat dan merekam lalu lintas bahkan jika itu dienkripsi.
- Banyak orang menggunakan kata sandi yang sama untuk banyak sistem seperti pekerjaan, email, dan pribadi.
- Workstation pengguna akhir yang dikompromikan mungkin memiliki keystroke logger.

Remediasi

Untuk mengubah kebijakan kata sandi, lihat Menyetel kebijakan kata sandi akun untuk pengguna IAM di Panduan Pengguna IAM. Untuk Aktifkan kedaluwarsa kata sandi, masukkan **`90`** atau nomor yang lebih kecil.

[IAM.18] Memastikan peran dukungan telah dibuat untuk mengelola insiden dengan AWS Support

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v3.0.0/1.17, Tolok Ukur Yayasan CIS v1.4.0/1.17, Tolok Ukur Yayasan CIS AWS v1.2.0/1.20 AWS

Kategori: Lindungi > Manajemen akses yang aman

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS:::Account`

AWS Config aturan: **iam-policy-in-use**

Jenis jadwal: Periodik

Parameter:

- `policyARN`: `arn:partition:iam::aws:policy/AWSSupportAccess` (tidak dapat disesuaikan)
- `policyUsageType`: `ANY` (tidak dapat disesuaikan)

AWS menyediakan pusat dukungan yang dapat digunakan untuk pemberitahuan dan respons insiden, serta dukungan teknis dan layanan pelanggan.

Buat peran IAM untuk memungkinkan pengguna yang berwenang mengelola insiden dengan Support AWS . Dengan menerapkan hak istimewa terkecil untuk kontrol akses, peran IAM akan memerlukan kebijakan IAM yang sesuai untuk memungkinkan akses pusat dukungan untuk mengelola insiden dengan. AWS Support

> **Note**
>
> AWS Config harus diaktifkan di semua Wilayah tempat Anda menggunakan Security Hub. Namun, perekaman sumber daya global dapat diaktifkan dalam satu Wilayah. Jika Anda hanya merekam sumber daya global dalam satu Wilayah, maka Anda dapat menonaktifkan kontrol ini di semua Wilayah kecuali Wilayah tempat Anda merekam sumber daya global.

Remediasi

Untuk mengatasi masalah ini, buat peran untuk memungkinkan pengguna yang berwenang mengelola AWS Support insiden.

Untuk membuat peran yang akan digunakan untuk AWS Support akses

1. Buka konsol IAM di https://console.aws.amazon.com/iam/.
2. Di panel navigasi IAM, pilih Peran, lalu pilih Buat peran.
3. Untuk tipe Peran, pilih Yang Lain Akun AWS.
4. Untuk ID Akun, masukkan Akun AWS ID yang Akun AWS ingin Anda berikan akses ke sumber daya Anda.

Jika pengguna atau grup yang akan mengambil peran ini berada di akun yang sama, maka masukkan nomor akun lokal.

> **Note**
>
> Administrator akun yang ditentukan dapat memberikan izin untuk mengasumsikan peran ini kepada setiap pengguna dalam akun tersebut. Untuk melakukannya, administrator melampirkan kebijakan kepada pengguna atau grup yang memberikan izin untuk tindakan `sts:AssumeRole`. Dalam kebijakan itu, sumber daya harus menjadi peran ARN.

5. Pilih Berikutnya: Izin.
6. Cari kebijakan terkelola`AWSSupportAccess`.
7. Pilih kotak centang untuk kebijakan `AWSSupportAccess` terkelola.
8. Pilih Berikutnya: Tanda.
9. (Opsional) Untuk menambahkan metadata ke peran, lampirkan tag sebagai pasangan nilai kunci.

   Untuk informasi selengkapnya tentang penggunaan tag di IAM, lihat Menandai pengguna dan peran IAM di Panduan Pengguna IAM.
10. Pilih Berikutnya: Tinjau.
11. Untuk Nama peran, masukkan nama peran Anda.

    Nama peran harus unik di dalam diri Anda Akun AWS. Mereka tidak peka huruf besar/kecil.
12. (Opsional) Untuk Deskripsi peran, masukkan deskripsi.
13. Tinjau peran, lalu pilih Buat peran.

[IAM.19] MFA harus diaktifkan untuk semua pengguna IAM

Persyaratan terkait: PCI DSS v3.2.1/8.3.1, Nist.800-53.r5 AC-2 (1), Nist.800-53.r5 AC-3 (15), Nist.800-53.r5 IA-2 (1), Nist.800-53.r5 IA-2 (2), Nist.800-53.r5 IA-2 (6), Nist.800-53.r5 IA-2 (6), Nist.ST.800-53.R5 IA-2 (8)

Kategori: Lindungi > Manajemen akses yang aman

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::IAM::User`

AWS Config aturan: **`iam-user-mfa-enabled`**

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah pengguna IAM mengaktifkan otentikasi multi-faktor (MFA).

> **Note**
>
> AWS Config harus diaktifkan di semua Wilayah tempat Anda menggunakan Security Hub. Namun, perekaman sumber daya global dapat diaktifkan dalam satu Wilayah. Jika Anda hanya merekam sumber daya global dalam satu Wilayah, maka Anda dapat menonaktifkan kontrol ini di semua Wilayah kecuali Wilayah tempat Anda merekam sumber daya global.

Remediasi

Untuk menambahkan MFA bagi pengguna IAM, lihat Mengaktifkan perangkat MFA untuk pengguna di AWS Panduan Pengguna IAM.

[IAM.20] Hindari penggunaan pengguna root

> **Important**
>
> Security Hub menghentikan kontrol ini pada April 2024. Untuk informasi selengkapnya, lihat Ubah log untuk kontrol Security Hub.

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v1.2.0/1.1

Kategori: Lindungi > Manajemen akses yang aman

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::IAM::User`

AWS Config aturan: `use-of-root-account-test` (aturan Security Hub khusus)

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah a Akun AWS memiliki batasan pada penggunaan pengguna root. Kontrol mengevaluasi sumber daya berikut:

- Topik Amazon Simple Notification Service (Amazon SNS)
- AWS CloudTrail jalan setapak
- Filter metrik yang terkait dengan CloudTrail jejak
- CloudWatch Alarm Amazon berdasarkan filter

Pemeriksaan ini menghasilkan `FAILED` temuan jika satu atau beberapa pernyataan berikut benar:

- Tidak ada CloudTrail jejak di akun.
- CloudTrail Jejak diaktifkan, tetapi tidak dikonfigurasi dengan setidaknya satu jejak Multi-wilayah yang mencakup acara manajemen baca dan tulis.
- CloudTrail Jejak diaktifkan, tetapi tidak terkait dengan grup CloudWatch log Log.
- Filter metrik yang tepat yang ditentukan oleh Center for Internet Security (CIS) tidak digunakan. Filter metrik yang ditentukan adalah`'{$.userIdentity.type="Root" && $.userIdentity.invokedBy NOT EXISTS && $.eventType !="AwsServiceEvent"}'`.
- Tidak ada CloudWatch alarm berdasarkan filter metrik di akun.
- CloudWatch alarm yang dikonfigurasi untuk mengirim notifikasi ke topik SNS terkait tidak dipicu berdasarkan kondisi alarm.
- Topik SNS tidak sesuai dengan batasan untuk mengirim pesan ke topik SNS.
- Topik SNS tidak memiliki setidaknya satu pelanggan.

Pemeriksaan ini menghasilkan status kontrol `NO_DATA` jika satu atau beberapa pernyataan berikut benar:

- Jejak multi-wilayah berbasis di Wilayah yang berbeda. Security Hub hanya dapat menghasilkan temuan di Wilayah tempat jejak itu berada.
- Jejak multi-wilayah milik akun yang berbeda. Security Hub hanya dapat menghasilkan temuan untuk akun yang memiliki jejak.

Pemeriksaan ini menghasilkan status kontrol `WARNING` jika satu atau beberapa pernyataan berikut benar:

- Akun saat ini tidak memiliki topik SNS yang direferensikan dalam alarm. CloudWatch
- Akun saat ini tidak memiliki akses ke topik SNS saat menjalankan `ListSubscriptionsByTopic` SNS API.

> **Note**
>
> Sebaiknya gunakan jejak organisasi untuk mencatat peristiwa dari banyak akun di suatu organisasi. Jejak organisasi adalah jalur Multi-wilayah secara default dan hanya dapat dikelola oleh akun AWS Organizations manajemen atau akun administrator yang CloudTrail didelegasikan. Menggunakan jejak organisasi menghasilkan status kontrol NO_DATA untuk kontrol yang dievaluasi di akun anggota organisasi. Di akun anggota, Security Hub hanya menghasilkan temuan untuk sumber daya milik anggota. Temuan yang berkaitan dengan jejak organisasi dihasilkan di akun pemilik sumber daya. Anda dapat melihat temuan ini di akun administrator yang didelegasikan Security Hub menggunakan agregasi lintas wilayah.

Sebagai praktik terbaik, gunakan kredensyal pengguna root Anda hanya jika diperlukan untuk melakukan tugas manajemen akun dan layanan. Terapkan kebijakan IAM secara langsung ke grup dan peran tetapi tidak untuk pengguna. Untuk petunjuk cara menyiapkan administrator untuk penggunaan sehari-hari, lihat Membuat pengguna dan grup admin IAM pertama Anda di Panduan Pengguna IAM.

Remediasi

Langkah-langkah untuk mengatasi masalah ini termasuk menyiapkan topik Amazon SNS, jejak, CloudTrail filter metrik, dan alarm untuk filter metrik.

Untuk membuat topik Amazon SNS

1. Buka konsol Amazon SNS di https://console.aws.amazon.com/sns/v3/home.
2. Buat topik Amazon SNS yang menerima semua alarm CIS.

   Buat setidaknya satu pelanggan untuk topik tersebut. Untuk informasi lebih lanjut, lihat Memulai dengan Amazon SNS di Panduan Developer Amazon Simple Notification Service.

Selanjutnya, siapkan aktif CloudTrail yang berlaku untuk semua Wilayah. Untuk melakukannya, ikuti langkah-langkah remediasi dithe section called “[CloudTrail.1] CloudTrail harus diaktifkan dan

dikonfigurasi dengan setidaknya satu jejak Multi-wilayah yang mencakup acara manajemen baca dan tulis".

Catat nama grup CloudWatch log Log yang Anda kaitkan dengan CloudTrail jejak. Anda membuat filter metrik untuk grup log tersebut.

Terakhir, buat filter metrik dan alarm.

Untuk membuat filter metrik dan alarm

1. Buka CloudWatch konsol di https://console.aws.amazon.com/cloudwatch/.
2. Pada panel navigasi, pilih Grup log.
3. Pilih kotak centang untuk grup CloudWatch log Log yang terkait dengan CloudTrail jejak yang Anda buat.
4. Dari Tindakan, pilih Buat Filter Metrik.
5. Di bawah Tentukan pola, lakukan hal berikut:
   a. Salin pola berikut dan kemudian tempelkan ke bidang Filter Pattern.

      ```
      {$.userIdentity.type="Root" && $.userIdentity.invokedBy NOT EXISTS &&
       $.eventType !="AwsServiceEvent"}
      ```

   b. Pilih Selanjutnya.
6. Di bawah Tetapkan Metrik, lakukan hal berikut:
   a. Di Nama filter, masukkan nama untuk filter metrik Anda.
   b. Untuk Metric Namespace, masukkan. **`LogMetrics`**

      Jika Anda menggunakan namespace yang sama untuk semua filter metrik log CIS Anda, maka semua metrik Benchmark CIS dikelompokkan bersama.
   c. Untuk Nama Metrik, masukkan nama untuk metrik. Ingat nama metrik. Anda harus memilih metrik saat membuat alarm.
   d. Untuk Metric value (Nilai metrik), masukkan **`1`**.
   e. Pilih Selanjutnya.
7. Di bawah Tinjau dan buat, verifikasi informasi yang Anda berikan untuk filter metrik baru. Kemudian, pilih Buat filter metrik.
8. Di panel navigasi, pilih Grup log, lalu pilih filter yang Anda buat di bawah Filter metrik.

9. Pilih kotak centang untuk filter. Pilih Buat alarm.
10. Di bawah Tentukan metrik dan kondisi, lakukan hal berikut:
    a. Dalam Kondisi, untuk Ambang, pilih Statis.
    b. Untuk Tentukan kondisi alarm, pilih Greater/Equal.
    c. Untuk Tentukan nilai ambang batas, masukkan**1**.
    d. Pilih Selanjutnya.
11. Di bawah Konfigurasi tindakan, lakukan hal berikut:
    a. Di bawah Pemicu status alarm, pilih Dalam alarm.
    b. Di bawah Pilih topik SNS, pilih Pilih topik SNS yang sudah ada.
    c. Untuk Kirim pemberitahuan ke, masukkan nama topik SNS yang Anda buat di prosedur sebelumnya.
    d. Pilih Selanjutnya.
12. Di bawah Tambahkan nama dan deskripsi, masukkan Nama dan Deskripsi untuk alarm, seperti**`CIS-1.1-RootAccountUsage`**. Lalu pilih Selanjutnya.
13. Di bawah Pratinjau dan buat, tinjau konfigurasi alarm. Kemudian pilih Buat alarm.

[IAM.21] Kebijakan terkelola pelanggan IAM yang Anda buat seharusnya tidak mengizinkan tindakan wildcard untuk layanan

Persyaratan terkait: Nist.800-53.r5 AC-2, Nist.800-53.r5 AC-2 (1), Nist.800-53.r5 AC-3, Nist.800-53.r5 AC-3 (15), Nist.800-53.r5 AC-3 (7), Nist.800-53.r5 AC-5, Nist.800-53.r5 AC-5, Nist.800-500-53.r5 3.R5 AC-6, NIST.800-53.R5 AC-6 (10), Nist.800-53.r5 AC-6 (2), Nist.800-53.r5 AC-6 (3)

Kategori: Deteksi > Manajemen akses aman

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::IAM::Policy`

AWS Config aturan: **`iam-policy-no-statements-with-full-access`**

Jenis jadwal: Perubahan dipicu

Parameter:

- `excludePermissionBoundaryPolicy`: `True` (tidak dapat disesuaikan)

Kontrol ini memeriksa apakah kebijakan berbasis identitas IAM yang Anda buat memiliki pernyataan Izinkan yang menggunakan wildcard * untuk memberikan izin untuk semua tindakan pada layanan apa pun. Kontrol gagal jika ada pernyataan kebijakan yang disertakan `"Effect": "Allow"` dengan`"Action": "Service:*"`.

Misalnya, pernyataan berikut dalam kebijakan menghasilkan temuan yang gagal.

```
"Statement": [
{
  "Sid": "EC2-Wildcard",
  "Effect": "Allow",
  "Action": "ec2:*",
  "Resource": "*"
}
```

Kontrol juga gagal jika Anda menggunakannya `"Effect": "Allow""NotAction": "service:*"`. Dalam hal ini, `NotAction` elemen menyediakan akses ke semua tindakan dalam Layanan AWS, kecuali untuk tindakan yang ditentukan dalam`NotAction`.

Kontrol ini hanya berlaku untuk kebijakan IAM yang dikelola pelanggan. Ini tidak berlaku untuk kebijakan IAM yang dikelola oleh AWS.

Saat Anda menetapkan izin Layanan AWS, penting untuk mencakup tindakan IAM yang diizinkan dalam kebijakan IAM Anda. Anda harus membatasi tindakan IAM hanya pada tindakan yang diperlukan. Ini membantu Anda memberikan izin hak istimewa paling sedikit. Kebijakan yang terlalu permisif dapat menyebabkan eskalasi hak istimewa jika kebijakan tersebut dilampirkan pada prinsipal IAM yang mungkin tidak memerlukan izin.

Dalam beberapa kasus, Anda mungkin ingin mengizinkan tindakan IAM yang memiliki awalan serupa, seperti `DescribeFlowLogs` dan. `DescribeAvailabilityZones` Dalam kasus resmi ini, Anda dapat menambahkan wildcard akhiran ke awalan umum. Misalnya, `ec2:Describe*`.

Kontrol ini lolos jika Anda menggunakan tindakan IAM awalan dengan wildcard berakhiran. Misalnya, pernyataan berikut dalam kebijakan menghasilkan temuan yang dilewatkan.

```
"Statement": [
{
  "Sid": "EC2-Wildcard",
  "Effect": "Allow",
  "Action": "ec2:Describe*",
  "Resource": "*"
```

```
}
```

Saat mengelompokkan tindakan IAM terkait dengan cara ini, Anda juga dapat menghindari melebihi batas ukuran kebijakan IAM.

> **Note**
>
> AWS Config harus diaktifkan di semua Wilayah tempat Anda menggunakan Security Hub. Namun, perekaman sumber daya global dapat diaktifkan dalam satu Wilayah. Jika Anda hanya merekam sumber daya global dalam satu Wilayah, maka Anda dapat menonaktifkan kontrol ini di semua Wilayah kecuali Wilayah tempat Anda merekam sumber daya global.

Remediasi

Untuk mengatasi masalah ini, perbarui kebijakan IAM Anda sehingga tidak mengizinkan hak administratif “*” penuh. Untuk detail tentang cara mengedit kebijakan IAM, lihat Mengedit kebijakan IAM di Panduan Pengguna IAM.

[IAM.22] Kredensyal pengguna IAM yang tidak digunakan selama 45 hari harus dihapus

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v3.0.0/1.12, Tolok Ukur Yayasan CIS v1.4.0/1.12 AWS

Kategori: Lindungi > Manajemen akses yang aman

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::IAM::User`

AWS Config aturan: **`iam-user-unused-credentials-check`**

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah pengguna IAM Anda memiliki kata sandi atau kunci akses aktif yang belum digunakan selama 45 hari atau lebih. Untuk melakukannya, ia memeriksa apakah `maxCredentialUsageAge` parameter AWS Config aturan sama dengan 45 atau lebih.

Pengguna dapat mengakses AWS sumber daya menggunakan berbagai jenis kredensil, seperti kata sandi atau kunci akses.

CIS merekomendasikan agar Anda menghapus atau menonaktifkan semua kredensil yang telah tidak digunakan selama 45 hari atau lebih. Menonaktifkan atau menghapus kredensyal yang tidak perlu mengurangi jendela peluang untuk kredensyal yang terkait dengan akun yang disusupi atau ditinggalkan untuk digunakan.

AWS Config Aturan untuk kontrol ini menggunakan operasi `GenerateCredentialReport`API `GetCredentialReport`dan, yang hanya diperbarui setiap empat jam. Perubahan pada pengguna IAM dapat memakan waktu hingga empat jam untuk dapat dilihat oleh kontrol ini.

> **Note**
>
> AWS Config harus diaktifkan di semua Wilayah tempat Anda menggunakan Security Hub. Namun, Anda dapat mengaktifkan perekaman sumber daya global dalam satu Wilayah. Jika Anda hanya merekam sumber daya global dalam satu Wilayah, maka Anda dapat menonaktifkan kontrol ini di semua Wilayah kecuali Wilayah tempat Anda merekam sumber daya global.

Remediasi

Saat Anda melihat informasi pengguna di konsol IAM, ada kolom untuk usia kunci Access, Usia kata sandi, dan Aktivitas terakhir. Jika nilai di salah satu kolom ini lebih besar dari 45 hari, buat kredensil untuk pengguna tersebut tidak aktif.

Anda juga dapat menggunakan laporan kredensi untuk memantau pengguna dan mengidentifikasi mereka yang tidak memiliki aktivitas selama 45 hari atau lebih. Anda dapat mengunduh laporan kredensi dalam `.csv` format dari konsol IAM.

Setelah Anda mengidentifikasi akun yang tidak aktif atau kredensi yang tidak digunakan, nonaktifkan akun tersebut. Untuk petunjuk, lihat Membuat, mengubah, atau menghapus kata sandi pengguna (konsol) IAM di Panduan Pengguna IAM.

[IAM.23] Penganalisis Akses IAM harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::AccessAnalyzer::Analyzer`

AWS Config aturan: `tagged-accessanalyzer-analyzer` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList	Daftar tag yang memenuhi AWS persyaratan	`No default value`

Kontrol ini memeriksa apakah penganalisis yang dikelola oleh AWS Identity and Access Management Access Analyzer (IAM Access Analyzer) memiliki tag dengan kunci tertentu yang ditentukan dalam parameter. `requiredTagKeys` Kontrol gagal jika penganalisis tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika penganalisis tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke analyzer, lihat TagResourcedi Referensi API AWS IAM Access Analyzer.

[IAM.24] Peran IAM harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::IAM::Role`

AWS Config aturan: `tagged-iam-role` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList	Daftar tag yang memenuhi AWS persyaratan	`No default value`

Kontrol ini memeriksa apakah peran AWS Identity and Access Management (IAM) memiliki tag dengan kunci tertentu yang ditentukan dalam parameter`requiredTagKeys`. Kontrol gagal

jika peran tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika peran tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke peran IAM, lihat Menandai sumber daya IAM di Panduan Pengguna IAM.

[IAM.25] Pengguna IAM harus diberi tag

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::IAM::User`

AWS Config aturan: `tagged-iam-user` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList	Daftar tag yang memenuhi AWS persyaratan	`No default value`

Kontrol ini memeriksa apakah pengguna AWS Identity and Access Management (IAM) memiliki tag dengan kunci tertentu yang ditentukan dalam parameter`requiredTagKeys`. Kontrol gagal jika pengguna tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika pengguna tidak diberi tag dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS

Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke pengguna IAM, lihat Menandai sumber daya IAM di Panduan Pengguna IAM.

[IAM.26] Sertifikat SSL/TLS kedaluwarsa yang dikelola di IAM harus dihapus

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v3.0.0/1.19

Kategori: Identifikasi > Kepatuhan

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::IAM::ServerCertificate`

AWS Config aturan: **`iam-server-certificate-expiration-check`**

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah sertifikat server SSL/TLS aktif yang dikelola di IAM telah kedaluwarsa. Kontrol gagal jika sertifikat server SSL/TLS yang kedaluwarsa tidak dihapus.

Untuk mengaktifkan koneksi HTTPS ke situs web atau aplikasi Anda AWS, Anda memerlukan sertifikat server SSL/TLS. Anda dapat menggunakan IAM atau AWS Certificate Manager (ACM) untuk menyimpan dan menyebarkan sertifikat server. Gunakan IAM sebagai manajer sertifikat hanya jika Anda harus mendukung koneksi HTTPS di Wilayah AWS yang tidak didukung oleh ACM. IAM mengenkripsi kunci pribadi Anda dengan aman dan menyimpan versi terenkripsinya dalam penyimpanan sertifikat IAM SSL. IAM mendukung penerapan sertifikat server di semua Wilayah, tetapi Anda harus mendapatkan sertifikat dari penyedia eksternal untuk digunakan. AWS Anda tidak dapat mengunggah sertifikat ACM ke IAM. Selain itu, Anda tidak dapat mengelola sertifikat dari konsol IAM. Menghapus sertifikat SSL/TLS yang kedaluwarsa menghilangkan risiko bahwa sertifikat yang tidak valid disebarkan secara tidak sengaja ke sumber daya, yang dapat merusak kredibilitas aplikasi atau situs web yang mendasarinya.

Remediasi

Untuk menghapus sertifikat server dari IAM, lihat Mengelola sertifikat server di IAM di Panduan Pengguna IAM.

[IAM.27] Identitas IAM seharusnya tidak memiliki kebijakan yang dilampirkan AWSCloudShellFullAccess

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v3.0.0/1.22

Kategori: Lindungi > Manajemen akses aman > Kebijakan IAM yang aman

Tingkat keparahan: Sedang

Jenis sumber daya:`AWS::IAM::Role`,`AWS::IAM::User`, `AWS::IAM::Group`

AWS Config aturan: **`iam-policy-blacklisted-check`**

Jenis jadwal: Perubahan dipicu

Parameter:

- “PolicyArns”: “arn:aws:iam: :aws:policy/, arn:aws-cn:iam: :aws:policy/, arn ::iam: AWSCloudShellFullAccess :aws:policy/” AWSCloudShellFullAccess aws-us-gov AWSCloudShellFullAccess

Kontrol ini memeriksa apakah identitas IAM (pengguna, peran, atau grup) memiliki kebijakan AWS terkelola yang `AWSCloudShellFullAccess` dilampirkan. Kontrol gagal jika identitas IAM memiliki `AWSCloudShellFullAccess` kebijakan yang dilampirkan.

AWS CloudShell menyediakan cara mudah untuk menjalankan perintah CLI terhadap. Layanan AWS Kebijakan AWS terkelola `AWSCloudShellFullAccess` menyediakan akses penuh CloudShell, yang memungkinkan kemampuan mengunggah dan mengunduh file antara sistem lokal pengguna dan CloudShell lingkungan. Dalam CloudShell lingkungan, pengguna memiliki izin sudo, dan dapat mengakses internet. Akibatnya, melampirkan kebijakan terkelola ini ke identitas IAM memberi mereka kemampuan untuk menginstal perangkat lunak transfer file dan memindahkan data dari CloudShell ke server internet eksternal. Sebaiknya ikuti prinsip hak istimewa paling sedikit dan melampirkan izin yang lebih sempit ke identitas IAM Anda.

Remediasi

Untuk melepaskan *AWSCloudShellFullAccess* kebijakan dari identitas IAM, lihat Menambahkan dan menghapus izin identitas IAM di Panduan Pengguna IAM.

[IAM.28] IAM Access Analyzer penganalisis akses eksternal harus diaktifkan

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v3.0.0/1.20

Kategori: Deteksi > Layanan deteksi > Pemantauan penggunaan istimewa

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::AccessAnalyzer::Analzyer`

AWS Config aturan: **`iam-external-access-analyzer-enabled`**

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah Akun AWS penganalisis akses eksternal IAM Access Analyzer diaktifkan. Kontrol gagal jika akun tidak mengaktifkan penganalisis akses eksternal di pilihan Wilayah AWS Anda saat ini.

Penganalisis akses eksternal IAM Access Analyzer membantu mengidentifikasi sumber daya di organisasi dan akun Anda, seperti bucket Amazon Simple Storage Service (Amazon S3) atau peran IAM, yang dibagikan dengan entitas eksternal. Ini membantu Anda menghindari akses yang tidak diinginkan ke sumber daya dan data Anda. IAM Access Analyzer bersifat Regional dan harus diaktifkan di setiap Wilayah. Untuk mengidentifikasi sumber daya yang dibagikan dengan prinsipal eksternal, penganalisis akses menggunakan penalaran berbasis logika untuk menganalisis kebijakan berbasis sumber daya di lingkungan Anda. AWS Saat mengaktifkan penganalisis akses eksternal, Anda membuat penganalisis untuk seluruh organisasi atau akun Anda.

Remediasi

Untuk mengaktifkan penganalisis akses eksternal di Wilayah tertentu, lihat Mengaktifkan IAM Access Analyzer di Panduan Pengguna IAM. Anda harus mengaktifkan penganalisis di setiap Wilayah tempat Anda ingin memantau akses ke sumber daya Anda.

AWS IoT kontrol

Kontrol ini terkait dengan AWS IoT sumber daya.

Kontrol ini mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[IoT.1] profil AWS IoT Core keamanan harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::IoT::SecurityProfile`

AWS Config aturan: `tagged-iot-securityprofile` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList	Daftar tag yang memenuhi AWS persyaratan	`No default value`

Kontrol ini memeriksa apakah profil AWS IoT Core keamanan memiliki tag dengan kunci tertentu yang ditentukan dalam parameter`requiredTagKeys`. Kontrol gagal jika profil keamanan tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika profil keamanan tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat

menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke profil AWS IoT Core keamanan, lihat Menandai AWS IoT sumber daya Anda di Panduan AWS IoT Pengembang.

[IoT.2] tindakan AWS IoT Core mitigasi harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::IoT::MitigationAction`

AWS Config aturan: `tagged-iot-mitigationaction` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya	StringList	Daftar tag yang memenuhi	`No default value`

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
	yang dievaluasi. Kunci tag peka huruf besar dan kecil.		AWS persyaratan	

Kontrol ini memeriksa apakah tindakan AWS IoT Core mitigasi memiliki tag dengan kunci spesifik yang ditentukan dalam parameter. `requiredTagKeys` Kontrol gagal jika tindakan mitigasi tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter. `requiredTagKeys` Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika tindakan mitigasi tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke tindakan AWS IoT Core mitigasi, lihat Menandai AWS IoT sumber daya Anda di Panduan Pengembang.AWS IoT

AWS IoT Core Dimensi [IoT.3] harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::IoT::Dimension`

AWS Config aturan: `tagged-iot-dimension` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList	Daftar tag yang memenuhi AWS persyaratan	`No default value`

Kontrol ini memeriksa apakah AWS IoT Core dimensi memiliki tag dengan kunci tertentu yang ditentukan dalam parameter`requiredTagKeys`. Kontrol gagal jika dimensi tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika dimensi tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke

AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke AWS IoT Core dimensi, lihat Menandai AWS IoT sumber daya Anda di Panduan AWS IoT Pengembang.

[IoT.4] AWS IoT Core otorisasi harus diberi tag

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::IoT::Authorizer`

AWS Config aturan: `tagged-iot-authorizer` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList	Daftar tag yang memenuhi	`No default value`

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
			AWS persyaratan	

Kontrol ini memeriksa apakah AWS IoT Core otorisasi memiliki tag dengan kunci tertentu yang ditentukan dalam parameter`requiredTagKeys`. Kontrol gagal jika otorisasi tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika otorisasi tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke AWS IoT Core otorisasi, lihat Menandai AWS IoT sumber daya Anda di Panduan AWS IoT Pengembang.

[IoT.5] alias AWS IoT Core peran harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::IoT::RoleAlias`

AWS Config aturan: `tagged-iot-rolealias` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList	Daftar tag yang memenuhi AWS persyaratan	`No default value`

Kontrol ini memeriksa apakah alias AWS IoT Core peran memiliki tag dengan kunci tertentu yang ditentukan dalam parameter`requiredTagKeys`. Kontrol gagal jika alias peran tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika alias peran tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke

AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke alias AWS IoT Core peran, lihat Menandai AWS IoT sumber daya Anda di Panduan AWS IoT Pengembang.

AWS IoT Core Kebijakan [IoT.6] harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::IoT::Policy`

AWS Config aturan: `tagged-iot-policy` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList	Daftar tag yang memenuhi	`No default value`

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
			AWS persyaratan	

Kontrol ini memeriksa apakah AWS IoT Core kebijakan memiliki tag dengan kunci spesifik yang ditentukan dalam parameter`requiredTagKeys`. Kontrol gagal jika kebijakan tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika kebijakan tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke AWS IoT Core kebijakan, lihat Menandai AWS IoT sumber daya Anda di Panduan AWS IoT Pengembang.

Kontrol Amazon Kinesis

Kontrol ini terkait dengan sumber daya Kinesis.

Kontrol ini mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[Kinesis.1] Aliran kinesis harus dienkripsi saat istirahat

Persyaratan terkait: Nist.800-53.r5 CA-9 (1), NIST.800-53.R5 CM-3 (6), Nist.800-53.r5 SC-13, Nist.800-53.r5 SC-28, Nist.800-53.r5 SC-28 (1), Nist.800-53.r5 SC-7 (10), Nist.800-53.r5 SC-7 (10), Nist.800-53.r5 SC-7 (10), Nist.800-53.r5 SC-7 (10), Nist.800-53.r5 SC-7 (10), Nist.800-53.r5 SC-7 (10), Nist.800-53.r5 SC-7 (10), ST.800-53.R5 SI-7 (6)

Kategori: Lindungi > Perlindungan Data > Enkripsi data-at-rest

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::Kinesis::Stream`

AWS Config aturan: **`kinesis-stream-encrypted`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah Kinesis Data Streams dienkripsi saat istirahat dengan enkripsi sisi server. Kontrol ini gagal jika aliran Kinesis tidak dienkripsi saat istirahat dengan enkripsi sisi server.

Enkripsi sisi server adalah fitur di Amazon Kinesis Data Streams yang secara otomatis mengenkripsi data sebelum diam dengan menggunakan file. AWS KMS key Data dienkripsi sebelum ditulis ke lapisan penyimpanan aliran Kinesis, dan didekripsi setelah diambil dari penyimpanan. Akibatnya, data Anda dienkripsi saat istirahat dalam layanan Amazon Kinesis Data Streams.

Remediasi

Untuk informasi tentang mengaktifkan enkripsi sisi server untuk aliran Kinesis, lihat Bagaimana cara memulai enkripsi sisi server? di Panduan Pengembang Amazon Kinesis.

[Kinesis.2] Aliran kinesis harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::Kinesis::Stream`

AWS Config aturan: `tagged-kinesis-stream` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList	Daftar tag yang memenuhi AWS persyaratan	Tidak ada nilai default

Kontrol ini memeriksa apakah aliran data Amazon Kinesis memiliki tag dengan kunci tertentu yang ditentukan dalam parameter. `requiredTagKeys` Kontrol gagal jika aliran data tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika aliran data tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke aliran data Kinesis, lihat Menandai aliran Anda di Amazon Kinesis Data Streams di Panduan Pengembang Amazon Kinesis.

AWS Key Management Service kontrol

Kontrol ini terkait dengan AWS KMS sumber daya.

Kontrol ini mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[KMS.1] Kebijakan yang dikelola pelanggan IAM tidak boleh mengizinkan tindakan dekripsi pada semua kunci KMS

Persyaratan terkait: Nist.800-53.r5 AC-2, Nist.800-53.r5 AC-2 (1), Nist.800-53.r5 AC-3, Nist.800-53.r5 AC-3 (15), Nist.800-53.r5 AC-3 (7), Nist.800-53.r5 AC-5, Nist.800-53.r5 AC-5, Nist.800-500-53.r5 3.R5 AC-6, NIST.800-53.R5 AC-6 (3)

Kategori: Lindungi > Manajemen akses yang aman

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::IAM::Policy`

AWS Config aturan: **`iam-customer-policy-blocked-kms-actions`**

Jenis jadwal: Perubahan dipicu

Parameter:

- `blockedActionsPatterns: kms:ReEncryptFrom, kms:Decrypt`(tidak dapat disesuaikan)
- `excludePermissionBoundaryPolicy`: `True` (tidak dapat disesuaikan)

Memeriksa apakah versi default dari kebijakan terkelola pelanggan IAM mengizinkan prinsipal untuk menggunakan tindakan AWS KMS dekripsi pada semua sumber daya. Kontrol gagal jika kebijakan cukup terbuka untuk mengizinkan `kms:Decrypt` atau `kms:ReEncryptFrom` tindakan pada semua kunci KMS.

Kontrol hanya memeriksa kunci KMS dalam elemen Resource dan tidak memperhitungkan persyaratan apa pun dalam elemen Kondisi kebijakan. Selain itu, kontrol mengevaluasi kebijakan terkelola pelanggan yang terlampir dan tidak terikat. Itu tidak memeriksa kebijakan sebaris atau kebijakan AWS terkelola.

Dengan AWS KMS, Anda mengontrol siapa yang dapat menggunakan kunci KMS Anda dan mendapatkan akses ke data terenkripsi Anda. Kebijakan IAM menentukan tindakan identitas (pengguna, grup, atau peran) yang dapat dilakukan pada sumber daya mana. Mengikuti praktik terbaik keamanan, AWS merekomendasikan agar Anda mengizinkan hak istimewa paling sedikit. Dengan kata lain, Anda harus memberikan identitas hanya `kms:ReEncryptFrom` izin `kms:Decrypt` atau dan hanya untuk kunci yang diperlukan untuk melakukan tugas. Jika tidak, pengguna mungkin menggunakan kunci yang tidak sesuai untuk data Anda.

Alih-alih memberikan izin untuk semua kunci, tentukan kumpulan kunci minimum yang dibutuhkan pengguna untuk mengakses data terenkripsi. Kemudian desain kebijakan yang memungkinkan pengguna untuk hanya menggunakan kunci tersebut. Misalnya, jangan izinkan `kms:Decrypt` izin pada semua kunci KMS. Sebagai gantinya, izinkan `kms:Decrypt` hanya pada kunci di Wilayah tertentu untuk akun Anda. Dengan mengadopsi prinsip hak istimewa terkecil, Anda dapat mengurangi risiko pengungkapan data Anda yang tidak diinginkan.

Remediasi

Untuk mengubah kebijakan terkelola pelanggan IAM, lihat Mengedit kebijakan yang dikelola pelanggan di Panduan Pengguna IAM. Saat mengedit kebijakan Anda, untuk `Resource` bidang tersebut, berikan Nama Sumber Daya Amazon (ARN) kunci atau kunci tertentu yang ingin Anda izinkan untuk mengaktifkan tindakan dekripsi.

[KMS.2] Prinsipal IAM tidak boleh memiliki kebijakan inline IAM yang memungkinkan tindakan dekripsi pada semua kunci KMS

Persyaratan terkait: Nist.800-53.r5 AC-2, Nist.800-53.r5 AC-2 (1), Nist.800-53.r5 AC-3, Nist.800-53.r5 AC-3 (15), Nist.800-53.r5 AC-3 (7), Nist.800-53.r5 AC-5, Nist.800-53.r5 AC-5, Nist.800-500-53.r5 3.R5 AC-6, NIST.800-53.R5 AC-6 (3)

Kategori: Lindungi > Manajemen akses yang aman

Tingkat keparahan: Sedang

Jenis sumber daya:

- `AWS::IAM::Group`
- `AWS::IAM::Role`
- `AWS::IAM::User`

AWS Config aturan: **`iam-inline-policy-blocked-kms-actions`**

Jenis jadwal: Perubahan dipicu

Parameter:

- `blockedActionsPatterns: kms:ReEncryptFrom, kms:Decrypt`(tidak dapat disesuaikan)

Kontrol ini memeriksa apakah kebijakan inline yang disematkan dalam identitas IAM Anda (peran, pengguna, atau grup) memungkinkan tindakan AWS KMS dekripsi dan enkripsi ulang pada semua kunci KMS. Kontrol gagal jika kebijakan cukup terbuka untuk mengizinkan `kms:Decrypt` atau `kms:ReEncryptFrom` tindakan pada semua kunci KMS.

Kontrol hanya memeriksa kunci KMS dalam elemen Resource dan tidak memperhitungkan persyaratan apa pun dalam elemen Kondisi kebijakan.

Dengan AWS KMS, Anda mengontrol siapa yang dapat menggunakan kunci KMS Anda dan mendapatkan akses ke data terenkripsi Anda. Kebijakan IAM menentukan tindakan identitas (pengguna, grup, atau peran) yang dapat dilakukan pada sumber daya mana. Mengikuti praktik terbaik keamanan, AWS merekomendasikan agar Anda mengizinkan hak istimewa paling sedikit. Dengan kata lain, Anda harus memberikan identitas hanya izin yang mereka butuhkan dan hanya untuk kunci yang diperlukan untuk melakukan tugas. Jika tidak, pengguna mungkin menggunakan kunci yang tidak sesuai untuk data Anda.

Alih-alih memberikan izin untuk semua kunci, tentukan kumpulan kunci minimum yang dibutuhkan pengguna untuk mengakses data terenkripsi. Kemudian desain kebijakan yang memungkinkan pengguna untuk hanya menggunakan kunci tersebut. Misalnya, jangan izinkan `kms:Decrypt` izin pada semua kunci KMS. Sebagai gantinya, izinkan izin hanya pada kunci tertentu di Wilayah tertentu untuk akun Anda. Dengan mengadopsi prinsip hak istimewa terkecil, Anda dapat mengurangi risiko pengungkapan data Anda yang tidak diinginkan.

Remediasi

Untuk mengubah kebijakan sebaris IAM, lihat Mengedit kebijakan sebaris di Panduan Pengguna IAM. Saat mengedit kebijakan Anda, untuk `Resource` bidang tersebut, berikan Nama Sumber Daya Amazon (ARN) kunci atau kunci tertentu yang ingin Anda izinkan untuk mengaktifkan tindakan dekripsi.

[KMS.3] tidak AWS KMS keys boleh dihapus secara tidak sengaja

Persyaratan terkait: Nist.800-53.r5 SC-12, Nist.800-53.R5 SC-12 (2)

Kategori: Lindungi > Perlindungan data > Perlindungan penghapusan data

Tingkat keparahan: Kritis

Jenis sumber daya: `AWS::KMS::Key`

AWS Config aturan: `kms-cmk-not-scheduled-for-deletion-2` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah kunci KMS dijadwalkan untuk dihapus. Kontrol gagal jika kunci KMS dijadwalkan untuk dihapus.

Kunci KMS tidak dapat dipulihkan setelah dihapus. Data yang dienkripsi di bawah kunci KMS juga tidak dapat dipulihkan secara permanen jika kunci KMS dihapus. Jika data bermakna telah dienkripsi di bawah kunci KMS yang dijadwalkan untuk dihapus, pertimbangkan untuk mendekripsi data atau mengenkripsi ulang data di bawah kunci KMS baru kecuali Anda sengaja melakukan penghapusan kriptografi.

Ketika kunci KMS dijadwalkan untuk dihapus, periode tunggu wajib diberlakukan untuk memberikan waktu untuk membalikkan penghapusan, jika dijadwalkan dalam kesalahan. Masa tunggu default adalah 30 hari, tetapi dapat dikurangi menjadi sesingkat 7 hari ketika kunci KMS dijadwalkan untuk dihapus. Selama masa tunggu, penghapusan yang dijadwalkan dapat dibatalkan dan kunci KMS tidak akan dihapus.

Untuk informasi tambahan mengenai menghapus kunci KMS, lihat Menghapus kunci KMS di Panduan Pengembang.AWS Key Management Service

Remediasi

Untuk membatalkan penghapusan kunci KMS terjadwal, lihat Untuk membatalkan penghapusan kunci di bawah Penjadwalan dan pembatalan penghapusan kunci (konsol) di Panduan Pengembang.AWS Key Management Service

[KMS.4] rotasi AWS KMS tombol harus diaktifkan

Persyaratan terkait: PCI DSS v3.2.1/3.6.4, Tolok Ukur Yayasan CIS v3.0.0/3.6, Tolok Ukur Yayasan CIS v1.4.0/3.8, Tolok Ukur AWS Yayasan CIS v1.2.0/2.8, NIST.800-53.r5 SC-12, Nist.800-53.r5 AWS SC-12 (2), Nist.800-53.r5 SC-28 (3) AWS

Kategori: Lindungi > Perlindungan Data > Enkripsi data-at-rest

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::KMS::Key`

AWS Config aturan: **`cmk-backing-key-rotation-enabled`**

Jenis jadwal: Periodik

Parameter: Tidak ada

AWS KMS memungkinkan pelanggan untuk memutar kunci dukungan, yang merupakan bahan kunci yang disimpan AWS KMS dan diikat ke ID kunci kunci KMS. Ini adalah kunci pendukung yang digunakan untuk melakukan operasi kriptografi seperti enkripsi dan dekripsi. Rotasi kunci otomatis saat ini mempertahankan semua kunci pendukung sebelumnya sehingga dekripsi data terenkripsi dapat berlangsung secara transparan.

CIS merekomendasikan agar Anda mengaktifkan rotasi kunci KMS. Memutar kunci enkripsi membantu mengurangi dampak potensial dari kunci yang dikompromikan karena data yang dienkripsi dengan kunci baru tidak dapat diakses dengan kunci sebelumnya yang mungkin telah diekspos.

Remediasi

Untuk mengaktifkan rotasi tombol KMS, lihat Cara mengaktifkan dan menonaktifkan rotasi tombol otomatis di Panduan AWS Key Management Service Pengembang.

AWS Lambda kontrol

Kontrol ini terkait dengan sumber daya Lambda.

Kontrol ini mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[Lambda.1] Kebijakan fungsi Lambda harus melarang akses publik

Persyaratan terkait: PCI DSS v3.2.1/1.2.1, PCI DSS v3.2.1/1.3.1, PCI DSS v3.2.1/1.3.2, PCI DSS v3.2.1/1.3.4, PCI DSS v3.2.1/7.2.1, Nist.800-53.R5 AC-21, Nist.800-53.r5 AC-3, Nist.800-53.r5 AC-3 (7), NIST.800-53.R5 AC-4, NIST.800-53.R5 AC-4 (21), Nist.800-53.r5 AC-6, Nist.800-53.r5 SC-7, Nist.800-53.r5 SC-7 (11), Nist.800-53.r5 SC-7 (16), Nist.800-53.r5 SC-7 (20), NIST.800-53.R5 SC-7 (21), Nist.800-53.r5 SC-7 (3), Nist.800-53.r5 SC-7 (4), Nist.800-53.r5 SC-7 (9)

Kategori: Lindungi > Konfigurasi jaringan aman

Tingkat keparahan: Kritis

Jenis sumber daya: `AWS::Lambda::Function`

AWS Config aturan: **`lambda-function-public-access-prohibited`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah kebijakan berbasis sumber daya fungsi Lambda melarang akses publik di luar akun Anda. Kontrol gagal jika akses publik diizinkan. Kontrol juga gagal jika fungsi Lambda dipanggil dari Amazon S3, dan kebijakan tidak menyertakan kondisi untuk membatasi akses publik, seperti. `AWS:SourceAccount` Sebaiknya gunakan kondisi S3 lainnya beserta `AWS:SourceAccount` kebijakan bucket Anda untuk akses yang lebih disempurnakan.

Fungsi Lambda tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke kode fungsi Anda.

Remediasi

Untuk mengatasi masalah ini, Anda harus memperbarui kebijakan berbasis sumber daya fungsi Anda untuk menghapus izin atau menambahkan kondisi. `AWS:SourceAccount` Anda hanya dapat memperbarui kebijakan berbasis sumber daya dari Lambda API atau. AWS CLI

Untuk memulai, tinjau kebijakan berbasis sumber daya di konsol Lambda. Identifikasi pernyataan kebijakan yang memiliki nilai `Principal` bidang yang membuat kebijakan publik, seperti `"*"` atau`{ "AWS": "*" }`.

Anda tidak dapat mengedit kebijakan dari konsol. Untuk menghapus izin dari fungsi, jalankan `remove-permission`perintah dari file. AWS CLI

```
$ aws lambda remove-permission --function-name <function-name> --statement-
id <statement-id>
```

Ganti *<function-name>* dengan nama fungsi Lambda, dan *<statement-id>* dengan pernyataan ID (`Sid`) dari pernyataan yang ingin Anda hapus.

[Lambda.2] Fungsi Lambda harus menggunakan runtime yang didukung

Persyaratan terkait: NIST.800-53.R5 CA-9 (1), NIST.800-53.R5 CM-2, NIST.800-53.R5 SI-2, NIST.800-53.R5 SI-2 (2), NIST.800-53.R5 SI-2 (4), NIST.800-53.R5 SI-2 (5)

Kategori: Lindungi > Pengembangan aman

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::Lambda::Function`

AWS Config aturan: **`lambda-function-settings-check`**

Jenis jadwal: Perubahan dipicu

Parameter:

- `runtime`: `dotnet8, dotnet6, java21, java17, java11, java8.al2, nodejs20.x, nodejs18.x, nodejs16.x, python3.12, python3.11, python3.10, python3.9, python3.8, ruby3.3, ruby3.2` (tidak dapat disesuaikan)

Kontrol ini memeriksa apakah setelan runtime AWS Lambda fungsi cocok dengan nilai yang diharapkan yang ditetapkan untuk runtime yang didukung dalam setiap bahasa. Kontrol gagal jika fungsi Lambda tidak menggunakan runtime yang didukung, yang disebutkan sebelumnya di bawah parameter. Security Hub mengabaikan fungsi yang memiliki tipe paket. `Image`

Lambda runtime dibangun di sekitar kombinasi sistem operasi, bahasa pemrograman, dan pustaka perangkat lunak yang tunduk pada pemeliharaan dan pembaruan keamanan. Jika komponen runtime tidak lagi didukung untuk pembaruan keamanan, Lambda menghentikan runtime. Meskipun Anda tidak dapat membuat fungsi yang menggunakan runtime usang, fungsi ini masih tersedia untuk memproses peristiwa pemanggilan. Sebaiknya pastikan fungsi Lambda Anda terkini dan tidak

menggunakan lingkungan runtime yang tidak digunakan lagi. Untuk daftar runtime yang didukung, lihat runtime Lambda di AWS Lambda Panduan Pengembang.

Remediasi

Untuk informasi selengkapnya tentang runtime yang didukung dan jadwal penghentian, lihat kebijakan penghentian waktu proses di Panduan Pengembang.AWS Lambda Saat Anda memigrasikan runtime ke versi terbaru, ikuti sintaks dan panduan dari penerbit bahasa tersebut. Kami juga merekomendasikan menerapkan pembaruan runtime untuk membantu mengurangi risiko dampak pada beban kerja Anda jika terjadi ketidakcocokan versi runtime yang jarang terjadi.

[Lambda.3] Fungsi Lambda harus dalam VPC

Persyaratan terkait: PCI DSS v3.2.1/1.2.1, PCI DSS v3.2.1/1.3.1, PCI DSS v3.2.1/1.3.2, PCI DSS v3.2.1/1.3.4, Nist.800-53.r5 AC-21, Nist.800-53.r5 AC-3, Nist.800-53.r5 AC-3 (7), Nist.800-53.r5 00-53.r5 AC-4, Nist.800-53.r5 AC-4 (21), Nist.800-53.r5 AC-6, Nist.800-53.r5 SC-7, Nist.800-53.r5 SC-7 (11), Nist.800-53.r5 SC-7 (16), Nist.800-53.r5 SC-7 (20), NIST.800-53.R5 SC-7 (21), NIST.800-53.R5 SC-7 (3), NIST.800-53.R5 SC-7 (4), NIST.800-53.R5 SC-7 (9)

Kategori: Lindungi > Konfigurasi jaringan aman

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::Lambda::Function`

AWS Config aturan: **`lambda-inside-vpc`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah fungsi Lambda digunakan di cloud pribadi virtual (VPC). Kontrol gagal jika fungsi Lambda tidak diterapkan di VPC. Security Hub tidak mengevaluasi konfigurasi perutean subnet VPC untuk menentukan jangkauan publik. Anda mungkin melihat temuan yang gagal untuk sumber daya Lambda @Edge.

Menyebarkan sumber daya dalam VPC memperkuat keamanan dan kontrol atas konfigurasi jaringan. Penerapan tersebut juga menawarkan skalabilitas dan toleransi kesalahan yang tinggi di beberapa Availability Zone. Anda dapat menyesuaikan penerapan VPC untuk memenuhi beragam persyaratan aplikasi.

Remediasi

Untuk mengonfigurasi fungsi yang ada untuk terhubung ke subnet pribadi di VPC Anda, lihat Mengonfigurasi akses VPC di Panduan Pengembang.AWS Lambda Sebaiknya pilih setidaknya dua subnet pribadi untuk ketersediaan tinggi dan setidaknya satu grup keamanan yang memenuhi persyaratan konektivitas fungsi.

[Lambda.5] Fungsi VPC Lambda harus beroperasi di beberapa Availability Zone

Persyaratan terkait: Nist.800-53.r5 CP-10, Nist.800-53.R5 CP-6 (2), Nist.800-53.R5 SC-36, Nist.800-53.R5 SC-5 (2), Nist.800-53.r5 SI-13 (5)

Kategori: Pulihkan > Ketahanan > Ketersediaan tinggi

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::Lambda::Function`

AWS Config aturan: **`lambda-vpc-multi-az-check`**

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`availabilityZones`	Jumlah minimum Availability Zone	Enum	`2, 3, 4, 5, 6`	2

Kontrol ini memeriksa apakah AWS Lambda fungsi yang terhubung ke virtual private cloud (VPC) beroperasi setidaknya dalam jumlah Availability Zone (AZ) yang ditentukan. Kontrol gagal jika fungsi tidak beroperasi setidaknya dalam jumlah AZ yang ditentukan. Kecuali Anda memberikan nilai parameter khusus untuk jumlah minimum AZ, Security Hub menggunakan nilai default dua AZ.

Menyebarkan sumber daya di beberapa AZ adalah praktik AWS terbaik untuk memastikan ketersediaan tinggi dalam arsitektur Anda. Ketersediaan adalah pilar inti dalam kerahasiaan, integritas, dan model keamanan triad ketersediaan. Semua fungsi Lambda yang terhubung ke

VPC harus memiliki penerapan Multi-AZ untuk memastikan bahwa satu zona kegagalan tidak menyebabkan gangguan total operasi.

Remediasi

Jika Anda mengonfigurasi fungsi Anda untuk terhubung ke VPC di akun Anda, tentukan subnet di beberapa AZ untuk memastikan ketersediaan tinggi. Untuk petunjuk, lihat Mengonfigurasi akses VPC di Panduan AWS Lambda Pengembang.

Lambda secara otomatis menjalankan fungsi lain di beberapa AZ untuk memastikan bahwa itu tersedia untuk memproses peristiwa jika terjadi gangguan layanan dalam satu zona.

[Lambda.6] Fungsi Lambda harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::Lambda::Function`

AWS Config aturan: `tagged-lambda-function` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList	Daftar tag yang memenuhi AWS persyaratan	`No default value`

Kontrol ini memeriksa apakah suatu AWS Lambda fungsi memiliki tag dengan kunci tertentu yang ditentukan dalam parameter`requiredTagKeys`. Kontrol gagal jika fungsi tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan

gagal jika fungsi tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke fungsi Lambda, lihat Menggunakan tag pada fungsi Lambda di Panduan Pengembang.AWS Lambda

Kontrol Amazon Macie

Kontrol ini terkait dengan sumber daya Macie.

Kontrol ini mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[Macie.1] Amazon Macie harus diaktifkan

Persyaratan terkait: NIST.800-53.R5 CA-7, NIST.800-53.R5 CA-9 (1), Nist.800-53.R5 RA-5, Nist.800-53.R5 SA-8 (19), NIST.800-53.R5 SI-4

Kategori: Deteksi > Layanan deteksi

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::::Account`

AWS Config aturan: **`macie-status-check`**

Jenis jadwal: Periodik

Kontrol ini memeriksa apakah Amazon Macie diaktifkan untuk sebuah akun. Kontrol gagal jika Macie tidak diaktifkan untuk akun.

Amazon Macie menemukan data sensitif menggunakan pembelajaran mesin dan pencocokan pola, memberikan visibilitas ke risiko keamanan data, dan memungkinkan perlindungan otomatis terhadap risiko tersebut. Macie secara otomatis dan terus-menerus mengevaluasi bucket Amazon Simple Storage Service (Amazon S3) Anda untuk keamanan dan kontrol akses, serta menghasilkan temuan untuk memberi tahu Anda tentang potensi masalah terkait keamanan atau privasi data Amazon S3 Anda. Macie juga mengotomatiskan penemuan dan pelaporan data sensitif, seperti informasi identitas pribadi (PII), untuk memberi Anda pemahaman yang lebih baik tentang data yang Anda simpan di Amazon S3. Untuk mempelajari lebih lanjut, lihat Panduan Pengguna Amazon Macie.

Remediasi

Untuk mengaktifkan Macie, lihat Mengaktifkan Macie di Panduan Pengguna Amazon Macie.

[Macie.2] Penemuan data sensitif otomatis Macie harus diaktifkan

Persyaratan terkait: NIST.800-53.R5 CA-7, NIST.800-53.R5 CA-9 (1), Nist.800-53.R5 RA-5, Nist.800-53.R5 SA-8 (19), NIST.800-53.R5 SI-4

Kategori: Deteksi > Layanan deteksi

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::::Account`

AWS Config aturan: **`macie-auto-sensitive-data-discovery-check`**

Jenis jadwal: Periodik

Kontrol ini memeriksa apakah penemuan data sensitif otomatis diaktifkan untuk akun administrator Amazon Macie. Kontrol gagal jika penemuan data sensitif otomatis tidak diaktifkan untuk akun administrator Macie. Kontrol ini hanya berlaku untuk akun administrator.

Macie mengotomatiskan penemuan dan pelaporan data sensitif, seperti informasi identitas pribadi (PII), di bucket Amazon Simple Storage Service (Amazon S3). Dengan penemuan data sensitif otomatis, Macie terus mengevaluasi inventaris bucket Anda dan menggunakan teknik pengambilan sampel untuk mengidentifikasi dan memilih objek S3 yang representatif dari bucket Anda. Macie kemudian menganalisis objek yang dipilih, memeriksanya untuk data sensitif. Seiring kemajuan analisis, Macie memperbarui statistik, data inventaris, dan informasi lain yang diberikannya tentang data S3 Anda. Macie juga menghasilkan temuan untuk melaporkan data sensitif yang ditemukannya.

Remediasi

Untuk membuat dan mengonfigurasi tugas penemuan data sensitif otomatis untuk menganalisis objek di bucket S3, lihat Mengonfigurasi penemuan data sensitif otomatis untuk akun Anda di Panduan Pengguna Amazon Macie.

Kontrol MSK Amazon

Kontrol ini terkait dengan sumber daya Amazon Managed Streaming for Apache Kafka (Amazon MSK).

Kontrol ini mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[MSK.1] Cluster MSK harus dienkripsi saat transit di antara node broker

Persyaratan terkait: Nist.800-53.r5 AC-4, Nist.800-53.r5 SC-13, Nist.800-53.r5 SC-23, Nist.800-53.r5 SC-23 (3), Nist.800-53.r5 SC-7 (4), Nist.800-53.r5 SC-8, Nist.800-53.r5 R5 SC-8 (1), NIST.800-53.R5 SC-8 (2)

Kategori: Lindungi > Perlindungan Data > Enkripsi data-in-transit

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::MSK::Cluster`

AWS Config aturan: **`msk-in-cluster-node-require-tls`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah kluster MSK Amazon dienkripsi dalam perjalanan dengan HTTPS (TLS) di antara node broker cluster. Kontrol gagal jika komunikasi teks biasa diaktifkan untuk koneksi node broker cluster.

HTTPS menawarkan lapisan keamanan ekstra karena menggunakan TLS untuk memindahkan data dan dapat digunakan untuk membantu mencegah penyerang potensial menggunakan person-in-the-middle atau serangan serupa untuk menguping atau memanipulasi lalu lintas jaringan. Secara default, Amazon MSK mengenkripsi data dalam perjalanan dengan TLS. Namun, Anda dapat mengganti default ini pada saat Anda membuat cluster. Sebaiknya gunakan koneksi terenkripsi melalui HTTPS (TLS) untuk koneksi node broker.

Remediasi

Untuk memperbarui setelan enkripsi untuk kluster MSK, lihat Memperbarui setelan keamanan klaster di Panduan Pengembang Amazon Managed Streaming for Apache Kafka.

[MSK.2] Kluster MSK seharusnya telah meningkatkan pemantauan yang dikonfigurasi

Persyaratan terkait: NIST.800-53.R5 CA-7, NIST.800-53.R5 SI-2

Kategori: Deteksi > Layanan deteksi

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::MSK::Cluster`

AWS Config aturan: **`msk-enhanced-monitoring-enabled`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah klaster MSK Amazon telah meningkatkan pemantauan yang dikonfigurasi, yang ditentukan oleh tingkat pemantauan setidaknya`PER_TOPIC_PER_BROKER`. Kontrol gagal jika tingkat pemantauan untuk cluster diatur ke `DEFAULT` atau`PER_BROKER`.

Tingkat `PER_TOPIC_PER_BROKER` pemantauan memberikan wawasan yang lebih terperinci tentang kinerja klaster MSK Anda, dan juga menyediakan metrik yang terkait dengan pemanfaatan sumber daya, seperti penggunaan CPU dan memori. Ini membantu Anda mengidentifikasi kemacetan kinerja dan pola pemanfaatan sumber daya untuk masing-masing topik dan broker. Visibilitas ini, pada gilirannya, dapat mengoptimalkan kinerja broker Kafka Anda.

Remediasi

Untuk mengonfigurasi pemantauan yang disempurnakan untuk klaster MSK, selesaikan langkah-langkah berikut:

1. Buka konsol Amazon MSK di https://console.aws.amazon.com/msk/home?region=us-east-1#/home/.
2. Pada panel navigasi, silakan pilih Klaster. Kemudian, pilih cluster.
3. Untuk Tindakan, pilih Edit pemantauan.
4. Pilih opsi untuk pemantauan tingkat topik yang ditingkatkan.
5. Pilih Simpan perubahan.

Untuk informasi selengkapnya tentang tingkat pemantauan, lihat Memperbarui setelan keamanan klaster di Panduan Pengembang Amazon Managed Streaming for Apache Kafka.

Kontrol Amazon MQ

Kontrol ini terkait dengan sumber daya Amazon MQ.

Kontrol ini mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[MQ.2] Broker ActiveMQ harus mengalirkan log audit ke CloudWatch

Persyaratan terkait: Nist.800-53.r5 AU-2, Nist.800-53.R5 AU-3, Nist.800-53.R5 AU-12, Nist.800-53.R5 SI-4

Kategori: Identifikasi > Logging

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::AmazonMQ::Broker`

AWS Config aturan: **`mq-cloudwatch-audit-log-enabled`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah broker Amazon MQ ActiveMQ mengalirkan log audit ke Amazon Logs. CloudWatch Kontrol gagal jika broker tidak mengalirkan log audit ke CloudWatch Log.

Dengan menerbitkan log broker ActiveMQ CloudWatch ke Log, Anda dapat CloudWatch membuat alarm dan metrik yang meningkatkan visibilitas informasi terkait keamanan.

Remediasi

Untuk melakukan streaming log broker ActiveMQ CloudWatch ke Log, lihat Mengonfigurasi Amazon MQ untuk log ActiveMQ di Panduan Pengembang Amazon MQ.

[MQ.3] Broker Amazon MQ harus mengaktifkan peningkatan versi minor otomatis

Persyaratan terkait: NIST.800-53.R5 CM-3, NIST.800-53.R5 SI-2

Kategori: Identifikasi > Kerentanan, tambalan, dan manajemen versi

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::AmazonMQ::Broker`

AWS Config aturan: **`mq-auto-minor-version-upgrade-enabled`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah broker Amazon MQ mengaktifkan peningkatan versi minor otomatis. Kontrol gagal jika broker tidak mengaktifkan peningkatan versi minor otomatis.

Saat Amazon MQ merilis dan mendukung versi mesin broker baru, perubahannya kompatibel dengan aplikasi yang ada dan tidak menghentikan fungsionalitas yang ada. Pembaruan versi mesin broker otomatis melindungi Anda dari risiko keamanan, membantu memperbaiki bug, dan meningkatkan fungsionalitas.

> **Note**
>
> Ketika broker yang terkait dengan peningkatan versi minor otomatis berada di tambalan terbaru dan menjadi tidak didukung, Anda harus mengambil tindakan manual untuk meningkatkan.

Remediasi

Untuk mengaktifkan pemutakhiran versi minor otomatis untuk broker MQ, lihat Memutakhirkan versi mesin minor secara otomatis di Panduan Pengembang Amazon MQ.

[MQ.4] Broker Amazon MQ harus diberi tag

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::AmazonMQ::Broker`

AWS Config aturan: `tagged-amazonmq-broker` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList	Daftar tag yang memenuhi AWS persyaratan	`No default value`

Kontrol ini memeriksa apakah broker Amazon MQ memiliki tag dengan kunci spesifik yang ditentukan dalam parameter. `requiredTagKeys` Kontrol gagal jika broker tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika broker tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan

terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke broker Amazon MQ, lihat Menandai sumber daya di Panduan Pengembang Amazon MQ.

[MQ.5] Broker ActiveMQ harus menggunakan mode penerapan aktif/siaga

Persyaratan terkait: Nist.800-53.r5 CP-10, Nist.800-53.R5 CP-6 (2), Nist.800-53.R5 SC-36, Nist.800-53.R5 SC-5 (2), Nist.800-53.r5 SI-13 (5)

Kategori: Pulihkan > Ketahanan > Ketersediaan tinggi

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::AmazonMQ::Broker`

AWS Config aturan: **`mq-active-deployment-mode`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah mode penerapan untuk broker Amazon MQ ActiveMQ diatur ke aktif/siaga. Kontrol gagal jika broker instans tunggal (diaktifkan secara default) ditetapkan sebagai mode penerapan.

Penerapan aktif/siaga menyediakan ketersediaan tinggi untuk broker Amazon MQ ActiveMQ Anda di file. Wilayah AWS Mode penerapan aktif/siaga mencakup dua instance broker di dua Availability Zone yang berbeda, dikonfigurasi dalam pasangan redundan. Pialang ini berkomunikasi secara

serempak dengan aplikasi Anda, yang dapat mengurangi waktu henti dan kehilangan data jika terjadi kegagalan.

Remediasi

Untuk membuat broker ActiveMQ baru dengan mode penerapan aktif/siaga, lihat Membuat dan mengonfigurasi broker ActiveMQ di Panduan Pengembang Amazon MQ. Untuk mode Deployment, pilih Active/Standby broker. Anda tidak dapat mengubah mode penerapan untuk broker yang ada. Sebagai gantinya, Anda harus membuat broker baru dan menyalin pengaturan dari broker lama.

[MQ.6] Broker RabbitMQ harus menggunakan mode penerapan cluster

Persyaratan terkait: Nist.800-53.r5 CP-10, Nist.800-53.R5 CP-6 (2), Nist.800-53.R5 SC-36, Nist.800-53.R5 SC-5 (2), Nist.800-53.r5 SI-13 (5

Kategori: Pulihkan > Ketahanan > Ketersediaan tinggi

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::AmazonMQ::Broker`

AWS Config aturan: **`mq-rabbit-deployment-mode`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah mode penerapan untuk broker Amazon MQ RabbitMQ disetel ke penerapan cluster. Kontrol gagal jika broker instans tunggal (diaktifkan secara default) ditetapkan sebagai mode penerapan.

Penerapan cluster memberikan ketersediaan tinggi untuk broker Amazon MQ RabbitMQ Anda di file. Wilayah AWS Penyebaran cluster adalah pengelompokan logis dari tiga node broker RabbitMQ, masing-masing dengan volume Amazon Elastic Block Store (Amazon EBS) sendiri dan status bersama. Penyebaran cluster memastikan bahwa data direplikasi ke semua node di cluster, yang dapat mengurangi waktu henti dan hilangnya data jika terjadi kegagalan.

Remediasi

Untuk membuat broker RabbitMQ baru dengan mode penerapan cluster, lihat Membuat dan menghubungkan ke broker RabbitMQ di Panduan Pengembang Amazon MQ. Untuk mode Deployment, pilih Penerapan cluster. Anda tidak dapat mengubah mode penerapan untuk broker

yang ada. Sebagai gantinya, Anda harus membuat broker baru dan menyalin pengaturan dari broker lama.

Kontrol Amazon Neptunus

Kontrol ini terkait dengan sumber daya Neptunus.

Kontrol ini mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[Neptunus.1] Cluster DB Neptunus harus dienkripsi saat istirahat

Persyaratan terkait: Nist.800-53.r5 CA-9 (1), NIST.800-53.R5 CM-3 (6), Nist.800-53.r5 SC-13, Nist.800-53.r5 SC-28, Nist.800-53.r5 SC-28 (1), Nist.800-53.r5 SC-7 (10), Nist.800-53.r5 SC-7 (10), Nist.800-53.r5 SC-7 (10), Nist.800-53.r5 SC-7 (10), Nist.800-53.r5 SC-7 (10), Nist.800-53.r5 SC-7 (10), Nist.800-53.r5 SC-7 (10), ST.800-53.R5 SI-7 (6)

Kategori: Lindungi > Perlindungan Data > Enkripsi data-at-rest

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::RDS::DBCluster`

AWS Config aturan: **`neptune-cluster-encrypted`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah cluster DB Neptunus dienkripsi saat istirahat. Kontrol gagal jika cluster DB Neptunus tidak dienkripsi saat istirahat.

Data saat istirahat mengacu pada data apa pun yang disimpan dalam penyimpanan persisten dan tidak mudah menguap untuk durasi berapa pun. Enkripsi membantu Anda melindungi kerahasiaan data tersebut, mengurangi risiko bahwa pengguna yang tidak sah dapat mengaksesnya. Mengenkripsi kluster DB Neptunus Anda melindungi data dan metadata Anda dari akses yang tidak sah. Ini juga memenuhi persyaratan kepatuhan untuk data-at-rest enkripsi sistem file produksi.

Remediasi

Anda dapat mengaktifkan enkripsi saat istirahat saat Anda membuat cluster DB Neptunus. Anda tidak dapat mengubah pengaturan enkripsi setelah membuat cluster. Untuk informasi selengkapnya, lihat Mengenkripsi sumber daya Neptunus saat istirahat di Panduan Pengguna Neptunus.

[Neptune.2] Cluster DB Neptunus harus menerbitkan log audit ke Log CloudWatch

Persyaratan terkait: Nist.800-53.r5 AC-2 (4), Nist.800-53.r5 AC-4 (26), Nist.800-53.r5 AC-6 (9), Nist.800-53.r5 AU-10, Nist.800-53.r5 AU-12, Nist.800-53.r5 AU-2, Nist.800-53.r5 5 AU-3, NIST.800-53.R5 AU-6 (1), NIST.800-53.R5 AU-6 (3), NIST.800-53.R5 AU-6 (4), NIST.800-53.R5 AU-6 (5), NIST.800-53.R5 AU-9 (7), NIST.800-53.R5 CA-7, NIST.800-53.R5 SC-7 (9), NIST.800-53.R5 SI-20, NIST.800-53.R5 SI-3 (8), NIST.800-53.r5 SI-4 (20), Nist.800-53.r5 SI-4 (5), NIST.800-53.r5 5 SI-7 (8)

Kategori: Identifikasi > Logging

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::RDS::DBCluster`

AWS Config aturan: **`neptune-cluster-cloudwatch-log-export-enabled`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah klaster DB Neptunus menerbitkan log audit ke Amazon Logs. CloudWatch Kontrol gagal jika kluster DB Neptunus tidak mempublikasikan log audit ke Log. CloudWatch `EnableCloudWatchLogsExport`harus diatur ke`Audit`.

Amazon Neptunus dan CloudWatch Amazon terintegrasi sehingga Anda dapat mengumpulkan dan menganalisis metrik kinerja. Neptunus secara otomatis mengirimkan metrik CloudWatch ke dan juga mendukung Alarm. CloudWatch Log audit sangat dapat disesuaikan. Saat Anda mengaudit database, setiap operasi pada data dapat dipantau dan dicatat ke jejak audit, termasuk informasi tentang cluster database mana yang diakses dan bagaimana caranya. Sebaiknya kirim log ini CloudWatch untuk membantu Anda memantau kluster DB Neptunus Anda.

Remediasi

Untuk memublikasikan log audit Neptunus CloudWatch ke Log, lihat Menerbitkan log Neptunus ke Log CloudWatch Amazon di Panduan Pengguna Neptunus. Di bagian Log ekspor, pilih Audit.

[Neptune.3] Snapshot cluster Neptunus DB seharusnya tidak publik

Persyaratan terkait: Nist.800-53.r5 AC-21, Nist.800-53.r5 AC-3, Nist.800-53.r5 AC-3 (7), Nist.800-53.r5 AC-4, Nist.800-53.r5 AC-4 (21), Nist.800-53.r5 AC-6, Nist.800-53.r5 R5 SC-7,

Nist.800-53.r5 SC-7 (11), NIST.800-53.R5 SC-7 (16), Nist.800-53.r5 SC-7 (20), Nist.800-53.r5 SC-7 (21), Nist.800-53.r5 SC-7 (3), Nist.800-53.r5 5 SC-7 (4), NIST.800-53.R5 SC-7 (9)

Kategori: Lindungi > Konfigurasi jaringan aman > Sumber daya tidak dapat diakses publik

Tingkat keparahan: Kritis

Jenis sumber daya: `AWS::RDS::DBClusterSnapshot`

AWS Config aturan: **`neptune-cluster-snapshot-public-prohibited`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah snapshot cluster DB manual Neptunus bersifat publik. Kontrol gagal jika snapshot cluster DB manual Neptunus bersifat publik.

Snapshot manual cluster Neptunus DB tidak boleh dipublikasikan kecuali dimaksudkan. Jika Anda membagikan snapshot manual yang tidak terenkripsi sebagai publik, snapshot tersedia untuk semua. Akun AWS Cuplikan publik dapat mengakibatkan eksposur data yang tidak diinginkan.

Remediasi

Untuk menghapus akses publik untuk snapshot kluster DB manual Neptunus, lihat Berbagi snapshot cluster DB di Panduan Pengguna Neptunus.

[Neptunus.4] Cluster DB Neptunus harus mengaktifkan perlindungan penghapusan

Persyaratan terkait: Nist.800-53.r5 CA-9 (1), Nist.800-53.R5 CM-2, Nist.800-53.R5 CM-2 (2), Nist.800-53.r5 CM-3, Nist.800-53.r5 SC-5 (2)

Kategori: Lindungi > Perlindungan data > Perlindungan penghapusan data

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::RDS::DBCluster`

AWS Config aturan: **`neptune-cluster-deletion-protection-enabled`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah cluster DB Neptunus mengaktifkan perlindungan penghapusan. Kontrol gagal jika cluster DB Neptunus tidak mengaktifkan perlindungan penghapusan.

Mengaktifkan perlindungan penghapusan klaster menawarkan lapisan perlindungan tambahan terhadap penghapusan atau penghapusan database yang tidak disengaja oleh pengguna yang tidak sah. Cluster DB Neptunus tidak dapat dihapus saat perlindungan penghapusan diaktifkan. Anda harus menonaktifkan perlindungan penghapusan terlebih dahulu sebelum permintaan penghapusan berhasil.

Remediasi

Untuk mengaktifkan perlindungan penghapusan klaster DB Neptunus yang ada, lihat Memodifikasi cluster DB menggunakan konsol, CLI, dan API di Panduan Pengguna Amazon Aurora.

[Neptunus.5] Cluster DB Neptunus harus mengaktifkan cadangan otomatis

Persyaratan terkait: NIST.800-53.R5 SI-12

Kategori: Pulih> Ketahanan > Cadangan diaktifkan

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::RDS::DBCluster`

AWS Config aturan: **`neptune-cluster-backup-retention-check`**

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub	
`minimumBackupRetentionPeriod`	Periode retensi cadangan minimum dalam beberapa hari	Bilangan Bulat	7 untuk 35	7	

Kontrol ini memeriksa apakah cluster DB Neptunus telah mengaktifkan pencadangan otomatis, dan periode retensi cadangan lebih besar dari atau sama dengan kerangka waktu yang ditentukan. Kontrol gagal jika cadangan tidak diaktifkan untuk cluster DB Neptunus, atau jika periode retensi kurang dari kerangka waktu yang ditentukan. Kecuali Anda memberikan nilai parameter khusus untuk periode penyimpanan cadangan, Security Hub menggunakan nilai default 7 hari.

Pencadangan membantu Anda pulih lebih cepat dari insiden keamanan dan memperkuat ketahanan sistem Anda. Dengan mengotomatiskan cadangan untuk cluster DB Neptunus Anda, Anda akan dapat memulihkan sistem Anda ke titik waktu tertentu dan meminimalkan waktu henti dan kehilangan data.

Remediasi

Untuk mengaktifkan pencadangan otomatis dan menetapkan periode retensi cadangan untuk kluster DB Neptunus Anda, lihat Mengaktifkan pencadangan otomatis di Panduan Pengguna Amazon RDS. Untuk periode retensi Backup, pilih nilai yang lebih besar dari atau sama dengan 7.

[Neptune.6] Snapshot cluster Neptunus DB harus dienkripsi saat istirahat

Persyaratan terkait: Nist.800-53.r5 CA-9 (1), NIST.800-53.R5 CM-3 (6), Nist.800-53.r5 SC-13, Nist.800-53.r5 SC-28, Nist.800-53.r5 SC-28 (1), Nist.800-53.r5 SC-7 (10), Nist.800-53.r5 SC-7 (10), Nist.800-53.r5 SC-7 (10), Nist.800-53.r5 SC-7 (10), Nist.800-53.r5 SC-7 (10), Nist.800-53.r5 SC-7 (10), Nist.800-53.r5 SC-7 (10), ST.800-53.R5 SC-7 (18)

Kategori: Lindungi > Perlindungan Data > Enkripsi data-at-rest

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::RDS::DBClusterSnapshot`

AWS Config aturan: **`neptune-cluster-snapshot-encrypted`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah snapshot cluster Neptunus DB dienkripsi saat istirahat. Kontrol gagal jika cluster DB Neptunus tidak dienkripsi saat istirahat.

Data saat istirahat mengacu pada data apa pun yang disimpan dalam penyimpanan persisten dan tidak mudah menguap untuk durasi berapa pun. Enkripsi membantu Anda melindungi kerahasiaan

data tersebut, mengurangi risiko bahwa pengguna yang tidak sah mendapatkan akses ke sana. Data dalam snapshot cluster DB Neptunus harus dienkripsi saat istirahat untuk lapisan keamanan tambahan.

Remediasi

Anda tidak dapat mengenkripsi snapshot cluster Neptunus DB yang ada. Sebagai gantinya, Anda harus mengembalikan snapshot ke cluster DB baru dan mengaktifkan enkripsi pada cluster. Anda dapat membuat snapshot terenkripsi dari cluster terenkripsi. Untuk petunjuknya, lihat Memulihkan dari snapshot cluster DB dan Membuat snapshot cluster DB di Neptunus di Panduan Pengguna Neptunus.

[Neptunus.7] Cluster DB Neptunus harus mengaktifkan otentikasi basis data IAM

Persyaratan terkait: Nist.800-53.r5 AC-2 (1), Nist.800-53.r5 AC-3, Nist.800-53.r5 AC-3 (15), Nist.800-53.r5 AC-3 (7), Nist.800-53.r5 AC-6

Kategori: Lindungi > Manajemen akses aman > Otentikasi tanpa kata sandi

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::RDS::DBCluster`

AWS Config aturan: **`neptune-cluster-iam-database-authentication`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah cluster DB Neptunus memiliki otentikasi database IAM diaktifkan. Kontrol gagal jika otentikasi database IAM tidak diaktifkan untuk cluster DB Neptunus.

Autentikasi database IAM untuk kluster database Amazon Neptunus menghilangkan kebutuhan untuk menyimpan kredensyal pengguna dalam konfigurasi database karena otentikasi dikelola secara eksternal menggunakan IAM. Ketika autentikasi database IAM diaktifkan, setiap permintaan harus ditandatangani menggunakan AWS Signature Version 4.

Remediasi

Secara default, otentikasi database IAM dinonaktifkan saat Anda membuat cluster DB Neptunus. Untuk mengaktifkannya, lihat Mengaktifkan otentikasi database IAM di Neptunus di Panduan Pengguna Neptunus.

[Neptunus.8] Cluster DB Neptunus harus dikonfigurasi untuk menyalin tag ke snapshot

Persyaratan terkait: NIST.800-53.R5 CA-9 (1), Nist.800-53.R5 CM-2, Nist.800-53.R5 CM-2 (2)

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::RDS::DBCluster`

AWS Config aturan: **`neptune-cluster-copy-tags-to-snapshot-enabled`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah cluster DB Neptunus dikonfigurasi untuk menyalin semua tag ke snapshot saat snapshot dibuat. Kontrol gagal jika cluster DB Neptunus tidak dikonfigurasi untuk menyalin tag ke snapshot.

Identifikasi dan inventaris aset TI Anda adalah aspek penting dari tata kelola dan keamanan. Anda harus menandai snapshot dengan cara yang sama seperti cluster database Amazon RDS induknya. Menyalin tag memastikan bahwa metadata untuk snapshot DB cocok dengan cluster database induk, dan kebijakan akses untuk snapshot DB juga cocok dengan instans DB induk.

Remediasi

Untuk menyalin tag ke snapshot untuk cluster DB Neptunus, lihat Menyalin tag di Neptunus di Panduan Pengguna Neptunus.

[Neptunus.9] Cluster DB Neptunus harus digunakan di beberapa Availability Zone

Persyaratan terkait: Nist.800-53.r5 CP-10, Nist.800-53.R5 CP-6 (2), Nist.800-53.R5 SC-36, Nist.800-53.R5 SC-5 (2), Nist.800-53.r5 SI-13 (5)

Kategori: Pulihkan > Ketahanan > Ketersediaan tinggi

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::RDS::DBCluster`

AWS Config aturan: **`neptune-cluster-multi-az-enabled`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah kluster DB Amazon Neptunus memiliki instance baca-replika di beberapa Availability Zones (AZ). Kontrol gagal jika cluster digunakan hanya dalam satu AZ.

Jika AZ tidak tersedia dan selama peristiwa pemeliharaan rutin, replika baca berfungsi sebagai target failover untuk instance utama. Artinya, jika instans primer gagal, Neptune mempromosikan instans replika baca menjadi instans primer. Sebaliknya, jika klaster DB Anda tidak menyertakan instans replika baca, klaster DB Anda tetap tidak tersedia ketika instans primer gagal sampai telah dibuat ulang. Membuat ulang instans primer membutuhkan waktu lebih lama daripada mempromosikan replika baca. Untuk memastikan ketersediaan tinggi, sebaiknya Anda membuat satu atau lebih instance read-replica yang memiliki kelas instans DB yang sama dengan instans utama dan berada di AZ yang berbeda dari instance utama.

Remediasi

Untuk menerapkan cluster DB Neptunus di beberapa AZ, lihat Instance DB Read-replika di cluster DB Neptunus di Panduan Pengguna Neptunus.

AWS Network Firewall kontrol

Kontrol ini terkait dengan sumber daya Network Firewall.

Kontrol ini mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[NetworkFirewall.1] Firewall Firewall Jaringan harus digunakan di beberapa Availability Zone

Persyaratan terkait: Nist.800-53.r5 CP-10, Nist.800-53.R5 CP-6 (2), Nist.800-53.R5 SC-36, Nist.800-53.R5 SC-5 (2), Nist.800-53.r5 SI-13 (5)

Kategori: Pulihkan > Ketahanan > Ketersediaan tinggi

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::NetworkFirewall::Firewall`

AWS Config aturan: **`netfw-multi-az-enabled`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini mengevaluasi apakah firewall yang dikelola AWS Network Firewall digunakan di beberapa Availability Zones (AZ). Kontrol gagal jika firewall digunakan hanya dalam satu AZ.

AWS Infrastruktur global mencakup banyak Wilayah AWS. AZ secara fisik terpisah, lokasi terisolasi di setiap Wilayah yang dihubungkan oleh latensi rendah, throughput tinggi, dan jaringan yang sangat redundan. Dengan menerapkan firewall Network Firewall di beberapa AZ, Anda dapat menyeimbangkan dan mengalihkan lalu lintas di antara AZ, yang membantu Anda merancang solusi yang sangat tersedia.

Remediasi

Menyebarkan firewall Network Firewall di beberapa AZ

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, di bawah Network Firewall, pilih Firewall.
3. Pada halaman Firewall, pilih firewall yang ingin Anda edit.
4. Pada halaman detail firewall, pilih tab Detail Firewall.
5. Di bagian Kebijakan terkait dan VPC, pilih Edit
6. Untuk menambahkan AZ baru, pilih Add New Subnet. Pilih AZ dan subnet yang ingin Anda gunakan. Pastikan Anda memilih setidaknya dua AZ.
7. Pilih Simpan.

[NetworkFirewall.2] Pencatatan Firewall Jaringan harus diaktifkan

Persyaratan terkait: Nist.800-53.r5 AC-2 (12), Nist.800-53.r5 AC-2 (4), Nist.800-53.r5 AC-4 (26), Nist.800-53.r5 AC-6 (9), Nist.800-53.r5 AU-10, Nist.800-53.r5 AU-12, Nist.800-800-53.r5 AU-2, NIST.800-53.R5 AU-3, NIST.800-53.R5 AU-6 (3), Nist.800-53.r5 AU-6 (4), Nist.800-53.r5 AU-9 (7), Nist.800-53.r5 CA-7, Nist.800-53.r5 SC-7 (9), Nist.800-53.r5 SC-7 (9), Nist.800-53.r5 ST.800-53.R5 SI-3 (8), NIST.800-53.R5 SI-4, NIST.800-53.R5 SI-4 (20), NIST.800-53.R5 SI-7 (8)

Kategori: Identifikasi > Logging

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::NetworkFirewall::LoggingConfiguration`

AWS Config aturan: **`netfw-logging-enabled`**

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah logging diaktifkan untuk AWS Network Firewall firewall. Kontrol gagal jika logging tidak diaktifkan untuk setidaknya satu jenis log atau jika tujuan logging tidak ada.

Logging membantu Anda menjaga keandalan, ketersediaan, dan kinerja firewall Anda. Di Network Firewall, logging memberi Anda informasi rinci tentang lalu lintas jaringan, termasuk waktu mesin stateful menerima aliran paket, informasi rinci tentang aliran paket, dan tindakan aturan stateful yang diambil terhadap aliran paket.

Remediasi

Untuk mengaktifkan logging untuk firewall, lihat Memperbarui konfigurasi logging firewall di Panduan AWS Network Firewall Pengembang.

[NetworkFirewall.3] Kebijakan Network Firewall harus memiliki setidaknya satu kelompok aturan yang terkait

Persyaratan terkait: NIST.800-53.R5 CA-9 (1), NIST.800-53.R5 CM-2

Kategori: Lindungi > Konfigurasi Jaringan Aman

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::NetworkFirewall::FirewallPolicy`

AWS Config aturan: **`netfw-policy-rule-group-associated`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah kebijakan Network Firewall memiliki grup aturan stateful atau stateless yang terkait. Kontrol gagal jika kelompok aturan stateless atau stateful tidak ditugaskan.

Kebijakan firewall menentukan cara firewall Anda memantau dan menangani lalu lintas di Amazon Virtual Private Cloud (Amazon VPC). Konfigurasi kelompok aturan stateless dan stateful membantu memfilter paket dan arus lalu lintas, dan mendefinisikan penanganan lalu lintas default.

Remediasi

Untuk menambahkan grup aturan ke kebijakan Network Firewall, lihat Memperbarui kebijakan firewall di Panduan AWS Network Firewall Pengembang. Untuk informasi tentang membuat dan mengelola grup aturan, lihat Grup aturan di AWS Network Firewall.

[NetworkFirewall.4] Tindakan stateless default untuk kebijakan Network Firewall harus drop atau forward untuk paket penuh

Persyaratan terkait: NIST.800-53.R5 CA-9 (1), NIST.800-53.R5 CM-2

Kategori: Lindungi > Konfigurasi Jaringan Aman

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::NetworkFirewall::FirewallPolicy`

AWS Config aturan: **`netfw-policy-default-action-full-packets`**

Jenis jadwal: Perubahan dipicu

Parameter:

- `statelessDefaultActions: aws:drop,aws:forward_to_sfe`(tidak dapat disesuaikan)

Kontrol ini memeriksa apakah tindakan stateless default untuk paket penuh untuk kebijakan Network Firewall adalah drop atau forward. Kontrol lolos jika `Drop` atau `Forward` dipilih, dan gagal jika `Pass` dipilih.

Kebijakan firewall menentukan bagaimana firewall Anda memantau dan menangani lalu lintas di Amazon VPC. Anda mengonfigurasi grup aturan stateless dan stateful untuk memfilter paket dan arus lalu lintas. Default untuk `Pass` dapat memungkinkan lalu lintas yang tidak diinginkan.

Remediasi

Untuk mengubah kebijakan firewall, lihat Memperbarui kebijakan firewall di Panduan AWS Network Firewall Pengembang. Untuk tindakan default Stateless, pilih Edit. Kemudian, pilih Jatuhkan atau Teruskan ke grup aturan stateful sebagai Tindakan.

[NetworkFirewall.5] Tindakan stateless default untuk kebijakan Network Firewall harus drop atau forward untuk paket yang terfragmentasi

Persyaratan terkait: NIST.800-53.R5 CA-9 (1), NIST.800-53.R5 CM-2

Kategori: Lindungi > Konfigurasi Jaringan Aman

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::NetworkFirewall::FirewallPolicy`

AWS Config aturan: **`netfw-policy-default-action-fragment-packets`**

Jenis jadwal: Perubahan dipicu

Parameter:

- `statelessFragDefaultActions (Required) : aws:drop, aws:forward_to_sfe`(tidak dapat disesuaikan)

Kontrol ini memeriksa apakah tindakan stateless default untuk paket terfragmentasi untuk kebijakan Network Firewall adalah drop atau forward. Kontrol lolos jika `Drop` atau `Forward` dipilih, dan gagal jika `Pass` dipilih.

Kebijakan firewall menentukan bagaimana firewall Anda memantau dan menangani lalu lintas di Amazon VPC. Anda mengonfigurasi grup aturan stateless dan stateful untuk memfilter paket dan arus lalu lintas. Default untuk `Pass` dapat memungkinkan lalu lintas yang tidak diinginkan.

Remediasi

Untuk mengubah kebijakan firewall, lihat Memperbarui kebijakan firewall di Panduan AWS Network Firewall Pengembang. Untuk tindakan default Stateless, pilih Edit. Kemudian, pilih Jatuhkan atau Teruskan ke grup aturan stateful sebagai Tindakan.

[NetworkFirewall.6] Grup aturan Stateless Network Firewall tidak boleh kosong

Persyaratan terkait: Nist.800-53.r5 AC-4 (21), Nist.800-53.r5 SC-7, Nist.800-53.r5 SC-7 (11), Nist.800-53.r5 SC-7 (16), Nist.800-53.r5 SC-7 (21), Nist.800-53.r5 SC-7 (5)

Kategori: Lindungi > Konfigurasi Jaringan Aman

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::NetworkFirewall::RuleGroup`

AWS Config aturan: **`netfw-stateless-rule-group-not-empty`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah grup aturan stateless AWS Network Firewall berisi aturan. Kontrol gagal jika tidak ada aturan dalam kelompok aturan.

Grup aturan berisi aturan yang menentukan bagaimana firewall Anda memproses lalu lintas di VPC Anda. Grup aturan stateless kosong, ketika ada dalam kebijakan firewall, mungkin memberi kesan bahwa grup aturan akan memproses lalu lintas. Namun, ketika grup aturan stateless kosong, itu tidak memproses lalu lintas.

Remediasi

Untuk menambahkan aturan ke grup aturan Firewall Jaringan, lihat Memperbarui grup aturan stateful di Panduan AWS Network Firewall Pengembang. Pada halaman detail firewall, untuk grup aturan Stateless, pilih Edit untuk menambahkan aturan.

[NetworkFirewall.7] Firewall Firewall Jaringan harus diberi tag

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::NetworkFirewall::Firewall`

AWS Config aturan: `tagged-networkfirewall-firewall` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList	Daftar tag yang memenuhi AWS persyaratan	`No default value`

Kontrol ini memeriksa apakah AWS Network Firewall firewall memiliki tag dengan kunci spesifik yang ditentukan dalam parameter`requiredTagKeys`. Kontrol gagal jika firewall tidak memiliki kunci tag

atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika firewall tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke firewall Network Firewall, lihat Menandai AWS Network Firewall sumber daya di Panduan AWS Network Firewall Pengembang.

[NetworkFirewall.8] Kebijakan firewall Network Firewall harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::NetworkFirewall::FirewallPolicy`

AWS Config aturan: `tagged-networkfirewall-firewallpolicy` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList	Daftar tag yang memenuhi AWS persyaratan	`No default value`

Kontrol ini memeriksa apakah kebijakan AWS Network Firewall firewall memiliki tag dengan kunci spesifik yang ditentukan dalam parameter`requiredTagKeys`. Kontrol gagal jika kebijakan firewall tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika kebijakan firewall tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS

Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke kebijakan Network Firewall, lihat Menandai AWS Network Firewall sumber daya di Panduan AWS Network Firewall Pengembang.

[NetworkFirewall.9] Firewall Firewall Jaringan harus mengaktifkan perlindungan penghapusan

Persyaratan terkait: Nist.800-53.r5 CA-9 (1), Nist.800-53.R5 CM-2, Nist.800-53.R5 CM-2 (2), Nist.800-53.r5 CM-3, Nist.800-53.r5 SC-5 (2)

Kategori: Lindungi > Keamanan Jaringan

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::NetworkFirewall::Firewall`

AWS Config aturan: **`netfw-deletion-protection-enabled`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah AWS Network Firewall firewall memiliki perlindungan penghapusan yang diaktifkan. Kontrol gagal jika perlindungan penghapusan tidak diaktifkan untuk firewall.

AWS Network Firewall adalah firewall jaringan stateful, dikelola dan layanan deteksi intrusi yang memungkinkan Anda untuk memeriksa dan memfilter lalu lintas ke, dari, atau antara Virtual Private Clouds (VPC) Anda. Pengaturan perlindungan penghapusan melindungi terhadap penghapusan firewall yang tidak disengaja.

Remediasi

Untuk mengaktifkan proteksi penghapusan pada firewall Network Firewall yang ada, lihat Memperbarui firewall di Panduan AWS Network Firewall Pengembang. Untuk Ubah perlindungan, pilih Aktifkan. Anda juga dapat mengaktifkan perlindungan penghapusan dengan menjalankan UpdateFirewallDeleteProtectionAPI dan menyetel bidang ke. `DeleteProtection` `true`

Kontrol OpenSearch Layanan Amazon

Kontrol ini terkait dengan sumber daya OpenSearch Layanan.

Kontrol ini mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[Opensearch.1] OpenSearch domain harus mengaktifkan enkripsi saat istirahat

Persyaratan terkait: PCI DSS v3.2.1/1.2.1, PCI DSS v3.2.1/1.3.1, PCI DSS v3.2.1/1.3.4, PCI DSS v3.2.1/7.2.1, Nist.800-53.R5 CA-9 (1), Nist.800-53.r5 CM-3 (6), Nist.800-53.r5 SC-13, Nist.800-53.r5 SC-13, ST.800-53.R5 SC-28, NIST.800-53.R5 SC-28 (1), NIST.800-53.R5 SI-7 (6)

Kategori: Lindungi > Perlindungan Data > Enkripsi data-at-rest

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::OpenSearch::Domain`

AWS Config aturan: **`opensearch-encrypted-at-rest`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah OpenSearch domain memiliki encryption-at-rest konfigurasi yang diaktifkan. Pemeriksaan gagal jika enkripsi saat istirahat tidak diaktifkan.

Untuk lapisan keamanan tambahan untuk data sensitif, Anda harus mengonfigurasi domain OpenSearch Layanan Anda untuk dienkripsi saat istirahat. Saat Anda mengonfigurasi enkripsi data saat istirahat, AWS KMS menyimpan dan mengelola kunci enkripsi Anda. Untuk melakukan enkripsi, AWS KMS gunakan algoritma Advanced Encryption Standard dengan kunci 256-bit (AES-256).

Untuk mempelajari lebih lanjut tentang enkripsi OpenSearch Layanan saat istirahat, lihat Enkripsi data saat istirahat untuk OpenSearch Layanan Amazon di Panduan Pengembang OpenSearch Layanan Amazon.

Remediasi

Untuk mengaktifkan enkripsi saat istirahat untuk OpenSearch domain baru dan yang sudah ada, lihat Mengaktifkan enkripsi data saat istirahat di Panduan Pengembang OpenSearch Layanan Amazon.

[Opensearch.2] OpenSearch domain tidak boleh diakses publik

Persyaratan terkait: PCI DSS v3.2.1/1.2.1, PCI DSS v3.2.1/1.3.1, PCI DSS v3.2.1/1.3.2, PCI DSS v3.2.1/1.3.4, PCI DSS v3.2.1/1.3.6, Nist.800-53.R5 AC-21, Nist.800-53.r5 AC-3, Nist.800-53.r5 5 AC-3 (7), NIST.800-53.R5 AC-4, NIST.800-53.R5 AC-4 (21), Nist.800-53.r5 AC-6, Nist.800-53.r5 SC-7, Nist.800-53.r5 SC-7 (11), Nist.800-53.r5 SC-7 (16), Nist.800-53.r5 SC-7 (20), NIST.800-53.R5 SC-7 (21), Nist.800-53.r5 SC-7 (3), Nist.800-53.r5 SC-7 (4), Nist.800-53.r5 SC-7 (9)

Kategori: Lindungi > Konfigurasi jaringan aman> Sumber daya dalam VPC

Tingkat keparahan: Kritis

Jenis sumber daya: `AWS::OpenSearch::Domain`

AWS Config aturan: **`opensearch-in-vpc-only`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah OpenSearch domain berada dalam VPC. Itu tidak mengevaluasi konfigurasi perutean subnet VPC untuk menentukan akses publik.

Anda harus memastikan bahwa OpenSearch domain tidak dilampirkan ke subnet publik. Lihat Kebijakan berbasis sumber daya di Panduan Pengembang Layanan Amazon OpenSearch . Anda juga harus memastikan bahwa VPC Anda dikonfigurasi sesuai dengan praktik terbaik yang disarankan. Lihat Praktik terbaik keamanan untuk VPC Anda di Panduan Pengguna Amazon VPC.

OpenSearch domain yang digunakan dalam VPC dapat berkomunikasi dengan sumber daya VPC melalui AWS jaringan pribadi, tanpa perlu melintasi internet publik. Konfigurasi ini meningkatkan postur keamanan dengan membatasi akses ke data dalam perjalanan. VPC menyediakan sejumlah kontrol jaringan untuk mengamankan akses ke OpenSearch domain, termasuk ACL jaringan dan grup keamanan. Security Hub merekomendasikan agar Anda memigrasikan OpenSearch domain publik ke VPC untuk memanfaatkan kontrol ini.

Remediasi

Jika Anda membuat domain dengan titik akhir publik, Anda tidak dapat menempatkannya di dalam VPC nanti. Sebagai gantinya, Anda harus membuat domain baru dan memigrasi data Anda. Begitu juga sebaliknya. Jika Anda membuat domain dalam VPC, domain tersebut tidak dapat memiliki titik akhir publik. Sebagai gantinya, Anda harus membuat domain lain atau menonaktifkan kontrol ini.

Untuk petunjuknya, lihat Meluncurkan domain OpenSearch Layanan Amazon Anda dalam VPC di Panduan Pengembang Layanan OpenSearch Amazon.

[Opensearch.3] OpenSearch domain harus mengenkripsi data yang dikirim antar node

Persyaratan terkait: Nist.800-53.r5 AC-4, Nist.800-53.r5 SC-13, Nist.800-53.r5 SC-23, Nist.800-53.r5 SC-23 (3), Nist.800-53.r5 SC-7 (4), Nist.800-53.r5 SC-8, Nist.800-53.r5 R5 SC-8 (1), NIST.800-53.R5 SC-8 (2)

Kategori: Lindungi > Perlindungan Data > Enkripsi data-in-transit

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::OpenSearch::Domain`

AWS Config aturan: **`opensearch-node-to-node-encryption-check`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah OpenSearch domain telah mengaktifkan node-to-node enkripsi. Kontrol ini gagal jika node-to-node enkripsi dinonaktifkan pada domain.

HTTPS (TLS) dapat digunakan untuk membantu mencegah penyerang potensial menguping atau memanipulasi lalu lintas jaringan menggunakan atau serangan serupa. person-in-the-middle Hanya koneksi terenkripsi melalui HTTPS (TLS) yang diizinkan. Mengaktifkan node-to-node enkripsi untuk OpenSearch domain memastikan bahwa komunikasi intra-cluster dienkripsi dalam perjalanan.

Mungkin ada penalti kinerja yang terkait dengan konfigurasi ini. Anda harus mengetahui dan menguji trade-off kinerja sebelum mengaktifkan opsi ini.

Remediasi

Untuk mengaktifkan node-to-node enkripsi pada OpenSearch domain, lihat Mengaktifkan node-to-node enkripsi di Panduan Pengembang OpenSearch Layanan Amazon.

[Opensearch.4] login kesalahan OpenSearch domain ke Log harus diaktifkan CloudWatch

Persyaratan terkait: Nist.800-53.r5 AC-2 (4), Nist.800-53.r5 AC-4 (26), Nist.800-53.r5 AC-6 (9), Nist.800-53.r5 AU-10, Nist.800-53.r5 AU-12, Nist.800-53.r5 AU-2, Nist.800-53.r5 5 AU-3,

NIST.800-53.R5 AU-6 (3), NIST.800-53.R5 AU-6 (4), NIST.800-53.R5 CA-7, NIST.800-53.R5 SC-7 (9), NIST.800-53.R5 SI-4 (20), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-4 (20), nistST.800-53.R5 SI-7 (8)

Kategori: Identifikasi > Logging

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::OpenSearch::Domain`

AWS Config aturan: **`opensearch-logs-to-cloudwatch`**

Jenis jadwal: Perubahan dipicu

Parameter:

- `logtype = 'error'`(tidak dapat disesuaikan)

Kontrol ini memeriksa apakah OpenSearch domain dikonfigurasi untuk mengirim log kesalahan ke CloudWatch Log. Kontrol ini gagal jika error logging ke tidak CloudWatch diaktifkan untuk domain.

Anda harus mengaktifkan log kesalahan untuk OpenSearch domain dan mengirim log tersebut ke CloudWatch Log untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.

Remediasi

Untuk mengaktifkan penerbitan log, lihat Mengaktifkan penerbitan log (konsol) di Panduan Pengembang OpenSearch Layanan Amazon.

[Opensearch.5] OpenSearch domain harus mengaktifkan pencatatan audit

Persyaratan terkait: Nist.800-53.r5 AC-2 (4), Nist.800-53.r5 AC-4 (26), Nist.800-53.r5 AC-6 (9), Nist.800-53.r5 AU-10, Nist.800-53.r5 AU-12, Nist.800-53.r5 AU-2, Nist.800-53.r5 5 AU-3, NIST.800-53.R5 AU-6 (3), NIST.800-53.R5 AU-6 (4), NIST.800-53.R5 CA-7, NIST.800-53.R5 SC-7 (9), NIST.800-53.R5 SI-4 (20), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-4 (20), nistST.800-53.R5 SI-7 (8)

Kategori: Identifikasi > Logging

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::OpenSearch::Domain`

AWS Config aturan: **`opensearch-audit-logging-enabled`**

Jenis jadwal: Perubahan dipicu

Parameter:

- `cloudWatchLogsLogGroupArnList`(tidak dapat disesuaikan) - Security Hub tidak mengisi parameter ini. Daftar grup CloudWatch log Log yang dipisahkan koma yang harus dikonfigurasi untuk log audit.

Aturan ini adalah `NON_COMPLIANT` jika grup CloudWatch log Log OpenSearch domain tidak ditentukan dalam daftar parameter ini.

Kontrol ini memeriksa apakah OpenSearch domain telah mengaktifkan pencatatan audit. Kontrol ini gagal jika OpenSearch domain tidak mengaktifkan pencatatan audit.

Log audit sangat dapat disesuaikan. Mereka memungkinkan Anda melacak aktivitas pengguna di OpenSearch klaster Anda, termasuk keberhasilan dan kegagalan otentikasi, permintaan, perubahan indeksOpenSearch, dan kueri penelusuran yang masuk.

Remediasi

Untuk petunjuk cara mengaktifkan log audit, lihat Mengaktifkan log audit di Panduan Pengembang OpenSearch Layanan Amazon.

[Opensearch.6] OpenSearch domain harus memiliki setidaknya tiga node data

Persyaratan terkait: Nist.800-53.r5 CP-10, Nist.800-53.R5 CP-6 (2), Nist.800-53.R5 SC-36, Nist.800-53.R5 SC-5 (2), Nist.800-53.r5 SI-13 (5)

Kategori: Pulihkan > Ketahanan > Ketersediaan tinggi

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::OpenSearch::Domain`

AWS Config aturan: **`opensearch-data-node-fault-tolerance`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah OpenSearch domain dikonfigurasi dengan setidaknya tiga node data dan `zoneAwarenessEnabled` adalah`true`. Kontrol ini gagal untuk OpenSearch domain jika `instanceCount` kurang dari 3 atau `zoneAwarenessEnabled` kurang`false`.

OpenSearch Domain membutuhkan setidaknya tiga node data untuk ketersediaan tinggi dan toleransi kesalahan. Menyebarkan OpenSearch domain dengan setidaknya tiga node data memastikan operasi cluster jika node gagal.

Remediasi

Untuk memodifikasi jumlah node data dalam OpenSearch domain

1. Masuk ke AWS konsol dan buka konsol OpenSearch Layanan Amazon di https://console.aws.amazon.com/aos/.
2. Di bawah Domain saya, pilih nama domain yang akan diedit, dan pilih Edit.
3. Di bawah Data node mengatur Jumlah node ke angka yang lebih besar dari`3`. Jika Anda menerapkan ke tiga Availability Zone, setel nomor ke kelipatan tiga untuk memastikan distribusi yang sama di seluruh Availability Zone.
4. Pilih Kirim.

[Opensearch.7] OpenSearch domain harus mengaktifkan kontrol akses berbutir halus

Persyaratan terkait: Nist.800-53.r5 AC-2 (1), Nist.800-53.r5 AC-3, Nist.800-53.r5 AC-3 (15), Nist.800-53.r5 AC-3 (7), Nist.800-53.r5 AC-5, Nist.800-53.r5 AC-6

Kategori: Lindungi > Manajemen Akses Aman > Tindakan API sensitif dibatasi

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::OpenSearch::Domain`

AWS Config aturan: **`opensearch-access-control-enabled`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah OpenSearch domain memiliki kontrol akses berbutir halus yang diaktifkan. Kontrol gagal jika kontrol akses berbutir halus tidak diaktifkan. Kontrol akses berbutir halus membutuhkan OpenSearch parameter `advanced-security-options` yang akan diaktifkanupdate-domain-config.

Kontrol akses berbutir halus menawarkan cara tambahan untuk mengontrol akses ke data Anda di Layanan Amazon. OpenSearch

Remediasi

Untuk mengaktifkan kontrol akses berbutir halus, lihat Kontrol akses berbutir halus di OpenSearch Layanan Amazon di Panduan Pengembang Layanan Amazon. OpenSearch

[Opensearch.8] Koneksi ke OpenSearch domain harus dienkripsi menggunakan kebijakan keamanan TLS terbaru

Persyaratan terkait: Nist.800-53.r5 AC-17 (2), Nist.800-53.r5 AC-4, Nist.800-53.r5 IA-5 (1), Nist.800-53.r5 SC-12 (3), Nist.800-53.r5 SC-13, Nist.800-53.r5 SC-23, Nist.800-53.r5 SC-23, Nist.800-53.r5 00-53.r5 SC-23 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.R5 SC-8, Nist.800-53.r5 SC-8 (1), NIST.800-53.r5 SC-8 (2), NIST.800-53.r5 SI-7 (6)

Kategori: Lindungi > Perlindungan Data > Enkripsi data-in-transit

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::OpenSearch::Domain`

AWS Config aturan: **`opensearch-https-required`**

Jenis jadwal: Perubahan dipicu

Parameter:

- `tlsPolicies: Policy-Min-TLS-1-2-PFS-2023-10`(tidak dapat disesuaikan)

Kontrol ini memeriksa apakah titik akhir domain OpenSearch Layanan Amazon dikonfigurasi untuk menggunakan kebijakan keamanan TLS terbaru. Kontrol gagal jika titik akhir OpenSearch domain

tidak dikonfigurasi untuk menggunakan kebijakan terbaru yang didukung atau jika HTTPS tidak diaktifkan.

HTTPS (TLS) dapat digunakan untuk membantu mencegah penyerang potensial menggunakan person-in-the-middle atau serangan serupa untuk menguping atau memanipulasi lalu lintas jaringan. Hanya koneksi terenkripsi melalui HTTPS (TLS) yang diizinkan. Mengenkripsi data dalam perjalanan dapat memengaruhi kinerja. Anda harus menguji aplikasi Anda dengan fitur ini untuk memahami profil kinerja dan dampak TLS. TLS 1.2 menyediakan beberapa peningkatan keamanan dibandingkan versi TLS sebelumnya.

Remediasi

Untuk mengaktifkan enkripsi TLS, gunakan operasi UpdateDomainConfigAPI. Konfigurasikan DomainEndpointOptionsbidang untuk menentukan nilai untuk`TLSSecurityPolicy`. Untuk informasi selengkapnya, lihat ode-to-node enkripsi N di Panduan Pengembang OpenSearch Layanan Amazon.

[Opensearch.9] domain harus ditandai OpenSearch

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::OpenSearch::Domain`

AWS Config aturan: `tagged-opensearch-domain` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList	Daftar tag yang memenuhi AWS persyaratan	`No default value`

Kontrol ini memeriksa apakah domain OpenSearch Layanan Amazon memiliki tag dengan kunci tertentu yang ditentukan dalam parameter`requiredTagKeys`. Kontrol gagal jika domain tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika domain tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke domain OpenSearch Layanan, lihat Bekerja dengan tag di Panduan Pengembang OpenSearch Layanan Amazon.

[Opensearch.10] OpenSearch domain harus memiliki pembaruan perangkat lunak terbaru yang diinstal

Persyaratan terkait: NIST.800-53.R5 SI-2, NIST.800-53.R5 SI-2 (2), NIST.800-53.R5 SI-2 (4), Nist.800-53.R5 SI-2 (5)

Kategori: Identifikasi > Kerentanan, tambalan, dan manajemen versi

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::OpenSearch::Domain`

AWS Config aturan: **`opensearch-update-check`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah domain OpenSearch Layanan Amazon memiliki pembaruan perangkat lunak terbaru yang diinstal. Kontrol gagal jika pembaruan perangkat lunak tersedia tetapi tidak diinstal untuk domain.

OpenSearch Pembaruan perangkat lunak layanan menyediakan perbaikan, pembaruan, dan fitur platform terbaru yang tersedia untuk lingkungan. Menjaga up-to-date instalasi patch membantu menjaga keamanan dan ketersediaan domain. Jika tidak ada tindakan yang diambil pada pembaruan yang diperlukan, perangkat lunak layanan diperbarui secara otomatis (biasanya setelah 2 minggu). Kami merekomendasikan penjadwalan pembaruan selama waktu lalu lintas rendah ke domain untuk meminimalkan gangguan layanan.

Remediasi

Untuk menginstal pembaruan perangkat lunak untuk OpenSearch domain, lihat Memulai pembaruan di Panduan Pengembang OpenSearch Layanan Amazon.

[Opensearch.11] OpenSearch domain harus memiliki setidaknya tiga node primer khusus

Persyaratan terkait: Nist.800-53.r5 CP-10, Nist.800-53.r5 CP-2, Nist.800-53.R5 SC-5, Nist.800-53.r5 SC-36, Nist.800-53.r5 SI-13

Kategori: Pulihkan > Ketahanan > Ketersediaan tinggi

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::OpenSearch::Domain`

AWS Config aturan: **`opensearch-primary-node-fault-tolerance`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah domain OpenSearch Layanan Amazon dikonfigurasi dengan setidaknya tiga node utama khusus. Kontrol gagal jika domain memiliki kurang dari tiga node utama khusus.

OpenSearch Layanan menggunakan node primer khusus untuk meningkatkan stabilitas cluster. Node utama khusus melakukan tugas manajemen klaster, tetapi tidak menyimpan data atau menanggapi permintaan unggahan data. Kami menyarankan Anda menggunakan Multi-AZ dengan standby, yang menambahkan tiga node utama khusus untuk setiap domain produksi OpenSearch .

Remediasi

Untuk mengubah jumlah node utama untuk OpenSearch domain, lihat Membuat dan mengelola domain OpenSearch Layanan Amazon di Panduan Pengembang OpenSearch Layanan Amazon.

AWS Private Certificate Authority kontrol

Kontrol ini terkait dengan AWS Private CA sumber daya.

Kontrol ini mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[PCA.1] otoritas sertifikat AWS Private CA root harus dinonaktifkan

Persyaratan terkait: NIST.800-53.R5 CA-9 (1), NIST.800-53.R5 CM-2

Kategori: Lindungi > Konfigurasi jaringan aman

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::ACMPCA::CertificateAuthority`

AWS Config aturan: **`acm-pca-root-ca-disabled`**

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah AWS Private CA memiliki otoritas sertifikat root (CA) yang dinonaktifkan. Kontrol gagal jika root CA diaktifkan.

Dengan AWS Private CA, Anda dapat membuat hierarki CA yang mencakup CA root dan CA bawahan. Anda harus meminimalkan penggunaan CA root untuk tugas sehari-hari, terutama di lingkungan produksi. CA root hanya boleh digunakan untuk menerbitkan sertifikat untuk CA perantara. Hal ini memungkinkan CA akar disimpan dari bahaya sementara CA perantara melakukan tugas harian menerbitkan sertifikat entitas akhir.

Remediasi

Untuk menonaktifkan root CA, lihat Memperbarui status CA di Panduan AWS Private Certificate Authority Pengguna.

Kontrol Layanan Amazon Relational Database Service

Kontrol ini terkait dengan sumber daya Amazon RDS.

Kontrol ini mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[RDS.1] Snapshot RDS harus pribadi

Persyaratan terkait: PCI DSS v3.2.1/1.2.1, PCI DSS v3.2.1/1.3.1, PCI DSS v3.2.1/1.3.4, PCI DSS v3.2.1/1.3.6, PCI DSS v3.2.1/7.2.1, Nist.800-53.R5 AC-21, Nist.800-53.r5 AC-3, Nist.800-53.r5 5 AC-3 (7), NIST.800-53.R5 AC-4, NIST.800-53.R5 AC-4 (21), Nist.800-53.r5 AC-6, Nist.800-53.r5 SC-7, Nist.800-53.r5 SC-7 (11), Nist.800-53.r5 SC-7 (16), Nist.800-53.r5 SC-7 (20), NIST.800-53.R5 SC-7 (21), Nist.800-53.r5 SC-7 (3), Nist.800-53.r5 SC-7 (4), Nist.800-53.r5 SC-7 (9)

Kategori: Lindungi > Konfigurasi jaringan aman

Tingkat keparahan: Kritis

Jenis sumber daya:`AWS::RDS::DBClusterSnapshot`, `AWS::RDS::DBSnapshot`

AWS Config aturan: **`rds-snapshots-public-prohibited`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah snapshot Amazon RDS bersifat publik. Kontrol gagal jika snapshot RDS bersifat publik. Kontrol ini mengevaluasi instans RDS, instans Aurora DB, instans DB Neptune, dan cluster Amazon DocumentDB.

Snapshot RDS digunakan untuk mencadangkan data pada instans RDS Anda pada titik waktu tertentu. Mereka dapat digunakan untuk mengembalikan status instans RDS sebelumnya.

Snapshot RDS tidak boleh bersifat publik kecuali dimaksudkan. Jika Anda membagikan snapshot manual yang tidak terenkripsi sebagai publik, ini membuat snapshot tersedia untuk semua. Akun AWS Hal ini dapat mengakibatkan eksposur data yang tidak diinginkan dari instans RDS Anda.

Perhatikan bahwa jika konfigurasi diubah untuk mengizinkan akses publik, AWS Config aturan mungkin tidak dapat mendeteksi perubahan hingga 12 jam. Sampai AWS Config aturan mendeteksi perubahan, cek lolos meskipun konfigurasi melanggar aturan.

Untuk mempelajari lebih lanjut tentang berbagi snapshot DB, lihat Berbagi snapshot DB di Panduan Pengguna Amazon RDS.

Remediasi

Untuk menghapus akses publik dari snapshot RDS, lihat Berbagi snapshot di Panduan Pengguna Amazon RDS. Untuk visibilitas snapshot DB, kami memilih Private.

[RDS.2] Instans RDS DB harus melarang akses publik, sebagaimana ditentukan oleh urasi PubliclyAccessible AWS Config

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v3.0.0/2.3.3, PCI DSS v3.2.1/1.2.1, PCI DSS v3.2.1/1.3.1, PCI DSS v3.2.1/1.3.2, PCI DSS v3.2.1/1.3.4, PCI DSS v3.2.1/1.3.6, PCI DSS v3.2.1/7.2.1, Nist.800-53.R5 AC-4, Nist.800-53.r5 AC-4 (21), Nist.800-53.r5 SC-7, Nist.800-53.r5 SC-7 (11), Nist.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (21), Nist.800-53.r5 SC-7 (4), Nist.800-53.R5 SC-7 (5)

Kategori: Lindungi > Konfigurasi jaringan aman

Tingkat keparahan: Kritis

Jenis sumber daya: `AWS::RDS::DBInstance`

AWS Config aturan: **`rds-instance-public-access-check`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah instans Amazon RDS dapat diakses publik dengan mengevaluasi `PubliclyAccessible` bidang dalam item konfigurasi instans.

Instans Neptunus DB dan cluster Amazon DocumentDB tidak memiliki bendera dan tidak dapat dievaluasi. `PubliclyAccessible` Namun, kontrol ini masih dapat menghasilkan temuan untuk sumber daya ini. Anda dapat menekan temuan ini.

`PubliclyAccessible`Nilai dalam konfigurasi instans RDS menunjukkan apakah instans DB dapat diakses publik. Ketika instans DB dikonfigurasi dengan`PubliclyAccessible`, itu adalah instance yang menghadap Internet dengan nama DNS yang dapat diselesaikan secara publik, yang diselesaikan ke alamat IP publik. Ketika instans DB tidak dapat diakses publik, itu adalah instance internal dengan nama DNS yang menyelesaikan ke alamat IP pribadi.

Kecuali jika Anda bermaksud agar instans RDS Anda dapat diakses publik, instans RDS tidak boleh dikonfigurasi dengan nilai. `PubliclyAccessible` Melakukannya mungkin memungkinkan lalu lintas yang tidak perlu ke instance database Anda.

Remediasi

Untuk menghapus akses publik dari instans RDS DB, lihat Memodifikasi instans Amazon RDS DB di Panduan Pengguna Amazon RDS. Untuk akses Publik, pilih No.

[RDS.3] Instans RDS DB harus mengaktifkan enkripsi saat istirahat

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v3.0.0/2.3.1, Tolok Ukur Yayasan CIS v1.4.0/2.3.1, Nist.800-53.r5 CA-9 (1), Nist.800-53.r5 AWS CM-3 (6), Nist.800-53.r5 SC-13, Nist.800-53.r5 SC-28, Nist.800-53.r5 SC-28, Nist.800-53.r5 SC-28, Nist.800-53.r5 SC-28 -28 (1), NIST.800-53.R5 SC-7 (10), NIST.800-53.R5 SI-7 (6)

Kategori: Lindungi > Perlindungan Data > Enkripsi data-at-rest

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::RDS::DBInstance`

AWS Config aturan: **`rds-storage-encrypted`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah enkripsi penyimpanan diaktifkan untuk instans Amazon RDS DB Anda.

Kontrol ini ditujukan untuk instans RDS DB. Namun, itu juga dapat menghasilkan temuan untuk instans Aurora DB, instans DB Neptunus, dan cluster Amazon DocumentDB. Jika temuan ini tidak berguna, maka Anda bisa menekannya.

Untuk lapisan keamanan tambahan untuk data sensitif Anda dalam instans RDS DB, Anda harus mengonfigurasi instans RDS DB Anda untuk dienkripsi saat istirahat. Untuk mengenkripsi instans dan snapshot RDS DB Anda saat istirahat, aktifkan opsi enkripsi untuk instans RDS DB Anda. Data yang dienkripsi saat istirahat mencakup penyimpanan yang mendasari untuk instans DB, pencadangan otomatisnya, replika baca, dan snapshot.

Instans DB terenkripsi RDS menggunakan algoritme enkripsi AES-256 standar terbuka untuk mengenkripsi data Anda di server yang menghosting instans RDS DB Anda. Setelah data Anda dienkripsi, Amazon RDS menangani otentikasi akses dan dekripsi data Anda secara transparan dengan dampak minimal pada kinerja. Anda tidak perlu memodifikasi aplikasi klien database Anda untuk menggunakan enkripsi.

Enkripsi Amazon RDS saat ini tersedia untuk semua mesin database dan jenis penyimpanan. Enkripsi Amazon RDS tersedia untuk sebagian besar kelas instans DB. Untuk mempelajari tentang kelas instans DB yang tidak mendukung enkripsi Amazon RDS, lihat Mengenkripsi sumber daya Amazon RDS di Panduan Pengguna Amazon RDS.

Remediasi

Untuk informasi tentang mengenkripsi instans DB di Amazon RDS, lihat Mengenkripsi sumber daya Amazon RDS di Panduan Pengguna Amazon RDS.

[RDS.4] Snapshot cluster RDS dan snapshot database harus dienkripsi saat istirahat

Persyaratan terkait: Nist.800-53.r5 CA-9 (1), NIST.800-53.R5 CM-3 (6), Nist.800-53.r5 SC-13, Nist.800-53.r5 SC-28, Nist.800-53.r5 SC-28 (1), Nist.800-53.r5 SC-7 (10), Nist.800-53.r5 SC-7 (10), Nist.800-53.r5 SC-7 (10), Nist.800-53.r5 SC-7 (10), Nist.800-53.r5 SC-7 (10), Nist.800-53.r5 SC-7 (10), Nist.800-53.r5 SC-7 (10), ST.800-53.R5 SI-7 (6)

Kategori: Lindungi > Perlindungan Data > Enkripsi data-at-rest

Tingkat keparahan: Sedang

Jenis sumber daya:`AWS::RDS::DBClusterSnapshot`, `AWS::RDS::DBSnapshot`

AWS Config aturan: **`rds-snapshot-encrypted`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah snapshot RDS DB dienkripsi. Kontrol gagal jika snapshot RDS DB tidak dienkripsi.

Kontrol ini ditujukan untuk instans RDS DB. Namun, ini juga dapat menghasilkan temuan untuk snapshot instans Aurora DB, instans DB Neptune, dan cluster Amazon DocumentDB. Jika temuan ini tidak berguna, maka Anda bisa menekannya.

Mengenkripsi data saat istirahat mengurangi risiko bahwa pengguna yang tidak diautentikasi mendapatkan akses ke data yang disimpan pada disk. Data dalam snapshot RDS harus dienkripsi saat istirahat untuk lapisan keamanan tambahan.

Remediasi

Untuk mengenkripsi snapshot RDS, lihat Mengenkripsi sumber daya Amazon RDS di Panduan Pengguna Amazon RDS. Saat Anda mengenkripsi instans RDS DB, data terenkripsi mencakup penyimpanan yang mendasari untuk instance, pencadangan otomatisnya, replika baca, dan snapshot.

Anda hanya dapat mengenkripsi instans RDS DB saat Anda membuatnya, bukan setelah instans DB dibuat. Namun, karena Anda dapat mengenkripsi salinan snapshot yang tidak dienkripsi, Anda dapat menambahkan enkripsi secara efektif ke instans DB yang tidak terenkripsi. Artinya, Anda dapat membuat snapshot instans DB, lalu membuat salinan terenkripsi dari snapshot tersebut. Anda kemudian dapat memulihkan instans DB dari snapshot terenkripsi untuk menghasilkan salinan terenkripsi dari instans DB asli.

[RDS.5] Instans RDS DB harus dikonfigurasi dengan beberapa Availability Zone

Persyaratan terkait: Nist.800-53.r5 CP-10, Nist.800-53.R5 CP-6 (2), Nist.800-53.R5 SC-36, Nist.800-53.R5 SC-5 (2), Nist.800-53.r5 SI-13 (5)

Kategori: Pulihkan > Ketahanan > Ketersediaan tinggi

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::RDS::DBInstance`

AWS Config aturan: **`rds-multi-az-support`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah ketersediaan tinggi diaktifkan untuk instans RDS DB Anda.

Instans RDS DB harus dikonfigurasi untuk beberapa Availability Zones (AZ). Ini memastikan ketersediaan data yang disimpan. Penerapan multi-AZ memungkinkan failover otomatis jika ada masalah dengan ketersediaan AZ dan selama pemeliharaan RDS reguler.

Remediasi

Untuk menerapkan instans DB Anda di beberapa AZ, Memodifikasi instans DB menjadi penerapan instans DB multi-AZ di Panduan Pengguna Amazon RDS.

[RDS.6] Pemantauan yang ditingkatkan harus dikonfigurasi untuk instans RDS DB

Persyaratan terkait: NIST.800-53.R5 CA-7, NIST.800-53.R5 SI-2

Kategori: Deteksi > Layanan deteksi

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::RDS::DBInstance`

AWS Config aturan: **`rds-enhanced-monitoring-enabled`**

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub	
`monitoringInterval`	Jumlah detik antara pemantauan interval pengumpulan metrik	Enum	`1`, `5`, `10`, `15`, `30`, `60`	Tidak ada nilai default	

Kontrol ini memeriksa apakah pemantauan yang disempurnakan diaktifkan untuk instans DB Amazon Relational Database Service (Amazon RDS). Kontrol gagal jika pemantauan yang ditingkatkan tidak diaktifkan untuk instance. Jika Anda memberikan nilai khusus untuk `monitoringInterval`

parameter, kontrol hanya akan diteruskan jika metrik pemantauan yang disempurnakan dikumpulkan untuk instance pada interval yang ditentukan.

Di Amazon RDS, Enhanced Monitoring memungkinkan respons yang lebih cepat terhadap perubahan kinerja di infrastruktur yang mendasarinya. Perubahan kinerja ini dapat mengakibatkan kurangnya ketersediaan data. Enhanced Monitoring menyediakan metrik real-time dari sistem operasi yang dijalankan instans RDS DB Anda. Agen diinstal pada instance. Agen dapat memperoleh metrik lebih akurat daripada yang mungkin dari lapisan hypervisor.

Metrik Pemantauan Ditingkatkan berguna ketika Anda ingin melihat bagaimana proses atau thread yang berbeda pada instans DB menggunakan CPU. Untuk informasi selengkapnya, lihat Pemantauan yang Ditingkatkan di Panduan Pengguna Amazon RDS.

Remediasi

Untuk petunjuk mendetail tentang mengaktifkan Pemantauan yang Ditingkatkan untuk instans DB Anda, lihat Menyiapkan dan mengaktifkan Pemantauan yang Ditingkatkan di Panduan Pengguna Amazon RDS.

[RDS.7] Cluster RDS harus mengaktifkan perlindungan penghapusan

Persyaratan terkait: Nist.800-53.r5 CM-3, Nist.800-53.R5 SC-5 (2)

Kategori: Lindungi > Perlindungan data > Perlindungan penghapusan data

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::RDS::DBCluster`

AWS Config aturan: **`rds-cluster-deletion-protection-enabled`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah klaster RDS DB memiliki perlindungan penghapusan yang diaktifkan. Kontrol gagal jika klaster RDS DB tidak mengaktifkan perlindungan penghapusan.

Kontrol ini ditujukan untuk instans RDS DB. Namun, itu juga dapat menghasilkan temuan untuk instans Aurora DB, instans DB Neptunus, dan cluster Amazon DocumentDB. Jika temuan ini tidak berguna, maka Anda bisa menekannya.

Mengaktifkan perlindungan penghapusan klaster adalah lapisan perlindungan tambahan terhadap penghapusan atau penghapusan database yang tidak disengaja oleh entitas yang tidak sah.

Ketika perlindungan penghapusan diaktifkan, klaster RDS tidak dapat dihapus. Sebelum permintaan penghapusan berhasil, perlindungan penghapusan harus dinonaktifkan.

Remediasi

Untuk mengaktifkan perlindungan penghapusan klaster RDS DB, lihat Memodifikasi cluster DB menggunakan konsol, CLI, dan API di Panduan Pengguna Amazon RDS. Untuk perlindungan penghapusan, pilih Aktifkan perlindungan penghapusan.

[RDS.8] Instans RDS DB harus mengaktifkan perlindungan penghapusan

Persyaratan terkait: NIST.800-53.R5 CM-3, NIST.800-53.R5 SC-5 (2), Nist.800-53.R5 SI-13 (5)

Kategori: Lindungi > Perlindungan data > Perlindungan penghapusan data

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::RDS::DBInstance`

AWS Config aturan: **`rds-instance-deletion-protection-enabled`**

Jenis jadwal: Perubahan dipicu

Parameter:

- `databaseEngines`: `mariadb,mysql,custom-oracle-ee,oracle-ee-cdb,oracle-se2-cdb,oracle-ee,oracle-se2,oracle-se1,oracle-se,postgres,sqlserver-ee,sqlserver-se,sqlserver-ex,sqlserver-web` (tidak dapat disesuaikan)

Kontrol ini memeriksa apakah instans RDS DB Anda yang menggunakan salah satu mesin database yang terdaftar memiliki perlindungan penghapusan diaktifkan. Kontrol gagal jika instans RDS DB tidak mengaktifkan perlindungan penghapusan.

Mengaktifkan perlindungan penghapusan instance adalah lapisan perlindungan tambahan terhadap penghapusan atau penghapusan database yang tidak disengaja oleh entitas yang tidak sah.

Sementara perlindungan penghapusan diaktifkan, instans RDS DB tidak dapat dihapus. Sebelum permintaan penghapusan berhasil, perlindungan penghapusan harus dinonaktifkan.

Remediasi

Untuk mengaktifkan perlindungan penghapusan instans RDS DB, lihat Memodifikasi instans Amazon RDS DB di Panduan Pengguna Amazon RDS. Untuk perlindungan penghapusan, pilih Aktifkan perlindungan penghapusan.

[RDS.9] Instans RDS DB harus menerbitkan log ke Log CloudWatch

Persyaratan terkait: Nist.800-53.r5 AC-2 (4), Nist.800-53.r5 AC-4 (26), Nist.800-53.r5 AC-6 (9), Nist.800-53.r5 AU-10, Nist.800-53.r5 AU-12, Nist.800-53.r5 AU-2, Nist.800-53.r5 5 AU-3, NIST.800-53.R5 AU-6 (3), NIST.800-53.R5 AU-6 (4), NIST.800-53.R5 CA-7, NIST.800-53.R5 SC-7 (8), NIST.800-53.R5 SI-3 (8), NIST.800-53.R5 SI-4 (20), NIST.800-53.R5 SI-7 (8)

Kategori: Identifikasi > Logging

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::RDS::DBInstance`

AWS Config aturan: **`rds-logging-enabled`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah instans Amazon RDS DB dikonfigurasi untuk mempublikasikan log berikut ke Amazon CloudWatch Logs. Kontrol gagal jika instance tidak dikonfigurasi untuk mempublikasikan log berikut ke CloudWatch Log:

- Oracle: (Peringatan, Audit, Jejak, Pendengar)
- PostgreSQL: (Postgresql, Upgrade)
- MySQL: (Audit, Kesalahan, Umum,) SlowQuery
- MariaDB: (Audit, Kesalahan, Umum,) SlowQuery
- SQL Server: (Kesalahan, Agen)
- Aurora: (Audit, Kesalahan, Umum,) SlowQuery
- Aurora-MySQL: (Audit, Kesalahan, Umum,) SlowQuery
- Aurora-PostgreSQL: (Postgresql, Tingkatkan).

Database RDS harus mengaktifkan log yang relevan. Database logging menyediakan catatan rinci permintaan yang dibuat untuk RDS. Log database dapat membantu audit keamanan dan akses dan dapat membantu mendiagnosis masalah ketersediaan.

Remediasi

Untuk memublikasikan log database RDS ke CloudWatch Log, lihat Menentukan log yang akan dipublikasikan ke CloudWatch Log di Panduan Pengguna Amazon RDS.

[RDS.10] Otentikasi IAM harus dikonfigurasi untuk instance RDS

Persyaratan terkait: Nist.800-53.r5 AC-2 (1), Nist.800-53.r5 AC-3, Nist.800-53.r5 AC-3 (15), Nist.800-53.r5 AC-3 (7), Nist.800-53.r5 AC-6

Kategori: Lindungi > Manajemen akses aman > Otentikasi tanpa kata sandi

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::RDS::DBInstance`

AWS Config aturan: **`rds-instance-iam-authentication-enabled`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah instans RDS DB memiliki otentikasi database IAM diaktifkan. Kontrol gagal jika otentikasi IAM tidak dikonfigurasi untuk instans RDS DB. Kontrol ini hanya mengevaluasi instans RDS dengan jenis mesin berikut:`mysql`,,,, `postgres` `auroraaurora-mysql`, `aurora-postgresql` dan. `mariadb` Instance RDS juga harus berada di salah satu status berikut untuk menghasilkan temuan:`available`,, `backing-upstorage-optimization`, atau`storage-full`.

Autentikasi basis data IAM memungkinkan otentikasi ke instance database dengan token otentikasi, bukan kata sandi. Lalu lintas jaringan ke dan dari database dienkripsi menggunakan SSL. Untuk informasi selengkapnya, lihat autentikasi database IAM di Panduan Pengguna Amazon Aurora.

Remediasi

Untuk mengaktifkan autentikasi database IAM pada instans RDS DB, lihat Mengaktifkan dan menonaktifkan autentikasi database IAM di Panduan Pengguna Amazon RDS.

[RDS.11] Instans RDS harus mengaktifkan pencadangan otomatis

Persyaratan terkait: Nist.800-53.r5 CP-10, Nist.800-53.r5 CP-6, Nist.800-53.R5 CP-6 (1), Nist.800-53.r5 CP-6 (2), Nist.800-53.r5 CP-9, Nist.800-53.r5 SC-5 (2), Nist.800-53.r5 SC-5 (2), Nist.800-53.r5 00-53.R5 SI-12, NIST.800-53.R5 SI-13 (5)

Kategori: Pulih> Ketahanan > Cadangan diaktifkan

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::RDS::DBInstance`

AWS Config aturan: **`db-instance-backup-enabled`**

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub	
`backupRetentionMinimum`	Periode retensi cadangan minimum dalam beberapa hari	Bilangan Bulat	7 untuk 35	7	
`checkReadReplicas`	Memeriksa apakah instans RDS DB memiliki cadangan yang diaktifkan untuk replika baca	Boolean	Tidak dapat disesuaikan	`false`	

Kontrol ini memeriksa apakah instans Amazon Relational Database Service telah mengaktifkan pencadangan otomatis, dan periode retensi cadangan yang lebih besar dari atau sama dengan kerangka waktu yang ditentukan. Replika baca dikecualikan dari evaluasi. Kontrol gagal jika cadangan tidak diaktifkan untuk instance, atau jika periode retensi kurang dari kerangka waktu yang ditentukan. Kecuali Anda memberikan nilai parameter khusus untuk periode penyimpanan cadangan, Security Hub menggunakan nilai default 7 hari.

Pencadangan membantu Anda pulih lebih cepat dari insiden keamanan dan memperkuat ketahanan sistem Anda. Amazon RDS memungkinkan Anda mengonfigurasi snapshot volume instans penuh harian. Untuk informasi selengkapnya tentang pencadangan otomatis Amazon RDS, lihat Bekerja dengan Pencadangan di Panduan Pengguna Amazon RDS.

Remediasi

Untuk mengaktifkan pencadangan otomatis pada instans RDS DB, lihat Mengaktifkan pencadangan otomatis di Panduan Pengguna Amazon RDS.

[RDS.12] Otentikasi IAM harus dikonfigurasi untuk cluster RDS

Persyaratan terkait: Nist.800-53.r5 AC-2 (1), Nist.800-53.r5 AC-3, Nist.800-53.r5 AC-3 (15), Nist.800-53.r5 AC-3 (7), Nist.800-53.r5 AC-6

Kategori: Lindungi > Manajemen akses aman > Otentikasi tanpa kata sandi

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::RDS::DBCluster`

AWS Config aturan: **`rds-cluster-iam-authentication-enabled`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah kluster Amazon RDS DB memiliki otentikasi database IAM yang diaktifkan.

Autentikasi basis data IAM memungkinkan otentikasi bebas kata sandi ke instance database. Otentikasi menggunakan token otentikasi. Lalu lintas jaringan ke dan dari database dienkripsi menggunakan SSL. Untuk informasi selengkapnya, lihat autentikasi database IAM di Panduan Pengguna Amazon Aurora.

Remediasi

Untuk mengaktifkan autentikasi IAM untuk kluster DB, lihat Mengaktifkan dan menonaktifkan autentikasi database IAM di Panduan Pengguna Amazon Aurora.

[RDS.13] Peningkatan versi minor otomatis RDS harus diaktifkan

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v3.0.0/2.3.2, Nist.800-53.R5 SI-2, NIST.800-53.R5 SI-2 (2), Nist.800-53.R5 SI-2 (4), NIST.800-53.R5 SI-2 (5)

Kategori: Identifikasi > Kerentanan, tambalan, dan manajemen versi

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::RDS::DBInstance`

AWS Config aturan: **`rds-automatic-minor-version-upgrade-enabled`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah upgrade versi minor otomatis diaktifkan untuk instance database RDS.

Mengaktifkan upgrade versi minor otomatis memastikan bahwa pembaruan versi minor terbaru ke sistem manajemen basis data relasional (RDBMS) diinstal. Upgrade ini mungkin termasuk patch keamanan dan perbaikan bug. Tetap up to date dengan instalasi patch adalah langkah penting dalam mengamankan sistem.

Remediasi

Untuk mengaktifkan upgrade versi minor otomatis untuk instans DB yang ada, lihat Memodifikasi instans Amazon RDS DB di Panduan Pengguna Amazon RDS. Untuk upgrade versi minor otomatis, pilih Ya.

[RDS.14] Cluster Amazon Aurora seharusnya mengaktifkan backtracking

Persyaratan terkait: Nist.800-53.r5 CP-10, Nist.800-53.r5 CP-6, Nist.800-53.R5 CP-6 (1), Nist.800-53.r5 CP-6 (2), Nist.800-53.r5 CP-9, Nist.800-53.r5 SI-13 (5)

Kategori: Pulih> Ketahanan > Cadangan diaktifkan

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::RDS::DBCluster`

AWS Config aturan: **`aurora-mysql-backtracking-enabled`**

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub	
`BacktrackWindowInHours`	Jumlah jam untuk mundur cluster Aurora MySQL	Ganda	`0.1` untuk `72`	Tidak ada nilai default	

Kontrol ini memeriksa apakah klaster Amazon Aurora telah mengaktifkan backtracking. Kontrol gagal jika cluster tidak mengaktifkan backtracking. Jika Anda memberikan nilai kustom untuk `BacktrackWindowInHours` parameter, kontrol hanya akan diteruskan jika cluster mundur untuk jangka waktu yang ditentukan.

Cadangan membantu Anda pulih lebih cepat dari insiden keamanan. Mereka juga memperkuat ketahanan sistem Anda. Aurora backtracking mengurangi waktu untuk memulihkan database ke titik waktu. Hal ini tidak memerlukan database restore untuk melakukannya.

Remediasi

Untuk mengaktifkan backtracking Aurora, lihat Mengonfigurasi backtracking di Panduan Pengguna Amazon Aurora.

Perhatikan bahwa Anda tidak dapat mengaktifkan backtracking pada klaster yang ada. Sebagai gantinya, Anda dapat membuat klon yang mengaktifkan backtracking. Untuk informasi selengkapnya tentang batasan backtracking Aurora, lihat daftar batasan di Ikhtisar mundur.

[RDS.15] Cluster RDS DB harus dikonfigurasi untuk beberapa Availability Zone

Persyaratan terkait: Nist.800-53.r5 CP-10, Nist.800-53.R5 CP-6 (2), Nist.800-53.R5 SC-36, Nist.800-53.R5 SC-5 (2), Nist.800-53.r5 SI-13 (5)

Kategori: Pulihkan > Ketahanan > Ketersediaan tinggi

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::RDS::DBCluster`

AWS Config aturan: **`rds-cluster-multi-az-enabled`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah ketersediaan tinggi diaktifkan untuk kluster RDS DB Anda. Kontrol gagal jika klaster RDS DB tidak digunakan di beberapa Availability Zones (AZ).

Cluster RDS DB harus dikonfigurasi untuk beberapa AZ untuk memastikan ketersediaan data yang disimpan. Penerapan ke beberapa AZ memungkinkan failover otomatis jika terjadi masalah ketersediaan AZ dan selama acara pemeliharaan RDS reguler.

Remediasi

Untuk menerapkan cluster DB Anda di beberapa AZ, Memodifikasi instans DB menjadi penerapan instans DB multi-AZ di Panduan Pengguna Amazon RDS.

Langkah-langkah remediasi berbeda untuk database global Aurora. Untuk mengonfigurasi beberapa Availability Zone untuk database global Aurora, pilih cluster DB Anda. Kemudian, pilih Actions and Add reader, dan tentukan beberapa AZ. Untuk informasi selengkapnya, lihat Menambahkan Replika Aurora ke cluster DB di Panduan Pengguna Amazon Aurora.

[RDS.16] Cluster RDS DB harus dikonfigurasi untuk menyalin tag ke snapshot

Persyaratan terkait: NIST.800-53.R5 CA-9 (1), Nist.800-53.R5 CM-2, Nist.800-53.R5 CM-2 (2)

Kategori: Identifikasi > Persediaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::RDS::DBCluster`

AWS Config aturan: `rds-cluster-copy-tags-to-snapshots-enabled` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah cluster RDS DB dikonfigurasi untuk menyalin semua tag ke snapshot saat snapshot dibuat.

Identifikasi dan inventaris aset TI Anda adalah aspek penting dari tata kelola dan keamanan. Anda harus memiliki visibilitas semua cluster RDS DB Anda sehingga Anda dapat menilai postur keamanan

mereka dan mengambil tindakan pada area kelemahan potensial. Snapshot harus ditandai dengan cara yang sama seperti cluster database RDS induknya. Mengaktifkan pengaturan ini memastikan bahwa snapshot mewarisi tag cluster database induknya.

Remediasi

Untuk secara otomatis menyalin tag ke snapshot untuk klaster RDS DB, lihat Memodifikasi cluster DB menggunakan konsol, CLI, dan API di Panduan Pengguna Amazon Aurora. Pilih Salin tag ke snapshot.

[RDS.17] Instans RDS DB harus dikonfigurasi untuk menyalin tag ke snapshot

Persyaratan terkait: NIST.800-53.R5 CA-9 (1), Nist.800-53.R5 CM-2, Nist.800-53.R5 CM-2 (2)

Kategori: Identifikasi > Persediaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::RDS::DBInstance`

AWS Config aturan: `rds-instance-copy-tags-to-snapshots-enabled` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah instance RDS DB dikonfigurasi untuk menyalin semua tag ke snapshot saat snapshot dibuat.

Identifikasi dan inventaris aset TI Anda adalah aspek penting dari tata kelola dan keamanan. Anda harus memiliki visibilitas semua instans RDS DB Anda sehingga Anda dapat menilai postur keamanan mereka dan mengambil tindakan pada area kelemahan potensial. Snapshot harus diberi tag dengan cara yang sama seperti instance database RDS induknya. Mengaktifkan pengaturan ini memastikan bahwa snapshot mewarisi tag dari instance database induknya.

Remediasi

Untuk secara otomatis menyalin tag ke snapshot untuk instans RDS DB, lihat Memodifikasi instans Amazon RDS DB di Panduan Pengguna Amazon RDS. Pilih Salin tag ke snapshot.

[RDS.18] Instans RDS harus digunakan di VPC

Persyaratan terkait: Nist.800-53.r5 AC-21, Nist.800-53.r5 AC-3, Nist.800-53.r5 AC-3 (7), Nist.800-53.r5 AC-4, Nist.800-53.r5 AC-4 (21), Nist.800-53.r5 AC-6, Nist.800-53.r5 R5 SC-7, Nist.800-53.r5 SC-7 (11), NIST.800-53.R5 SC-7 (16), Nist.800-53.r5 SC-7 (20), Nist.800-53.r5 SC-7 (21), Nist.800-53.r5 SC-7 (3), Nist.800-53.r5 5 SC-7 (4), NIST.800-53.R5 SC-7 (9)

Kategori: Lindungi > Konfigurasi jaringan aman> Sumber daya dalam VPC

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::RDS::DBInstance`

AWS Config aturan: `rds-deployed-in-vpc` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah instans Amazon RDS diterapkan pada EC2-VPC.

VPC menyediakan sejumlah kontrol jaringan untuk mengamankan akses ke sumber daya RDS. Kontrol ini termasuk titik akhir VPC, ACL jaringan, dan grup keamanan. Untuk memanfaatkan kontrol ini, kami sarankan Anda membuat instans RDS di EC2-VPC.

Remediasi

Untuk petunjuk cara memindahkan instans RDS ke VPC, lihat Memperbarui VPC untuk instans DB di Panduan Pengguna Amazon RDS.

[RDS.19] Langganan pemberitahuan acara RDS yang ada harus dikonfigurasi untuk peristiwa klaster penting

Persyaratan terkait: NIST.800-53.R5 CA-7, NIST.800-53.R5 SI-2

Kategori: Deteksi > Layanan deteksi > Pemantauan aplikasi

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::RDS::EventSubscription`

AWS Config aturan: `rds-cluster-event-notifications-configured` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah langganan peristiwa Amazon RDS yang ada untuk kluster database telah mengaktifkan notifikasi untuk jenis sumber berikut dan pasangan nilai kunci kategori peristiwa:

```
DBCluster: ["maintenance","failure"]
```

Kontrol berlalu jika tidak ada langganan acara yang ada di akun Anda.

Pemberitahuan acara RDS menggunakan Amazon SNS untuk membuat Anda mengetahui perubahan ketersediaan atau konfigurasi sumber daya RDS Anda. Pemberitahuan ini memungkinkan respons cepat. Untuk informasi tambahan tentang pemberitahuan peristiwa RDS, lihat Menggunakan pemberitahuan peristiwa Amazon RDS di Panduan Pengguna Amazon RDS.

Remediasi

Untuk berlangganan notifikasi peristiwa klaster RDS, lihat Berlangganan pemberitahuan acara Amazon RDS di Panduan Pengguna Amazon RDS. Gunakan nilai berikut:

Bidang	Nilai
Jenis sumber	Klaster
Cluster untuk dimasukkan	Semua cluster
Kategori acara untuk disertakan	Pilih kategori acara tertentu atau Semua kategori acara

[RDS.20] Langganan pemberitahuan acara RDS yang ada harus dikonfigurasi untuk peristiwa instance basis data penting

Persyaratan terkait: NIST.800-53.R5 CA-7, NIST.800-53.R5 SI-2

Kategori: Deteksi > Layanan deteksi > Pemantauan aplikasi

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::RDS::EventSubscription`

AWS Config aturan: `rds-instance-event-notifications-configured` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah langganan peristiwa Amazon RDS yang ada untuk instans database telah mengaktifkan notifikasi untuk jenis sumber berikut dan pasangan nilai kunci kategori peristiwa:

```
DBInstance: ["maintenance","configuration change","failure"]
```

Kontrol berlalu jika tidak ada langganan acara yang ada di akun Anda.

Pemberitahuan peristiwa RDS menggunakan Amazon SNS untuk membuat Anda mengetahui perubahan ketersediaan atau konfigurasi sumber daya RDS Anda. Pemberitahuan ini memungkinkan respons cepat. Untuk informasi tambahan tentang pemberitahuan peristiwa RDS, lihat Menggunakan pemberitahuan peristiwa Amazon RDS di Panduan Pengguna Amazon RDS.

Remediasi

Untuk berlangganan notifikasi kejadian instans RDS, lihat Berlangganan notifikasi peristiwa Amazon RDS di Panduan Pengguna Amazon RDS. Gunakan nilai berikut:

Bidang	Nilai
Jenis sumber	Instans
Contoh untuk disertakan	Semua contoh
Kategori acara untuk disertakan	Pilih kategori acara tertentu atau Semua kategori acara

[RDS.21] Langganan pemberitahuan acara RDS harus dikonfigurasi untuk peristiwa grup parameter basis data penting

Persyaratan terkait: NIST.800-53.R5 CA-7, NIST.800-53.R5 SI-2

Kategori: Deteksi > Layanan deteksi > Pemantauan aplikasi

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::RDS::EventSubscription`

AWS Config aturan: `rds-pg-event-notifications-configured` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah langganan acara Amazon RDS ada dengan notifikasi diaktifkan untuk jenis sumber berikut, pasangan nilai kunci kategori peristiwa. Kontrol berlalu jika tidak ada langganan acara yang ada di akun Anda.

```
DBParameterGroup: ["configuration change"]
```

Pemberitahuan peristiwa RDS menggunakan Amazon SNS untuk membuat Anda mengetahui perubahan ketersediaan atau konfigurasi sumber daya RDS Anda. Pemberitahuan ini memungkinkan respons cepat. Untuk informasi tambahan tentang pemberitahuan peristiwa RDS, lihat Menggunakan pemberitahuan peristiwa Amazon RDS di Panduan Pengguna Amazon RDS.

Remediasi

Untuk berlangganan pemberitahuan peristiwa grup parameter database RDS, lihat Berlangganan pemberitahuan peristiwa Amazon RDS di Panduan Pengguna Amazon RDS. Gunakan nilai berikut:

Bidang	Nilai
Jenis sumber	Grup parameter
Kelompok parameter untuk disertakan	Semua kelompok parameter
Kategori acara untuk disertakan	Pilih kategori acara tertentu atau Semua kategori acara

[RDS.22] Langganan pemberitahuan acara RDS harus dikonfigurasi untuk acara grup keamanan basis data penting

Persyaratan terkait: NIST.800-53.R5 CA-7, NIST.800-53.R5 SI-2

Kategori: Deteksi > Layanan Deteksi > Pemantauan aplikasi

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::RDS::EventSubscription`

AWS Config aturan: `rds-sg-event-notifications-configured` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah langganan acara Amazon RDS ada dengan notifikasi diaktifkan untuk jenis sumber berikut, pasangan nilai kunci kategori peristiwa. Kontrol berlalu jika tidak ada langganan acara yang ada di akun Anda.

```
DBSecurityGroup: ["configuration change","failure"]
```

Pemberitahuan peristiwa RDS menggunakan Amazon SNS untuk membuat Anda mengetahui perubahan ketersediaan atau konfigurasi sumber daya RDS Anda. Pemberitahuan ini memungkinkan respons yang cepat. Untuk informasi tambahan tentang pemberitahuan peristiwa RDS, lihat Menggunakan pemberitahuan peristiwa Amazon RDS di Panduan Pengguna Amazon RDS.

Remediasi

Untuk berlangganan notifikasi kejadian instans RDS, lihat Berlangganan notifikasi peristiwa Amazon RDS di Panduan Pengguna Amazon RDS. Gunakan nilai berikut:

Bidang	Nilai
Jenis sumber	Grup keamanan
Kelompok keamanan untuk memasukkan	Semua kelompok keamanan
Kategori acara untuk disertakan	Pilih kategori acara tertentu atau Semua kategori acara

[RDS.23] Instans RDS tidak boleh menggunakan port default mesin database

Persyaratan terkait: Nist.800-53.r5 AC-4, NIST.800-53.R5 AC-4 (21), Nist.800-53.r5 SC-7, Nist.800-53.r5 SC-7 (11), Nist.800-53.r5 SC-7 (16), Nist.800-53.r5 SC-7 (21), Nist.800-53.r5 SC-7

(21), Nist.800-53.r5 SC-7 (21), Nist.800-53.r5 SC-7 (21), Nist.800-53.r5 SC-7 (21), Nist.800-53.r5 SC-7 (21), Nist.800-53.r5 SC-7 (21), ST.800-53.R5 SC-7 (4), NIST.800-53.R5 SC-7 (5)

Kategori: Lindungi > Konfigurasi jaringan aman

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::RDS::DBInstance`

AWS Config aturan: `rds-no-default-ports` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah cluster RDS atau instance menggunakan port selain port default mesin database. Kontrol gagal jika cluster atau instance RDS menggunakan port default.

Jika Anda menggunakan port yang dikenal untuk menyebarkan cluster atau instance RDS, penyerang dapat menebak informasi tentang cluster atau instance. Penyerang dapat menggunakan informasi ini bersama dengan informasi lain untuk terhubung ke cluster atau instance RDS atau mendapatkan informasi tambahan tentang aplikasi Anda.

Ketika Anda mengubah port, Anda juga harus memperbarui string koneksi yang ada yang digunakan untuk terhubung ke port lama. Anda juga harus memeriksa grup keamanan instans DB untuk memastikan bahwa itu termasuk aturan masuk yang memungkinkan konektivitas pada port baru.

Remediasi

Untuk mengubah port default instans RDS DB yang ada, lihat Memodifikasi instans Amazon RDS DB di Panduan Pengguna Amazon RDS. Untuk mengubah port default kluster RDS DB yang ada, lihat Memodifikasi cluster DB menggunakan konsol, CLI, dan API di Panduan Pengguna Amazon Aurora. Untuk port Database, ubah nilai port ke nilai non-default.

[RDS.24] Kluster Database RDS harus menggunakan nama pengguna administrator khusus

Persyaratan terkait: NIST.800-53.R5 CA-9 (1), NIST.800-53.R5 CM-2

Kategori: Identifikasi > Konfigurasi Sumber Daya

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::RDS::DBCluster`

AWS Config aturan: `rds-cluster-default-admin-check`

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah kluster database Amazon RDS telah mengubah nama pengguna admin dari nilai defaultnya. Kontrol tidak berlaku untuk mesin jenis neptunus (Neptunus DB) atau docdb (DocumentDB). Aturan ini akan gagal jika nama pengguna admin diatur ke nilai default.

Saat membuat database Amazon RDS, Anda harus mengubah nama pengguna admin default menjadi nilai unik. Nama pengguna default adalah pengetahuan publik dan harus diubah selama pembuatan database RDS. Mengubah nama pengguna default mengurangi risiko akses yang tidak diinginkan.

Remediasi

Untuk mengubah nama pengguna admin yang terkait dengan kluster database Amazon RDS, buat kluster database RDS baru dan ubah nama pengguna admin default saat membuat database.

[RDS.25] Instans database RDS harus menggunakan nama pengguna administrator khusus

Persyaratan terkait: NIST.800-53.R5 CA-9 (1), NIST.800-53.R5 CM-2

Kategori: Identifikasi > Konfigurasi Sumber Daya

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::RDS::DBInstance`

AWS Config aturan: `rds-instance-default-admin-check`

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah Anda telah mengubah nama pengguna administratif untuk instans database Amazon Relational Database Service (Amazon RDS) dari nilai default. Kontrol tidak berlaku

untuk mesin jenis neptunus (Neptunus DB) atau docdb (DocumentDB). Kontrol gagal jika nama pengguna administratif diatur ke nilai default.

Nama pengguna administratif default pada database Amazon RDS adalah pengetahuan publik. Saat membuat database Amazon RDS, Anda harus mengubah nama pengguna administratif default ke nilai unik untuk mengurangi risiko akses yang tidak diinginkan.

Remediasi

Untuk mengubah nama pengguna administratif yang terkait dengan instance database RDS, pertama buat instance database RDS baru. Ubah nama pengguna administratif default saat membuat database.

[RDS.26] Instans RDS DB harus dilindungi oleh rencana cadangan

Kategori: Pulih> Ketahanan > Cadangan diaktifkan

Persyaratan terkait: Nist.800-53.r5 CP-10, Nist.800-53.r5 CP-6, Nist.800-53.R5 CP-6 (1), Nist.800-53.r5 CP-6 (2), Nist.800-53.r5 CP-9, Nist.800-53.r5 SC-5 (2), Nist.800-53.r5 SC-5 (2), Nist.800-53.r5 00-53.R5 SI-12, NIST.800-53.R5 SI-13 (5)

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::RDS::DBInstance`

AWS Config aturan: **`rds-resources-protected-by-backup-plan`**

Jenis jadwal: Periodik

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub	
`backupVaultLockCheck`	Kontrol menghasilkan `PASSED` temuan jika parameter disetel ke true dan sumber daya	Boolean	`true` atau `false`	Tidak ada nilai default	

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub	
	menggunakan AWS Backup Vault Lock.				

Kontrol ini mengevaluasi jika instans Amazon RDS DB dicakup oleh paket cadangan. Kontrol ini gagal jika instans RDS DB tidak tercakup oleh rencana cadangan. Jika Anda menyetel `backupVaultLockCheck` parameter sama dengan`true`, kontrol hanya akan diteruskan jika instance dicadangkan di brankas yang AWS Backup terkunci.

AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya yang memusatkan dan mengotomatiskan pencadangan data di seluruh. Layanan AWS Dengan AWS Backup, Anda dapat membuat kebijakan cadangan yang disebut rencana cadangan. Anda dapat menggunakan paket ini untuk menentukan persyaratan pencadangan Anda, seperti seberapa sering mencadangkan data Anda dan berapa lama untuk menyimpan cadangan tersebut. Menyertakan instans RDS DB dalam paket cadangan membantu Anda melindungi data Anda dari kehilangan atau penghapusan yang tidak diinginkan.

Remediasi

Untuk menambahkan instans RDS DB ke paket AWS Backup cadangan, lihat Menetapkan sumber daya ke paket cadangan di Panduan AWS Backup Pengembang.

[RDS.27] Cluster RDS DB harus dienkripsi saat istirahat

Persyaratan terkait: Nist.800-53.r5 CA-9 (1), NIST.800-53.R5 CM-3 (6), Nist.800-53.r5 SC-13, Nist.800-53.r5 SC-28, Nist.800-53.r5 SC-28 (1), Nist.800-53.r5 SC-7 (10), Nist.800-53.r5 SC-7 (10), Nist.800-53.r5 SC-7 (10), Nist.800-53.r5 SC-7 (10), Nist.800-53.r5 SC-7 (10), Nist.800-53.r5 SC-7 (10), Nist.800-53.r5 SC-7 (10), ST.800-53.R5 SI-7 (6)

Kategori: Lindungi > Perlindungan Data > Enkripsi data-at-rest

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::RDS::DBCluster`

AWS Config aturan: **`rds-cluster-encrypted-at-rest`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah cluster RDS DB dienkripsi saat istirahat. Kontrol gagal jika cluster RDS DB tidak dienkripsi saat istirahat.

Data saat istirahat mengacu pada data apa pun yang disimpan dalam penyimpanan persisten dan tidak mudah menguap untuk durasi berapa pun. Enkripsi membantu Anda melindungi kerahasiaan data tersebut, mengurangi risiko bahwa pengguna yang tidak sah dapat mengaksesnya. Mengenkripsi kluster RDS DB Anda melindungi data dan metadata Anda terhadap akses yang tidak sah. Ini juga memenuhi persyaratan kepatuhan untuk data-at-rest enkripsi sistem file produksi.

Remediasi

Anda dapat mengaktifkan enkripsi saat istirahat saat Anda membuat cluster RDS DB. Anda tidak dapat mengubah pengaturan enkripsi setelah membuat cluster. Untuk informasi selengkapnya, lihat Mengenkripsi klaster Amazon Aurora DB di Panduan Pengguna Amazon Aurora.

[RDS.28] Cluster RDS DB harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::RDS::DBCluster`

AWS Config aturan: `tagged-rds-dbcluster` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList	Daftar tag yang memenuhi	Tidak ada nilai default

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
			AWS persyaratan	

Kontrol ini memeriksa apakah cluster Amazon RDS DB memiliki tag dengan kunci spesifik yang ditentukan dalam parameter`requiredTagKeys`. Kontrol gagal jika cluster DB tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika cluster DB tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke kluster RDS DB, lihat Menandai sumber daya Amazon RDS di Panduan Pengguna Amazon RDS.

[RDS.29] Snapshot cluster RDS DB harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::RDS::DBClusterSnapshot`

AWS Config aturan: `tagged-rds-dbclustersnapshot` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList	Daftar tag yang memenuhi AWS persyaratan	Tidak ada nilai default

Kontrol ini memeriksa apakah snapshot kluster Amazon RDS DB memiliki tag dengan kunci spesifik yang ditentukan dalam parameter. `requiredTagKeys` Kontrol gagal jika snapshot cluster DB tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika snapshot cluster DB tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke

AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke snapshot klaster RDS DB, lihat Menandai sumber daya Amazon RDS di Panduan Pengguna Amazon RDS.

[RDS.30] Instans RDS DB harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::RDS::DBInstance`

AWS Config aturan: `tagged-rds-dbinstance` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList	Daftar tag yang memenuhi	Tidak ada nilai default

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
			AWS persyaratan	

Kontrol ini memeriksa apakah instans Amazon RDS DB memiliki tag dengan kunci spesifik yang ditentukan dalam parameter`requiredTagKeys`. Kontrol gagal jika instans DB tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika instance DB tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke instans RDS DB, lihat Menandai sumber daya Amazon RDS di Panduan Pengguna Amazon RDS.

[RDS.31] Grup keamanan RDS DB harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::RDS::DBSecurityGroup`

AWS Config aturan: `tagged-rds-dbsecuritygroup` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList	Daftar tag yang memenuhi AWS persyaratan	Tidak ada nilai default

Kontrol ini memeriksa apakah grup keamanan Amazon RDS DB memiliki tag dengan kunci spesifik yang ditentukan dalam parameter`requiredTagKeys`. Kontrol gagal jika grup keamanan DB tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika grup keamanan DB tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke

AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke grup keamanan RDS DB, lihat Menandai sumber daya Amazon RDS di Panduan Pengguna Amazon RDS.

[RDS.32] Snapshot RDS DB harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::RDS::DBSnapshot`

AWS Config aturan: `tagged-rds-dbsnapshot` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList	Daftar tag yang memenuhi	Tidak ada nilai default

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
			AWS persyaratan	

Kontrol ini memeriksa apakah snapshot Amazon RDS DB memiliki tag dengan kunci tertentu yang ditentukan dalam parameter. `requiredTagKeys` Kontrol gagal jika snapshot DB tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika snapshot DB tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke snapshot RDS DB, lihat Menandai sumber daya Amazon RDS di Panduan Pengguna Amazon RDS.

[RDS.33] Grup subnet RDS DB harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::RDS::DBSubnetGroup`

AWS Config aturan: `tagged-rds-dbsubnetgroups` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList	Daftar tag yang memenuhi AWS persyaratan	Tidak ada nilai default

Kontrol ini memeriksa apakah grup subnet Amazon RDS DB memiliki tag dengan kunci spesifik yang ditentukan dalam parameter. `requiredTagKeys` Kontrol gagal jika grup subnet DB tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika grup subnet DB tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke

AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke grup subnet RDS DB, lihat Menandai sumber daya Amazon RDS di Panduan Pengguna Amazon RDS.

[RDS.34] Cluster Aurora MySQL DB harus menerbitkan log audit ke Log CloudWatch

Persyaratan terkait: Nist.800-53.r5 AC-2 (4), Nist.800-53.r5 AC-4 (26), Nist.800-53.r5 AC-6 (9), Nist.800-53.r5 AU-10, Nist.800-53.r5 AU-12, Nist.800-53.r5 AU-2, Nist.800-53.r5 5 AU-3, NIST.800-53.R5 AU-6 (3), NIST.800-53.R5 AU-6 (4), NIST.800-53.R5 CA-7, NIST.800-53.R5 SC-7 (9), NIST.800-53.R5 SI-4 (20), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-4 (20), nistST.800-53.R5 SI-7 (8)

Kategori: Identifikasi > Logging

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::RDS::DBCluster`

AWS Config aturan: **`rds-aurora-mysql-audit-logging-enabled`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah kluster DB MySQL Amazon Aurora dikonfigurasi untuk mempublikasikan log audit ke Amazon Logs. CloudWatch Kontrol gagal jika klaster tidak dikonfigurasi

untuk mempublikasikan log audit ke CloudWatch Log. Kontrol tidak menghasilkan temuan untuk cluster Aurora Serverless v1 DB.

Log audit menangkap catatan aktivitas database, termasuk upaya login, modifikasi data, perubahan skema, dan peristiwa lain yang dapat diaudit untuk tujuan keamanan dan kepatuhan. Saat mengonfigurasi klaster DB MySQL Aurora untuk mempublikasikan log audit ke grup log di Amazon Logs, Anda dapat melakukan analisis data CloudWatch log secara real-time. CloudWatch Log menyimpan log dalam penyimpanan yang sangat tahan lama. Anda juga dapat membuat alarm dan melihat metrik di. CloudWatch

> **Note**
>
> Cara alternatif untuk mempublikasikan log audit ke CloudWatch Log adalah dengan mengaktifkan audit lanjutan dan menyetel parameter DB tingkat cluster ke. `server_audit_logs_upload` `1` Default untuk `server_audit_logs_upload` `parameter` adalah`0`. Namun, kami sarankan Anda menggunakan instruksi remediasi berikut sebagai gantinya untuk melewati kontrol ini.

Remediasi

Untuk mempublikasikan log audit klaster MySQL DB Aurora ke Log, CloudWatch lihat Menerbitkan log MySQL Amazon Aurora ke Log Amazon di Panduan Pengguna Amazon Aurora. CloudWatch

[RDS.35] Cluster RDS DB harus mengaktifkan peningkatan versi minor otomatis

Persyaratan terkait: NIST.800-53.R5 SI-2, NIST.800-53.R5 SI-2 (2), NIST.800-53.R5 SI-2 (4), Nist.800-53.R5 SI-2 (5)

Kategori: Identifikasi > Kerentanan, tambalan, dan manajemen versi

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::RDS::DBCluster`

AWS Config aturan: **`rds-cluster-auto-minor-version-upgrade-enable`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah pemutakhiran versi minor otomatis diaktifkan untuk cluster DB Multi-AZ Amazon RDS. Kontrol gagal jika upgrade versi minor otomatis tidak diaktifkan untuk cluster DB multi-AZ.

RDS menyediakan upgrade versi minor otomatis sehingga Anda dapat menjaga cluster DB multi-AZ Anda tetap up to date. Versi minor dapat memperkenalkan fitur perangkat lunak baru, perbaikan bug, patch keamanan, dan peningkatan kinerja. Dengan mengaktifkan upgrade versi minor otomatis pada cluster database RDS, cluster, bersama dengan instance di cluster, akan menerima pembaruan otomatis ke versi minor ketika versi baru tersedia. Pembaruan diterapkan secara otomatis selama jendela pemeliharaan.

Remediasi

Untuk mengaktifkan pemutakhiran versi minor otomatis pada klaster DB multi-AZ, lihat Memodifikasi klaster DB Multi-AZ di Panduan Pengguna Amazon RDS.

Kontrol Amazon Redshift

Kontrol ini terkait dengan sumber daya Amazon Redshift.

Kontrol ini mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[Redshift.1] Cluster Amazon Redshift harus melarang akses publik

Persyaratan terkait: PCI DSS v3.2.1/1.2.1, PCI DSS v3.2.1/1.3.1, PCI DSS v3.2.1/1.3.2, PCI DSS v3.2.1/1.3.4, PCI DSS v3.2.1/1.3.6, Nist.800-53.R5 AC-21, Nist.800-53.r5 AC-3, Nist.800-53.r5 5 AC-3 (7), NIST.800-53.R5 AC-4, NIST.800-53.R5 AC-4 (21), Nist.800-53.r5 AC-6, Nist.800-53.r5 SC-7, Nist.800-53.r5 SC-7 (11), Nist.800-53.r5 SC-7 (16), Nist.800-53.r5 SC-7 (20), NIST.800-53.R5 SC-7 (21), Nist.800-53.r5 SC-7 (3), Nist.800-53.r5 SC-7 (4), Nist.800-53.r5 SC-7 (9)

Kategori: Lindungi > Konfigurasi jaringan aman > Sumber daya tidak dapat diakses publik

Tingkat keparahan: Kritis

Jenis sumber daya: `AWS::Redshift::Cluster`

AWS Config aturan: **`redshift-cluster-public-access-check`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah klaster Amazon Redshift dapat diakses publik. Ini mengevaluasi `PubliclyAccessible` bidang dalam item konfigurasi cluster.

`PubliclyAccessible`Atribut konfigurasi klaster Amazon Redshift menunjukkan apakah klaster dapat diakses publik. Ketika cluster dikonfigurasi dengan `PubliclyAccessible` set to`true`, itu adalah instance yang menghadap Internet yang memiliki nama DNS yang dapat diselesaikan secara publik, yang diselesaikan ke alamat IP publik.

Ketika cluster tidak dapat diakses publik, itu adalah instance internal dengan nama DNS yang menyelesaikan ke alamat IP pribadi. Kecuali jika Anda bermaksud agar cluster Anda dapat diakses oleh publik, cluster tidak boleh dikonfigurasi dengan `PubliclyAccessible` set to`true`.

Remediasi

Untuk memperbarui klaster Amazon Redshift untuk menonaktifkan akses publik, lihat Memodifikasi klaster di Panduan Manajemen Pergeseran Merah Amazon. Setel Dapat diakses publik ke No.

[Redshift.2] Koneksi ke cluster Amazon Redshift harus dienkripsi saat transit

Persyaratan terkait: Nist.800-53.r5 AC-4, Nist.800-53.r5 SC-13, Nist.800-53.r5 SC-23, Nist.800-53.r5 SC-23 (3), Nist.800-53.r5 SC-7 (4), Nist.800-53.r5 SC-8, Nist.800-53.r5 R5 SC-8 (1), NIST.800-53.R5 SC-8 (2)

Kategori: Lindungi > Perlindungan Data > Enkripsi data-in-transit

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::Redshift::Cluster` `AWS::Redshift::ClusterParameterGroup`

AWS Config aturan: **`redshift-require-tls-ssl`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah koneksi ke kluster Amazon Redshift diperlukan untuk menggunakan enkripsi dalam perjalanan. Pemeriksaan gagal jika parameter cluster Amazon Redshift `require_SSL` tidak disetel ke. `True`

TLS dapat digunakan untuk membantu mencegah penyerang potensial menggunakan person-in-the-middle atau serangan serupa untuk menguping atau memanipulasi lalu lintas jaringan. Hanya koneksi

terenkripsi melalui TLS yang diizinkan. Mengenkripsi data dalam perjalanan dapat memengaruhi kinerja. Anda harus menguji aplikasi Anda dengan fitur ini untuk memahami profil kinerja dan dampak TLS.

Remediasi

Untuk memperbarui grup parameter Amazon Redshift agar memerlukan enkripsi, lihat Memodifikasi grup parameter di Panduan Manajemen Pergeseran Merah Amazon. Setel `require_ssl` ke Benar.

[Redshift.3] Cluster Amazon Redshift harus mengaktifkan snapshot otomatis

Persyaratan terkait: Nist.800-53.r5 CP-10, Nist.800-53.r5 CP-6, Nist.800-53.R5 CP-6 (1), Nist.800-53.r5 CP-6 (2), Nist.800-53.r5 CP-9, Nist.800-53.r5 SC-5 (2), Nist.800-53.r5 SC-5 (2), Nist.800-53.r5 00-53.R5 SC-7 (10), NIST.800-53.R5 SI-13 (5)

Kategori: Pulih> Ketahanan > Cadangan diaktifkan

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::Redshift::Cluster`

AWS Config aturan: **`redshift-backup-enabled`**

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub	
`MinRetentionPeriod`	Periode retensi snapshot minimum dalam beberapa hari	Bilangan Bulat	7 untuk 35	7	

Kontrol ini memeriksa apakah klaster Amazon Redshift mengaktifkan snapshot otomatis, dan periode retensi yang lebih besar dari atau sama dengan kerangka waktu yang ditentukan. Kontrol gagal jika snapshot otomatis tidak diaktifkan untuk cluster, atau jika periode retensi kurang dari kerangka waktu

yang ditentukan. Kecuali Anda memberikan nilai parameter khusus untuk periode retensi snapshot, Security Hub menggunakan nilai default 7 hari.

Cadangan membantu Anda pulih lebih cepat dari insiden keamanan. Mereka memperkuat ketahanan sistem Anda. Amazon Redshift mengambil snapshot periodik secara default. Kontrol ini memeriksa apakah snapshot otomatis diaktifkan dan dipertahankan setidaknya selama tujuh hari. Untuk detail selengkapnya tentang snapshot otomatis Amazon Redshift, lihat Snapshot otomatis di Panduan Manajemen Pergeseran Merah Amazon.

Remediasi

Untuk memperbarui periode retensi snapshot untuk klaster Amazon Redshift, lihat Memodifikasi klaster di Panduan Manajemen Pergeseran Merah Amazon. Untuk Backup, atur retensi Snapshot ke nilai 7 atau lebih tinggi.

[Redshift.4] Cluster Amazon Redshift harus mengaktifkan pencatatan audit

Persyaratan terkait: Nist.800-53.r5 AC-2 (4), Nist.800-53.r5 AC-4 (26), Nist.800-53.r5 AC-6 (9), Nist.800-53.r5 AU-10, Nist.800-53.r5 AU-12, Nist.800-53.r5 AU-2, Nist.800-53.r5 5 AU-3, NIST.800-53.R5 AU-6 (3), NIST.800-53.R5 AU-6 (4), NIST.800-53.R5 CA-7, NIST.800-53.R5 SC-7 (9), NIST.800-53.R5 SI-4 (20), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-4 (20), nistST.800-53.R5 SI-7 (8)

Kategori: Identifikasi > Logging

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::Redshift::Cluster`

AWS Config aturan: `redshift-cluster-audit-logging-enabled` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

- `loggingEnabled = true`(tidak dapat disesuaikan)

Kontrol ini memeriksa apakah klaster Amazon Redshift mengaktifkan pencatatan audit.

Pencatatan audit Amazon Redshift memberikan informasi tambahan tentang koneksi dan aktivitas pengguna di klaster Anda. Data ini dapat disimpan dan diamankan di Amazon S3 dan dapat membantu dalam audit dan investigasi keamanan. Untuk informasi selengkapnya, lihat Pencatatan audit database di Panduan Manajemen Pergeseran Merah Amazon.

Remediasi

Untuk mengonfigurasi pencatatan audit untuk klaster Amazon Redshift, lihat Mengonfigurasi audit menggunakan konsol di Panduan Manajemen Amazon Redshift.

[Redshift.6] Amazon Redshift harus mengaktifkan peningkatan otomatis ke versi utama

Persyaratan terkait: NIST.800-53.R5 CA-9 (1), Nist.800-53.R5 CM-2, Nist.800-53.R5 CP-9, Nist.800-53.r5 SC-5 (2), Nist.800-53.R5 SI-2, NIST.800-53.R5 SI-2 (2), NIST.800-53.R5 3.R5 SI-2 (4), NIST.800-53.R5 SI-2 (5)

Kategori: Identifikasi > Kerentanan, tambalan, dan manajemen versi

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::Redshift::Cluster`

AWS Config aturan: **`redshift-cluster-maintenancesettings-check`**

Jenis jadwal: Perubahan dipicu

Parameter:

- `allowVersionUpgrade = true`(tidak dapat disesuaikan)

Kontrol ini memeriksa apakah pemutakhiran versi utama otomatis diaktifkan untuk klaster Amazon Redshift.

Mengaktifkan pemutakhiran versi utama otomatis memastikan bahwa pembaruan versi utama terbaru ke kluster Amazon Redshift diinstal selama jendela pemeliharaan. Pembaruan ini mungkin termasuk patch keamanan dan perbaikan bug. Tetap up to date dengan instalasi patch adalah langkah penting dalam mengamankan sistem.

Remediasi

Untuk mengatasi masalah ini dari AWS CLI, gunakan perintah Amazon `modify-cluster` Redshift untuk menyetel `--allow-version-upgrade` atribut.

```
aws redshift modify-cluster --cluster-identifier clustername --allow-version-upgrade
```

Di *clustername* mana nama cluster Amazon Redshift Anda.

[Redshift.7] Cluster Redshift harus menggunakan perutean VPC yang ditingkatkan

Persyaratan terkait: Nist.800-53.r5 AC-4, NIST.800-53.R5 AC-4 (21), Nist.800-53.r5 SC-7, Nist.800-53.r5 SC-7 (11), Nist.800-53.r5 SC-7 (20), Nist.800-53.r5 SC-7 (21), Nist.800-53.r5 SC-7 (21), Nist.800-53.r5 SC-7 (21), Nist.800-53.r5 SC-7 (21), Nist.800-53.r5 SC-7 (21), Nist.800-53.r5 SC-7 (21), ST.800-53.R5 SC-7 (4), NIST.800-53.R5 SC-7 (9)

Kategori: Lindungi > Konfigurasi jaringan aman > Akses pribadi API

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::Redshift::Cluster`

AWS Config aturan: **`redshift-enhanced-vpc-routing-enabled`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah klaster Amazon Redshift telah `EnhancedVpcRouting` diaktifkan.

Perutean VPC yang disempurnakan memaksa semua `COPY` dan `UNLOAD` lalu lintas antara cluster dan repositori data untuk melewati VPC Anda. Anda kemudian dapat menggunakan fitur VPC seperti grup keamanan dan daftar kontrol akses jaringan untuk mengamankan lalu lintas jaringan. Anda juga dapat menggunakan VPC Flow Logs untuk memantau lalu lintas jaringan.

Remediasi

Untuk petunjuk remediasi terperinci, lihat Mengaktifkan perutean VPC yang disempurnakan di Panduan Manajemen Pergeseran Merah Amazon.

[Redshift.8] Cluster Amazon Redshift tidak boleh menggunakan nama pengguna Admin default

Persyaratan terkait: NIST.800-53.R5 CA-9 (1), NIST.800-53.R5 CM-2

Kategori: Identifikasi > Konfigurasi Sumber Daya

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::Redshift::Cluster`

AWS Config aturan: **`redshift-default-admin-check`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah klaster Amazon Redshift telah mengubah nama pengguna admin dari nilai defaultnya. Kontrol ini akan gagal jika nama pengguna admin untuk cluster Redshift disetel ke. `awsuser`

Saat membuat klaster Redshift, Anda harus mengubah nama pengguna admin default menjadi nilai unik. Nama pengguna default adalah pengetahuan publik dan harus diubah pada konfigurasi. Mengubah nama pengguna default mengurangi risiko akses yang tidak diinginkan.

Remediasi

Anda tidak dapat mengubah nama pengguna admin untuk klaster Amazon Redshift Anda setelah dibuat. Untuk membuat cluster baru, ikuti instruksi di sini.

[Redshift.9] Cluster Redshift tidak boleh menggunakan nama database default

Persyaratan terkait: NIST.800-53.R5 CA-9 (1), NIST.800-53.R5 CM-2

Kategori: Identifikasi > Konfigurasi Sumber Daya

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::Redshift::Cluster`

AWS Config aturan: **`redshift-default-db-name-check`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah klaster Amazon Redshift telah mengubah nama database dari nilai defaultnya. Kontrol akan gagal jika nama database untuk cluster Redshift diatur ke. `dev`

Saat membuat cluster Redshift, Anda harus mengubah nama database default menjadi nilai unik. Nama default adalah pengetahuan publik dan harus diubah pada konfigurasi. Sebagai contoh, nama

terkenal dapat menyebabkan akses yang tidak disengaja jika digunakan dalam kondisi kebijakan IAM.

Remediasi

Anda tidak dapat mengubah nama database untuk klaster Amazon Redshift setelah dibuat. Untuk petunjuk cara membuat klaster baru, lihat Memulai Amazon Redshift di Panduan Memulai Pergeseran Merah Amazon.

[Redshift.10] Cluster Redshift harus dienkripsi saat istirahat

Persyaratan terkait: Nist.800-53.R5 CA-9 (1), Nist.800-53.R5 CM-3 (6), Nist.800-53.r5 SC-13, Nist.800-53.r5 SC-28, Nist.800-53.r5 SC-28 (1), Nist.800-53.r5 SI-7 (6)

Kategori: Lindungi > Perlindungan Data > Enkripsi data-at-rest

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::Redshift::Cluster`

AWS Config aturan: **`redshift-cluster-kms-enabled`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah cluster Amazon Redshift dienkripsi saat istirahat. Kontrol gagal jika klaster Redshift tidak dienkripsi saat istirahat atau jika kunci enkripsi berbeda dari kunci yang disediakan dalam parameter aturan.

Di Amazon Redshift, Anda dapat mengaktifkan enkripsi database untuk cluster Anda untuk membantu melindungi data saat istirahat. Saat Anda mengaktifkan enkripsi untuk cluster, blok data dan metadata sistem dienkripsi untuk cluster dan snapshot-nya. Enkripsi data saat istirahat adalah praktik terbaik yang disarankan karena menambahkan lapisan manajemen akses ke data Anda. Mengenkripsi cluster Redshift saat istirahat mengurangi risiko bahwa pengguna yang tidak sah dapat mengakses data yang disimpan pada disk.

Remediasi

Untuk memodifikasi klaster Redshift agar menggunakan enkripsi KMS, lihat Mengubah enkripsi klaster di Panduan Manajemen Pergeseran Merah Amazon.

[Redshift.11] Cluster Redshift harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::Redshift::Cluster`

AWS Config aturan: `tagged-redshift-cluster` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList	Daftar tag yang memenuhi AWS persyaratan	`No default value`

Kontrol ini memeriksa apakah klaster Amazon Redshift memiliki tag dengan kunci spesifik yang ditentukan dalam parameter. `requiredTagKeys` Kontrol gagal jika cluster tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika cluster tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke

AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke klaster Redshift, lihat Menandai sumber daya di Amazon Redshift di Panduan Manajemen Pergeseran Merah Amazon.

[Redshift.12] Langganan pemberitahuan acara Redshift harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::Redshift::EventSubscription`

AWS Config aturan: `tagged-redshift-eventsubscription` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList	Daftar tag yang memenuhi	`No default value`

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
			AWS persyaratan	

Kontrol ini memeriksa apakah snapshot klaster Amazon Redshift memiliki tag dengan kunci spesifik yang ditentukan dalam parameter. `requiredTagKeys` Kontrol gagal jika snapshot cluster tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika snapshot cluster tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke langganan notifikasi peristiwa Redshift, lihat Menandai sumber daya di Amazon Redshift di Panduan Manajemen Pergeseran Merah Amazon.

[Redshift.13] Snapshot cluster Redshift harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::Redshift::ClusterSnapshot`

AWS Config aturan: `tagged-redshift-clustersnapshot` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList	Daftar tag yang memenuhi AWS persyaratan	`No default value`

Kontrol ini memeriksa apakah snapshot klaster Amazon Redshift memiliki tag dengan kunci spesifik yang ditentukan dalam parameter. `requiredTagKeys` Kontrol gagal jika snapshot cluster tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika snapshot cluster tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke

AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke snapshot klaster Redshift, lihat Menandai sumber daya di Amazon Redshift di Panduan Manajemen Pergeseran Merah Amazon.

[Redshift.14] Grup subnet cluster Redshift harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::Redshift::ClusterSubnetGroup`

AWS Config aturan: `tagged-redshift-clustersubnetgroup` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList	Daftar tag yang memenuhi	`No default value`

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
			AWS persyaratan	

Kontrol ini memeriksa apakah grup subnet klaster Amazon Redshift memiliki tag dengan kunci spesifik yang ditentukan dalam parameter. `requiredTagKeys` Kontrol gagal jika grup subnet cluster tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika grup subnet cluster tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke grup subnet klaster Redshift, lihat Menandai sumber daya di Amazon Redshift di Panduan Manajemen Pergeseran Merah Amazon.

[Redshift.15] Grup keamanan Redshift harus mengizinkan masuknya port cluster hanya dari asal yang dibatasi

Kategori: Lindungi > Konfigurasi jaringan aman > Konfigurasi grup keamanan

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::Redshift::Cluster`

AWS Config aturan: **`redshift-unrestricted-port-access`**

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah grup keamanan yang terkait dengan klaster Amazon Redshift memiliki aturan masuk yang mengizinkan akses ke port cluster dari internet (0.0.0.0/0 atau: :/0). Kontrol gagal jika aturan masuknya grup keamanan mengizinkan akses ke port cluster dari internet.

Mengizinkan akses masuk yang tidak terbatas ke port cluster Redshift (alamat IP dengan akhiran /0) dapat mengakibatkan akses atau insiden keamanan yang tidak sah. Kami merekomendasikan untuk menerapkan prinsip akses hak istimewa paling rendah saat membuat grup keamanan dan mengonfigurasi aturan masuk.

Remediasi

Untuk membatasi masuknya port klaster Redshift ke asal terbatas, lihat Bekerja dengan aturan grup keamanan di Panduan Pengguna Amazon VPC. Perbarui aturan di mana rentang port cocok dengan port cluster Redshift dan rentang port IP adalah 0.0.0.0/0.

Amazon Route 53 kontrol

Kontrol ini terkait dengan sumber daya Route 53.

Kontrol ini mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[Route53.1] Pemeriksaan kesehatan rute 53 harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::Route53::HealthCheck`

AWS Config aturan: `tagged-route53-healthcheck` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList	Daftar tag yang memenuhi AWS persyaratan	Tidak ada nilai default

Kontrol ini memeriksa apakah pemeriksaan kesehatan Amazon Route 53 memiliki tag dengan kunci spesifik yang ditentukan dalam parameter`requiredTagKeys`. Kontrol gagal jika pemeriksaan kesehatan tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika pemeriksaan kesehatan tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke pemeriksaan kesehatan Route 53, lihat Penamaan dan penandaan pemeriksaan kesehatan di Panduan Pengembang Amazon Route 53.

[Route53.2] Route 53 zona yang dihosting publik harus mencatat kueri DNS

Persyaratan terkait: Nist.800-53.r5 AC-2 (4), Nist.800-53.r5 AC-4 (26), Nist.800-53.r5 AC-6 (9), Nist.800-53.r5 AU-10, Nist.800-53.r5 AU-12, Nist.800-53.r5 AU-2, Nist.800-53.r5 5 AU-3, NIST.800-53.R5 AU-6 (3), NIST.800-53.R5 AU-6 (4), NIST.800-53.R5 CA-7, NIST.800-53.R5 SC-7 (9), NIST.800-53.R5 SI-4 (20), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-4 (20), nistST.800-53.R5 SI-7 (8)

Kategori: Identifikasi > Logging

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::Route53::HostedZone`

AWS Config aturan: **`route53-query-logging-enabled`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah pencatatan kueri DNS diaktifkan untuk zona host publik Amazon Route 53. Kontrol gagal jika pencatatan kueri DNS tidak diaktifkan untuk zona host publik Route 53.

Mencatat kueri DNS untuk zona yang dihosting Route 53 memenuhi persyaratan keamanan dan kepatuhan DNS dan memberikan visibilitas. Log mencakup informasi seperti domain atau subdomain yang ditanyakan, tanggal dan waktu kueri, jenis catatan DNS (misalnya, A atau AAAA), dan kode

respons DNS (misalnya, atau). `NoError` `ServFail` Saat pencatatan kueri DNS diaktifkan, Route 53 menerbitkan file log ke Amazon CloudWatch Logs.

Remediasi

Untuk mencatat kueri DNS untuk zona host publik Route 53, lihat Mengonfigurasi pencatatan untuk kueri DNS di Panduan Pengembang Amazon Route 53.

Kontrol Layanan Penyimpanan Sederhana Amazon

Kontrol ini terkait dengan sumber daya Amazon S3.

Kontrol ini mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[S3.1] Bucket tujuan umum S3 harus mengaktifkan pengaturan akses publik blok

> **Important**
>
> Pada 12 Maret 2024, judul kontrol ini berubah menjadi judul yang ditampilkan. Untuk informasi selengkapnya, lihat Ubah log untuk kontrol Security Hub.

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v3.0.0/2.1.4, Tolok Ukur Yayasan CIS AWS v1.4.0/2.1.5, PCI DSS v3.2.1/1.2.1, PCI DSS v3.2.1/1.3.1, PCI DSS v3.2.1/1.3.2, PCI DSS v3.2.1/1.3.4, PCI DSS v3.2.1/1.3.6, NIST.800-53.R5 AC-21, Nist.800-53.r5 AC-3, Nist.800-53.r5 AC-3 (7), Nist.800-53.r5 AC-4, Nist.800-53.r5 AC-4 (21), Nist.800-53.r5 AC-6, Nist.800-53.r5 SC-7, Nist.800-53.r5 5 SC-7 (11), NIST.800-53.R5 SC-7 (16), NIST.800-53.R5 SC-7 (20), Nist.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), Nist.800-53.r5 SC-7 (4), NIST.800-53.r5 3.r5 SC-7 (9)

Kategori: Lindungi > Konfigurasi jaringan aman

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::::Account`

AWS Config aturan: **`s3-account-level-public-access-blocks-periodic`**

Jenis jadwal: Periodik

Parameter:

- `ignorePublicAcls`: `true` (tidak dapat disesuaikan)
- `blockPublicPolicy`: `true` (tidak dapat disesuaikan)
- `blockPublicAcls`: `true` (tidak dapat disesuaikan)
- `restrictPublicBuckets`: `true` (tidak dapat disesuaikan)

Kontrol ini memeriksa apakah setelan akses publik blok Amazon S3 sebelumnya dikonfigurasi pada tingkat akun untuk bucket tujuan umum S3. Kontrol gagal jika satu atau lebih pengaturan akses publik blok diatur ke`false`.

Kontrol gagal jika salah satu pengaturan diatur ke`false`, atau jika salah satu pengaturan tidak dikonfigurasi.

Blok akses publik Amazon S3 dirancang untuk menyediakan kontrol di seluruh Akun AWS atau pada tingkat bucket S3 individual untuk memastikan bahwa objek tidak pernah memiliki akses publik. Akses publik diberikan kepada bucket dan objek melalui daftar kontrol akses (ACL), kebijakan bucket, atau keduanya.

Kecuali jika Anda bermaksud agar bucket S3 Anda dapat diakses publik, Anda harus mengonfigurasi fitur Amazon S3 Block Public Access level akun.

Untuk mempelajari selengkapnya, lihat Menggunakan Amazon S3 Blokir Akses Publik di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

Remediasi

Untuk mengaktifkan Amazon S3 Blokir Akses Publik untuk Anda Akun AWS, lihat Mengonfigurasi setelan blokir akses publik untuk akun Anda di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

[S3.2] Bucket tujuan umum S3 harus memblokir akses baca publik

> **Important**
>
> Pada 12 Maret 2024, judul kontrol ini berubah menjadi judul yang ditampilkan. Untuk informasi selengkapnya, lihat Ubah log untuk kontrol Security Hub.

Persyaratan terkait: PCI DSS v3.2.1/1.2.1, PCI DSS v3.2.1/1.3.1, PCI DSS v3.2.1/1.3.2, PCI DSS v3.2.1/1.3.6, PCI DSS v3.2.1/7.2.1, Nist.800-53.R5 AC-21, Nist.800-53.r5 AC-3, Nist.800-53.r5 AC-3

(7), NIST.800-53.R5 AC-4, NIST.800-53.R5 AC-4 (21), Nist.800-53.r5 AC-6, Nist.800-53.r5 SC-7, Nist.800-53.r5 SC-7 (11), Nist.800-53.r5 SC-7 (16), Nist.800-53.r5 SC-7 (20), NIST.800-53.R5 SC-7 (21), Nist.800-53.r5 SC-7 (3), Nist.800-53.r5 SC-7 (4), Nist.800-53.r5 SC-7 (9)

Kategori: Lindungi > Konfigurasi jaringan aman

Tingkat keparahan: Kritis

Jenis sumber daya: `AWS::S3::Bucket`

AWS Config aturan: **`s3-bucket-public-read-prohibited`**

Jenis jadwal: Berkala dan perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah bucket tujuan umum Amazon S3 mengizinkan akses baca publik. Ini mengevaluasi pengaturan blokir akses publik, kebijakan bucket, dan daftar kontrol akses bucket (ACL). Kontrol gagal jika bucket mengizinkan akses baca publik.

Beberapa kasus penggunaan mungkin mengharuskan semua orang di internet dapat membaca dari bucket S3 Anda. Namun, situasi itu jarang terjadi. Untuk memastikan integritas dan keamanan data Anda, bucket S3 Anda tidak boleh dibaca publik.

Remediasi

Untuk memblokir akses baca publik di bucket Amazon S3, lihat Mengonfigurasi blokir setelan akses publik untuk bucket S3 Anda di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

[S3.3] Bucket tujuan umum S3 harus memblokir akses tulis publik

> **Important**
>
> Pada 12 Maret 2024, judul kontrol ini berubah menjadi judul yang ditampilkan. Untuk informasi selengkapnya, lihat Ubah log untuk kontrol Security Hub.

Persyaratan terkait: PCI DSS v3.2.1/1.2.1, PCI DSS v3.2.1/1.3.1, PCI DSS v3.2.1/1.3.2, PCI DSS v3.2.1/1.3.4, PCI DSS v3.2.1/1.3.6, PCI DSS v3.2.1/7.2.1, Nist.800-53.r5 AC-21, Nist.800-53.r5 AC-21, Nist.800-53.r5 AC-21 -3, Nist.800-53.r5 AC-3 (7), Nist.800-53.r5 AC-4, Nist.800-53.r5 AC-4 (21), Nist.800-53.r5 AC-6, Nist.800-53.r5 SC-7, Nist.800-53.r5 SC-7 (11), Nist.800-53.r5 SC-7

(11), Nist.800-53.r5 00-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.R5 SC-7 (21), Nist.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9)

Kategori: Lindungi > Konfigurasi jaringan aman

Tingkat keparahan: Kritis

Jenis sumber daya: `AWS::S3::Bucket`

AWS Config aturan: **`s3-bucket-public-write-prohibited`**

Jenis jadwal: Berkala dan perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah bucket tujuan umum Amazon S3 mengizinkan akses tulis publik. Ini mengevaluasi pengaturan blokir akses publik, kebijakan bucket, dan daftar kontrol akses bucket (ACL). Kontrol gagal jika bucket mengizinkan akses tulis publik.

Beberapa kasus penggunaan mengharuskan semua orang di internet dapat menulis ke bucket S3 Anda. Namun, situasi itu jarang terjadi. Untuk memastikan integritas dan keamanan data Anda, bucket S3 Anda tidak boleh ditulis secara publik.

Remediasi

Untuk memblokir akses tulis publik di bucket Amazon S3, lihat Mengonfigurasi setelan blokir akses publik untuk bucket S3 Anda di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

[S3.5] Bucket tujuan umum S3 harus memerlukan permintaan untuk menggunakan SSL

> **Important**
>
> Pada 12 Maret 2024, judul kontrol ini berubah menjadi judul yang ditampilkan. Untuk informasi selengkapnya, lihat Ubah log untuk kontrol Security Hub.

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v3.0.0/2.1.1, Tolok Ukur Yayasan CIS AWS v1.4.0/2.1.2, PCI DSS v3.2.1/4.1, Nist.800-53.r5 AC-17 (2), Nist.800-53.r5 AC-4, Nist.800-53.r5 IA-5 (1), Nist.800-53.r5 SC-12 (3), Nist.800-53.r5 SC-13, Nist.800-53.r5 SC-23, Nist.800-53.r5 SC-23 (3), Nist.800-53.r5 SC-7 (4), Nist.800-53.r5 SC-8, Nist.800-53.r5 SC-8 (1), Nist.800-53.r5 SC-8 (1), Nist.800-53.r5 00-53.R5 SC-8 (2), NIST.800-53.R5 SI-7 (6)

Kategori: Lindungi > Manajemen akses yang aman

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::S3::Bucket`

AWS Config aturan: **`s3-bucket-ssl-requests-only`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah bucket tujuan umum Amazon S3 memiliki kebijakan yang mengharuskan permintaan untuk menggunakan SSL. Kontrol gagal jika kebijakan bucket tidak memerlukan permintaan untuk menggunakan SSL.

Bucket S3 harus memiliki kebijakan yang mengharuskan semua permintaan (`Action: S3:*`) hanya menerima transmisi data melalui HTTPS dalam kebijakan sumber daya S3, yang ditunjukkan oleh kunci kondisi. `aws:SecureTransport`

Remediasi

Untuk memperbarui kebijakan bucket Amazon S3 untuk menolak transportasi yang tidak aman, lihat Menambahkan kebijakan bucket menggunakan konsol Amazon S3 di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

Tambahkan pernyataan kebijakan yang mirip dengan yang ada di kebijakan berikut. Ganti `DOC-EXAMPLE-BUCKET` dengan nama bucket yang sedang Anda modifikasi.

```
{
    "Id": "ExamplePolicy",
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowSSLRequestsOnly",
            "Action": "s3:*",
            "Effect": "Deny",
            "Resource": [
                "arn:aws:s3:::DOC-EXAMPLE-BUCKET",
                "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
            ],
            "Condition": {
                "Bool": {
                    "aws:SecureTransport": "false"
```

```
                }
            },
            "Principal": "*"
        }
    ]
}
```

Untuk informasi selengkapnya, lihat Kebijakan bucket S3 apa yang harus saya gunakan untuk mematuhi AWS Config aturan s3-? bucket-ssl-requests-only di Pusat Pengetahuan AWS Resmi.

[S3.6] Kebijakan bucket tujuan umum S3 harus membatasi akses ke yang lain Akun AWS

> **Important**
>
> Pada 12 Maret 2024, judul kontrol ini berubah menjadi judul yang ditampilkan. Untuk informasi selengkapnya, lihat Ubah log untuk kontrol Security Hub.

Persyaratan terkait: NIST.800-53.R5 CA-9 (1), NIST.800-53.R5 CM-2

Kategori: Lindungi > Manajemen akses aman > Tindakan operasi API sensitif dibatasi

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::S3::Bucket`

AWS Configaturan: `s3-bucket-blacklisted-actions-prohibited`

Jenis jadwal: Perubahan dipicu

Parameter:

- `blacklistedactionpatterns`: `s3:DeleteBucketPolicy, s3:PutBucketAcl, s3:PutBucketPolicy, s3:PutEncryptionConfiguration, s3:PutObjectAcl` (tidak dapat disesuaikan)

Kontrol ini memeriksa apakah kebijakan bucket tujuan umum Amazon S3 mencegah prinsipal dari pihak lain Akun AWS melakukan tindakan yang ditolak pada sumber daya di bucket S3. Kontrol gagal jika kebijakan bucket mengizinkan satu atau beberapa tindakan sebelumnya untuk prinsipal di tempat lain. Akun AWS

Menerapkan akses hak istimewa paling sedikit sangat penting untuk mengurangi risiko keamanan dan dampak kesalahan atau niat jahat. Jika kebijakan bucket S3 mengizinkan akses dari akun eksternal, hal itu dapat mengakibatkan eksfiltrasi data oleh ancaman orang dalam atau penyerang.

`blacklistedactionpatterns`Parameter ini memungkinkan evaluasi aturan yang berhasil untuk ember S3. Parameter memberikan akses ke akun eksternal untuk pola tindakan yang tidak termasuk dalam `blacklistedactionpatterns` daftar.

Remediasi

Untuk memperbarui kebijakan bucket Amazon S3 guna menghapus izin, lihat. Menambahkan kebijakan bucket dengan menggunakan konsol Amazon S3 di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

Pada halaman Edit kebijakan bucket, di kotak teks pengeditan kebijakan, lakukan salah satu tindakan berikut:

- Hapus pernyataan yang memberikan Akun AWS akses lain ke tindakan yang ditolak.
- Hapus tindakan yang ditolak yang diizinkan dari pernyataan.

[S3.7] Ember tujuan umum S3 harus menggunakan replikasi lintas wilayah

> **Important**
>
> Pada 12 Maret 2024, judul kontrol ini berubah menjadi judul yang ditampilkan. Untuk informasi selengkapnya, lihat Ubah log untuk kontrol Security Hub.

Persyaratan terkait: PCI DSS v3.2.1/2.2, Nist.800-53.r5 AU-9 (2), Nist.800-53.r5 CP-10, Nist.800-53.r5 CP-6, Nist.800-53.r5 CP-6 (1), Nist.800-53.r5 CP-6 (2), Nist.800-53.r5 5 CP-9, NIST.800-53.R5 SC-36 (2), NIST.800-53.R5 SC-5 (2), NIST.800-53.R5 SI-13 (5)

Kategori: Lindungi > Manajemen akses yang aman

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::S3::Bucket`

AWS Config aturan: **`s3-bucket-cross-region-replication-enabled`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah bucket tujuan umum Amazon S3 mengaktifkan replikasi lintas wilayah. Kontrol gagal jika bucket tidak mengaktifkan replikasi lintas wilayah.

Replikasi adalah penyalinan objek secara otomatis dan asinkron di seluruh ember dalam hal yang sama atau berbeda. Wilayah AWS Replikasi menyalin objek dan pembaruan objek yang baru dibuat dari bucket sumber ke bucket atau bucket tujuan. AWS praktik terbaik merekomendasikan replikasi untuk ember sumber dan tujuan yang dimiliki oleh yang sama. Akun AWS Selain ketersediaan, Anda harus mempertimbangkan pengaturan pengerasan sistem lainnya.

Remediasi

Untuk mengaktifkan Replikasi Lintas Wilayah pada bucket S3, lihat Mengonfigurasi replikasi untuk bucket sumber dan tujuan yang dimiliki oleh akun yang sama di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon. Untuk bucket Source, pilih Apply to all objects in the bucket.

[S3.8] Bucket tujuan umum S3 harus memblokir akses publik

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v3.0.0/2.1.4, Tolok Ukur Yayasan CIS AWS v1.4.0/2.1.5, Nist.800-53.r5 AC-21, Nist.800-53.r5 AC-3, Nist.800-53.r5 AC-3 (7), Nist.800-53.r5 AC-4, Nist.800-53.r5 AC-4 (21), Nist.800-53.r5 AC-6, Nist.800-53.r5 SC-7, Nist.800-53.r5 SC-7 (11), Nist.800-53.r5 SC-7 (16), Nist.800-53.r5 SC-7 (20), Nist.800-53.r5 SC-7 (21), Nist.800-53.r5 SC-7 (21), Nist.800-53.r5 SC-7 (21), Nist.800-53.r5 ST.800-53.r5 SC-7 (3), NIST.800-53.R5 SC-7 (4), NIST.800-53.R5 SC-7 (9)

Kategori: Lindungi > Manajemen akses yang aman > Kontrol akses

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::S3::Bucket`

AWS Config aturan: **`s3-bucket-level-public-access-prohibited`**

Jenis jadwal: Perubahan dipicu

Parameter:

- `excludedPublicBuckets`(tidak dapat disesuaikan) - Daftar terpisah koma dari nama bucket S3 publik yang diizinkan yang diketahui

Kontrol ini memeriksa apakah bucket tujuan umum Amazon S3 memblokir akses publik di tingkat bucket. Kontrol gagal jika salah satu pengaturan berikut diatur ke`false`:

- `ignorePublicAcls`
- `blockPublicPolicy`
- `blockPublicAcls`
- `restrictPublicBuckets`

Blokir Akses Publik pada tingkat bucket S3 menyediakan kontrol untuk memastikan bahwa objek tidak pernah memiliki akses publik. Akses publik diberikan kepada bucket dan objek melalui daftar kontrol akses (ACL), kebijakan bucket, atau keduanya.

Kecuali jika Anda bermaksud agar bucket S3 dapat diakses publik, Anda harus mengonfigurasi fitur Amazon S3 Block Public Access level bucket.

Remediasi

Untuk informasi tentang cara menghapus akses publik pada tingkat bucket, lihat Memblokir akses publik ke penyimpanan Amazon S3 Anda di Panduan Pengguna Amazon S3.

[S3.9] Bucket tujuan umum S3 harus mengaktifkan pencatatan akses server

> **Important**
>
> Pada 12 Maret 2024, judul kontrol ini berubah menjadi judul yang ditampilkan. Untuk informasi selengkapnya, lihat Ubah log untuk kontrol Security Hub.

Persyaratan terkait: Nist.800-53.r5 AC-2 (4), Nist.800-53.r5 AC-4 (26), Nist.800-53.r5 AC-6 (9), Nist.800-53.r5 AU-10, Nist.800-53.r5 AU-12, Nist.800-53.r5 AU-2, Nist.800-53.r5 5 AU-3, NIST.800-53.R5 AU-6 (3), NIST.800-53.R5 AU-6 (4), NIST.800-53.R5 CA-7, NIST.800-53.R5 SC-7 (9), NIST.800-53.R5 SI-4 (20), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-4 (20), nistST.800-53.R5 SI-7 (8)

Kategori: Identifikasi > Logging

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::S3::Bucket`

AWS Config aturan: **`s3-bucket-logging-enabled`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah pencatatan akses server diaktifkan untuk bucket tujuan umum Amazon S3. Kontrol gagal jika pencatatan akses server tidak diaktifkan. Saat logging diaktifkan, Amazon S3 mengirimkan log akses untuk bucket sumber ke bucket target yang dipilih. Bucket target harus Wilayah AWS sama dengan bucket sumber dan tidak boleh memiliki periode retensi default yang dikonfigurasi. Bucket logging target tidak perlu mengaktifkan pencatatan akses server, dan Anda harus menekan temuan untuk bucket ini.

Pencatatan akses server menyediakan catatan terperinci tentang permintaan yang dibuat ke ember. Log akses server dapat membantu dalam audit keamanan dan akses. Untuk informasi selengkapnya, lihat Praktik Terbaik Keamanan untuk Amazon S3: Aktifkan pencatatan akses server Amazon S3.

Remediasi

Untuk mengaktifkan pencatatan akses server Amazon S3, lihat Mengaktifkan pencatatan akses server Amazon S3 di Panduan Pengguna Amazon S3.

[S3.10] Bucket tujuan umum S3 dengan versi diaktifkan harus memiliki konfigurasi Siklus Hidup

> **Important**
>
> Pada 12 Maret 2024, judul kontrol ini berubah menjadi judul yang ditampilkan. Security Hub menghentikan kontrol ini pada April 2024 dari standar Praktik Terbaik Keamanan AWS Dasar, tetapi masih termasuk dalam standar NIST SP 800-53 Rev. 5. Untuk informasi selengkapnya, lihat Ubah log untuk kontrol Security Hub.

Persyaratan terkait: Nist.800-53.r5 CP-10, Nist.800-53.R5 CP-6 (2), Nist.800-53.R5 CP-9, Nist.800-53.r5 SC-5 (2), Nist.800-53.r5 SI-13 (5)

Kategori: Identifikasi > Logging

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::S3::Bucket`

AWS Config aturan: **`s3-version-lifecycle-policy-check`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah bucket berversi tujuan umum Amazon S3 memiliki konfigurasi Siklus Hidup. Kontrol gagal jika bucket tidak memiliki konfigurasi Siklus Hidup.

Sebaiknya buat konfigurasi Siklus Hidup untuk bucket S3 untuk membantu menentukan tindakan yang ingin dilakukan Amazon S3 selama masa pakai objek.

Remediasi

Untuk informasi selengkapnya tentang mengonfigurasi siklus hidup di bucket Amazon S3, lihat Menyetel konfigurasi siklus hidup pada bucket dan Mengelola siklus hidup penyimpanan Anda.

[S3.11] Bucket tujuan umum S3 harus mengaktifkan pemberitahuan acara

> **Important**
>
> Pada 12 Maret 2024, judul kontrol ini berubah menjadi judul yang ditampilkan. Security Hub menghentikan kontrol ini pada April 2024 dari standar Praktik Terbaik Keamanan AWS Dasar, tetapi masih termasuk dalam standar NIST SP 800-53 Rev. 5:. Untuk informasi selengkapnya, lihat Ubah log untuk kontrol Security Hub.

Persyaratan terkait: NIST.800-53.R5 CA-7, NIST.800-53.R5 SI-3 (8), NIST.800-53.R5 SI-4, NIST.800-53.R5 SI-4 (4)

Kategori: Identifikasi > Logging

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::S3::Bucket`

AWS Config aturan: **`s3-event-notifications-enabled`**

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`eventTypes`	Daftar jenis acara S3 pilihan	EnumList (maksimal 28 item)	`s3:IntelligentTiering`, `s3:LifecycleExpiration:*`, `s3:LifecycleExpiration:Delete`, `s3:LifecycleExpiration:DeleteMarkerCreated`, `s3:LifecycleTransition`, `s3:ObjectAcl:Put`, `s3:ObjectCreated:*`, `s3:ObjectCreated:CompleteMultipartUpload`, `s3:ObjectCreated:Copy`, `s3:Object`	Tidak ada nilai default

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
			`Created:Post`, `s3:ObjectCreated:Put`, `s3:ObjectRemoved:*`, `s3:ObjectRemoved:Delete`, `s3:ObjectRemoved:DeleteMarkerCreated`, `s3:ObjectRestore:*`, `s3:ObjectRestore:Completed`, `s3:ObjectRestore:Delete`, `s3:ObjectRestore:Post`, `s3:ObjectTagging:*`, `s3:Object`	

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
			`Tagging:Delete, s3:ObjectTagging:Put, s3:ReducedRedundancyLostObject, s3:Replication:*, s3:Replication:OperationFailedReplication, s3:Replication:OperationMissedThreshold, s3:Replication:OperationNotTracked, s3:Replication:OperationReplicatedAfterThreshold,`	

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
			`s3:TestEvent`	

Kontrol ini memeriksa apakah Pemberitahuan Peristiwa S3 diaktifkan pada bucket tujuan umum Amazon S3. Kontrol gagal jika Pemberitahuan Acara S3 tidak diaktifkan di bucket. Jika Anda memberikan nilai kustom untuk `eventTypes` parameter, kontrol hanya akan diteruskan jika pemberitahuan peristiwa diaktifkan untuk jenis peristiwa yang ditentukan.

Saat mengaktifkan Pemberitahuan Acara S3, Anda menerima peringatan saat peristiwa tertentu terjadi yang memengaruhi bucket S3 Anda. Misalnya, Anda dapat diberi tahu tentang pembuatan objek, penghapusan objek, dan restorasi objek. Pemberitahuan ini dapat mengingatkan tim terkait untuk modifikasi yang tidak disengaja atau disengaja yang dapat menyebabkan akses data yang tidak sah.

Remediasi

Untuk informasi tentang mendeteksi perubahan pada bucket dan objek S3, lihat Pemberitahuan Acara Amazon S3 di Panduan Pengguna Amazon S3.

[S3.12] ACL tidak boleh digunakan untuk mengelola akses pengguna ke bucket tujuan umum S3

> **Important**
>
> Pada 12 Maret 2024, judul kontrol ini berubah menjadi judul yang ditampilkan. Untuk informasi selengkapnya, lihat Ubah log untuk kontrol Security Hub.

Persyaratan terkait: Nist.800-53.r5 AC-2 (1), Nist.800-53.r5 AC-3, Nist.800-53.r5 AC-3 (15), Nist.800-53.r5 AC-3 (7), Nist.800-53.r5 AC-6

Kategori: Lindungi > Manajemen akses yang aman > Kontrol akses

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::S3::Bucket`

AWS Config aturan: **`s3-bucket-acl-prohibited`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah bucket tujuan umum Amazon S3 menyediakan izin pengguna dengan daftar kontrol akses (ACL). Kontrol gagal jika ACL dikonfigurasi untuk mengelola akses pengguna di bucket.

ACL adalah mekanisme kontrol akses lama yang mendahului IAM. Alih-alih ACL, sebaiknya gunakan kebijakan bucket S3 atau kebijakan AWS Identity and Access Management (IAM) untuk mengelola akses ke bucket S3 Anda.

Remediasi

Untuk melewati kontrol ini, Anda harus menonaktifkan ACL untuk bucket S3 Anda. Untuk petunjuknya, lihat Mengontrol kepemilikan objek dan menonaktifkan ACL untuk bucket Anda di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

Untuk membuat kebijakan bucket S3, lihat Menambahkan kebijakan bucket menggunakan konsol Amazon S3. Untuk membuat kebijakan pengguna IAM di bucket S3, lihat Mengontrol akses ke bucket dengan kebijakan pengguna.

[S3.13] Bucket tujuan umum S3 harus memiliki konfigurasi Siklus Hidup

> **Important**
>
> Pada 12 Maret 2024, judul kontrol ini berubah menjadi judul yang ditampilkan. Untuk informasi selengkapnya, lihat Ubah log untuk kontrol Security Hub.

Persyaratan terkait: Nist.800-53.r5 CP-10, Nist.800-53.R5 CP-6 (2), Nist.800-53.R5 CP-9, Nist.800-53.r5 SC-5 (2), Nist.800-53.r5 SI-13 (5)

Kategori: Lindungi > Perlindungan data

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::S3::Bucket`

AWS Config aturan: **`s3-lifecycle-policy-check`**

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`targetTransitionDays`	Jumlah hari setelah pembuatan objek ketika objek dialihkan ke kelas penyimpanan tertentu	Bilangan Bulat	`1` untuk `36500`	Tidak ada nilai default
`targetExpirationDays`	Jumlah hari setelah pembuatan objek saat objek dihapus	Bilangan Bulat	`1` untuk `36500`	Tidak ada nilai default
`targetTransitionStorageClass`	Jenis kelas penyimpanan S3 tujuan	Enum	`STANDARD_IA`, `INTELLIGENT_TIERING`, `ONEZONE_IA`, `GLACIER`, `GLACIER_IR`, `DEEP_ARCHIVE`	Tidak ada nilai default

Kontrol ini memeriksa apakah bucket tujuan umum Amazon S3 memiliki konfigurasi Siklus Hidup. Kontrol gagal jika bucket tidak memiliki konfigurasi Siklus Hidup. Jika Anda memberikan nilai kustom untuk satu atau beberapa parameter sebelumnya, kontrol hanya akan diteruskan jika kebijakan menyertakan kelas penyimpanan, waktu penghapusan, atau waktu transisi yang ditentukan.

Membuat konfigurasi Siklus Hidup untuk bucket S3 menentukan tindakan yang ingin dilakukan Amazon S3 selama masa pakai objek. Misalnya, Anda dapat mentransisikan objek ke kelas penyimpanan lain, mengarsipkannya, atau menghapusnya setelah jangka waktu tertentu.

Remediasi

Untuk informasi tentang mengonfigurasi kebijakan siklus hidup di bucket Amazon S3, lihat Menyetel konfigurasi siklus hidup di bucket dan lihat Mengelola siklus hidup penyimpanan di Panduan Pengguna Amazon S3.

[S3.14] Bucket tujuan umum S3 harus mengaktifkan versi

> **Important**
>
> Pada 12 Maret 2024, judul kontrol ini berubah menjadi judul yang ditampilkan. Untuk informasi selengkapnya, lihat Ubah log untuk kontrol Security Hub.

Kategori: Lindungi > Perlindungan data > Perlindungan penghapusan data

Persyaratan terkait: Nist.800-53.r5 AU-9 (2), Nist.800-53.r5 CP-10, Nist.800-53.r5 CP-6, Nist.800-53.r5 CP-6 (1), Nist.800-53.r5 CP-6 (2), Nist.800-53.r5 CP-9, Nist.800-800-53.R5 SC-5 (2), NIST.800-53.R5 SI-12, NIST.800-53.R5 SI-13 (5)

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::S3::Bucket`

AWS Config aturan: **`s3-bucket-versioning-enabled`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah bucket tujuan umum Amazon S3 mengaktifkan versi. Kontrol gagal jika pembuatan versi ditangguhkan untuk bucket.

Pembuatan versi menyimpan beberapa varian objek dalam bucket S3 yang sama. Anda dapat menggunakan pembuatan versi untuk mempertahankan, mengambil, dan memulihkan versi sebelumnya dari objek yang disimpan di bucket S3 Anda. Pembuatan versi membantu Anda pulih dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

> **Tip**
>
> Karena jumlah objek bertambah dalam bucket karena pembuatan versi, Anda dapat mengatur konfigurasi Siklus Hidup untuk mengarsipkan atau menghapus objek berversi secara otomatis berdasarkan aturan. Untuk informasi selengkapnya, lihat Manajemen Siklus Hidup Amazon S3 untuk Objek Berversi.

Remediasi

Untuk menggunakan pembuatan versi pada bucket S3, lihat Mengaktifkan pembuatan versi pada bucket di Panduan Pengguna Amazon S3.

[S3.15] Bucket tujuan umum S3 harus mengaktifkan Object Lock

> **Important**
>
> Pada 12 Maret 2024, judul kontrol ini berubah menjadi judul yang ditampilkan. Untuk informasi selengkapnya, lihat Ubah log untuk kontrol Security Hub.

Kategori: Lindungi > Perlindungan data > Perlindungan penghapusan data

Persyaratan terkait: Nist.800-53.r5 CP-6 (2)

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::S3::Bucket`

AWS Config aturan: **`s3-bucket-default-lock-enabled`**

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`mode`	Mode retensi Kunci Objek S3	Enum	`GOVERNANCE` ,	Tidak ada nilai default

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
			`COMPLIANCE`	

Kontrol ini memeriksa apakah bucket tujuan umum Amazon S3 mengaktifkan Object Lock. Kontrol gagal jika Object Lock tidak diaktifkan untuk bucket. Jika Anda memberikan nilai kustom untuk `mode` parameter, kontrol hanya akan diteruskan jika S3 Object Lock menggunakan mode retensi yang ditentukan.

Anda dapat menggunakan S3 Object Lock untuk menyimpan objek menggunakan model write-once-read-many (WORM). Object Lock dapat membantu mencegah objek di bucket S3 dihapus atau ditimpa untuk jangka waktu tertentu atau tanpa batas waktu. Anda dapat menggunakan S3 Object Lock untuk memenuhi persyaratan peraturan yang memerlukan penyimpanan WORM, atau menambahkan lapisan perlindungan tambahan terhadap perubahan dan penghapusan objek.

Remediasi

Untuk mengonfigurasi Object Lock untuk bucket S3 baru dan yang sudah ada, lihat Mengonfigurasi Kunci Objek S3 di Panduan Pengguna Amazon S3.

[S3.17] Ember tujuan umum S3 harus dienkripsi saat istirahat AWS KMS keys

> **Important**
>
> Pada 12 Maret 2024, judul kontrol ini berubah menjadi judul yang ditampilkan. Untuk informasi selengkapnya, lihat Ubah log untuk kontrol Security Hub.

Kategori: Lindungi > Perlindungan Data > Enkripsi data-at-rest

Persyaratan terkait: Nist.800-53.r5 SC-12 (2), NIST.800-53.R5 CM-3 (6), Nist.800-53.r5 SC-13, Nist.800-53.r5 SC-28, Nist.800-53.r5 SC-28 (1), Nist.800-53.r5 SC-7 (10), Nist.800-53.r5 SC-7 (10), Nist.800-53.r5 SC-7 (10), Nist.800-53.r5 SC-7 (10), Nist.800-53.r5 SC-7 (10), Nist.800-53.r5 SC-7 (10), Nist.800-53.r5 SC-7 (10), ST.800-53.R5 CA-9 (1), NIST.800-53.R5 SI-7 (6), NIST.800-53.R5 AU-9

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::S3::Bucket`

AWS Config aturan: **`s3-default-encryption-kms`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah bucket tujuan umum Amazon S3 dienkripsi dengan (SSE-KMS atau AWS KMS key DSSE-KMS). Kontrol gagal jika bucket dienkripsi dengan enkripsi default (SSE-S3).

Server-side encryption (SSE) adalah enkripsi data di tujuannya oleh aplikasi atau layanan yang menerimanya. Kecuali Anda menentukan sebaliknya, bucket S3 menggunakan kunci terkelola Amazon S3 (SSE-S3) secara default untuk enkripsi sisi server. Namun, untuk kontrol tambahan, Anda dapat memilih untuk mengonfigurasi bucket untuk menggunakan enkripsi sisi server dengan AWS KMS keys (SSE-KMS atau DSSE-KMS) sebagai gantinya. Amazon S3 mengenkripsi data Anda pada tingkat objek saat menulisnya ke disk di pusat AWS data dan mendekripsi untuk Anda saat Anda mengaksesnya.

Remediasi

Untuk mengenkripsi bucket S3 menggunakan SSE-KMS, lihat Menentukan enkripsi sisi server dengan (SSE-KMS) di Panduan Pengguna Amazon AWS KMS S3. Untuk mengenkripsi bucket S3 menggunakan DSSE-KMS, lihat Menentukan enkripsi sisi server dua lapis dengan (AWS KMS keys DSSE-KMS) di Panduan Pengguna Amazon S3.

[S3.19] Titik akses S3 harus mengaktifkan pengaturan akses publik blok

Persyaratan terkait: Nist.800-53.r5 AC-21, Nist.800-53.r5 AC-3, Nist.800-53.r5 AC-3 (7), Nist.800-53.r5 AC-4, Nist.800-53.r5 AC-4 (21), Nist.800-53.r5 AC-6, Nist.800-53.r5 R5 SC-7, Nist.800-53.r5 SC-7 (11), NIST.800-53.R5 SC-7 (16), Nist.800-53.r5 SC-7 (20), Nist.800-53.r5 SC-7 (21), Nist.800-53.r5 SC-7 (3), Nist.800-53.r5 5 SC-7 (4), NIST.800-53.R5 SC-7 (9)

Kategori: Lindungi > Manajemen akses aman > Sumber daya tidak dapat diakses publik

Tingkat keparahan: Kritis

Jenis sumber daya: `AWS::S3::AccessPoint`

AWS Config aturan: **`s3-access-point-public-access-blocks`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah titik akses Amazon S3 telah mengaktifkan pengaturan akses publik blok. Kontrol gagal jika blokir pengaturan akses publik tidak diaktifkan untuk titik akses.

Fitur Akses Publik Blok Amazon S3 membantu Anda mengelola akses ke sumber daya S3 di tiga tingkatan: tingkat akun, bucket, dan titik akses. Pengaturan di setiap level dapat dikonfigurasi secara independen, memungkinkan Anda memiliki tingkat pembatasan akses publik yang berbeda untuk data Anda. Pengaturan titik akses tidak dapat secara individual mengganti pengaturan yang lebih ketat di tingkat yang lebih tinggi (level akun atau bucket yang ditetapkan ke titik akses). Sebaliknya, pengaturan pada tingkat titik akses bersifat aditif, yang berarti mereka melengkapi dan bekerja bersama pengaturan di tingkat lain. Kecuali jika Anda bermaksud jalur akses S3 dapat diakses publik, Anda harus mengaktifkan blokir pengaturan akses publik.

Remediasi

Saat ini, Amazon S3 tidak mendukung perubahan pengaturan akses publik blokir titik akses setelah titik akses dibuat. Semua pengaturan akses publik blok diaktifkan secara default saat Anda membuat titik akses baru. Kami menyarankan Anda tetap mengaktifkan semua pengaturan kecuali Anda tahu bahwa Anda memiliki kebutuhan khusus untuk menonaktifkan salah satu pengaturan tersebut. Untuk informasi selengkapnya, lihat Mengelola akses publik ke titik akses di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

[S3.20] Bucket tujuan umum S3 harus mengaktifkan penghapusan MFA

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v3.0.0/2.1.2, Tolok Ukur Yayasan CIS v1.4.0/2.1.3, Nist.800-53.r5 CA-9 (1), Nist.800-53.r5 AWS CM-2, Nist.800-53.r5 CM-2 (2), Nist.800-53.r5 CM-3, Nist.800-53.r5 SCM-3 -5 (2)

Kategori: Lindungi > Perlindungan data > Perlindungan penghapusan data

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::S3::Bucket`

AWS Config aturan: **`s3-bucket-mfa-delete-enabled`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah penghapusan autentikasi multi-faktor (MFA) diaktifkan pada bucket berversi tujuan umum Amazon S3. Kontrol gagal jika penghapusan MFA tidak diaktifkan di bucket. Kontrol tidak menghasilkan temuan untuk bucket yang memiliki konfigurasi Siklus Hidup.

Saat bekerja dengan Pembuatan Versi S3 di bucket Amazon S3, Anda dapat menambahkan lapisan keamanan lain secara opsional dengan mengonfigurasi bucket untuk mengaktifkan penghapusan MFA. Saat melakukannya, pemilik bucket harus menyertakan dua bentuk autentikasi dalam setiap permintaan untuk menghapus sebuah versi atau mengubah status Penentuan Versi bucket. MFA delete memberikan keamanan tambahan jika kredensi keamanan Anda dikompromikan. Penghapusan MFA juga dapat membantu mencegah penghapusan bucket yang tidak disengaja dengan mengharuskan pengguna yang memulai tindakan penghapusan untuk membuktikan kepemilikan fisik perangkat MFA dengan kode MFA dan menambahkan lapisan gesekan dan keamanan ekstra ke tindakan penghapusan.

> **Note**
>
> Fitur penghapusan MFA memerlukan pembuatan versi bucket sebagai dependensi. Bucket versioning adalah metode untuk menyimpan beberapa variasi objek S3 dalam bucket yang sama. Selain itu, hanya pemilik bucket yang masuk sebagai pengguna root yang dapat mengaktifkan penghapusan MFA dan melakukan tindakan penghapusan pada bucket S3.

Remediasi

Untuk mengaktifkan Pembuatan Versi S3 dan mengonfigurasi penghapusan MFA pada bucket, lihat Mengonfigurasi penghapusan MFA di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

[S3.22] Bucket tujuan umum S3 harus mencatat peristiwa penulisan tingkat objek

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v3.0.0/3.8

Kategori: Identifikasi > Logging

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::::Account`

AWS Config aturan: **`cloudtrail-all-write-s3-data-event-check`**

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah an Akun AWS memiliki setidaknya satu jejak AWS CloudTrail Multi-wilayah yang mencatat semua peristiwa data tulis untuk bucket Amazon S3. Kontrol gagal jika akun tidak memiliki jejak Multi-wilayah yang mencatat peristiwa data tulis untuk bucket S3.

Operasi tingkat objek S3, seperti,`GetObject`, dan `DeleteObjectPutObject`, disebut peristiwa data. Secara default, CloudTrail tidak mencatat peristiwa data, tetapi Anda dapat mengonfigurasi jejak untuk mencatat peristiwa data untuk bucket S3. Saat mengaktifkan pencatatan tingkat objek untuk peristiwa data tulis, Anda dapat mencatat setiap akses objek (file) individual dalam bucket S3. Mengaktifkan pencatatan tingkat objek dapat membantu Anda memenuhi persyaratan kepatuhan data, melakukan analisis keamanan komprehensif, memantau pola perilaku pengguna tertentu dalam diri Anda Akun AWS, dan mengambil tindakan pada aktivitas API tingkat objek dalam bucket S3 Anda dengan menggunakan Amazon Events. CloudWatch Kontrol ini menghasilkan `PASSED` temuan jika Anda mengonfigurasi jejak Multi-wilayah yang mencatat hanya penulisan atau semua jenis peristiwa data untuk semua bucket S3.

Remediasi

Untuk mengaktifkan pencatatan tingkat objek untuk bucket S3, lihat Mengaktifkan pencatatan CloudTrail peristiwa untuk bucket dan objek S3 di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

[S3.23] Bucket tujuan umum S3 harus mencatat peristiwa pembacaan tingkat objek

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v3.0.0/3.9

Kategori: Identifikasi > Logging

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::::Account`

AWS Config aturan: **`cloudtrail-all-read-s3-data-event-check`**

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah an Akun AWS memiliki setidaknya satu jejak AWS CloudTrail Multi-wilayah yang mencatat semua peristiwa data baca untuk bucket Amazon S3. Kontrol gagal jika akun tidak memiliki jejak Multi-wilayah yang mencatat peristiwa data baca untuk bucket S3.

Operasi tingkat objek S3, seperti,`GetObject`, dan `DeleteObjectPutObject`, disebut peristiwa data. Secara default, CloudTrail tidak mencatat peristiwa data, tetapi Anda dapat mengonfigurasi jejak untuk mencatat peristiwa data untuk bucket S3. Saat mengaktifkan pencatatan tingkat objek untuk peristiwa data baca, Anda dapat mencatat setiap akses objek (file) individual dalam bucket S3. Mengaktifkan pencatatan tingkat objek dapat membantu Anda memenuhi persyaratan kepatuhan data, melakukan analisis keamanan komprehensif, memantau pola perilaku pengguna tertentu dalam diri Anda Akun AWS, dan mengambil tindakan pada aktivitas API tingkat objek dalam bucket S3 Anda dengan menggunakan Amazon Events. CloudWatch Kontrol ini menghasilkan `PASSED` temuan jika Anda mengonfigurasi jejak Multi-wilayah yang mencatat read-only atau semua jenis peristiwa data untuk semua bucket S3.

Remediasi

Untuk mengaktifkan pencatatan tingkat objek untuk bucket S3, lihat Mengaktifkan pencatatan CloudTrail peristiwa untuk bucket dan objek S3 di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

SageMaker Kontrol Amazon

Kontrol ini terkait dengan SageMaker sumber daya.

Kontrol ini mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[SageMaker.1] Instans SageMaker notebook Amazon seharusnya tidak memiliki akses internet langsung

Persyaratan terkait: PCI DSS v3.2.1/1.2.1, PCI DSS v3.2.1/1.3.1, PCI DSS v3.2.1/1.3.2, PCI DSS v3.2.1/1.3.4, PCI DSS v3.2.1/1.3.6, Nist.800-53.R5 AC-21, Nist.800-53.r5 AC-3, Nist.800-53.r5 5 AC-3 (7), NIST.800-53.R5 AC-4, NIST.800-53.R5 AC-4 (21), Nist.800-53.r5 AC-6, Nist.800-53.r5 SC-7, Nist.800-53.r5 SC-7 (11), Nist.800-53.r5 SC-7 (16), Nist.800-53.r5 SC-7 (20), NIST.800-53.R5 SC-7 (21), Nist.800-53.r5 SC-7 (3), Nist.800-53.r5 SC-7 (4), Nist.800-53.r5 SC-7 (9)

Kategori: Lindungi > Konfigurasi jaringan aman

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::SageMaker::NotebookInstance`

AWS Config aturan: **`sagemaker-notebook-no-direct-internet-access`**

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah akses internet langsung dinonaktifkan untuk instance SageMaker notebook. Kontrol gagal jika `DirectInternetAccess` bidang diaktifkan untuk instance notebook.

Jika Anda mengonfigurasi SageMaker instans Anda tanpa VPC, maka secara default akses internet langsung diaktifkan pada instans Anda. Anda harus mengonfigurasi instans Anda dengan VPC dan mengubah pengaturan default menjadi Nonaktifkan — Akses internet melalui VPC. Untuk melatih atau meng-host model dari notebook, Anda memerlukan akses internet. Untuk mengaktifkan akses internet, VPC Anda harus memiliki antarmuka endpoint (AWS PrivateLink) atau gateway NAT dan grup keamanan yang memungkinkan koneksi keluar. Untuk mempelajari lebih lanjut tentang cara menghubungkan instans notebook ke sumber daya di VPC, lihat Menyambungkan instans notebook ke sumber daya di VPC di Panduan Pengembang Amazon. SageMaker Anda juga harus memastikan bahwa akses ke SageMaker konfigurasi Anda terbatas hanya untuk pengguna yang berwenang. Batasi izin IAM yang memungkinkan pengguna mengubah SageMaker pengaturan dan sumber daya.

Remediasi

Anda tidak dapat mengubah setelan akses internet setelah membuat instance notebook. Sebagai gantinya, Anda dapat menghentikan, menghapus, dan membuat ulang instance dengan akses internet yang diblokir. Untuk menghapus instance notebook yang mengizinkan akses internet langsung, lihat Menggunakan instance notebook untuk membuat model: Bersihkan di Panduan SageMaker Pengembang Amazon. Untuk membuat ulang instance notebook yang menolak akses internet, lihat Membuat instance notebook. Untuk Jaringan, akses internet langsung, pilih Nonaktifkan — Akses internet melalui VPC.

[SageMaker.2] instance SageMaker notebook harus diluncurkan dalam VPC khusus

Persyaratan terkait: Nist.800-53.r5 AC-21, Nist.800-53.r5 AC-3, Nist.800-53.r5 AC-3 (7), Nist.800-53.r5 AC-4, Nist.800-53.r5 AC-4 (21), Nist.800-53.r5 AC-6, Nist.800-53.r5 R5 SC-7, Nist.800-53.r5 SC-7 (11), NIST.800-53.R5 SC-7 (16), Nist.800-53.r5 SC-7 (20), Nist.800-53.r5 SC-7 (21), Nist.800-53.r5 SC-7 (3), Nist.800-53.r5 5 SC-7 (4), NIST.800-53.R5 SC-7 (9)

Kategori: Lindungi > Konfigurasi jaringan aman> Sumber daya dalam VPC

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::SageMaker::NotebookInstance`

AWS Config aturan: **`sagemaker-notebook-instance-inside-vpc`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah instance SageMaker notebook Amazon diluncurkan dalam cloud pribadi virtual kustom (VPC). Kontrol ini gagal jika instance SageMaker notebook tidak diluncurkan dalam VPC kustom atau jika diluncurkan di SageMaker VPC layanan.

Subnet adalah berbagai alamat IP dalam VPC. Sebaiknya simpan sumber daya Anda di dalam VPC kustom bila memungkinkan untuk memastikan perlindungan jaringan yang aman dari infrastruktur Anda. VPC Amazon adalah jaringan virtual yang didedikasikan untuk Anda. Akun AWS Dengan Amazon VPC, Anda dapat mengontrol akses jaringan dan konektivitas internet instans SageMaker Studio dan notebook Anda.

Remediasi

Anda tidak dapat mengubah pengaturan VPC setelah membuat instance notebook. Sebagai gantinya, Anda dapat menghentikan, menghapus, dan membuat ulang instance. Untuk petunjuknya, lihat Menggunakan instance notebook untuk membuat model: Bersihkan di Panduan SageMaker Pengembang Amazon.

[SageMaker.3] Pengguna seharusnya tidak memiliki akses root ke instance SageMaker notebook

Persyaratan terkait: Nist.800-53.r5 AC-2 (1), Nist.800-53.r5 AC-3 (15), Nist.800-53.r5 AC-3 (7), Nist.800-53.r5 AC-6, Nist.800-53.r5 AC-6 (10), Nist.800-53.r5 AC-6 (2)

Kategori: Lindungi > Manajemen akses aman > Pembatasan akses pengguna root

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::SageMaker::NotebookInstance`

AWS Config aturan: **`sagemaker-notebook-instance-root-access-check`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah akses root diaktifkan untuk instance SageMaker notebook Amazon. Kontrol gagal jika akses root dihidupkan untuk instance SageMaker notebook.

Sesuai dengan prinsip hak istimewa terkecil, ini adalah praktik terbaik keamanan yang disarankan untuk membatasi akses root ke sumber daya instans untuk menghindari izin penyediaan secara tidak sengaja.

Remediasi

Untuk membatasi akses root ke instance SageMaker notebook, lihat Mengontrol akses root ke instance SageMaker notebook di Panduan SageMaker Pengembang Amazon.

[SageMaker.4] varian produksi SageMaker titik akhir harus memiliki jumlah instance awal yang lebih besar dari 1

Persyaratan terkait: Nist.800-53.r5 CP-10, Nist.800-53.r5 SC-5, Nist.800-53.R5 SC-36, Nist.800-53.r5 SA-13

Kategori: Pulihkan > Ketahanan > Ketersediaan tinggi

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::SageMaker::EndpointConfig`

AWS Config aturan: **`sagemaker-endpoint-config-prod-instance-count`**

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah varian produksi SageMaker endpoint Amazon memiliki jumlah instans awal yang lebih besar dari 1. Kontrol gagal jika varian produksi titik akhir hanya memiliki 1 instance awal.

Varian produksi yang berjalan dengan jumlah instans lebih dari 1 mengizinkan redundansi instans Multi-AZ yang dikelola oleh. SageMaker Menyebarkan sumber daya di beberapa Availability Zone adalah praktik AWS terbaik untuk menyediakan ketersediaan tinggi dalam arsitektur Anda. Ketersediaan tinggi membantu Anda pulih dari insiden keamanan.

> **Note**
>
> Kontrol ini hanya berlaku untuk konfigurasi endpoint berbasis instance.

Remediasi

Untuk informasi selengkapnya tentang parameter konfigurasi titik akhir, lihat Membuat konfigurasi titik akhir di Panduan SageMaker Pengembang Amazon.

AWS Secrets Manager kontrol

Kontrol ini terkait dengan sumber daya Secrets Manager.

Kontrol ini mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[SecretsManager.1] Rahasia Secrets Manager harus mengaktifkan rotasi otomatis

Persyaratan terkait: Nist.800-53.r5 AC-2 (1), Nist.800-53.r5 AC-3 (15)

Kategori: Lindungi > Pengembangan aman

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::SecretsManager::Secret`

AWS Config aturan: **`secretsmanager-rotation-enabled-check`**

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`maximumAllowedRota`	Jumlah hari maksimum yang diizinkan untuk frekuensi rotasi rahasia	Bilangan Bulat	1 untuk 365	Tidak ada nilai default

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`tionFrequency`				

Kontrol ini memeriksa apakah rahasia yang disimpan AWS Secrets Manager dikonfigurasi dengan rotasi otomatis. Kontrol gagal jika rahasia tidak dikonfigurasi dengan rotasi otomatis. Jika Anda memberikan nilai khusus untuk `maximumAllowedRotationFrequency` parameter, kontrol hanya akan berlalu jika rahasia diputar secara otomatis dalam jendela waktu yang ditentukan.

Secrets Manager membantu Anda meningkatkan postur keamanan organisasi Anda. Rahasia mencakup kredensyal basis data, kata sandi, dan kunci API pihak ketiga. Anda dapat menggunakan Secrets Manager untuk menyimpan rahasia secara terpusat, mengenkripsi rahasia secara otomatis, mengontrol akses ke rahasia, dan memutar rahasia dengan aman dan otomatis.

Secrets Manager dapat memutar rahasia. Anda dapat menggunakan rotasi untuk mengganti rahasia jangka panjang dengan rahasia jangka pendek. Memutar rahasia Anda membatasi berapa lama pengguna yang tidak sah dapat menggunakan rahasia yang disusupi. Untuk alasan ini, Anda harus sering memutar rahasia Anda. Untuk mempelajari lebih lanjut tentang rotasi, lihat Memutar AWS Secrets Manager rahasia Anda di Panduan AWS Secrets Manager Pengguna.

Remediasi

Untuk mengaktifkan rotasi otomatis rahasia Secrets Manager, lihat Mengatur rotasi otomatis untuk AWS Secrets Manager rahasia menggunakan konsol di Panduan AWS Secrets Manager Pengguna. Anda harus memilih dan mengkonfigurasi AWS Lambda fungsi untuk rotasi.

[SecretsManager.2] Rahasia Secrets Manager yang dikonfigurasi dengan rotasi otomatis harus berhasil diputar

Persyaratan terkait: Nist.800-53.r5 AC-2 (1), Nist.800-53.r5 AC-3 (15)

Kategori: Lindungi > Pengembangan aman

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::SecretsManager::Secret`

AWS Config aturan: **`secretsmanager-scheduled-rotation-success-check`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah AWS Secrets Manager rahasia berhasil diputar berdasarkan jadwal rotasi. Kontrol gagal jika `RotationOccurringAsScheduled` ada`false`. Kontrol hanya mengevaluasi rahasia yang telah dihidupkan rotasi.

Secrets Manager membantu Anda meningkatkan postur keamanan organisasi Anda. Rahasia mencakup kredensyal basis data, kata sandi, dan kunci API pihak ketiga. Anda dapat menggunakan Secrets Manager untuk menyimpan rahasia secara terpusat, mengenkripsi rahasia secara otomatis, mengontrol akses ke rahasia, dan memutar rahasia dengan aman dan otomatis.

Secrets Manager dapat memutar rahasia. Anda dapat menggunakan rotasi untuk mengganti rahasia jangka panjang dengan rahasia jangka pendek. Memutar rahasia Anda membatasi berapa lama pengguna yang tidak sah dapat menggunakan rahasia yang disusupi. Untuk alasan ini, Anda harus sering memutar rahasia Anda.

Selain mengonfigurasi rahasia untuk diputar secara otomatis, Anda harus memastikan bahwa rahasia tersebut berhasil diputar berdasarkan jadwal rotasi.

Untuk mempelajari lebih lanjut tentang rotasi, lihat Memutar AWS Secrets Manager rahasia Anda di Panduan AWS Secrets Manager Pengguna.

Remediasi

Jika rotasi otomatis gagal, maka Secrets Manager mungkin mengalami kesalahan dengan konfigurasi. Untuk memutar rahasia di Secrets Manager, Anda menggunakan fungsi Lambda yang mendefinisikan cara berinteraksi dengan database atau layanan yang memiliki rahasia.

Untuk bantuan mendiagnosis dan memperbaiki kesalahan umum yang terkait dengan rotasi rahasia, lihat Memecahkan masalah AWS Secrets Manager rotasi rahasia di Panduan Pengguna.AWS Secrets Manager

[SecretsManager.3] Hapus rahasia Secrets Manager yang tidak digunakan

Persyaratan terkait: Nist.800-53.r5 AC-2 (1), Nist.800-53.r5 AC-3 (15)

Kategori: Lindungi > Manajemen akses yang aman

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::SecretsManager::Secret`

AWS Config aturan: **`secretsmanager-secret-unused`**

Jenis jadwal: Periodik

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`unusedForDays`	Jumlah hari maksimum yang rahasia dapat tetap tidak digunakan	Bilangan Bulat	1 untuk 365	90

Kontrol ini memeriksa apakah AWS Secrets Manager rahasia telah diakses dalam jangka waktu yang ditentukan. Kontrol gagal jika rahasia tidak digunakan di luar kerangka waktu yang ditentukan. Kecuali Anda memberikan nilai parameter khusus untuk periode akses, Security Hub menggunakan nilai default 90 hari.

Menghapus rahasia yang tidak digunakan sama pentingnya dengan memutar rahasia. Rahasia yang tidak digunakan dapat disalahgunakan oleh mantan pengguna mereka, yang tidak lagi membutuhkan akses ke rahasia ini. Selain itu, karena semakin banyak pengguna mendapatkan akses ke rahasia, seseorang mungkin salah menangani dan membocorkannya ke entitas yang tidak sah, yang meningkatkan risiko penyalahgunaan. Menghapus rahasia yang tidak digunakan membantu mencabut akses rahasia dari pengguna yang tidak lagi membutuhkannya. Ini juga membantu mengurangi biaya penggunaan Secrets Manager. Oleh karena itu, penting untuk secara rutin menghapus rahasia yang tidak digunakan.

Remediasi

Untuk menghapus rahasia Secrets Manager yang tidak aktif, lihat Menghapus AWS Secrets Manager rahasia di Panduan AWS Secrets Manager Pengguna.

[SecretsManager.4] Rahasia Secrets Manager harus diputar dalam jumlah hari tertentu

Persyaratan terkait: Nist.800-53.r5 AC-2 (1), Nist.800-53.r5 AC-3 (15)

Kategori: Lindungi > Manajemen akses yang aman

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::SecretsManager::Secret`

AWS Config aturan: **`secretsmanager-secret-periodic-rotation`**

Jenis jadwal: Periodik

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`maxDaysSinceRotation`	Jumlah hari maksimum yang rahasia dapat tetap tidak berubah	Bilangan Bulat	1 untuk `180`	`90`

Kontrol ini memeriksa apakah sebuah AWS Secrets Manager rahasia diputar setidaknya sekali dalam jangka waktu yang ditentukan. Kontrol gagal jika rahasia tidak diputar setidaknya ini sering. Kecuali Anda memberikan nilai parameter khusus untuk periode rotasi, Security Hub menggunakan nilai default 90 hari.

Rahasia berputar dapat membantu Anda mengurangi risiko penggunaan rahasia Anda yang tidak sah dalam diri Anda. Akun AWS Contohnya termasuk kredensi basis data, kata sandi, kunci API pihak ketiga, dan bahkan teks arbitrer. Jika Anda tidak mengubah rahasia Anda untuk jangka waktu yang lama, rahasianya lebih mungkin dikompromikan.

Karena semakin banyak pengguna mendapatkan akses ke rahasia, kemungkinan besar seseorang salah menangani dan membocorkannya ke entitas yang tidak sah. Rahasia dapat dibocorkan melalui log dan data cache. Mereka dapat dibagikan untuk tujuan debugging dan tidak diubah atau dicabut setelah debugging selesai. Untuk semua alasan ini, rahasia harus sering diputar.

Anda dapat mengonfigurasi rotasi otomatis untuk rahasia di AWS Secrets Manager. Dengan rotasi otomatis, Anda dapat mengganti rahasia jangka panjang dengan rahasia jangka pendek, secara signifikan mengurangi risiko kompromi. Kami menyarankan Anda mengonfigurasi rotasi otomatis

untuk rahasia Secrets Manager Anda. Untuk informasi selengkapnya, lihat Memutar rahasia AWS Secrets Manager Anda di Panduan Pengguna AWS Secrets Manager .

Remediasi

Untuk mengaktifkan rotasi otomatis rahasia Secrets Manager, lihat Mengatur rotasi otomatis untuk AWS Secrets Manager rahasia menggunakan konsol di Panduan AWS Secrets Manager Pengguna. Anda harus memilih dan mengkonfigurasi AWS Lambda fungsi untuk rotasi.

[SecretsManager.5] Rahasia Secrets Manager harus diberi tag

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::SecretsManager::Secret`

AWS Config aturan: `tagged-secretsmanager-secret` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList	Daftar tag yang memenuhi AWS persyaratan	`No default value`

Kontrol ini memeriksa apakah AWS Secrets Manager rahasia memiliki tag dengan kunci tertentu yang ditentukan dalam parameter`requiredTagKeys`. Kontrol gagal jika rahasia tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika rahasia tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke rahasia Secrets Manager, lihat Menandai AWS Secrets Manager rahasia di Panduan AWS Secrets Manager Pengguna.

AWS Service Catalog kontrol

Kontrol ini terkait dengan sumber daya Service Catalog.

Kontrol ini mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[ServiceCatalog.1] Portofolio Service Catalog harus dibagikan hanya dalam suatu organisasi AWS

Persyaratan terkait: Nist.800-53.r5 AC-3, Nist.800-53.r5 AC-4, Nist.800-53.r5 AC-6, Nist.800-53.r5 CM-8, Nist.800-53.r5 SC-7

Kategori: Lindungi > Manajemen akses yang aman

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::ServiceCatalog::Portfolio`

AWS Config aturan: **`servicecatalog-shared-within-organization`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah AWS Service Catalog berbagi portofolio dalam organisasi saat integrasi dengan AWS Organizations diaktifkan. Kontrol gagal jika portofolio tidak dibagikan dalam organisasi.

Berbagi portofolio hanya dalam Organizations membantu memastikan bahwa portofolio tidak dibagikan dengan salah Akun AWS. Untuk membagikan portofolio Service Catalog dengan akun di organisasi, Security Hub merekomendasikan penggunaan `ORGANIZATION_MEMBER_ACCOUNT` sebagai gantinya`ACCOUNT`. Ini menyederhanakan administrasi dengan mengatur akses yang diberikan ke akun di seluruh organisasi. Jika Anda memiliki kebutuhan bisnis untuk berbagi portofolio Service Catalog dengan akun eksternal, Anda dapat secara otomatis menekan temuan dari kontrol ini atau menonaktifkannya.

Remediasi

Untuk mengaktifkan berbagi portofolio dengan Organizations, lihat Berbagi dengan AWS Organizations di Panduan Administrator Service Catalog

Kontrol Layanan Email Sederhana Amazon

Kontrol ini terkait dengan sumber daya Amazon SES.

Kontrol ini mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[SES.1] Daftar kontak SES harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::SES::ContactList`

AWS Config aturan: `tagged-ses-contactlist` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList	Daftar tag yang memenuhi AWS persyaratan	Tidak ada nilai default

Kontrol ini memeriksa apakah daftar kontak Amazon SES memiliki tag dengan kunci tertentu yang ditentukan dalam parameter`requiredTagKeys`. Kontrol gagal jika daftar kontak tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika daftar kontak tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS

Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke daftar kontak Amazon SES, lihat TagResourcedi Referensi Amazon SES API v2.

[SES.2] Set konfigurasi SES harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::SES::ConfigurationSet`

AWS Config aturan: `tagged-ses-configurationset` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList	Daftar tag yang memenuhi AWS persyaratan	Tidak ada nilai default

Kontrol ini memeriksa apakah set konfigurasi Amazon SES memiliki tag dengan kunci spesifik yang ditentukan dalam parameter`requiredTagKeys`. Kontrol gagal jika set konfigurasi tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika set konfigurasi tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke set konfigurasi Amazon SES, lihat TagResourcedi Referensi Amazon SES API v2.

Kontrol Layanan Pemberitahuan Sederhana Amazon

Kontrol ini terkait dengan sumber daya Amazon SNS.

Kontrol ini mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[SNS.1] Topik SNS harus dienkripsi saat istirahat menggunakan AWS KMS

> **Important**
>
> Security Hub menghentikan kontrol ini pada April 2024 dari standar Praktik Terbaik Keamanan AWS Dasar, tetapi masih termasuk dalam standar NIST SP 800-53 Rev. 5. Untuk informasi selengkapnya, lihat Ubah log untuk kontrol Security Hub.

Persyaratan terkait: Nist.800-53.r5 CA-9 (1), NIST.800-53.R5 CM-3 (6), Nist.800-53.r5 SC-13, Nist.800-53.r5 SC-28, Nist.800-53.r5 SC-28 (1), Nist.800-53.r5 SC-7 (10), Nist.800-53.r5 SC-7 (10), Nist.800-53.r5 SC-7 (10), Nist.800-53.r5 SC-7 (10), Nist.800-53.r5 SC-7 (10), Nist.800-53.r5 SC-7 (10), Nist.800-53.r5 SC-7 (10), ST.800-53.R5 SI-7 (6)

Kategori: Lindungi > Perlindungan Data > Enkripsi data-at-rest

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::SNS::Topic`

AWS Config aturan: **`sns-encrypted-kms`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah topik Amazon SNS dienkripsi saat istirahat menggunakan kunci yang dikelola di (). AWS Key Management Service AWS KMS Kontrol gagal jika topik SNS tidak menggunakan kunci KMS untuk enkripsi sisi server (SSE). Secara default, SNS menyimpan pesan dan file menggunakan enkripsi disk. Untuk melewati kontrol ini, Anda harus memilih untuk menggunakan kunci KMS untuk enkripsi sebagai gantinya. Ini menambahkan lapisan keamanan tambahan dan memberikan lebih banyak fleksibilitas kontrol akses.

Mengenkripsi data saat istirahat mengurangi risiko data yang disimpan pada disk diakses oleh pengguna yang tidak diautentikasi. AWS Izin API diperlukan untuk mendekripsi data sebelum dapat dibaca. Kami merekomendasikan mengenkripsi topik SNS dengan kunci KMS untuk lapisan keamanan tambahan.

Remediasi

Untuk mengaktifkan SSE untuk topik SNS, lihat Mengaktifkan enkripsi sisi server (SSE) untuk topik Amazon SNS di Panduan Pengembang Layanan Pemberitahuan Sederhana Amazon. Sebelum Anda dapat menggunakan SSE, Anda juga harus mengonfigurasi AWS KMS key kebijakan untuk mengizinkan enkripsi topik dan enkripsi dan dekripsi pesan. Untuk informasi selengkapnya, lihat Mengonfigurasi AWS KMS izin di Panduan Pengembang Layanan Pemberitahuan Sederhana Amazon.

[SNS.2] Pencatatan status pengiriman harus diaktifkan untuk pesan notifikasi yang dikirim ke suatu topik

> **Important**
>
> Security Hub menghentikan kontrol ini pada April 2024. Untuk informasi selengkapnya, lihat Ubah log untuk kontrol Security Hub.

Persyaratan terkait: Nist.800-53.r5 AU-12, Nist.800-53.r5 AU-2

Kategori: Identifikasi > Logging

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::SNS::Topic`

AWS Config aturan: **`sns-topic-message-delivery-notification-enabled`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah pencatatan diaktifkan untuk status pengiriman pesan notifikasi yang dikirim ke topik Amazon SNS untuk titik akhir. Kontrol ini gagal jika pemberitahuan status pengiriman pesan tidak diaktifkan.

Logging adalah bagian penting dalam menjaga keandalan, ketersediaan, dan kinerja layanan. Mencatat status pengiriman pesan membantu memberikan wawasan operasional, seperti berikut ini:

- Mengetahui apakah pesan dikirim ke titik akhir Amazon SNS.
- Mengidentifikasi respon yang dikirim dari titik akhir Amazon SNS ke Amazon SNS.
- Menentukan waktu tinggal pesan (waktu antara stempel waktu publikasi dan penyerahan ke titik akhir Amazon SNS).

Remediasi

Untuk mengonfigurasi pencatatan status pengiriman untuk suatu topik, lihat Status pengiriman pesan Amazon SNS di Panduan Pengembang Layanan Pemberitahuan Sederhana Amazon.

[SNS.3] Topik SNS harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::SNS::Topic`

AWS Config aturan: `tagged-sns-topic` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList	Daftar tag yang memenuhi AWS persyaratan	`No default value`

Kontrol ini memeriksa apakah topik Amazon SNS memiliki tag dengan kunci tertentu yang ditentukan dalam parameter. `requiredTagKeys` Kontrol gagal jika topik tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika topik tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang

bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke topik SNS, lihat Mengonfigurasi tag topik Amazon SNS di Panduan Pengembang Layanan Pemberitahuan Sederhana Amazon.

Kontrol Layanan Antrian Sederhana Amazon

Kontrol ini terkait dengan sumber daya Amazon SQS.

Kontrol ini mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[SQS.1] Antrian Amazon SQS harus dienkripsi saat istirahat

Persyaratan terkait: Nist.800-53.r5 CA-9 (1), NIST.800-53.R5 CM-3 (6), Nist.800-53.r5 SC-13, Nist.800-53.r5 SC-28, Nist.800-53.r5 SC-28 (1), Nist.800-53.r5 SC-7 (10), Nist.800-53.r5 SC-7 (10), Nist.800-53.r5 SC-7 (10), Nist.800-53.r5 SC-7 (10), Nist.800-53.r5 SC-7 (10), Nist.800-53.r5 SC-7 (10), Nist.800-53.r5 SC-7 (10), ST.800-53.R5 SI-7 (6)

Kategori: Lindungi > Perlindungan Data > Enkripsi data-at-rest

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::SQS::Queue`

AWS Config aturan: `sqs-queue-encrypted` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah antrian Amazon SQS dienkripsi saat istirahat. Kontrol gagal jika antrian tidak dienkripsi dengan kunci yang dikelola SQS (SSE-SQS) atau kunci () (SSE-KMS). AWS Key Management Service AWS KMS

Mengenkripsi data saat istirahat mengurangi risiko pengguna yang tidak sah mengakses data yang disimpan di disk. Enkripsi sisi server (SSE) melindungi isi pesan dalam antrian SQS menggunakan kunci enkripsi yang dikelola SQS (SSE-SQS) atau kunci (SSE-KMS). AWS KMS

Remediasi

Untuk mengonfigurasi SSE untuk antrean SQS, lihat Mengonfigurasi enkripsi sisi server (SSE) untuk antrian (konsol) di Panduan Pengembang Layanan Antrian Sederhana Amazon.

[SQS.2] Antrian SQS harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::SQS::Queue`

AWS Config aturan: `tagged-sqs-queue` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList	Daftar tag yang memenuhi AWS persyaratan	`No default value`

Kontrol ini memeriksa apakah antrian Amazon SQS memiliki tag dengan kunci tertentu yang ditentukan dalam parameter. `requiredTagKeys` Kontrol gagal jika antrian tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika antrian tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke antrean yang ada menggunakan konsol Amazon SQS, lihat Mengonfigurasi tag alokasi biaya untuk antrean (konsol) Amazon SQS di Panduan Pengembang Layanan Antrian Sederhana Amazon.

AWS Step Functions kontrol

Kontrol ini terkait dengan sumber daya Step Functions.

Kontrol ini mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[StepFunctions.1] Mesin status Step Functions seharusnya mengaktifkan logging

Kategori: Identifikasi > Logging

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::StepFunctions::StateMachine`

AWS Config aturan: **`step-functions-state-machine-logging-enabled`**

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`logLevel`	Tingkat logging minimum	Enum	`ALL`, `ERROR`, `FATAL`	Tidak ada nilai default

Kontrol ini memeriksa apakah mesin AWS Step Functions status telah mengaktifkan pencatatan. Kontrol gagal jika mesin status tidak mengaktifkan logging. Jika Anda memberikan nilai khusus untuk `logLevel` parameter, kontrol hanya akan diteruskan jika mesin status mengaktifkan level logging yang ditentukan.

Pemantauan membantu Anda menjaga keandalan, ketersediaan, dan kinerja Step Functions. Anda harus mengumpulkan sebanyak mungkin data pemantauan dari Layanan AWS yang Anda gunakan sehingga Anda dapat lebih mudah men-debug kegagalan multi-titik. Memiliki konfigurasi logging yang ditentukan untuk mesin status Step Functions memungkinkan Anda melacak riwayat eksekusi dan hasil di Amazon CloudWatch Logs. Secara opsional, Anda hanya dapat melacak kesalahan atau peristiwa fatal.

Remediasi

Untuk mengaktifkan logging untuk mesin status Step Functions, lihat Mengkonfigurasi logging di Panduan AWS Step Functions Pengembang.

[StepFunctions.2] Aktivitas Step Functions harus diberi tag

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::StepFunctions::Activity`

AWS Config aturan: `tagged-stepfunctions-activity` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList	Daftar tag yang memenuhi AWS persyaratan	Tidak ada nilai default

Kontrol ini memeriksa apakah AWS Step Functions aktivitas memiliki tag dengan kunci tertentu yang ditentukan dalam parameter`requiredTagKeys`. Kontrol gagal jika aktivitas tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika aktivitas tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke

AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke aktivitas Step Functions, lihat Menandai di Step Functions di Panduan AWS Step Functions Pengembang.

AWS Transfer Family kontrol

Kontrol ini terkait dengan sumber daya Transfer Family.

Kontrol ini mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[Transfer.1] AWS Transfer Family alur kerja harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::Transfer::Workflow`

AWS Config aturan: `tagged-transfer-workflow` (aturan Security Hub khusus)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Jenis	Nilai kustom yang diizinkan	Nilai default Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList	Daftar tag yang memenuhi AWS persyaratan	`No default value`

Kontrol ini memeriksa apakah AWS Transfer Family alur kerja memiliki tag dengan kunci tertentu yang ditentukan dalam parameter`requiredTagKeys`. Kontrol gagal jika alur kerja tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika alur kerja tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke alur kerja Transfer Family (konsol)

1. Buka AWS Transfer Family konsol.
2. Pada panel navigasi, pilih Alur kerja. Kemudian, pilih alur kerja yang ingin Anda tag.
3. Pilih Kelola tag, dan tambahkan tag.

[Transfer.2] Server Transfer Family tidak boleh menggunakan protokol FTP untuk koneksi titik akhir

Persyaratan terkait: Nist.800-53.r5 CM-7, Nist.800-53.r5 IA-5, Nist.800-53.r5 SC-8

Kategori: Lindungi > Perlindungan Data > Enkripsi data-in-transit

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::Transfer::Server`

AWS Config aturan: **`transfer-family-server-no-ftp`**

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah AWS Transfer Family server menggunakan protokol selain FTP untuk koneksi endpoint. Kontrol gagal jika server menggunakan protokol FTP untuk klien untuk terhubung ke endpoint server.

FTP (File Transfer Protocol) menetapkan koneksi titik akhir melalui saluran yang tidak terenkripsi, meninggalkan data yang dikirim melalui saluran ini rentan terhadap intersepsi. Menggunakan SFTP (SSH File Transfer Protocol), FTPS (File Transfer Protocol Secure), atau AS2 (Applicability Statement 2) menawarkan lapisan keamanan ekstra dengan mengenkripsi data Anda dalam perjalanan dan dapat digunakan untuk membantu mencegah penyerang potensial menggunakan person-in-the-middle atau serangan serupa untuk menguping atau memanipulasi lalu lintas jaringan.

Remediasi

Untuk mengubah protokol server Transfer Family, lihat Mengedit protokol transfer file di AWS Transfer Family Panduan Pengguna.

AWS WAF kontrol

Kontrol ini terkait dengan AWS WAF sumber daya.

Kontrol ini mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[WAF.1] Pencatatan ACL Web Global AWS WAF Klasik harus diaktifkan

Persyaratan terkait: Nist.800-53.r5 AC-4 (26), Nist.800-53.R5 AU-10, Nist.800-53.R5 AU-12, Nist.800-53.r5 AU-2, Nist.800-53.r5 AU-3, Nist.800-53.r5 AU-6 (3), Nist.800-53.r5 AU-6 (4), NIST.800-53.R5 CA-7, NIST.800-53.R5 SC-7 (9), NIST.800-53.R5 SI-7 (8)

Kategori: Identifikasi > Logging

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::WAF::WebACL`

AWS Config aturan: **`waf-classic-logging-enabled`**

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah logging diaktifkan untuk ACL web AWS WAF global. Kontrol ini gagal jika logging tidak diaktifkan untuk ACL web.

Logging adalah bagian penting untuk menjaga keandalan, ketersediaan, dan kinerja AWS WAF global. Ini adalah persyaratan bisnis dan kepatuhan di banyak organisasi, dan memungkinkan Anda memecahkan masalah perilaku aplikasi. Ini juga memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web yang dilampirkan AWS WAF.

Remediasi

Untuk mengaktifkan pencatatan untuk ACL AWS WAF web, lihat Mencatat informasi lalu lintas ACL web di Panduan AWS WAF Pengembang.

[WAF.2] Aturan Regional AWS WAF Klasik harus memiliki setidaknya satu syarat

Persyaratan terkait: Nist.800-53.r5 AC-4 (21), Nist.800-53.R5 SC-7, Nist.800-53.R5 SC-7 (11), Nist.800-53.r5 SC-7 (16), Nist.800-53.r5 SC-7 (21)

Kategori: Lindungi > Konfigurasi jaringan aman

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::WAFRegional::Rule`

AWS Config aturan: **`waf-regional-rule-not-empty`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah aturan AWS WAF Regional memiliki setidaknya satu syarat. Kontrol gagal jika tidak ada kondisi dalam suatu aturan.

Aturan Regional WAF dapat berisi beberapa kondisi. Ketentuan aturan memungkinkan inspeksi lalu lintas dan mengambil tindakan yang ditentukan (izinkan, blokir, atau hitung). Tanpa kondisi apa pun, lalu lintas berlalu tanpa inspeksi. Aturan Regional WAF tanpa kondisi, tetapi dengan nama atau tag yang menyarankan izinkan, blokir, atau hitung, dapat menyebabkan asumsi yang salah bahwa salah satu tindakan tersebut terjadi.

Remediasi

Untuk menambahkan kondisi ke aturan kosong, lihat Menambahkan dan menghapus kondisi dalam aturan di Panduan AWS WAF Pengembang.

[WAF.3] Kelompok aturan Regional AWS WAF Klasik harus memiliki setidaknya satu aturan

Persyaratan terkait: Nist.800-53.r5 AC-4 (21), Nist.800-53.R5 SC-7, Nist.800-53.R5 SC-7 (11), Nist.800-53.r5 SC-7 (16), Nist.800-53.r5 SC-7 (21)

Kategori: Lindungi > Konfigurasi jaringan aman

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::WAFRegional::RuleGroup`

AWS Config aturan: **`waf-regional-rulegroup-not-empty`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah kelompok aturan AWS WAF Regional memiliki setidaknya satu aturan. Kontrol gagal jika tidak ada aturan dalam kelompok aturan.

Grup aturan Regional WAF dapat berisi beberapa aturan. Ketentuan aturan memungkinkan inspeksi lalu lintas dan mengambil tindakan yang ditentukan (izinkan, blokir, atau hitung). Tanpa aturan apa pun, lalu lintas berlalu tanpa inspeksi. Kelompok aturan Regional WAF tanpa aturan, tetapi dengan nama atau tag yang menyarankan izinkan, blokir, atau hitung, dapat menyebabkan asumsi yang salah bahwa salah satu tindakan tersebut terjadi.

Remediasi

Untuk menambahkan aturan dan ketentuan aturan ke grup aturan kosong, lihat Menambahkan dan menghapus aturan dari grup aturan AWS WAF Klasik serta Menambahkan dan menghapus kondisi dalam aturan di Panduan AWS WAF Pengembang.

[WAF.4] ACL web Regional AWS WAF klasik harus memiliki setidaknya satu aturan atau kelompok aturan

Persyaratan terkait: NIST.800-53.R5 CA-9 (1), NIST.800-53.R5 CM-2

Kategori: Lindungi > Konfigurasi jaringan aman

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::WAFRegional::WebACL`

AWS Config aturan: **`waf-regional-webacl-not-empty`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah ACL AWS WAF Classic Regional web berisi aturan WAF atau grup aturan WAF. Kontrol ini gagal jika ACL web tidak berisi aturan WAF atau grup aturan.

ACL web Regional WAF dapat berisi kumpulan aturan dan kelompok aturan yang memeriksa dan mengontrol permintaan web. Jika ACL web kosong, lalu lintas web dapat lewat tanpa terdeteksi atau ditindaklanjuti oleh WAF tergantung pada tindakan default.

Remediasi

Untuk menambahkan aturan atau grup aturan ke ACL web Regional AWS WAF Klasik kosong, lihat Mengedit ACL Web di Panduan AWS WAF Pengembang.

[WAF.6] Aturan global AWS WAF klasik harus memiliki setidaknya satu syarat

Persyaratan terkait: NIST.800-53.R5 CA-9 (1), NIST.800-53.R5 CM-2

Kategori: Lindungi > Konfigurasi jaringan aman

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::WAF::Rule`

AWS Config aturan: **`waf-global-rule-not-empty`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah aturan AWS WAF global berisi kondisi apa pun. Kontrol gagal jika tidak ada kondisi dalam suatu aturan.

Aturan global WAF dapat berisi beberapa kondisi. Ketentuan aturan memungkinkan inspeksi lalu lintas dan mengambil tindakan yang ditentukan (izinkan, blokir, atau hitung). Tanpa kondisi apa pun, lalu lintas berlalu tanpa inspeksi. Aturan global WAF tanpa kondisi, tetapi dengan nama atau tag yang menyarankan izinkan, blokir, atau hitung, dapat menyebabkan asumsi yang salah bahwa salah satu tindakan tersebut terjadi.

Remediasi

Untuk petunjuk cara membuat aturan dan menambahkan kondisi, lihat Membuat aturan dan menambahkan kondisi di Panduan AWS WAF Pengembang.

[WAF.7] Kelompok aturan global AWS WAF klasik harus memiliki setidaknya satu aturan

Persyaratan terkait: NIST.800-53.R5 CA-9 (1), NIST.800-53.R5 CM-2

Kategori: Lindungi > Konfigurasi jaringan aman

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::WAF::RuleGroup`

AWS Config aturan: **`waf-global-rulegroup-not-empty`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah grup aturan AWS WAF global memiliki setidaknya satu aturan. Kontrol gagal jika tidak ada aturan dalam kelompok aturan.

Grup aturan global WAF dapat berisi beberapa aturan. Ketentuan aturan memungkinkan inspeksi lalu lintas dan mengambil tindakan yang ditentukan (izinkan, blokir, atau hitung). Tanpa aturan apa pun, lalu lintas berlalu tanpa inspeksi. Grup aturan global WAF tanpa aturan, tetapi dengan nama atau tag yang menyarankan izinkan, blokir, atau hitung, dapat menyebabkan asumsi yang salah bahwa salah satu tindakan tersebut terjadi.

Remediasi

Untuk petunjuk cara menambahkan aturan ke grup aturan, lihat Membuat grup aturan AWS WAF Klasik di Panduan AWS WAF Pengembang.

[WAF.8] ACL web global AWS WAF klasik harus memiliki setidaknya satu aturan atau kelompok aturan

Persyaratan terkait: Nist.800-53.r5 AC-4 (21), Nist.800-53.R5 SC-7, Nist.800-53.R5 SC-7 (11), Nist.800-53.r5 SC-7 (16), Nist.800-53.r5 SC-7 (21)

Kategori: Lindungi > Konfigurasi jaringan aman

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::WAF::WebACL`

AWS Config aturan: **`waf-global-webacl-not-empty`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah ACL web AWS WAF global berisi setidaknya satu aturan WAF atau grup aturan WAF. Kontrol gagal jika ACL web tidak berisi aturan WAF atau grup aturan.

ACL web global WAF dapat berisi kumpulan aturan dan kelompok aturan yang memeriksa dan mengontrol permintaan web. Jika ACL web kosong, lalu lintas web dapat lewat tanpa terdeteksi atau ditindaklanjuti oleh WAF tergantung pada tindakan default.

Remediasi

Untuk menambahkan aturan atau grup aturan ke ACL web AWS WAF global yang kosong, lihat Mengedit ACL web di Panduan AWS WAF Pengembang. Untuk Filter, pilih Global (CloudFront).

[WAF.10] ACL AWS WAF web harus memiliki setidaknya satu aturan atau kelompok aturan

Persyaratan terkait: NIST.800-53.R5 CA-9 (1), NIST.800-53.R5 CM-2

Kategori: Lindungi > Konfigurasi jaringan aman

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::WAFv2::WebACL`

AWS Config aturan: **`wafv2-webacl-not-empty`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah daftar kontrol akses web AWS WAF V2 (web ACL) berisi setidaknya satu aturan atau grup aturan. Kontrol gagal jika ACL web tidak berisi aturan atau grup aturan apa pun.

ACL web memberi Anda kontrol halus atas semua permintaan web HTTP (S) yang ditanggapi oleh sumber daya Anda yang dilindungi. ACL web harus berisi kumpulan aturan dan kelompok aturan yang memeriksa dan mengontrol permintaan web. Jika ACL web kosong, lalu lintas web dapat lewat tanpa terdeteksi atau ditindaklanjuti dengan AWS WAF tergantung pada tindakan default.

Remediasi

Untuk menambahkan aturan atau grup aturan ke ACL web WAFV2 kosong, lihat Mengedit ACL Web di Panduan Pengembang.AWS WAF

[WAF.11] pencatatan ACL AWS WAF web harus diaktifkan

Persyaratan terkait: Nist.800-53.r5 AC-4 (26), Nist.800-53.R5 AU-10, Nist.800-53.R5 AU-12, Nist.800-53.r5 AU-2, Nist.800-53.r5 AU-3, Nist.800-53.r5 AU-6 (3), Nist.800-53.r5 AU-6 (4), NIST.800-53.R5 CA-7, NIST.800-53.R5 SC-7 (10), NIST.800-53.R5 SC-7 (9), NIST.800-53.R5 SI-7 (8)

Kategori: Identifikasi > Logging

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::WAFv2::WebACL`

AWS Config aturan: **`wafv2-logging-enabled`**

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah logging diaktifkan untuk daftar kontrol akses web AWS WAF V2 (web ACL). Kontrol ini gagal jika logging dinonaktifkan untuk ACL web.

Logging mempertahankan keandalan, ketersediaan, dan kinerja AWS WAF. Selain itu, penebangan adalah persyaratan bisnis dan kepatuhan di banyak organisasi. Dengan mencatat lalu lintas yang dianalisis oleh ACL web Anda, Anda dapat memecahkan masalah perilaku aplikasi.

Remediasi

Untuk mengaktifkan logging untuk ACL AWS WAF web, lihat Mengelola logging untuk ACL web di Panduan AWS WAF Pengembang.

AWS WAF Aturan [WAF.12] harus mengaktifkan metrik CloudWatch

Persyaratan terkait: Nist.800-53.r5 AC-4 (26), Nist.800-53.R5 AU-10, Nist.800-53.R5 AU-12, Nist.800-53.r5 AU-2, Nist.800-53.r5 AU-3, Nist.800-53.r5 AU-6 (3), Nist.800-53.r5 AU-6 (4), NIST.800-53.R5 CA-7, NIST.800-53.R5 SC-7 (10), NIST.800-53.R5 SC-7 (9), NIST.800-53.R5 SI-7 (8)

Kategori: Identifikasi > Logging

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::WAFv2::RuleGroup`

AWS Config aturan: **`wafv2-rulegroup-logging-enabled`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah AWS WAF aturan atau grup aturan mengaktifkan CloudWatch metrik Amazon. Kontrol gagal jika aturan atau grup aturan tidak mengaktifkan CloudWatch metrik.

Mengkonfigurasi CloudWatch metrik pada AWS WAF aturan dan grup aturan memberikan visibilitas ke arus lalu lintas. Anda dapat melihat aturan ACL mana yang dipicu dan permintaan mana yang diterima dan diblokir. Visibilitas ini dapat membantu Anda mengidentifikasi aktivitas berbahaya pada sumber daya terkait Anda.

Remediasi

Untuk mengaktifkan CloudWatch metrik pada grup AWS WAF aturan, panggil API. UpdateRuleGroup Untuk mengaktifkan CloudWatch metrik pada AWS WAF aturan, panggil UpdateWebACL API. Atur `CloudWatchMetricsEnabled` bidang `ketrue`. Saat Anda menggunakan AWS WAF konsol untuk membuat aturan atau grup aturan, CloudWatch metrik diaktifkan secara otomatis.

Melihat dan mengelola kontrol keamanan

Kontrol adalah perlindungan dalam standar keamanan yang membantu organisasi melindungi kerahasiaan, integritas, dan ketersediaan informasinya. Di Security Hub, kontrol terkait dengan AWS sumber daya tertentu.

Tampilan kontrol terkonsolidasi

Halaman Kontrol konsol Security Hub menampilkan semua kontrol yang tersedia saat ini Wilayah AWS (Anda dapat melihat kontrol dalam konteks standar dengan mengunjungi halaman standar Keamanan dan memilih standar yang diaktifkan). Security Hub menetapkan kontrol ID kontrol keamanan yang konsisten, judul, dan deskripsi di seluruh standar. ID kontrol mencakup nomor yang relevan Layanan AWS dan unik (misalnya, CodeBuild .3).

Informasi berikut tersedia di halaman Kontrol konsol Security Hub:

- Skor keamanan keseluruhan berdasarkan proporsi kontrol yang dilewati dibandingkan dengan jumlah total kontrol yang diaktifkan dengan data

- Persentase pemeriksaan keamanan yang gagal di semua kontrol yang diaktifkan
- Jumlah pemeriksaan keamanan yang lulus dan gagal untuk kontrol dengan tingkat keparahan yang berbeda-beda
- Daftar kontrol dibagi ke dalam tab yang berbeda berdasarkan status pemberdayaan. Kontrol yang tersedia yang tidak berlaku untuk salah satu standar yang diaktifkan muncul di kolom Dinonaktifkan. Kontrol yang belum diproses, seperti yang tidak tersedia di Wilayah Anda saat ini, muncul di kolom Tidak ada data. Jumlah kontrol di kolom Semua sama dengan jumlah kontrol di kolom data Gagal, Tidak Dikenal, Lulus, Dinonaktifkan, dan Tidak Ada.

Dari halaman Kontrol, Anda dapat memilih kontrol untuk melihat detailnya dan mengambil tindakan atas temuan yang dihasilkan oleh kontrol. Dari halaman ini, Anda juga dapat mengaktifkan atau menonaktifkan kontrol keamanan saat ini Akun AWS dan Wilayah AWS. Tindakan pemberdayaan dan penonaktifan dari halaman Kontrol berlaku di seluruh standar. Untuk informasi selengkapnya, lihat Mengaktifkan dan menonaktifkan kontrol di semua standar.

Untuk akun administrator, halaman Kontrol mencerminkan status kontrol di seluruh akun anggota. Jika pemeriksaan kontrol gagal di setidaknya satu akun anggota, kontrol akan muncul di tab Gagal pada halaman Kontrol. Jika Anda telah menetapkan Wilayah agregasi, halaman Kontrol mencerminkan status kontrol di semua Wilayah tertaut. Jika pemeriksaan kontrol gagal di setidaknya satu Wilayah tertaut, kontrol akan muncul di tab Gagal pada halaman Kontrol.

Tampilan kontrol terkonsolidasi menyebabkan perubahan mengontrol bidang pencarian di Format Pencarian AWS Keamanan (ASFF) yang dapat memengaruhi alur kerja. Untuk informasi selengkapnya, lihat Tampilan kontrol konsolidasi - perubahan ASFF.

Skor keamanan keseluruhan untuk kontrol

Halaman Kontrol menampilkan skor keamanan keseluruhan dari 0-100 persen. Skor keamanan keseluruhan dihitung berdasarkan proporsi kontrol yang dilewati dibandingkan dengan jumlah total kontrol yang diaktifkan dengan data.

> **Note**
>
> Untuk melihat skor keamanan keseluruhan untuk kontrol, Anda harus menambahkan izin untuk memanggil **`BatchGetControlEvaluations`**ke peran IAM yang Anda gunakan untuk mengakses Security Hub. Izin ini tidak diperlukan untuk melihat skor keamanan untuk standar tertentu.

Saat Anda mengaktifkan Security Hub, Security Hub menghitung skor keamanan awal dalam waktu 30 menit setelah kunjungan pertama Anda ke halaman Ringkasan atau halaman standar Keamanan di konsol Security Hub. Diperlukan waktu hingga 24 jam untuk skor keamanan pertama kali dihasilkan di Wilayah China dan AWS GovCloud (US) Region. Skor hanya dihasilkan untuk standar yang diaktifkan saat Anda mengunjungi halaman tersebut. Untuk melihat daftar standar yang saat ini diaktifkan, gunakan operasi `GetEnabledStandards`API. Selain itu, perekaman AWS Config sumber daya harus dikonfigurasi agar skor muncul. Skor keamanan keseluruhan adalah rata-rata skor keamanan standar.

Setelah menghasilkan skor pertama kali, Security Hub memperbarui skor keamanan setiap 24 jam. Security Hub menampilkan stempel waktu untuk menunjukkan kapan skor keamanan terakhir diperbarui.

Jika Anda telah menetapkan Wilayah agregasi, skor keamanan keseluruhan mencerminkan temuan kontrol di seluruh Wilayah tertaut.

Topik

Kategori kontrol

Setiap kontrol diberi kategori. Kategori untuk kontrol mencerminkan fungsi keamanan yang berlaku untuk kontrol.

Nilai kategori berisi kategori, subkategori dalam kategori, dan, secara opsional, pengklasifikasi dalam subkategori. Sebagai contoh:

- Identifikasi > Inventaris
- Lindungi > Perlindungan data > Enkripsi data dalam perjalanan

Berikut adalah deskripsi dari kategori, subkategori, dan pengklasifikasi yang tersedia.

Identifikasi

Mengembangkan pemahaman organisasi untuk mengelola risiko keamanan siber terhadap sistem, aset, data, dan kemampuan.

Inventaris

Sudahkah layanan menerapkan strategi penandaan sumber daya yang benar? Apakah strategi penandaan termasuk pemilik sumber daya?

Sumber daya apa yang digunakan layanan ini? Apakah mereka menyetujui sumber daya untuk layanan ini?

Apakah Anda memiliki visibilitas ke inventaris yang disetujui? Misalnya, apakah Anda menggunakan layanan seperti Amazon EC2 Systems Manager dan Service Catalog?

Pencatatan log

Sudahkah Anda mengaktifkan semua pencatatan yang relevan untuk layanan ini dengan aman? Contoh file log meliputi:

- Log Aliran VPC Amazon
- Log akses Elastic Load Balancing
- CloudFront Log Amazon
- CloudWatch Log Amazon
- Pencatatan Layanan Basis Data Relasional Amazon
- Log indeks lambat OpenSearch Layanan Amazon
- Penelusuran X-Ray
- AWS Directory Service log
- AWS Config barang
- Snapshot

Lindungi

Mengembangkan dan menerapkan perlindungan yang tepat untuk memastikan penyampaian layanan infrastruktur penting dan praktik pengkodean yang aman.

Manajemen akses yang aman

- Apakah layanan menggunakan praktik hak istimewa paling sedikit dalam IAM atau kebijakan sumber dayanya?
- Apakah kata sandi dan rahasia cukup kompleks? Apakah mereka diputar dengan tepat?
- Apakah layanan menggunakan otentikasi multi-faktor (MFA)?
- Apakah layanan menghindari pengguna root?
- Apakah kebijakan berbasis sumber daya memungkinkan akses publik?

Konfigurasi jaringan aman

- Apakah layanan menghindari akses jaringan jarak jauh publik dan tidak aman?
- Apakah layanan menggunakan VPC dengan benar? Misalnya, apakah pekerjaan diperlukan untuk berjalan di VPC?
- Apakah layanan mengelompokkan dan mengisolasi sumber daya sensitif dengan benar?

Perlindungan data

- Enkripsi data saat istirahat — Apakah layanan mengenkripsi data saat istirahat?
- Enkripsi data dalam perjalanan — Apakah layanan mengenkripsi data dalam perjalanan?
- Integritas data — Apakah layanan memvalidasi data untuk integritas?
- Perlindungan penghapusan data — Apakah layanan melindungi data dari penghapusan yang tidak disengaja?
- Pengelolaan/penggunaan data — Apakah Anda menggunakan layanan seperti Amazon Macie untuk melacak lokasi data sensitif Anda?

Perlindungan API

- Apakah layanan digunakan AWS PrivateLink untuk melindungi operasi API layanan?

Layanan pelindung

- Apakah layanan perlindungan yang benar ada? Apakah mereka memberikan jumlah pertanggungan yang benar?

Layanan pelindung membantu Anda menangkis serangan dan kompromi yang diarahkan pada layanan. Contoh layanan perlindungan AWS termasuk AWS Control Tower,, Vanta AWS WAF AWS Shield Advanced, Secrets Manager, IAM Access Analyzer, dan. AWS Resource Access Manager

Pengembangan yang aman

Apakah Anda menggunakan praktik pengkodean yang aman?

Apakah Anda menghindari kerentanan seperti Open Web Application Security Project (OWASP) Top Ten?

Mendeteksi

Mengembangkan dan menerapkan kegiatan yang sesuai untuk mengidentifikasi terjadinya peristiwa keamanan siber.

Layanan deteksi

Apakah layanan deteksi yang benar ada?

Apakah mereka memberikan jumlah pertanggungan yang benar?

Contoh layanan AWS deteksi termasuk Amazon GuardDuty, Amazon Inspector AWS Security Hub, Amazon Detective, CloudWatch Amazon AWS IoT Device Defender Alarm, dan. AWS Trusted Advisor

Menanggapi

Mengembangkan dan menerapkan kegiatan yang sesuai untuk mengambil tindakan terkait peristiwa keamanan siber yang terdeteksi.

Tindakan respons

Apakah Anda menanggapi peristiwa keamanan dengan cepat?

Apakah Anda memiliki temuan kritis atau tingkat keparahan tinggi yang aktif?

Forensik

Bisakah Anda memperoleh data forensik dengan aman untuk layanan ini? Misalnya, apakah Anda memperoleh snapshot Amazon EBS yang terkait dengan temuan positif sejati?

Sudahkah Anda membuat akun forensik?

Memulihkan

Mengembangkan dan mengimplementasikan kegiatan yang sesuai untuk mempertahankan rencana ketahanan dan untuk memulihkan kemampuan atau layanan apa pun yang terganggu karena peristiwa keamanan siber.

Ketangguhan

Apakah konfigurasi layanan mendukung kegagalan yang anggun, penskalaan elastis, dan ketersediaan tinggi?

Sudahkah Anda membuat cadangan?

Mengaktifkan dan menonaktifkan kontrol di semua standar

AWS Security Hub menghasilkan temuan untuk kontrol yang diaktifkan, dan mempertimbangkan semua kontrol yang diaktifkan saat menghitung skor keamanan. Anda dapat memilih untuk mengaktifkan dan menonaktifkan kontrol di semua standar keamanan atau mengonfigurasi status pemberdayaan secara berbeda dalam standar yang berbeda. Kami merekomendasikan opsi sebelumnya, di mana status pemberdayaan kontrol disejajarkan di semua standar yang Anda aktifkan. Bagian ini menjelaskan cara mengaktifkan dan menonaktifkan kontrol di seluruh standar. Untuk mengaktifkan atau menonaktifkan kontrol dalam satu atau lebih standar spesifik, lihatMengaktifkan dan menonaktifkan kontrol dalam standar tertentu.

Jika Anda telah menetapkan Wilayah agregasi, konsol Security Hub akan menampilkan kontrol dari semua Wilayah yang ditautkan. Jika kontrol tersedia di Wilayah tertaut tetapi tidak di Wilayah agregasi, Anda tidak dapat mengaktifkan atau menonaktifkan kontrol tersebut dari Wilayah agregasi.

> **Note**
>
> Petunjuk untuk mengaktifkan dan menonaktifkan kontrol bervariasi berdasarkan apakah Anda menggunakan konfigurasi pusat atau tidak. Bagian ini menjelaskan perbedaannya. Konfigurasi pusat tersedia untuk pengguna yang mengintegrasikan Security Hub dan AWS Organizations. Sebaiknya gunakan konfigurasi pusat untuk menyederhanakan proses mengaktifkan dan menonaktifkan kontrol di lingkungan multi-akun dan Multi-wilayah.

Mengaktifkan kontrol

Saat Anda mengaktifkan kontrol dalam standar, Security Hub mulai menjalankan pemeriksaan keamanan untuk kontrol dan menghasilkan temuan kontrol.

Security Hub mencakup status kontrol dalam perhitungan skor keamanan keseluruhan dan skor keamanan standar. Jika Anda mengaktifkan temuan kontrol konsolidasi, Anda menerima satu temuan untuk pemeriksaan keamanan bahkan jika Anda telah mengaktifkan kontrol dalam beberapa standar. Untuk informasi lebih lanjut, lihat Temuan kontrol konsolidasi.

Mengaktifkan kontrol di semua standar di beberapa akun dan Wilayah

Untuk mengaktifkan kontrol keamanan di beberapa akun dan Wilayah AWS, Anda harus menggunakan konfigurasi pusat.

Bila Anda menggunakan konfigurasi pusat, administrator yang didelegasikan dapat membuat kebijakan konfigurasi Security Hub yang mengaktifkan kontrol tertentu di seluruh standar yang diaktifkan. Anda kemudian dapat mengaitkan kebijakan konfigurasi dengan akun tertentu dan unit organisasi (OU) atau root. Kebijakan konfigurasi berlaku di Wilayah asal Anda (juga disebut Wilayah agregasi) dan semua Wilayah yang ditautkan.

Kebijakan konfigurasi menawarkan penyesuaian. Misalnya, Anda dapat memilih untuk mengaktifkan semua kontrol dalam satu OU, dan Anda dapat memilih untuk mengaktifkan hanya kontrol Amazon Elastic Compute Cloud (EC2) di OU lain. Tingkat perincian tergantung pada tujuan yang Anda maksudkan untuk cakupan keamanan di organisasi Anda. Untuk petunjuk cara membuat kebijakan konfigurasi yang memungkinkan kontrol tertentu di seluruh standar, lihatMembuat dan mengaitkan kebijakan konfigurasi Security Hub.

> **Note**
>
> Administrator yang didelegasikan dapat membuat kebijakan konfigurasi untuk mengelola kontrol di semua standar kecuali Standar yang Dikelola Layanan:. AWS Control Tower Kontrol untuk standar ini harus dikonfigurasi dalam AWS Control Tower layanan.

Jika Anda ingin beberapa akun mengonfigurasi kontrolnya sendiri daripada administrator yang didelegasikan, administrator yang didelegasikan dapat menetapkan akun tersebut sebagai dikelola sendiri. Akun yang dikelola sendiri harus mengonfigurasi kontrol secara terpisah di setiap Wilayah.

Mengaktifkan kontrol di semua standar dalam satu akun dan Wilayah

Jika Anda tidak menggunakan konfigurasi pusat atau akun yang dikelola sendiri, Anda tidak dapat menggunakan kebijakan konfigurasi untuk mengaktifkan kontrol secara terpusat di beberapa akun dan Wilayah. Namun, Anda dapat menggunakan langkah-langkah berikut untuk mengaktifkan kontrol dalam satu akun dan Wilayah.

Security Hub console

Untuk mengaktifkan kontrol lintas standar dalam satu akun dan Wilayah

1. Buka AWS Security Hub konsol di https://console.aws.amazon.com/securityhub/.
2. Pilih Kontrol dari panel navigasi.
3. Pilih tab Dinonaktifkan.
4. Pilih opsi di sebelah kontrol.
5. Pilih Aktifkan Kontrol (opsi ini tidak muncul untuk kontrol yang sudah diaktifkan).
6. Ulangi di setiap Wilayah di mana Anda ingin mengaktifkan kontrol.

Security Hub API

Untuk mengaktifkan kontrol lintas standar dalam satu akun dan Wilayah

1. Memanggil ListStandardsControlAssociationsAPI. Berikan ID kontrol keamanan.

   Contoh permintaan:

   ```
   {
       "SecurityControlId": "IAM.1"
   }
   ```

2. Memanggil BatchUpdateStandardsControlAssociationsAPI. Berikan Nama Sumber Daya Amazon (ARN) dari standar apa pun yang kontrol tidak diaktifkan. Untuk mendapatkan ARN standar, jalankan `DescribeStandards`.
3. Atur `AssociationStatus` parameter sama dengan`ENABLED`. Jika Anda mengikuti langkah-langkah ini untuk kontrol yang sudah diaktifkan, API akan mengembalikan respons kode status HTTP 200.

   Contoh permintaan:

```
{
    "StandardsControlAssociationUpdates": [{"SecurityControlId": "IAM.1",
 "StandardsArn": "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0", "AssociationStatus": "ENABLED"}, {"SecurityControlId": "IAM.1",
 "StandardsArn": "arn:aws:securityhub:::standards/aws-foundational-security-
best-practices/v/1.0.0", "AssociationStatus": "ENABLED"}]
}
```

4. Ulangi di setiap Wilayah di mana Anda ingin mengaktifkan kontrol.

AWS CLI

Untuk mengaktifkan kontrol lintas standar dalam satu akun dan Wilayah

1. Jalankan perintah list-standards-control-associations. Berikan ID kontrol keamanan.

```
aws securityhub  --region us-east-1 list-standards-control-associations --
security-control-id CloudTrail.1
```

2. Jalankan perintah batch-update-standards-control-associations. Berikan Nama Sumber Daya Amazon (ARN) dari standar apa pun yang kontrol tidak diaktifkan. Untuk mendapatkan ARN standar, jalankan `describe-standards` perintah.
3. Atur `AssociationStatus` parameter sama dengan`ENABLED`. Jika Anda mengikuti langkah-langkah ini untuk kontrol yang sudah diaktifkan, perintah akan mengembalikan respons kode status HTTP 200.

```
aws securityhub  --region us-east-1 batch-update-standards-control-associations
 --standards-control-association-updates '[{"SecurityControlId": "CloudTrail.1",
 "StandardsArn": "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0", "AssociationStatus": "ENABLED"}, {"SecurityControlId": "CloudTrail.1",
 "StandardsArn": "arn:aws:securityhub:::standards/cis-aws-foundations-benchmark/
v/1.4.0", "AssociationStatus": "ENABLED"}]'
```

4. Ulangi di setiap Wilayah di mana Anda ingin mengaktifkan kontrol.

Mengaktifkan kontrol baru secara otomatis dalam standar yang diaktifkan

Security Hub secara teratur merilis kontrol keamanan baru dan menambahkannya ke satu atau lebih standar. Anda dapat memilih apakah akan mengaktifkan kontrol baru secara otomatis dalam standar yang diaktifkan.

> **Note**
>
> Sebaiknya gunakan konfigurasi pusat untuk mengaktifkan kontrol baru secara otomatis. Jika kebijakan konfigurasi Anda menyertakan daftar kontrol yang akan dinonaktifkan (secara terprogram, ini mencerminkan `DisabledSecurityControlIdentifiers` parameter), Security Hub secara otomatis mengaktifkan semua kontrol lain di seluruh standar, termasuk kontrol yang baru dirilis. Jika kebijakan Anda menyertakan daftar kontrol yang akan diaktifkan (ini mencerminkan `EnabledSecurityControlIdentifiers` parameter), Security Hub secara otomatis menonaktifkan semua kontrol lainnya di seluruh standar, termasuk yang baru dirilis. Untuk informasi selengkapnya, lihat Cara kerja kebijakan konfigurasi Security Hub.

Pilih metode akses pilihan Anda, dan ikuti langkah-langkah untuk mengaktifkan kontrol baru secara otomatis dalam standar yang diaktifkan. Petunjuk berikut hanya berlaku jika Anda tidak menggunakan konfigurasi pusat.

Security Hub console

Untuk mengaktifkan kontrol baru secara otomatis

1. Buka AWS Security Hub konsol di https://console.aws.amazon.com/securityhub/.
2. Di panel navigasi, pilih Pengaturan, lalu pilih tab Umum.
3. Di bawah Kontrol, pilih Edit.
4. Aktifkan Aktifkan otomatis kontrol baru dalam standar yang diaktifkan.
5. Pilih Simpan.

Security Hub API

Untuk mengaktifkan kontrol baru secara otomatis

1. Memanggil UpdateSecurityHubConfigurationAPI.

2. Untuk mengaktifkan kontrol baru secara otomatis untuk standar yang diaktifkan, setel `AutoEnableControls` ke`true`. Jika Anda tidak ingin mengaktifkan kontrol baru secara otomatis, setel `AutoEnableControls` ke false.

AWS CLI

Untuk mengaktifkan kontrol baru secara otomatis

1. Jalankan perintah update-security-hub-configuration.
2. Untuk mengaktifkan kontrol baru secara otomatis untuk standar yang diaktifkan, tentukan`--auto-enable-controls`. Jika Anda tidak ingin mengaktifkan kontrol baru secara otomatis, tentukan`--no-auto-enable-controls`.

```
aws securityhub update-security-hub-configuration --auto-enable-controls | --no-auto-enable-controls
```

Contoh perintah

```
aws securityhub update-security-hub-configuration --auto-enable-controls
```

Menonaktifkan kontrol

Ketika Anda menonaktifkan kontrol di semua standar, hal berikut terjadi:

- Pemeriksaan keamanan untuk kontrol tidak lagi dilakukan.
- Tidak ada temuan tambahan yang dihasilkan untuk kontrol itu.
- Temuan yang ada diarsipkan secara otomatis setelah 3-5 hari (perhatikan bahwa ini adalah upaya terbaik).
- AWS Config Aturan terkait apa pun yang dibuat Security Hub akan dihapus.

Alih-alih menonaktifkan kontrol di semua standar, Anda bisa menonaktifkannya dalam satu atau lebih standar spesifik. Jika Anda melakukan ini, Security Hub tidak menjalankan pemeriksaan keamanan untuk kontrol standar tempat Anda menonaktifkannya, sehingga tidak memengaruhi skor keamanan untuk standar tersebut. Namun, Security Hub mempertahankan AWS Config aturan dan terus menjalankan pemeriksaan keamanan untuk kontrol jika diaktifkan dalam standar lain. Ini dapat

memengaruhi skor keamanan ringkasan Anda. Untuk petunjuk tentang mengonfigurasi kontrol dalam standar tertentu, lihatMengaktifkan dan menonaktifkan kontrol dalam standar tertentu.

Untuk mengurangi kebisingan temuan, akan berguna untuk menonaktifkan kontrol yang tidak relevan dengan lingkungan Anda. Untuk rekomendasi tentang kontrol mana yang harus dinonaktifkan, lihat Kontrol Security Hub yang mungkin ingin Anda nonaktifkan.

Ketika Anda menonaktifkan standar, semua kontrol yang berlaku untuk standar dinonaktifkan (namun, kontrol tersebut mungkin tetap diaktifkan dalam standar lain). Untuk informasi tentang menonaktifkan standar, lihat. the section called “Mengaktifkan dan menonaktifkan standar”

Saat Anda menonaktifkan standar, Security Hub tidak melacak kontrol mana yang berlaku yang dinonaktifkan. Jika Anda kemudian mengaktifkan kembali standar yang sama, semua kontrol yang berlaku untuk itu secara otomatis diaktifkan. Selain itu, menonaktifkan kontrol bukanlah tindakan permanen. Misalkan Anda menonaktifkan kontrol, dan kemudian Anda mengaktifkan standar yang sebelumnya dinonaktifkan. Jika standar mencakup kontrol itu, itu akan diaktifkan dalam standar itu. Saat Anda mengaktifkan standar di Security Hub, semua kontrol yang berlaku untuk standar tersebut akan diaktifkan secara otomatis. Anda dapat memilih untuk menonaktifkan kontrol tertentu.

Menonaktifkan kontrol di semua standar di beberapa akun dan Wilayah

Untuk menonaktifkan kontrol keamanan di beberapa akun dan Wilayah AWS, Anda harus menggunakan konfigurasi pusat.

Bila Anda menggunakan konfigurasi pusat, administrator yang didelegasikan dapat membuat kebijakan konfigurasi Security Hub yang menonaktifkan kontrol tertentu di seluruh standar yang diaktifkan. Anda kemudian dapat mengaitkan kebijakan konfigurasi dengan akun tertentu, OU, atau root. Kebijakan konfigurasi berlaku di Wilayah asal Anda (juga disebut Wilayah agregasi) dan semua Wilayah yang ditautkan.

Kebijakan konfigurasi menawarkan penyesuaian. Misalnya, Anda dapat memilih untuk menonaktifkan semua AWS CloudTrail kontrol dalam satu OU, dan Anda dapat memilih untuk menonaktifkan semua kontrol IAM di OU lain. Tingkat perincian tergantung pada tujuan yang Anda maksudkan untuk cakupan keamanan di organisasi Anda. Untuk petunjuk cara membuat kebijakan konfigurasi yang menonaktifkan kontrol tertentu di seluruh standar, lihatMembuat dan mengaitkan kebijakan konfigurasi Security Hub.

> **Note**
>
> Administrator yang didelegasikan dapat membuat kebijakan konfigurasi untuk mengelola kontrol di semua standar kecuali Standar yang Dikelola Layanan:. AWS Control Tower Kontrol untuk standar ini harus dikonfigurasi dalam AWS Control Tower layanan.

Jika Anda ingin beberapa akun mengonfigurasi kontrolnya sendiri daripada administrator yang didelegasikan, administrator yang didelegasikan dapat menetapkan akun tersebut sebagai dikelola sendiri. Akun yang dikelola sendiri harus mengonfigurasi kontrol secara terpisah di setiap Wilayah.

Menonaktifkan kontrol di semua standar dalam satu akun dan Wilayah

Jika Anda tidak menggunakan konfigurasi pusat atau akun yang dikelola sendiri, Anda tidak dapat menggunakan kebijakan konfigurasi untuk menonaktifkan kontrol secara terpusat di beberapa akun dan Wilayah. Namun, Anda dapat menggunakan langkah-langkah berikut untuk menonaktifkan kontrol dalam satu akun dan Wilayah.

Security Hub console

Untuk menonaktifkan kontrol di seluruh standar dalam satu akun dan Wilayah

1. Buka AWS Security Hub konsol di https://console.aws.amazon.com/securityhub/.
2. Pilih Kontrol dari panel navigasi.
3. Pilih opsi di sebelah kontrol.
4. Pilih Nonaktifkan Kontrol (opsi ini tidak muncul untuk kontrol yang sudah dinonaktifkan).
5. Pilih alasan untuk menonaktifkan kontrol, dan konfirmasikan dengan memilih Nonaktifkan.
6. Ulangi di setiap Wilayah di mana Anda ingin menonaktifkan kontrol.

Security Hub API

Untuk menonaktifkan kontrol di seluruh standar dalam satu akun dan Wilayah

1. Memanggil ListStandardsControlAssociationsAPI. Berikan ID kontrol keamanan.

   Contoh permintaan:

   ```
   {
   ```

```
    "SecurityControlId": "IAM.1"
}
```

2. Memanggil BatchUpdateStandardsControlAssociationsAPI. Berikan ARN dari standar apa pun tempat kontrol diaktifkan. Untuk mendapatkan ARN standar, jalankan `DescribeStandards`.
3. Atur `AssociationStatus` parameter sama dengan`DISABLED`. Jika Anda mengikuti langkah-langkah ini untuk kontrol yang sudah dinonaktifkan, API akan mengembalikan respons kode status HTTP 200.

   Contoh permintaan:

```
{
    "StandardsControlAssociationUpdates": [{"SecurityControlId": "IAM.1",
 "StandardsArn": "arn:aws:securityhub:::ruleset/cis-aws-foundations-
benchmark/v/1.2.0", "AssociationStatus": "DISABLED", "UpdatedReason": "Not
 applicable to environment"}, {"SecurityControlId": "IAM.1", "StandardsArn":
 "arn:aws:securityhub:::standards/aws-foundational-security-best-practices/
v/1.0.0", "AssociationStatus": "DISABLED", "UpdatedReason": "Not applicable to
 environment"}}]
}
```

4. Ulangi di setiap Wilayah di mana Anda ingin menonaktifkan kontrol.

AWS CLI

Untuk menonaktifkan kontrol di seluruh standar dalam satu akun dan Wilayah

1. Jalankan perintah list-standards-control-associations. Berikan ID kontrol keamanan.

```
aws securityhub  --region us-east-1 list-standards-control-associations --
security-control-id CloudTrail.1
```

2. Jalankan perintah batch-update-standards-control-associations. Berikan ARN dari standar apa pun tempat kontrol diaktifkan. Untuk mendapatkan ARN standar, jalankan `describe-standards` perintah.
3. Atur `AssociationStatus` parameter sama dengan`DISABLED`. Jika Anda mengikuti langkah-langkah ini untuk kontrol yang sudah dinonaktifkan, perintah akan mengembalikan respons kode status HTTP 200.

```
aws securityhub  --region us-east-1 batch-update-standards-control-associations
 --standards-control-association-updates '[{"SecurityControlId": "CloudTrail.1",
 "StandardsArn": "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0", "AssociationStatus": "DISABLED", "UpdatedReason": "Not applicable
 to environment"}, {"SecurityControlId": "CloudTrail.1", "StandardsArn":
 "arn:aws:securityhub:::standards/cis-aws-foundations-benchmark/v/1.4.0",
 "AssociationStatus": "DISABLED", "UpdatedReason": "Not applicable to
 environment"}]'
```

4. Ulangi di setiap Wilayah di mana Anda ingin menonaktifkan kontrol.

Mengaktifkan kontrol baru dalam standar yang diaktifkan secara otomatis

AWS Security Hub secara teratur merilis kontrol baru dan menambahkannya ke satu atau lebih standar. Anda dapat memilih apakah akan mengaktifkan kontrol baru secara otomatis dalam standar yang diaktifkan.

> **Note**
>
> Jika Anda menggunakan konfigurasi pusat dan menyertakan daftar kontrol khusus untuk dinonaktifkan dalam kebijakan konfigurasi Anda (secara terprogram, ini mencerminkan `DisabledSecurityControlIdentifiers` parameter, Security Hub secara otomatis mengaktifkan semua kontrol lain di seluruh standar, termasuk kontrol yang baru dirilis. Untuk informasi selengkapnya, lihat Cara kerja kebijakan konfigurasi Security Hub.

Sebaiknya gunakan konfigurasi pusat Security Hub untuk mengaktifkan kontrol keamanan baru secara otomatis. Anda dapat membuat kebijakan konfigurasi yang menyertakan daftar kontrol yang akan dinonaktifkan di seluruh standar. Semua kontrol lainnya, termasuk yang baru dirilis, diaktifkan secara default. Atau, Anda dapat membuat kebijakan yang menyertakan daftar kontrol yang akan diaktifkan di seluruh standar. Semua kontrol lainnya, termasuk yang baru dirilis, dinonaktifkan secara default. Untuk informasi selengkapnya, lihat Cara kerja konfigurasi pusat.

Security Hub tidak mengaktifkan kontrol baru saat ditambahkan ke standar yang belum Anda aktifkan.

Petunjuk berikut hanya berlaku jika Anda tidak menggunakan konfigurasi pusat.

Pilih metode akses pilihan Anda, dan ikuti langkah-langkah untuk mengaktifkan kontrol baru secara otomatis dalam standar yang diaktifkan.

Security Hub console

Untuk mengaktifkan kontrol baru secara otomatis

1. Buka AWS Security Hub konsol di https://console.aws.amazon.com/securityhub/.
2. Di panel navigasi, pilih Pengaturan, lalu pilih tab Umum.
3. Di bawah Kontrol, pilih Edit.
4. Aktifkan Aktifkan otomatis kontrol baru dalam standar yang diaktifkan.
5. Pilih Simpan.

Security Hub API

Untuk mengaktifkan kontrol baru secara otomatis

1. Jalankan `UpdateSecurityHubConfiguration`.
2. Untuk mengaktifkan kontrol baru secara otomatis untuk standar yang diaktifkan, setel `AutoEnableControls` ke`true`. Jika Anda tidak ingin mengaktifkan kontrol baru secara otomatis, setel `AutoEnableControls` ke false.

AWS CLI

Untuk mengaktifkan kontrol baru secara otomatis

1. Jalankan perintah `update-security-hub-configuration`.
2. Untuk mengaktifkan kontrol baru secara otomatis untuk standar yang diaktifkan, tentukan`--auto-enable-controls`. Jika Anda tidak ingin mengaktifkan kontrol baru secara otomatis, tentukan`--no-auto-enable-controls`.

```
aws securityhub update-security-hub-configuration --auto-enable-controls | --no-auto-enable-controls
```

Contoh perintah

```
aws securityhub update-security-hub-configuration --auto-enable-controls
```

Jika Anda tidak secara otomatis mengaktifkan kontrol baru, maka Anda harus mengaktifkannya secara manual. Untuk petunjuk, lihat the section called “Mengaktifkan dan menonaktifkan kontrol di semua standar”.

Parameter kontrol khusus

Beberapa kontrol Security Hub menggunakan parameter yang memengaruhi cara kontrol dievaluasi. Biasanya, kontrol tersebut dievaluasi terhadap nilai parameter default yang didefinisikan Security Hub. Namun, untuk subset kontrol ini, Anda dapat menyesuaikan nilai parameter. Saat Anda menyesuaikan nilai parameter untuk kontrol, Security Hub mulai mengevaluasi kontrol terhadap nilai yang Anda tentukan. Jika sumber daya yang mendasari kontrol memenuhi nilai kustom, Security Hub akan menghasilkan `PASSED` temuan. Jika sumber daya tidak memenuhi nilai kustom, Security Hub akan menghasilkan `FAILED` temuan.

Dengan menyesuaikan parameter kontrol, Anda dapat menyempurnakan praktik terbaik keamanan yang direkomendasikan dan dipantau oleh Security Hub agar sesuai dengan persyaratan bisnis dan harapan keamanan Anda. Alih-alih menekan temuan untuk kontrol, Anda dapat menyesuaikan satu atau lebih parameternya untuk mendapatkan temuan yang sesuai dengan kebutuhan keamanan Anda.

Berikut adalah beberapa contoh kasus penggunaan untuk parameter kontrol kustom:

- [CloudWatch.16] — grup CloudWatch log harus dipertahankan untuk jangka waktu tertentu

  Anda dapat menentukan periode waktu retensi.
- [IAM.7] — Kebijakan kata sandi untuk pengguna IAM harus memiliki konfigurasi yang kuat

  Anda dapat menentukan parameter yang terkait dengan kekuatan kata sandi.
- [EC2.18] - Grup keamanan hanya boleh mengizinkan lalu lintas masuk yang tidak terbatas untuk port resmi

  Anda dapat menentukan port mana yang diizinkan untuk mengizinkan lalu lintas masuk yang tidak dibatasi.
- [Lambda.5] - Fungsi VPC Lambda harus beroperasi di beberapa Availability Zone

  Anda dapat menentukan jumlah minimum Availability Zones yang menghasilkan temuan yang diteruskan.

Bagian ini menjelaskan cara menyesuaikan dan mengelola parameter kontrol.

Cara kerja parameter kontrol khusus

Kontrol dapat memiliki satu atau lebih parameter yang dapat disesuaikan. Jenis data yang mungkin untuk parameter kontrol individu meliputi yang berikut:

- Boolean
- Ganda
- Enum
- EnumList
- Bilangan Bulat
- IntegerList
- String
- StringList

Untuk beberapa kontrol, nilai parameter yang dapat diterima juga harus jatuh ke dalam rentang tertentu agar valid. Dalam kasus ini, Security Hub menyediakan jangkauan yang dapat diterima.

Security Hub memilih nilai parameter default dan terkadang memperbaruinya. Setelah Anda menyesuaikan parameter kontrol, nilainya terus menjadi nilai yang Anda tentukan untuk parameter kecuali Anda mengubahnya. Artinya, parameter berhenti melacak pembaruan ke nilai Security Hub default, meskipun nilai kustom parameter cocok dengan nilai default saat ini yang ditentukan oleh Security Hub. Berikut adalah contoh untuk kontrol [ACM.1] - Sertifikat yang diimpor dan diterbitkan ACM harus diperbarui setelah jangka waktu tertentu:

```
{
    "SecurityControlId": "ACM.1",
    "Parameters": {
        "daysToExpiration": {
            "ValueType": "CUSTOM",
            "Value": {
                "Integer": 30
            }
        }
    }
}
```

Dalam contoh sebelumnya, `daysToExpiration` parameter memiliki nilai kustom. `30` Nilai default saat ini untuk parameter ini juga`30`. Jika Security Hub mengubah nilai default menjadi`14`, parameter dalam contoh ini tidak akan melacak perubahan tersebut. Ini akan mempertahankan nilai`30`.

Jika Anda ingin melacak pemutakhiran ke nilai Security Hub default untuk parameter, setel `ValueType` bidang tersebut `DEFAULT` sebagai ganti`CUSTOM`. Untuk informasi selengkapnya, lihat Mengembalikan ke nilai parameter default dalam satu akun dan Wilayah.

Saat Anda mengubah nilai parameter, Anda juga memicu pemeriksaan keamanan baru yang mengevaluasi kontrol berdasarkan nilai baru. Security Hub kemudian menghasilkan temuan kontrol baru berdasarkan nilai baru. Selama pembaruan berkala untuk mengontrol temuan, Security Hub juga menggunakan nilai parameter baru. Jika Anda mengubah nilai parameter untuk kontrol, tetapi belum mengaktifkan standar apa pun yang menyertakan kontrol, Security Hub tidak melakukan pemeriksaan keamanan apa pun menggunakan nilai baru. Anda harus mengaktifkan setidaknya satu standar yang relevan untuk Security Hub untuk mengevaluasi kontrol berdasarkan nilai parameter baru.

Nilai parameter kustom berlaku di seluruh standar yang diaktifkan. Anda tidak dapat menyesuaikan parameter untuk kontrol yang tidak didukung di Wilayah Anda saat ini. Untuk daftar batas Regional untuk kontrol individu, lihatBatas regional pada kontrol.

Menyesuaikan parameter kontrol

Petunjuk untuk menyesuaikan parameter kontrol bervariasi berdasarkan apakah Anda menggunakan konfigurasi pusat. Konfigurasi pusat adalah fitur yang dapat digunakan administrator Security Hub yang didelegasikan untuk mengelola kapabilitas Security Hub di seluruh Wilayah AWS, akun, dan unit organisasi (OU) di organisasi mereka.

Jika organisasi Anda menggunakan konfigurasi pusat, administrator yang didelegasikan dapat membuat kebijakan konfigurasi yang menyertakan parameter kontrol kustom. Kebijakan ini dapat dikaitkan dengan akun anggota dan OU yang dikelola secara terpusat, dan berlaku di Wilayah asal Anda dan semua Wilayah yang ditautkan. Administrator yang didelegasikan juga dapat menetapkan satu atau lebih akun sebagai dikelola sendiri, yang memungkinkan pemilik akun untuk mengonfigurasi parameternya sendiri secara terpisah di setiap Wilayah. Jika organisasi Anda tidak menggunakan konfigurasi pusat, Anda harus menyesuaikan parameter kontrol secara terpisah di setiap akun dan Wilayah.

Menyesuaikan parameter kontrol di beberapa akun dan Wilayah

Saat menggunakan konfigurasi pusat, Anda dapat menyesuaikan parameter kontrol untuk akun dan OU yang dikelola secara terpusat di beberapa akun dan Wilayah. Sebaiknya gunakan konfigurasi pusat karena memungkinkan Anda menyelaraskan nilai parameter kontrol di berbagai bagian organisasi Anda. Misalnya, semua akun pengujian Anda mungkin menggunakan nilai parameter tertentu, dan semua akun produksi mungkin menggunakan nilai yang berbeda.

Jika Anda administrator Security Hub yang didelegasikan untuk organisasi yang menggunakan konfigurasi pusat, pilih metode pilihan Anda, dan ikuti langkah-langkah untuk menyesuaikan parameter kontrol di beberapa akun dan Wilayah.

Security Hub console

Untuk menyesuaikan parameter kontrol di beberapa akun dan Wilayah

1. Buka AWS Security Hub konsol di https://console.aws.amazon.com/securityhub/.

   Pastikan Anda masuk ke Wilayah asal.
2. Di panel navigasi, pilih Pengaturan dan Konfigurasi.
3. Pilih tab Kebijakan.
4. Untuk membuat kebijakan konfigurasi baru yang menyertakan parameter kustom, pilih Buat kebijakan. Untuk menentukan parameter kustom dalam kebijakan konfigurasi yang ada, pilih kebijakan, lalu pilih Edit.

   Untuk membuat kebijakan konfigurasi baru dengan parameter kustom

   1. Di bagian Kebijakan kustom, pilih standar keamanan dan kontrol yang ingin Anda aktifkan.
   2. Pilih Sesuaikan parameter kontrol.
   3. Pilih kontrol, lalu tentukan nilai kustom untuk satu atau beberapa parameter.
   4. Untuk menyesuaikan parameter untuk kontrol lainnya, pilih Sesuaikan kontrol tambahan.
   5. Di bagian Akun, pilih akun atau OU yang ingin Anda terapkan kebijakan.
   6. Pilih Selanjutnya.
   7. Pilih Buat kebijakan dan terapkan. Di Wilayah beranda dan semua Wilayah yang ditautkan, tindakan ini mengesampingkan pengaturan konfigurasi akun dan OU yang ada yang terkait dengan kebijakan konfigurasi ini. Akun dan OU dapat dikaitkan dengan kebijakan konfigurasi melalui aplikasi langsung atau warisan dari orang tua.

Untuk menambah atau mengedit parameter kustom dalam kebijakan konfigurasi yang ada

1. Di bagian Kontrol, di bawah Kebijakan khusus, tentukan nilai parameter kustom baru yang Anda inginkan.
2. Jika ini adalah pertama kalinya Anda menyesuaikan parameter kontrol dalam kebijakan ini, pilih Sesuaikan parameter kontrol, lalu pilih kontrol untuk disesuaikan. Untuk menyesuaikan parameter untuk kontrol lainnya, pilih Sesuaikan kontrol tambahan.
3. Di bagian Akun, verifikasi akun atau OU yang ingin Anda terapkan kebijakannya.
4. Pilih Selanjutnya.
5. Tinjau perubahan Anda, dan verifikasi bahwa perubahan tersebut benar. Setelah selesai, pilih Simpan kebijakan dan terapkan. Di Wilayah beranda dan semua Wilayah yang ditautkan, tindakan ini mengesampingkan pengaturan konfigurasi akun dan OU yang ada yang terkait dengan kebijakan konfigurasi ini. Akun dan OU dapat dikaitkan dengan kebijakan konfigurasi melalui aplikasi langsung atau warisan dari orang tua.

Security Hub API

Untuk menyesuaikan parameter kontrol di beberapa akun dan Wilayah

Untuk membuat kebijakan konfigurasi baru dengan parameter kustom

1. Memanggil CreateConfigurationPolicyAPI dari akun administrator yang didelegasikan di Wilayah beranda.
2. Untuk `SecurityControlCustomParameters` objek, berikan pengenal setiap kontrol yang ingin Anda sesuaikan.
3. Untuk `Parameters` objek, berikan nama setiap parameter yang ingin Anda sesuaikan. Untuk setiap parameter yang Anda sesuaikan, `CUSTOM` sediakan`ValueType`. Untuk`Value`, berikan tipe data parameter dan nilai kustom. `Value`Bidang tidak bisa kosong kapan `ValueType` ada`CUSTOM`. Jika permintaan Anda menghilangkan parameter yang didukung kontrol, parameter tersebut mempertahankan nilainya saat ini. Anda dapat menemukan parameter yang didukung, tipe data, dan nilai yang valid untuk kontrol dengan menjalankan GetSecurityControlDefinitionAPI.

Untuk menambah atau mengedit parameter kustom dalam kebijakan konfigurasi yang ada

1. Memanggil UpdateConfigurationPolicyAPI dari akun administrator yang didelegasikan di Wilayah beranda.
2. Untuk `Identifier` bidang, berikan Nama Sumber Daya Amazon (ARN) atau ID kebijakan konfigurasi yang ingin Anda perbarui.
3. Untuk `SecurityControlCustomParameters` objek, berikan pengenal setiap kontrol yang ingin Anda sesuaikan.
4. Untuk `Parameters` objek, berikan nama setiap parameter yang ingin Anda sesuaikan. Untuk setiap parameter yang Anda sesuaikan, `CUSTOM` sediakan`ValueType`. Untuk`Value`, berikan tipe data parameter dan nilai kustom. Jika permintaan Anda menghilangkan parameter yang didukung kontrol, parameter tersebut mempertahankan nilainya saat ini. Anda dapat menemukan parameter yang didukung, tipe data, dan nilai yang valid untuk kontrol dengan menjalankan GetSecurityControlDefinitionAPI.

Contoh permintaan API untuk membuat kebijakan konfigurasi baru:

```
{
    "Name": "SampleConfigurationPolicy",
    "Description": "Configuration policy for production accounts",
    "ConfigurationPolicy": {
        "SecurityHub": {
             "ServiceEnabled": true,
             "EnabledStandardIdentifiers": [
                    "arn:aws:securityhub:us-east-1::standards/aws-foundational-
security-best-practices/v/1.0.0"},
                    "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0"}
                ],
            "SecurityControlsConfiguration": {
                "DisabledSecurityControlIdentifiers": [
                    "CloudTrail.2"
                ],
                "SecurityControlCustomParameters": [
                    {
                        "SecurityControlId": "ACM.1",
                        "Parameters": {
                            "daysToExpiration": {
                                "ValueType": "CUSTOM",
                                "Value": {
```

```
                                "Integer": 15
                            }
                        }
                    }
                }
            ]
        }
    }
}
```

AWS CLI

Untuk menyesuaikan parameter kontrol di beberapa akun dan Wilayah

Untuk membuat kebijakan konfigurasi baru dengan parameter kustom

1. Jalankan create-configuration-policyperintah dari akun administrator yang didelegasikan di wilayah rumah.
2. Untuk `SecurityControlCustomParameters` objek, berikan pengenal setiap kontrol yang ingin Anda sesuaikan.
3. Untuk `Parameters` objek, berikan nama setiap parameter yang ingin Anda sesuaikan. Untuk setiap parameter yang Anda sesuaikan, `CUSTOM` sediakan`ValueType`. Untuk`Value`, berikan tipe data parameter dan nilai kustom. `Value`Bidang tidak bisa kosong kapan `ValueType` ada`CUSTOM`. Jika permintaan Anda menghilangkan parameter yang didukung kontrol, parameter tersebut mempertahankan nilainya saat ini. Anda dapat menemukan parameter yang didukung, tipe data, dan nilai yang valid untuk kontrol dengan menjalankan get-security-control-definitionperintah.

Untuk menambah atau mengedit parameter dalam kebijakan konfigurasi yang ada

1. Untuk menambah atau memperbarui parameter input kustom dalam kebijakan konfigurasi yang ada, jalankan update-configuration-policyperintah dari akun administrator yang didelegasikan di Wilayah beranda.
2. Untuk `identifier` bidang, berikan Nama Sumber Daya Amazon (ARN) atau ID kebijakan yang ingin Anda perbarui.
3. Untuk `SecurityControlCustomParameters` objek, berikan pengenal setiap kontrol yang ingin Anda sesuaikan.

4. Untuk `Parameters` objek, berikan nama setiap parameter yang ingin Anda sesuaikan. Untuk setiap parameter yang Anda sesuaikan, `CUSTOM` sediakan`ValueType`. Untuk`Value`, berikan tipe data parameter dan nilai kustom. Jika permintaan Anda menghilangkan parameter yang didukung kontrol, parameter tersebut mempertahankan nilainya saat ini. Anda dapat menemukan parameter yang didukung, tipe data, dan nilai yang valid untuk kontrol dengan menjalankan get-security-control-definitionperintah.

Contoh perintah untuk membuat kebijakan konfigurasi baru:

```
$ aws securityhub create-configuration-policy \
--region us-east-1 \
--name "SampleConfigurationPolicy" \
--description "Configuration policy for production accounts" \
--configuration-policy '{"SecurityHub": {"ServiceEnabled": true,
 "EnabledStandardIdentifiers": ["arn:aws:securityhub:us-east-1::standards/aws-
foundational-security-best-practices/v/1.0.0","arn:aws:securityhub:::ruleset/
cis-aws-foundations-benchmark/v/1.2.0"],"SecurityControlsConfiguration":
{"DisabledSecurityControlIdentifiers": ["CloudTrail.2"],
 "SecurityControlCustomParameters": [{"SecurityControlId": "ACM.1", "Parameters":
 {"daysToExpiration": {"ValueType": "CUSTOM", "Value": "Integer": 15}}}]}}}'
```

Menyesuaikan parameter kontrol dalam satu akun dan Wilayah

Jika Anda tidak menggunakan konfigurasi pusat atau memiliki akun yang dikelola sendiri, Anda dapat menyesuaikan parameter kontrol untuk akun Anda di satu Wilayah pada satu waktu

Pilih metode pilihan Anda, dan ikuti langkah-langkah untuk menyesuaikan parameter kontrol. Perubahan Anda hanya berlaku untuk akun Anda di Wilayah saat ini. Untuk menyesuaikan parameter kontrol di Wilayah tambahan, ulangi langkah-langkah berikut di setiap akun tambahan dan Wilayah tempat Anda ingin menyesuaikan parameter. Kontrol yang sama dapat menggunakan nilai parameter yang berbeda di Wilayah yang berbeda.

Security Hub console

Untuk menyesuaikan parameter kontrol dalam satu akun dan Wilayah

1. Buka AWS Security Hub konsol di https://console.aws.amazon.com/securityhub/.

2. Di panel navigasi, pilih Kontrol. Dalam tabel, pilih kontrol yang mendukung parameter khusus dan Anda ingin mengubah parameternya. Kolom parameter Kustom menunjukkan kontrol mana yang mendukung parameter kustom.
3. Pada halaman detail untuk kontrol, pilih tab Parameter, lalu pilih Edit.
4. Tentukan nilai parameter yang Anda inginkan.
5. Secara opsional, di bagian Alasan perubahan, pilih alasan untuk menyesuaikan parameter.
6. Pilih Simpan.

Security Hub API

Untuk menyesuaikan parameter kontrol dalam satu akun dan Wilayah

1. Memanggil UpdateSecurityControlAPI.
2. Untuk`SecurityControlId`, berikan ID kontrol yang ingin Anda sesuaikan.
3. Untuk `Parameters` objek, berikan nama setiap parameter yang ingin Anda sesuaikan. Untuk setiap parameter yang Anda sesuaikan, `CUSTOM` sediakan`ValueType`. Untuk`Value`, berikan tipe data parameter dan nilai kustom. Jika permintaan Anda menghilangkan parameter yang didukung kontrol, parameter tersebut mempertahankan nilainya saat ini. Anda dapat menemukan parameter yang didukung, tipe data, dan nilai yang valid untuk kontrol dengan menjalankan GetSecurityControlDefinitionAPI.
4. Secara opsional`LastUpdateReason`, untuk, berikan alasan untuk menyesuaikan parameter kontrol.

Contoh permintaan API:

```
{
    "SecurityControlId": "ACM.1",
    "Parameters": {
        "daysToExpiration": {
            "ValueType": "CUSTOM",
            "Value": {
                "Integer": 15
            }
        }
    },
    "LastUpdateReason": "Internal compliance requirement"
}
```

AWS CLI

Untuk menyesuaikan parameter kontrol dalam satu akun dan Wilayah

1. Jalankan perintah update-security-control.
2. Untuk`security-control-id`, berikan ID kontrol yang ingin Anda sesuaikan.
3. Untuk `parameters` objek, berikan nama setiap parameter yang ingin Anda sesuaikan. Untuk setiap parameter yang Anda sesuaikan, `CUSTOM` sediakan`ValueType`. Untuk`Value`, berikan tipe data parameter dan nilai kustom. Jika permintaan Anda menghilangkan parameter yang didukung kontrol, parameter tersebut mempertahankan nilainya saat ini. Anda dapat menemukan parameter yang didukung, tipe data, dan nilai yang valid untuk kontrol dengan menjalankan get-security-control-definitionperintah.
4. Secara opsional`last-update-reason`, untuk, berikan alasan untuk menyesuaikan parameter kontrol.

Contoh perintah:

```
$ aws securityhub update-security-control \
--region us-east-1 \
--security-control-id ACM.1 \
--parameters '{"daysToExpiration": {"ValueType": "CUSTOM", "Value": {"Integer":
 15}}}' \
--last-update-reason "Internal compliance requirement"
```

Memeriksa status parameter kontrol

Penting untuk memvalidasi dan memeriksa status perubahan untuk mengontrol parameter. Ini membantu memastikan bahwa kontrol berfungsi seperti yang Anda harapkan dan memberikan nilai keamanan yang diinginkan. Untuk memverifikasi bahwa pembaruan parameter berhasil, Anda dapat meninjau detail kontrol pada konsol Security Hub. Di konsol, pilih kontrol untuk menampilkan detailnya. Tab Parameter menunjukkan status perubahan parameter.

Secara terprogram, jika permintaan Anda untuk memperbarui parameter valid, nilai `UpdateStatus` `UPDATING` bidang adalah respons terhadap BatchGetSecurityControlsoperasi. Ini berarti bahwa pembaruan itu valid, tetapi temuan Anda mungkin belum menyertakan nilai parameter yang

diperbarui. Ketika nilai `UpdateState` berubah`READY`, temuan Anda mulai menyertakan nilai parameter yang diperbarui.

`UpdateSecurityControl`Operasi mengembalikan `InvalidInputException` respons untuk nilai parameter yang tidak valid. Tanggapan tersebut memberikan rincian tambahan tentang alasan kegagalan. Misalnya, Anda mungkin telah menetapkan nilai yang berada di luar rentang yang valid untuk parameter. Atau, Anda menentukan nilai yang tidak menggunakan tipe data yang benar. Kirim permintaan Anda lagi dengan masukan yang valid. Jika pemutakhiran parameter tidak berhasil, Security Hub mempertahankan nilai saat ini untuk parameter tersebut.

Jika terjadi kegagalan internal saat Anda mencoba memperbarui nilai parameter, Security Hub akan mencoba ulang secara otomatis jika Anda telah AWS Config mengaktifkannya. Untuk informasi selengkapnya, lihat Mengkonfigurasi AWS Config.

Meninjau parameter kontrol

Anda dapat meninjau nilai saat ini untuk parameter kontrol individual di akun Anda. Jika Anda menggunakan konfigurasi pusat, administrator Security Hub yang didelegasikan juga dapat meninjau nilai parameter yang ditentukan dalam kebijakan konfigurasi.

Pilih metode pilihan Anda, dan ikuti langkah-langkah untuk meninjau nilai parameter kontrol saat ini.

Security Hub console

Untuk meninjau nilai parameter saat ini

1. Buka AWS Security Hub konsol di https://console.aws.amazon.com/securityhub/.
2. Di panel navigasi, pilih Kontrol. Pilih kontrol.
3. Pilih tab Parameter. Tab ini menunjukkan nilai parameter saat ini untuk kontrol.

Security Hub API

Untuk meninjau nilai parameter saat ini

Panggil BatchGetSecurityControlsAPI, dan berikan satu atau beberapa ID kontrol keamanan atau ARN. `Parameters`Objek dalam respons menunjukkan nilai parameter saat ini untuk kontrol yang ditentukan.

Contoh permintaan API:

```
{
```

```
    "SecurityControlIds": ["APIGateway.1", "CloudWatch.15", "IAM.7"]
}
```

AWS CLI

Untuk meninjau nilai parameter saat ini

Jalankan batch-get-security-controlsperintah, dan berikan satu atau lebih ID kontrol keamanan atau ARN. `Parameters`Objek dalam respons menunjukkan nilai parameter saat ini untuk kontrol yang ditentukan.

Contoh perintah:

```
$ aws securityhub batch-get-security-controls \
--region us-east-1 \
--security-control-ids '["APIGateway.1", "CloudWatch.15", "IAM.7"]'
```

Pilih metode yang Anda inginkan untuk melihat nilai parameter saat ini dalam kebijakan konfigurasi pusat.

Security Hub console

Untuk meninjau nilai parameter saat ini dalam kebijakan konfigurasi

1. Buka AWS Security Hub konsol di https://console.aws.amazon.com/securityhub/.

   Masuk menggunakan kredensyal akun administrator Security Hub yang didelegasikan di Wilayah beranda.
2. Di panel navigasi, pilih Pengaturan dan Konfigurasi.
3. Pada tab Kebijakan, pilih kebijakan konfigurasi, lalu pilih Lihat detail. Detail kebijakan kemudian muncul, termasuk nilai parameter saat ini.

Security Hub API

Untuk meninjau nilai parameter saat ini dalam kebijakan konfigurasi

1. Memanggil GetConfigurationPolicyAPI dari akun administrator yang didelegasikan di Wilayah beranda.

2. Berikan ARN atau ID kebijakan konfigurasi yang detailnya ingin Anda lihat. Respons mencakup nilai parameter saat ini.

```
{
    "Identifier": "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
}
```

AWS CLI

Untuk meninjau nilai parameter saat ini dalam kebijakan konfigurasi

1. Jalankan get-configuration-policyperintah dari akun administrator yang didelegasikan di wilayah rumah.
2. Berikan ARN atau ID kebijakan konfigurasi yang detailnya ingin Anda lihat. Respons mencakup nilai parameter saat ini.

```
$ aws securityhub get-configuration-policy \
--region us-east-1 \
--identifier "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

Temuan kontrol Anda juga menunjukkan nilai parameter saat ini. DalamAWS Sintaks Security Finding Format (ASFF), nilai-nilai ini muncul di `Parameters` bidang `Compliance` objek. Untuk meninjau temuan di konsol Security Hub, pilih Temuan di panel navigasi. Untuk meninjau temuan secara terprogram, gunakan operasi. GetFindings

> **Note**
>
> Setelah merilis fitur parameter kontrol kustom, Security Hub akan memperbarui temuan kontrol yang ada untuk menyertakan bidang `Parameters` ASFF. Ini bisa memakan waktu hingga 24 jam.

Mengembalikan ke nilai parameter kontrol default

Parameter kontrol dapat memiliki nilai default yang didefinisikan Security Hub. Kami mungkin memperbarui nilai default untuk parameter untuk mencerminkan praktik terbaik keamanan yang berkembang. Jika Anda belum menentukan nilai kustom untuk parameter kontrol, kontrol secara otomatis melacak pembaruan tersebut dan menggunakan nilai default yang baru.

Anda dapat kembali menggunakan nilai parameter default untuk kontrol. Bagaimana Anda melakukan ini tergantung pada apakah Anda menggunakan konfigurasi pusat.

> **Note**
>
> Tidak semua parameter kontrol memiliki nilai Security Hub default. Dalam kasus seperti itu, ketika `ValueType` disetel ke`DEFAULT`, tidak ada nilai default tertentu yang digunakan Security Hub. Sebaliknya, Security Hub mengabaikan parameter tanpa adanya nilai khusus.

Mengembalikan ke nilai parameter default di beberapa akun dan Wilayah

Jika Anda menggunakan konfigurasi pusat, Anda dapat mengembalikan parameter kontrol untuk akun dan OU yang dikelola secara terpusat di beberapa akun dan Wilayah.

Pilih metode pilihan Anda, dan ikuti langkah-langkah untuk kembali ke nilai parameter default di beberapa akun dan Wilayah menggunakan konfigurasi pusat.

Security Hub console

Untuk kembali ke nilai parameter default di beberapa akun dan Wilayah

1. Buka AWS Security Hub konsol di https://console.aws.amazon.com/securityhub/.

   Masuk menggunakan kredensyal akun administrator yang didelegasikan Security Hub di Wilayah beranda.
2. Di panel navigasi, pilih Pengaturan dan Konfigurasi.
3. Pilih tab Kebijakan.
4. Pilih kebijakan, lalu pilih Edit.
5. Di bawah Kebijakan khusus, bagian Kontrol menampilkan daftar kontrol yang Anda tetapkan untuk parameter kustom.

6. Temukan kontrol yang memiliki satu atau lebih nilai parameter untuk dikembalikan. Kemudian, pilih Hapus untuk kembali ke nilai default.
7. Di bagian Akun, verifikasi akun atau OU yang ingin Anda terapkan kebijakannya.
8. Pilih Selanjutnya.
9. Tinjau perubahan Anda, dan verifikasi bahwa perubahan tersebut benar. Setelah selesai, pilih Simpan kebijakan dan terapkan. Di Wilayah beranda dan semua Wilayah yang ditautkan, tindakan ini mengesampingkan pengaturan konfigurasi akun dan OU yang ada yang terkait dengan kebijakan konfigurasi ini. Akun dan OU dapat dikaitkan dengan kebijakan konfigurasi melalui aplikasi langsung atau warisan dari orang tua.

Security Hub API

Untuk kembali ke nilai parameter default di beberapa akun dan Wilayah

1. Memanggil UpdateConfigurationPolicyAPI dari akun administrator yang didelegasikan di Wilayah beranda.
2. Untuk `Identifier` bidang, berikan Nama Sumber Daya Amazon (ARN) atau ID kebijakan yang ingin Anda perbarui.
3. Untuk `SecurityControlCustomParameters` objek, berikan pengidentifikasi setiap kontrol yang ingin Anda kembalikan satu atau beberapa parameter.
4. Dalam `Parameters` objek, untuk setiap parameter yang ingin Anda kembalikan, sediakan `DEFAULT` untuk `ValueType` bidang. Ketika `ValueType` diatur ke`DEFAULT`, Anda tidak perlu memberikan nilai untuk `Value` bidang tersebut. Jika nilai disertakan dalam permintaan Anda, Security Hub mengabaikannya. Jika permintaan Anda menghilangkan parameter yang didukung kontrol, parameter tersebut mempertahankan nilainya saat ini.

> **Warning**
>
> Jika Anda menghilangkan objek kontrol dari `SecurityControlCustomParameters` bidang, Security Hub mengembalikan semua parameter kustom untuk kontrol ke nilai defaultnya. Daftar yang benar-benar kosong untuk `SecurityControlCustomParameters` mengembalikan parameter kustom untuk semua kontrol ke nilai defaultnya.

Contoh permintaan API:

```
{
    "Identifier": "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "Name": "TestConfigurationPolicy",
    "Description": "Updated configuration policy",
    "UpdatedReason": "Revert ACM.1 parameter to default value",
    "ConfigurationPolicy": {
        "SecurityHub": {
             "ServiceEnabled": true,
             "EnabledStandardIdentifiers": [
                    "arn:aws:securityhub:us-east-1::standards/aws-foundational-
security-best-practices/v/1.0.0"},
                    "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0"}
                ],
             "SecurityControlsConfiguration": {
                "DisbledSecurityControlIdentifiers": [
                    "CloudTrail.2"
                ],
                "SecurityControlCustomParameters": [
                    {
                        "SecurityControlId": "ACM.1",
                        "Parameters": {
                            "daysToExpiration": {
                                "ValueType": "DEFAULT"
                             }
                         }
                    }
                ]
             }
        }
    }
}
```

AWS CLI

Untuk kembali ke nilai parameter default di beberapa akun dan Wilayah

1. Jalankan update-configuration-policyperintah dari akun administrator yang didelegasikan di wilayah rumah.

2. Untuk `identifier` bidang, berikan Nama Sumber Daya Amazon (ARN) atau ID kebijakan yang ingin Anda perbarui.
3. Untuk `SecurityControlCustomParameters` objek, berikan pengidentifikasi setiap kontrol yang ingin Anda kembalikan satu atau beberapa parameter.
4. Dalam `Parameters` objek, untuk setiap parameter yang ingin Anda kembalikan, sediakan `DEFAULT` untuk `ValueType` bidang. Ketika `ValueType` diatur ke`DEFAULT`, Anda tidak perlu memberikan nilai untuk `Value` bidang tersebut. Jika nilai disertakan dalam permintaan Anda, Security Hub mengabaikannya. Jika permintaan Anda menghilangkan parameter yang didukung kontrol, parameter tersebut mempertahankan nilainya saat ini.

> **Warning**
>
> Jika Anda menghilangkan objek kontrol dari `SecurityControlCustomParameters` bidang, Security Hub mengembalikan semua parameter kustom untuk kontrol ke nilai defaultnya. Daftar yang benar-benar kosong untuk `SecurityControlCustomParameters` mengembalikan parameter kustom untuk semua kontrol ke nilai defaultnya.

Contoh perintah:

```
$ aws securityhub create-configuration-policy \
--region us-east-1 \
--identifier "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111" \
--name "TestConfigurationPolicy" \
--description "Updated configuration policy" \
--updated-reason "Revert ACM.1 parameter to default value"
--configuration-policy '{"SecurityHub": {"ServiceEnabled": true,
 "EnabledStandardIdentifiers": ["arn:aws:securityhub:us-east-1::standards/aws-
foundational-security-best-practices/v/1.0.0","arn:aws:securityhub:::ruleset/
cis-aws-foundations-benchmark/v/1.2.0"],"SecurityControlsConfiguration":
{"DisabledSecurityControlIdentifiers": ["CloudTrail.2"],
 "SecurityControlCustomParameters": [{"SecurityControlId": "ACM.1", "Parameters":
 {"daysToExpiration": {"ValueType": "DEFAULT"}}}]}}}'
```

Mengembalikan ke nilai parameter default dalam satu akun dan Wilayah

Jika Anda tidak menggunakan konfigurasi pusat atau memiliki akun yang dikelola sendiri, Anda dapat kembali menggunakan nilai parameter default untuk akun Anda di satu Wilayah pada satu waktu.

Pilih metode yang Anda inginkan, dan ikuti langkah-langkah untuk kembali ke nilai parameter default untuk akun Anda di satu Wilayah. Untuk kembali ke nilai parameter default di Wilayah tambahan, ulangi langkah-langkah ini di setiap Wilayah tambahan.

> **Note**
>
> Jika Anda menonaktifkan Security Hub, parameter kontrol kustom Anda akan diatur ulang. Jika Anda mengaktifkan Security Hub lagi di masa mendatang, semua kontrol akan menggunakan nilai parameter default untuk memulai.

Security Hub console

Untuk kembali ke nilai parameter default dalam satu akun dan Wilayah

1. Buka AWS Security Hub konsol di https://console.aws.amazon.com/securityhub/.
2. Di panel navigasi, pilih Kontrol. Pilih kontrol yang ingin Anda kembalikan ke nilai parameter default.
3. Pada `Parameters` tab, pilih Disesuaikan di sebelah parameter kontrol. Kemudian, pilih Hapus kustomisasi. Parameter ini sekarang menggunakan nilai Security Hub default dan melacak update future ke nilai default.
4. Ulangi langkah sebelumnya untuk setiap nilai parameter yang ingin Anda kembalikan.

Security Hub API

Untuk kembali ke nilai parameter default dalam satu akun dan Wilayah

1. Memanggil UpdateSecurityControlAPI.
2. Untuk`SecurityControlId`, berikan ARN atau ID kontrol yang parameternya ingin Anda kembalikan.
3. Dalam `Parameters` objek, untuk setiap parameter yang ingin Anda kembalikan, sediakan `DEFAULT` untuk `ValueType` bidang. Ketika `ValueType` diatur ke`DEFAULT`, Anda tidak perlu

memberikan nilai untuk `Value` bidang tersebut. Jika nilai disertakan dalam permintaan Anda, Security Hub mengabaikannya.

4. Secara opsional, untuk`LastUpdateReason`, berikan alasan untuk kembali ke nilai parameter default.

Contoh permintaan API:

```
{
    "SecurityControlId": "ACM.1",
    "Parameters": {
        "daysToExpiration": {
            "ValueType": "DEFAULT"
        },
    "LastUpdateReason": "New internal requirement"
}
```

AWS CLI

Untuk kembali ke nilai parameter default dalam satu akun dan Wilayah

1. Jalankan perintah update-security-control.
2. Untuk`security-control-id`, berikan ARN atau ID kontrol yang parameternya ingin Anda kembalikan.
3. Dalam `parameters` objek, untuk setiap parameter yang ingin Anda kembalikan, sediakan `DEFAULT` untuk `ValueType` bidang. Ketika `ValueType` diatur ke`DEFAULT`, Anda tidak perlu memberikan nilai untuk `Value` bidang tersebut. Jika nilai disertakan dalam permintaan Anda, Security Hub mengabaikannya.
4. Secara opsional, untuk`last-update-reason`, berikan alasan untuk kembali ke nilai parameter default.

Contoh perintah:

```
$ aws securityhub update-security-control \
--region us-east-1 \
--security-control-id ACM.1 \
--parameters '{"daysToExpiration": {"ValueType": "DEFAULT"}}' \
--last-update-reason "New internal requirement"
```

Kontrol yang mendukung parameter kustom

Untuk daftar kontrol keamanan yang mendukung parameter kustom, Anda dapat merujuk ke halaman Kontrol di konsol Security Hub atauReferensi kontrol Security Hub. Untuk mengambil daftar ini secara terprogram, Anda dapat menggunakan operasi. ListSecurityControlDefinitions Dalam respons, `CustomizableProperties` objek menunjukkan kontrol mana yang mendukung parameter yang dapat disesuaikan.

Kontrol Security Hub yang mungkin ingin Anda nonaktifkan

Kami merekomendasikan untuk menonaktifkan beberapa AWS Security Hub kontrol untuk mengurangi kebisingan dan membatasi biaya.

Kontrol yang berhubungan dengan sumber daya global

Beberapa Layanan AWS mendukung sumber daya global, yang berarti Anda dapat mengakses sumber daya dari mana pun Wilayah AWS. Untuk menghemat biaya AWS Config, Anda dapat menonaktifkan perekaman sumber daya global di semua kecuali satu Wilayah. Namun, setelah Anda melakukannya, Security Hub tetap menjalankan pemeriksaan keamanan di semua Wilayah di mana kontrol diaktifkan dan menagih Anda berdasarkan jumlah cek per akun per Wilayah. Oleh karena itu, untuk mengurangi kebisingan dan menghemat biaya Security Hub, Anda juga harus menonaktifkan kontrol yang melibatkan sumber daya global di semua Wilayah kecuali Wilayah yang mencatat sumber daya global.

Jika kontrol melibatkan sumber daya global tetapi hanya tersedia di satu Wilayah, menonaktifkannya di Wilayah tersebut mencegah Anda mendapatkan temuan apa pun untuk sumber daya yang mendasarinya. Dalam hal ini, kami sarankan untuk tetap mengaktifkan kontrol. Saat menggunakan agregasi lintas wilayah, wilayah di mana kontrol tersedia harus merupakan Wilayah agregasi atau salah satu Wilayah yang ditautkan. Kontrol berikut melibatkan sumber daya global tetapi hanya tersedia di satu Wilayah:

- Semua CloudFront kontrol - Hanya tersedia di AS Timur (Virginia N.)
- GlobalAccelerator.1 — Hanya tersedia di AS Barat (Oregon)
- Route53.2 - Hanya tersedia di AS Timur (Virginia N.)
- WAF.1, WAF.6, WAF.7, dan WAF.8 - Hanya tersedia di AS Timur (Virginia N.)

> **Note**
>
> Jika Anda menggunakan konfigurasi pusat, Security Hub secara otomatis menonaktifkan kontrol yang melibatkan sumber daya global di semua Wilayah kecuali Wilayah asal. Kontrol lain yang Anda pilih untuk diaktifkan meskipun kebijakan konfigurasi diaktifkan di semua Wilayah yang tersedia. Untuk membatasi temuan untuk kontrol ini hanya pada satu Wilayah, Anda dapat memperbarui pengaturan AWS Config perekam dan menonaktifkan perekaman sumber daya global di semua Wilayah kecuali Wilayah asal. Saat Anda menggunakan konfigurasi pusat, Anda tidak memiliki cakupan untuk kontrol yang tidak tersedia di Wilayah asal dan Wilayah yang ditautkan. Untuk informasi selengkapnya tentang konfigurasi pusat, lihatCara kerja konfigurasi pusat.

Untuk kontrol dengan jenis jadwal berkala, menonaktifkannya di Security Hub diperlukan untuk mencegah penagihan. Menyetel AWS Config parameter `includeGlobalResourceTypes` ke `false` tidak memengaruhi kontrol Security Hub berkala.

Berikut ini adalah daftar kontrol Security Hub yang melibatkan sumber daya global:

- [Akun.1] Informasi kontak keamanan harus disediakan untuk Akun AWS
- [Akun.2] Akun AWS harus menjadi bagian dari organisasi AWS Organizations
- [CloudFront.1] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi
- [CloudFront.3] CloudFront distribusi harus memerlukan enkripsi dalam perjalanan
- [CloudFront.4] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi
- [CloudFront.5] CloudFront distribusi seharusnya mengaktifkan logging
- [CloudFront.6] CloudFront distribusi harus mengaktifkan WAF
- [CloudFront.7] CloudFront distribusi harus menggunakan sertifikat SSL/TLS khusus
- [CloudFront.8] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS
- [CloudFront.9] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus
- [CloudFront.10] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal khusus
- [CloudFront.12] CloudFront distribusi seharusnya tidak menunjukkan asal S3 yang tidak ada
- [CloudFront.13] CloudFront distribusi harus menggunakan kontrol akses asal
- [EventBridge.4] titik akhir EventBridge global harus mengaktifkan replikasi acara
- [GlobalAccelerator.1] Akselerator Akselerator Global harus diberi tag

- [IAM.1] Kebijakan IAM seharusnya tidak mengizinkan hak administratif “*” penuh
- [IAM.2] Pengguna IAM seharusnya tidak memiliki kebijakan IAM yang dilampirkan
- [IAM.3] Kunci akses pengguna IAM harus diputar setiap 90 hari atau kurang
- [IAM.4] Kunci akses pengguna root IAM seharusnya tidak ada
- [IAM.5] MFA harus diaktifkan untuk semua pengguna IAM yang memiliki kata sandi konsol
- [IAM.6] MFA perangkat keras harus diaktifkan untuk pengguna root
- [IAM.7] Kebijakan kata sandi untuk pengguna IAM harus memiliki konfigurasi yang kuat
- [IAM.8] Kredensyal pengguna IAM yang tidak digunakan harus dihapus
- [IAM.9] MFA harus diaktifkan untuk pengguna root
- [IAM.10] Kebijakan kata sandi untuk pengguna IAM harus memiliki urasi yang kuat AWS Config
- [IAM.11] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu huruf besar
- [IAM.12] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu huruf kecil
- [IAM.13] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu simbol
- [IAM.14] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu nomor
- [IAM.15] Pastikan kebijakan kata sandi IAM membutuhkan panjang kata sandi minimum 14 atau lebih
- [IAM.16] Pastikan kebijakan kata sandi IAM mencegah penggunaan kembali kata sandi
- [IAM.17] Pastikan kebijakan kata sandi IAM kedaluwarsa kata sandi dalam waktu 90 hari atau kurang
- [IAM.18] Memastikan peran dukungan telah dibuat untuk mengelola insiden dengan AWS Support
- [IAM.19] MFA harus diaktifkan untuk semua pengguna IAM
- [IAM.21] Kebijakan terkelola pelanggan IAM yang Anda buat seharusnya tidak mengizinkan tindakan wildcard untuk layanan
- [IAM.22] Kredensyal pengguna IAM yang tidak digunakan selama 45 hari harus dihapus
- [IAM.24] Peran IAM harus ditandai
- [IAM.25] Pengguna IAM harus diberi tag
- [IAM.26] Sertifikat SSL/TLS kedaluwarsa yang dikelola di IAM harus dihapus
- [IAM.27] Identitas IAM seharusnya tidak memiliki kebijakan yang dilampirkan AWSCloudShellFullAccess
- [KMS.1] Kebijakan yang dikelola pelanggan IAM tidak boleh mengizinkan tindakan dekripsi pada semua kunci KMS

- [KMS.2] Prinsipal IAM tidak boleh memiliki kebijakan inline IAM yang memungkinkan tindakan dekripsi pada semua kunci KMS
- [Route53.2] Route 53 zona yang dihosting publik harus mencatat kueri DNS
- [WAF.1] Pencatatan ACL Web Global AWS WAF Klasik harus diaktifkan
- [WAF.6] Aturan global AWS WAF klasik harus memiliki setidaknya satu syarat
- [WAF.7] Kelompok aturan global AWS WAF klasik harus memiliki setidaknya satu aturan
- [WAF.8] ACL web global AWS WAF klasik harus memiliki setidaknya satu aturan atau kelompok aturan
- [WAF.10] ACL AWS WAF web harus memiliki setidaknya satu aturan atau kelompok aturan
- [WAF.11] pencatatan ACL AWS WAF web harus diaktifkan

Kontrol yang berhubungan dengan CloudTrail logging

Kontrol ini berkaitan dengan penggunaan AWS Key Management Service (AWS KMS) untuk mengenkripsi log AWS CloudTrail jejak. Jika Anda mencatat jejak ini di akun logging terpusat, Anda hanya perlu mengaktifkan kontrol ini di akun dan Wilayah tempat pencatatan terpusat berlangsung.

> **Note**
>
> Jika Anda menggunakan konfigurasi pusat, status pengaktifan kontrol disejajarkan di seluruh Wilayah beranda dan Wilayah yang ditautkan. Anda tidak dapat menonaktifkan kontrol di beberapa Wilayah dan mengaktifkannya di wilayah lain. Dalam hal ini, tekan temuan dari kontrol berikut untuk mengurangi kebisingan temuan.

- [CloudTrail.2] CloudTrail harus mengaktifkan enkripsi saat istirahat

Kontrol yang menangani CloudWatch alarm

Jika Anda lebih suka menggunakan Amazon GuardDuty untuk deteksi anomali daripada CloudWatch alarm Amazon, Anda dapat menonaktifkan kontrol ini, yang berfokus pada alarm. CloudWatch

- [CloudWatch.1] Filter metrik log dan alarm harus ada untuk penggunaan pengguna “root”
- [CloudWatch.2] Pastikan filter metrik log dan alarm ada untuk panggilan API yang tidak sah
- [CloudWatch.3] Pastikan filter metrik log dan alarm ada untuk login Konsol Manajemen tanpa MFA

- [CloudWatch.4] Pastikan filter metrik log dan alarm ada untuk perubahan kebijakan IAM
- [CloudWatch.5] Pastikan filter metrik log dan alarm ada untuk perubahan CloudTrail AWS Config urasi
- [CloudWatch.6] Pastikan filter metrik log dan alarm ada untuk kegagalan AWS Management Console otentikasi
- [CloudWatch.7] Pastikan filter metrik log dan alarm ada untuk menonaktifkan atau menjadwalkan penghapusan kunci yang dikelola pelanggan
- [CloudWatch.8] Pastikan filter metrik log dan alarm ada untuk perubahan kebijakan bucket S3
- [CloudWatch.9] Pastikan filter metrik log dan alarm ada untuk perubahan AWS Config konfigurasi
- [CloudWatch.10] Pastikan filter metrik log dan alarm ada untuk perubahan grup keamanan
- [CloudWatch.11] Pastikan filter metrik log dan alarm ada untuk perubahan pada Daftar Kontrol Akses Jaringan (NACL)
- [CloudWatch.12] Pastikan filter metrik log dan alarm ada untuk perubahan pada gateway jaringan
- [CloudWatch.13] Pastikan filter metrik log dan alarm ada untuk perubahan tabel rute
- [CloudWatch.14] Pastikan filter metrik log dan alarm ada untuk perubahan VPC

Melihat detail untuk kontrol

Untuk setiap AWS Security Hub kontrol, Anda dapat menampilkan halaman detail yang berguna.

Bagian atas halaman detail kontrol memberikan ikhtisar kontrol, termasuk:

- Status pengaktifan — Bagian atas halaman memberi tahu Anda apakah kontrol diaktifkan untuk setidaknya satu standar di setidaknya satu akun anggota. Jika Anda telah menetapkan Wilayah agregasi, kontrol diaktifkan jika diaktifkan untuk setidaknya satu standar di setidaknya satu Wilayah. Jika kontrol dinonaktifkan, Anda dapat mengaktifkannya dari halaman ini. Jika kontrol diaktifkan, Anda dapat menonaktifkannya dari halaman ini. Untuk informasi selengkapnya, lihat the section called “Mengaktifkan dan menonaktifkan kontrol di semua standar”.
- Status kontrol — Status ini merangkum kinerja kontrol berdasarkan status kepatuhan temuan kontrol. Security Hub biasanya menghasilkan status kontrol awal dalam waktu 30 menit setelah kunjungan pertama Anda ke halaman Ringkasan atau halaman standar Keamanan di konsol Security Hub. Status hanya tersedia untuk kontrol yang diaktifkan saat Anda mengunjungi halaman tersebut. Gunakan operasi `UpdateStandardsControl`API untuk mengaktifkan atau menonaktifkan kontrol. Selain itu, perekaman AWS Config sumber daya harus dikonfigurasi agar status kontrol muncul. Setelah status kontrol dibuat untuk pertama kalinya, Security Hub

memperbarui status kontrol setiap 24 jam berdasarkan temuan dari 24 jam sebelumnya. Pada halaman detail standar dan halaman detail kontrol, Security Hub menampilkan stempel waktu untuk menunjukkan kapan status terakhir diperbarui.

Akun administrator melihat status kontrol gabungan di seluruh akun administrator dan akun anggota. Jika Anda telah menetapkan Wilayah agregasi, status kontrol mencakup temuan di semua Wilayah tertaut. Untuk informasi selengkapnya tentang status kontrol, lihatthe section called "Status kepatuhan dan status kontrol".

> **Note**
>
> Ini dapat memakan waktu hingga 24 jam setelah memungkinkan kontrol untuk status kontrol pertama kali yang akan dihasilkan di Wilayah China dan. AWS GovCloud (US) Region

Tab Standar dan Persyaratan mencantumkan standar yang dapat diaktifkan oleh kontrol dan persyaratan yang terkait dengan kontrol dari kerangka kerja kepatuhan yang berbeda.

Bagian bawah halaman detail berisi informasi tentang temuan aktif untuk kontrol. Temuan kontrol dihasilkan oleh pemeriksaan keamanan terhadap kontrol. Daftar temuan kontrol tidak termasuk temuan yang diarsipkan.

Daftar temuan menggunakan tab yang menampilkan subset daftar yang berbeda. Pada sebagian besar tab, daftar temuan menunjukkan temuan yang memiliki status alur kerja`NEW`,`NOTIFIED`, atau. `RESOLVED` Tab terpisah menampilkan `SUPPRESSED` temuan.

Untuk setiap temuan, daftar menyediakan akses untuk menemukan detail seperti status kepatuhan dan sumber daya terkait. Anda juga dapat mengatur status alur kerja setiap temuan dan mengirim temuan ke tindakan kustom. Untuk informasi selengkapnya, lihat the section called "Melihat dan mengambil tindakan atas temuan kontrol".

Melihat detail untuk kontrol

Pilih metode akses pilihan Anda, dan ikuti langkah-langkah ini untuk melihat detail untuk kontrol. Detail berlaku untuk akun saat ini dan Wilayah dan termasuk yang berikut:

- Judul dan deskripsi kontrol
- Tautan ke instruksi remediasi untuk temuan kontrol yang gagal
- Tingkat keparahan kontrol

- Status pemberdayaan kontrol
- (Di konsol) Daftar temuan terbaru untuk kontrol. Saat menggunakan Security Hub API atau AWS CLI, gunakan `GetFindings`untuk mengambil temuan kontrol.

Security Hub console

1. Buka AWS Security Hub konsol di https://console.aws.amazon.com/securityhub/.
2. Pilih Kontrol di panel navigasi.
3. Pilih kontrol.

Security Hub API

1. Jalankan`ListSecurityControlDefinitions`, dan berikan satu atau lebih ARN standar untuk mendapatkan daftar ID kontrol untuk standar itu. Untuk mendapatkan ARN standar, jalankan `DescribeStandards`. Jika Anda tidak menyediakan ARN standar, API ini mengembalikan semua ID kontrol Security Hub. API ini mengembalikan ID kontrol keamanan agnostik standar, bukan ID kontrol berbasis standar yang ada sebelum rilis fitur ini.

   Contoh permintaan:

   ```
   {
       "StandardsArn": "arn:aws:securityhub:::standards/aws-foundational-security-best-practices/v/1.0.0"
   }
   ```

2. Jalankan `BatchGetSecurityControls` untuk mendapatkan detail tentang satu atau lebih kontrol saat ini Akun AWS dan Wilayah AWS.

   Contoh permintaan:

   ```
   {
       "SecurityControlIds": ["Config.1", "IAM.1"]
   }
   ```

AWS CLI

1. Jalankan `list-security-control-definitions` perintah, dan berikan satu atau lebih ARN standar untuk mendapatkan daftar ID kontrol. Untuk mendapatkan ARN standar,

jalankan `describe-standards` perintah. Jika Anda tidak menyediakan ARN standar, perintah ini mengembalikan semua ID kontrol Security Hub. Perintah ini mengembalikan ID kontrol keamanan agnostik standar, bukan ID kontrol berbasis standar yang ada sebelum rilis fitur ini.

```
aws securityhub --region us-east-1 list-security-control-definitions --
standards-arn "arn:aws:securityhub:us-east-1::standards/aws-foundational-
security-best-practices/v/1.0.0"
```

2. Jalankan [batch-get-security-controls](#) perintah untuk mendapatkan detail tentang satu atau lebih kontrol saat ini Akun AWS dan Wilayah AWS.

```
aws securityhub --region us-east-1 batch-get-security-controls --security-
control-ids '["Config.1", "IAM.1"]'
```

Memfilter dan menyortir daftar kontrol

Pada halaman Kontrol, Anda dapat melihat daftar kontrol Anda. Anda dapat memfilter dan mengurutkan daftar untuk fokus pada subset kontrol tertentu.

- Semua diaktifkan (kontrol yang diaktifkan setidaknya dalam satu standar yang diaktifkan)
- Gagal (kontrol dengan `Failed` status)
- Tidak diketahui (kontrol dengan `Unknown` status)
- Lulus (kontrol dengan `Passed` status)
- Dinonaktifkan (kontrol yang dinonaktifkan di semua standar)
- Tidak ada data (kontrol tanpa temuan)
- Semua (semua kontrol, baik diaktifkan maupun dinonaktifkan, dan tanpa memperhatikan status kontrol atau jumlah temuan)

Untuk informasi selengkapnya tentang status kontrol, lihatStatus kepatuhan dan status kontrol.

Jika Anda menggunakan integrasi dengan AWS Organizations dan masuk ke akun AWS Security Hub administrator, tab Semua diaktifkan mencakup kontrol yang diaktifkan di setidaknya satu akun anggota. Jika Anda telah menetapkan Wilayah agregasi, tab Semua diaktifkan menyertakan kontrol yang diaktifkan di setidaknya satu Wilayah tertaut.

Tab Gagal ditampilkan secara default. Pada setiap tab, kontrol secara default diurutkan berdasarkan tingkat keparahan, dari Kritis ke Rendah. Anda juga dapat mengurutkan kontrol berdasarkan ID kontrol, status kepatuhan, tingkat keparahan, atau jumlah pemeriksaan yang gagal. Bilah pencarian memungkinkan Anda untuk mencari kontrol tertentu.

> **Tip**
>
> Jika Anda memiliki alur kerja otomatis berdasarkan temuan kontrol, sebaiknya gunakan bidang `SecurityControlId` atau `SecurityControlArn` ASFF sebagai filter, bukan `Title` atau. `Description` Bidang yang terakhir dapat berubah sesekali, sedangkan ID kontrol dan ARN adalah pengidentifikasi statis.

Memilih opsi di sebelah kontrol memunculkan panel samping yang menampilkan standar di mana kontrol saat ini diaktifkan. Anda juga dapat melihat standar di mana kontrol saat ini dinonaktifkan. Dari panel ini, Anda dapat menonaktifkan kontrol dengan menonaktifkannya di semua standar. Untuk informasi selengkapnya tentang mengaktifkan dan menonaktifkan kontrol di seluruh standar, lihat. Mengaktifkan dan menonaktifkan kontrol di semua standar Untuk akun administrator, informasi yang disajikan di panel samping mencerminkan semua akun anggota.

Pada Security Hub API, jalankan `ListSecurityControlDefinitions`untuk mendapatkan kembali daftar ID kontrol. Setelah Anda memiliki ID kontrol yang Anda minati, jalankan `BatchGetSecurityControls`untuk mendapatkan data tentang subset kontrol untuk saat ini Akun AWS dan Wilayah AWS.

Melihat dan mengambil tindakan atas temuan kontrol

Halaman detail kontrol menampilkan daftar temuan aktif untuk kontrol. Daftar ini tidak termasuk temuan yang diarsipkan.

Halaman detail kontrol mendukung pencarian agregasi. Jika Anda telah menetapkan Wilayah agregasi, status kontrol dan daftar pemeriksaan keamanan pada halaman detail kontrol mencakup pemeriksaan dari semua yang ditautkan Wilayah AWS.

Daftar ini menyediakan alat untuk memfilter dan mengurutkan temuan, sehingga Anda dapat fokus pada temuan yang lebih mendesak terlebih dahulu. Temuan dapat mencakup tautan ke detail sumber daya di konsol layanan terkait. Untuk kontrol yang didasarkan pada AWS Config aturan, Anda dapat melihat detail tentang aturan dan timeline konfigurasi.

Anda juga dapat menggunakan AWS Security Hub API untuk mengambil daftar temuan. Untuk informasi selengkapnya, lihat the section called “Meninjau detail temuan”.

Topik

- Melihat detail tentang pencarian kontrol dan menemukan sumber daya
- Temuan kontrol sampel
- Memfilter, menyortir, dan mengunduh temuan kontrol
- Mengambil tindakan atas temuan kontrol

Melihat detail tentang pencarian kontrol dan menemukan sumber daya

AWS Security Hub memberikan rincian berikut untuk setiap temuan kontrol untuk membantu Anda menyelidikinya:

- Riwayat perubahan yang dibuat pengguna terhadap temuan
- `.json`File untuk temuan
- Informasi tentang sumber daya yang terkait dengan temuan
- Aturan konfigurasi yang terkait dengan temuan
- Catatan bahwa pengguna telah menambahkan ke temuan

Bagian berikut menjelaskan cara mengakses detail ini.

Menemukan sejarah

Menemukan riwayat adalah fitur Security Hub yang memungkinkan Anda melacak perubahan yang dibuat pada temuan selama 90 hari terakhir.

Riwayat temuan tersedia untuk temuan kontrol dan temuan Security Hub lainnya. Untuk informasi selengkapnya, lihat Meninjau riwayat penemuan.

Melihat .json lengkap untuk sebuah temuan

Anda dapat menampilkan dan mengunduh temuan penuh `.json`.

Untuk menampilkan `.json`, di kolom Finding .json, pilih ikon.

Pada panel Finding JSON, untuk mengunduh `.json`, pilih Unduh.

Melihat informasi tentang sumber daya temuan

Kolom Resource berisi tipe sumber daya dan pengidentifikasi sumber daya.

Untuk menampilkan informasi tentang sumber daya, pilih pengenal sumber daya. Untuk Akun AWS, jika akun tersebut adalah akun anggota organisasi, maka informasi tersebut mencakup ID akun dan nama akun. Untuk akun yang diundang secara manual, informasi hanya menyertakan ID akun.

Jika Anda memiliki izin untuk melihat sumber daya dalam layanan aslinya, maka pengidentifikasi sumber daya menampilkan tautan ke layanan. Misalnya, untuk AWS pengguna, detail sumber daya menyediakan tautan ke tampilan detail pengguna di IAM.

Jika sumber daya berada di akun lain, Security Hub menampilkan pesan untuk memberi tahu Anda.

Melihat timeline konfigurasi untuk menemukan sumber daya

Salah satu jalan investigasi adalah garis waktu konfigurasi untuk sumber daya di. AWS Config

Jika Anda memiliki izin untuk melihat garis waktu konfigurasi untuk sumber daya pencarian, maka daftar temuan menyediakan tautan ke garis waktu.

Security Hub menampilkan pesan untuk memberi tahu Anda jika sumber daya berada di akun yang berbeda.

Untuk menavigasi ke timeline konfigurasi di AWS Config

1. Di kolom Selidiki, pilih ikon.
2. Pada menu, pilih Timeline konfigurasi. Jika Anda tidak memiliki akses ke timeline konfigurasi, maka tautan tidak muncul.

Melihat AWS Config aturan untuk menemukan sumber daya

Jika kontrol didasarkan pada AWS Config aturan, maka Anda mungkin juga ingin melihat detail untuk AWS Config aturan tersebut. Informasi AWS Config aturan dapat membantu Anda mendapatkan pemahaman yang lebih baik mengapa cek lulus atau gagal.

Jika Anda memiliki izin untuk melihat AWS Config aturan untuk kontrol, maka daftar temuan menyediakan tautan ke AWS Config aturan di AWS Config.

Security Hub menampilkan pesan untuk memberi tahu Anda jika sumber daya berada di akun yang berbeda.

Untuk menavigasi ke AWS Config aturan

1. Di kolom Selidiki, pilih ikonnya.
2. Pada menu, pilih Aturan Config. Jika Anda tidak memiliki akses ke AWS Config aturan, maka aturan Config tidak ditautkan.

Melihat catatan untuk temuan

Jika temuan memiliki catatan terkait, maka kolom Diperbarui menampilkan ikon catatan.

Untuk menampilkan catatan yang terkait dengan temuan

Di kolom Diperbarui, pilih ikon catatan.

Temuan kontrol sampel

Format temuan kontrol bervariasi tergantung pada apakah Anda telah mengaktifkan temuan kontrol konsolidasi. Saat Anda mengaktifkan fitur ini, Security Hub menghasilkan satu temuan untuk pemeriksaan kontrol bahkan ketika kontrol berlaku untuk beberapa standar yang diaktifkan. Untuk informasi selengkapnya, lihat Temuan kontrol terkonsolidasi.

Bagian berikut menunjukkan temuan kontrol sampel. Ini termasuk temuan dari setiap standar Security Hub ketika temuan kontrol konsolidasi dimatikan di akun Anda, dan temuan kontrol sampel di seluruh standar saat diaktifkan.

> **Note**
>
> Temuan akan mereferensikan berbagai bidang dan nilai di Wilayah dan AWS GovCloud (US) Wilayah China. Untuk informasi selengkapnya, lihat Dampak konsolidasi pada bidang dan nilai ASFF.

Temuan kontrol konsolidasi dimatikan

- Temuan sampel untuk AWS standar Praktik Terbaik Keamanan Dasar (FSBP)
- Temuan sampel untuk Tolok Ukur AWS Yayasan Center for Internet Security (CIS) v1.2.0
- Temuan sampel untuk Benchmark AWS Yayasan Center for Internet Security (CIS) v1.4.0
- Temuan sampel untuk Tolok Ukur AWS Yayasan Center for Internet Security (CIS) v3.0.0

- Temuan sampel untuk Institut Nasional Standar dan Teknologi (NIST) SP 800-53 Rev. 5
- Temuan sampel untuk Standar Keamanan Data Industri Kartu Pembayaran (PCI DSS)
- Temuan sampel untuk Standar Penandaan AWS Sumber Daya
- Temuan sampel untuk Standar yang Dikelola Layanan: AWS Control Tower

Temuan kontrol konsolidasi dihidupkan

- Temuan sampel di seluruh standar

Temuan sampel untuk FSBP


```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-2:123456789012:subscription/aws-foundational-
security-best-practices/v/1.0.0/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-2::product/aws/securityhub",
  "ProductName": "Security Hub",
  "CompanyName": "AWS",
  "Region": "us-east-2",
  "GeneratorId": "aws-foundational-security-best-practices/v/1.0.0/CloudTrail.2",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards/AWS-
Foundational-Security-Best-Practices"
  ],
  "FirstObservedAt": "2020-08-06T02:18:23.076Z",
  "LastObservedAt": "2021-09-28T16:10:06.956Z",
  "CreatedAt": "2020-08-06T02:18:23.076Z",
  "UpdatedAt": "2021-09-28T16:10:00.093Z",
  "Severity": {
    "Product": 40,
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
  },
  "Title": "CloudTrail.2 CloudTrail should have encryption at-rest enabled",
  "Description": "This AWS control checks whether AWS CloudTrail is configured to use
 the server side encryption (SSE) AWS Key Management Service (AWS KMS) customer master
 key (CMK) encryption. The check will pass if the KmsKeyId is defined.",
  "Remediation": {
```

```
    "Recommendation": {
      "Text": "For directions on how to correct this issue, consult the AWS Security
 Hub controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
    }
  },
  "ProductFields": {
    "StandardsArn": "arn:aws:securityhub:::standards/aws-foundational-security-best-
practices/v/1.0.0",
    "StandardsSubscriptionArn": "arn:aws:securityhub:us-
east-2:123456789012:subscription/aws-foundational-security-best-practices/v/1.0.0",
    "ControlId": "CloudTrail.2",
    "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/
remediation",
    "Related AWS Resources:0/name": "securityhub-cloud-trail-encryption-enabled-
fe95bf3f",
    "Related AWS Resources:0/type": "AWS::Config::ConfigRule",
    "StandardsControlArn": "arn:aws:securityhub:us-east-2:123456789012:control/aws-
foundational-security-best-practices/v/1.0.0/CloudTrail.2",
    "aws/securityhub/ProductName": "Security Hub",
    "aws/securityhub/CompanyName": "AWS",
    "Resources:0/Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWS MacieTrail-
DO-NOT-EDIT",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-2::product/aws/
securityhub/arn:aws:securityhub:us-east-2:123456789012:subscription/aws-foundational-
security-best-practices/v/1.0.0/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111"
  },
  "Resources": [
    {
      "Type": "AwsCloudTrailTrail",
      "Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWS MacieTrail-DO-NOT-
EDIT",
      "Partition": "aws",
      "Region": "us-east-2"
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "SecurityControlId": "CloudTrail.2",
    "AssociatedStandards": [{
      "StandardsId": "standards/aws-foundation-best-practices/v/1.0.0"
    }]
  },
```

```
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    },
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards/AWS-
Foundational-Security-Best-Practices"
    ]
  }
}
```

Temuan sampel untuk CIS AWS Foundations Benchmark v3.0.0

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-1:123456789012:subscription/cis-aws-foundations-
benchmark/v/3.0.0/2.2.1/finding/38a89798-6819-4fae-861f-9cca8034602c",
  "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/securityhub",
  "ProductName": "Security Hub",
  "CompanyName": "AWS",
  "Region": "us-east-1",
  "GeneratorId": "cis-aws-foundations-benchmark/v/3.0.0/2.2.1",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards/CIS AWS
 Foundations Benchmark"
  ],
  "FirstObservedAt": "2024-04-18T07:46:18.193Z",
  "LastObservedAt": "2024-04-23T07:47:01.137Z",
  "CreatedAt": "2024-04-18T07:46:18.193Z",
  "UpdatedAt": "2024-04-23T07:46:46.165Z",
  "Severity": {
    "Product": 40,
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
```

```
  },
  "Title": "2.2.1 EBS default encryption should be enabled",
  "Description": "Elastic Compute Cloud (EC2) supports encryption at rest when using
 the Elastic Block Store (EBS) service. While disabled by default, forcing encryption
 at EBS volume creation is supported.",
  "Remediation": {
    "Recommendation": {
      "Text": "For information on how to correct this issue, consult the AWS Security
 Hub controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/EC2.7/remediation"
    }
  },
  "ProductFields": {
    "StandardsArn": "arn:aws:securityhub:::standards/cis-aws-foundations-benchmark/
v/3.0.0",
    "StandardsSubscriptionArn": "arn:aws:securityhub:us-
east-1:123456789012:subscription/cis-aws-foundations-benchmark/v/3.0.0",
    "ControlId": "2.2.1",
    "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/EC2.7/
remediation",
    "RelatedAWSResources:0/name": "securityhub-ec2-ebs-encryption-by-default-2843ed9e",
    "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
    "StandardsControlArn": "arn:aws:securityhub:us-east-1:123456789012:control/cis-aws-
foundations-benchmark/v/3.0.0/2.2.1",
    "aws/securityhub/ProductName": "Security Hub",
    "aws/securityhub/CompanyName": "AWS",
    "aws/securityhub/annotation": "EBS Encryption by default is not enabled.",
    "Resources:0/Id": "arn:aws:iam::123456789012:root",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/
securityhub/arn:aws:securityhub:us-east-1:123456789012:subscription/cis-aws-
foundations-benchmark/v/3.0.0/2.2.1/finding/38a89798-6819-4fae-861f-9cca8034602c"
  },
  "Resources": [
    {
      "Type": "AwsAccount",
      "Id": "AWS::::Account:123456789012",
      "Partition": "aws",
      "Region": "us-east-1"
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "RelatedRequirements": [
      "CIS AWS Foundations Benchmark v3.0.0/2.2.1"
```

```
    ],
    "SecurityControlId": "EC2.7",
    "AssociatedStandards": [
      {
        "StandardsId": "standards/cis-aws-foundations-benchmark/v/3.0.0"
      }
    ]
  },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    },
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards/CIS AWS
 Foundations Benchmark"
    ]
  },
  "ProcessedAt": "2024-04-23T07:47:07.088Z"
}
```

Temuan sampel untuk CIS AWS Foundations Benchmark v1.4.0

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-1:123456789012:subscription/cis-aws-foundations-
benchmark/v/1.4.0/3.7/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/securityhub",
  "ProductName": "Security Hub",
  "CompanyName": "AWS",
  "Region": "us-east-1",
  "GeneratorId": "cis-aws-foundations-benchmark/v/1.4.0/3.7",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards/CIS AWS
 Foundations Benchmark"
  ],
  "FirstObservedAt": "2022-10-21T22:14:48.913Z",
```

```
  "LastObservedAt": "2022-12-22T22:24:56.980Z",
  "CreatedAt": "2022-10-21T22:14:48.913Z",
  "UpdatedAt": "2022-12-22T22:24:52.409Z",
  "Severity": {
    "Product": 40,
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
  },
  "Title": "3.7 Ensure CloudTrail logs are encrypted at rest using KMS CMKs",
  "Description": "AWS CloudTrail is a web service that records AWS API calls for an
 account and makes those logs available to users and resources in accordance with IAM
 policies. AWS Key Management Service (KMS) is a managed service that helps create
 and control the encryption keys used to encrypt account data, and uses Hardware
 Security Modules (HSMs) to protect the security of encryption keys. CloudTrail logs
 can be configured to leverage server side encryption (SSE) and AWS KMS customer
 created master keys (CMK) to further protect CloudTrail logs. It is recommended that
 CloudTrail be configured to use SSE-KMS.",
  "Remediation": {
    "Recommendation": {
      "Text": "For directions on how to correct this issue, consult the AWS Security
 Hub controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
    }
  },
  "ProductFields": {
    "StandardsArn": "arn:aws:securityhub:::standards/cis-aws-foundations-benchmark/
v/1.4.0",
    "StandardsSubscriptionArn": "arn:aws:securityhub:us-
east-1:123456789012:subscription/cis-aws-foundations-benchmark/v/1.4.0",
    "ControlId": "3.7",
    "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/
remediation",
    "RelatedAWSResources:0/name": "securityhub-cloud-trail-encryption-
enabled-855f82d1",
    "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
    "StandardsControlArn": "arn:aws:securityhub:us-east-1:123456789012:control/cis-aws-
foundations-benchmark/v/1.4.0/3.7",
    "aws/securityhub/ProductName": "Security Hub",
    "aws/securityhub/CompanyName": "AWS",
    "Resources:0/Id": "arn:aws:cloudtrail:us-west-2:123456789012:trail/AWS MacieTrail-
DO-NOT-EDIT",
```

```
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/
securityhub/arn:aws:securityhub:us-east-1:123456789012:subscription/cis-aws-
foundations-benchmark/v/1.4.0/3.7/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  },
  "Resources": [
    {
      "Type": "AwsCloudTrailTrail",
      "Id": "arn:aws:cloudtrail:us-west-2:123456789012:trail/AWS MacieTrail-DO-NOT-
EDIT",
      "Partition": "aws",
      "Region": "us-east-1"
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "RelatedRequirements": [
      "CIS AWS Foundations Benchmark v1.4.0/3.7"
    ],
    "SecurityControlId": "CloudTrail.2",
    "AssociatedStandards": [{
      "StandardsId": "standards/cis-aws-foundations-benchmark/v/1.4.0"
    }]
  },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    },
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards/CIS AWS
 Foundations Benchmark"
    ]
  }
}
```

Temuan sampel untuk CIS AWS Foundations Benchmark v1.2.0

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-2:123456789012:subscription/cis-aws-foundations-
benchmark/v/1.2.0/2.7/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-2::product/aws/securityhub",
  "ProductName": "Security Hub",
  "CompanyName": "AWS",
  "Region": "us-east-2",
  "GeneratorId": "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/
rule/2.7",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards/CIS AWS
 Foundations Benchmark"
  ],
  "FirstObservedAt": "2020-08-29T04:10:06.337Z",
  "LastObservedAt": "2021-09-28T16:10:05.350Z",
  "CreatedAt": "2020-08-29T04:10:06.337Z",
  "UpdatedAt": "2021-09-28T16:10:00.087Z",
  "Severity": {
    "Product": 40,
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
  },
  "Title": "2.7 Ensure CloudTrail logs are encrypted at rest using KMS CMKs",
  "Description": "AWS Key Management Service (KMS) is a managed service that helps
 create and control the encryption keys used to encrypt account data, and uses Hardware
 Security Modules (HSMs) to protect the security of encryption keys. CloudTrail
 logs can be configured to leverage server side encryption (SSE) and KMS customer
 created master keys (CMK) to further protect CloudTrail logs. It is recommended that
 CloudTrail be configured to use SSE-KMS.",
  "Remediation": {
    "Recommendation": {
      "Text": "For directions on how to correct this issue, consult the AWS Security
 Hub controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
    }
  },
  "ProductFields": {
    "StandardsGuideArn": "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0",
    "StandardsGuideSubscriptionArn": "arn:aws:securityhub:us-
east-2:123456789012:subscription/cis-aws-foundations-benchmark/v/1.2.0",
```

```
    "RuleId": "2.7",
    "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/
remediation",
    "Related AWS Resources:0/name": "securityhub-cloud-trail-encryption-enabled-
fe95bf3f",
    "Related AWS Resources:0/type": "AWS::Config::ConfigRule",
    "StandardsControlArn": "arn:aws:securityhub:us-east-2:123456789012:control/cis-aws-
foundations-benchmark/v/1.2.0/2.7",
    "aws/securityhub/ProductName": "Security Hub",
    "aws/securityhub/CompanyName": "AWS",
    "Resources:0/Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWS MacieTrail-
DO-NOT-EDIT",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-2::product/aws/
securityhub/arn:aws:securityhub:us-east-2:123456789012:subscription/cis-aws-
foundations-benchmark/v/1.2.0/2.7/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  },
  "Resources": [
    {
      "Type": "AwsCloudTrailTrail",
      "Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWS MacieTrail-DO-NOT-
EDIT",
      "Partition": "aws",
      "Region": "us-east-2"
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "SecurityControlId": "CloudTrail.2",
    "AssociatedStandards": [{
      "StandardsId": "ruleset/cis-aws-foundations-benchmark/v/1.2.0"
    }]
  },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    },
    "Types": [
```

```
      "Software and Configuration Checks/Industry and Regulatory Standards/CIS AWS
 Foundations Benchmark"
    ]
  }
}
```

Temuan sampel untuk NIST SP 800-53 Rev. 5

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-1:123456789012:subscription/nist-800-53/v/5.0.0/
CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/securityhub",
  "ProductName": "Security Hub",
  "CompanyName": "AWS",
  "Region": "us-east-1",
  "GeneratorId": "nist-800-53/v/5.0.0/CloudTrail.2",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards"
  ],
  "FirstObservedAt": "2023-02-17T14:22:46.726Z",
  "LastObservedAt": "2023-02-17T14:22:50.846Z",
  "CreatedAt": "2023-02-17T14:22:46.726Z",
  "UpdatedAt": "2023-02-17T14:22:46.726Z",
  "Severity": {
    "Product": 40,
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
  },
  "Title": "CloudTrail.2 CloudTrail should have encryption at-rest enabled",
  "Description": "This AWS control checks whether AWS CloudTrail is configured to use
 the server side encryption (SSE) AWS Key Management Service (AWS KMS) customer master
 key (CMK) encryption. The check will pass if the KmsKeyId is defined.",
  "Remediation": {
    "Recommendation": {
      "Text": "For directions on how to fix this issue, consult the AWS Security Hub
 NIST 800-53 R5 documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
    }
  },
  "ProductFields": {
```

```
    "StandardsArn": "arn:aws:securityhub:::standards/nist-800-53/v/5.0.0",
    "StandardsSubscriptionArn": "arn:aws:securityhub:us-
east-1:123456789012:subscription/nist-800-53/v/5.0.0",
    "ControlId": "CloudTrail.2",
    "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.9/
remediation",
    "RelatedAWSResources:0/name": "securityhub-cloud-trail-encryption-enabled-
fe95bf3f",
    "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
    "StandardsControlArn": "arn:aws:securityhub:us-east-2:123456789012:control/aws-
foundational-security-best-practices/v/1.0.0/CloudTrail.2",
    "aws/securityhub/ProductName": "Security Hub",
    "aws/securityhub/CompanyName": "AWS",
    "Resources:0/Id": "arn:aws:cloudtrail:us-west-2:123456789012:trail/AWS MacieTrail-
DO-NOT-EDIT",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/
securityhub/arn:aws:securityhub:us-east-1:123456789012:subscription/nist-800-53/
v/5.0.0/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  },
  "Resources": [
    {
      "Type": "AwsCloudTrailTrail",

      "Id": "arn:aws:cloudtrail:us-east-1:123456789012:trail/AWS MacieTrail-DO-NOT-
EDIT",

      "Partition": "aws",

      "Region": "us-east-1"
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "RelatedRequirements": [
        "NIST.800-53.r5 AU-9",
        "NIST.800-53.r5 CA-9(1)",
        "NIST.800-53.r5 CM-3(6)",
        "NIST.800-53.r5 SC-13",
        "NIST.800-53.r5 SC-28",
        "NIST.800-53.r5 SC-28(1)",
        "NIST.800-53.r5 SC-7(10)",
        "NIST.800-53.r5 SI-7(6)"
    ],
    "SecurityControlId": "CloudTrail.2",
```

```
    "AssociatedStandards": [
      {
        "StandardsId": "standards/nist-800-53/v/5.0.0"
      }
    ]
  },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    },
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards"
    ]
  },
  "ProcessedAt": "2023-02-17T14:22:53.572Z"
}
```

Temuan sampel untuk PCI DSS

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-2:123456789012:subscription/pci-dss/v/3.2.1/
PCI.CloudTrail.1/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-2::product/aws/securityhub",
  "ProductName": "Security Hub",
  "CompanyName": "AWS",
  "Region": "us-east-2",
  "GeneratorId": "pci-dss/v/3.2.1/PCI.CloudTrail.1",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards/PCI-DSS"
  ],
  "FirstObservedAt": "2020-08-06T02:18:23.089Z",
  "LastObservedAt": "2021-09-28T16:10:06.942Z",
  "CreatedAt": "2020-08-06T02:18:23.089Z",
  "UpdatedAt": "2021-09-28T16:10:00.090Z",
  "Severity": {
```

```
    "Product": 40,
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
  },
  "Title": "PCI.CloudTrail.1 CloudTrail logs should be encrypted at rest using AWS KMS
 CMKs",
  "Description": "This AWS control checks whether AWS CloudTrail is configured to use
 the server side encryption (SSE) AWS Key Management Service (AWS KMS) customer master
 key (CMK) encryption by checking if the KmsKeyId is defined.",
  "Remediation": {
    "Recommendation": {
      "Text": "For directions on how to correct this issue, consult the AWS Security
 Hub controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
    }
  },
  "ProductFields": {
    "StandardsArn": "arn:aws:securityhub:::standards/pci-dss/v/3.2.1",
    "StandardsSubscriptionArn": "arn:aws:securityhub:us-
east-2:123456789012:subscription/pci-dss/v/3.2.1",
    "ControlId": "PCI.CloudTrail.1",
    "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/
remediation",
    "Related AWS Resources:0/name": "securityhub-cloud-trail-encryption-enabled-
fe95bf3f",
    "Related AWS Resources:0/type": "AWS::Config::ConfigRule",
    "StandardsControlArn": "arn:aws:securityhub:us-east-2:123456789012:control/pci-dss/
v/3.2.1/PCI.CloudTrail.1",
    "aws/securityhub/ProductName": "Security Hub",
    "aws/securityhub/CompanyName": "AWS",
    "Resources:0/Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWS MacieTrail-
DO-NOT-EDIT",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-2::product/aws/
securityhub/arn:aws:securityhub:us-east-2:123456789012:subscription/pci-dss/v/3.2.1/
PCI.CloudTrail.1/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  },
  "Resources": [
    {
      "Type": "AwsCloudTrailTrail",
      "Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWS MacieTrail-DO-NOT-
EDIT",
      "Partition": "aws",
      "Region": "us-east-2"
```

```
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "RelatedRequirements": [
      "PCI DSS 3.4"
    ],
    "SecurityControlId": "CloudTrail.2",
    "AssociatedStandards": [{
      "StandardsId": "standards/pci-dss/v/3.2.1"
    }]
  },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    },
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards/PCI-DSS"
    ]
  }
}
```

Temuan sampel untuk Standar Penandaan AWS Sumber Daya

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:eu-central-1:123456789012:security-control/EC2.44/finding/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:eu-central-1::product/aws/securityhub",
  "ProductName": "Security Hub",
  "CompanyName": "AWS",
  "Region": "eu-central-1",
  "GeneratorId": "security-control/EC2.44",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards"
  ],
```

```
  "FirstObservedAt": "2024-02-19T21:00:32.206Z",
  "LastObservedAt": "2024-04-29T13:01:57.861Z",
  "CreatedAt": "2024-02-19T21:00:32.206Z",
  "UpdatedAt": "2024-04-29T13:01:41.242Z",
  "Severity": {
    "Label": "LOW",
    "Normalized": 1,
    "Original": "LOW"
  },
  "Title": "EC2 subnets should be tagged",
  "Description": "This control checks whether an Amazon EC2 subnet has tags with the
 specific keys defined in the parameter requiredTagKeys. The control fails if the
 subnet doesn't have any tag keys or if it doesn't have all the keys specified in
 the parameter requiredTagKeys. If the parameter requiredTagKeys isn't provided, the
 control only checks for the existence of a tag key and fails if the subnet isn't
 tagged with any key. System tags, which are automatically applied and begin with aws:,
 are ignored.",
  "Remediation": {
    "Recommendation": {
      "Text": "For information on how to correct this issue, consult the AWS Security
 Hub controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/EC2.44/remediation"
    }
  },
  "ProductFields": {
    "RelatedAWSResources:0/name": "securityhub-tagged-ec2-subnet-6ceafede",
    "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
    "aws/securityhub/ProductName": "Security Hub",
    "aws/securityhub/CompanyName": "AWS",
    "aws/securityhub/annotation": "No tags are present.",
    "Resources:0/Id": "arn:aws:ec2:eu-central-1:123456789012:subnet/
subnet-1234567890abcdef0",
    "aws/securityhub/FindingId": "arn:aws:securityhub:eu-central-1::product/aws/
securityhub/arn:aws:securityhub:eu-central-1:123456789012:security-control/EC2.44/
finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  },
  "Resources": [
    {
      "Type": "AwsEc2Subnet",
      "Id": "arn:aws:ec2:eu-central-1:123456789012:subnet/subnet-1234567890abcdef0",
      "Partition": "aws",
      "Region": "eu-central-1",
      "Details": {
        "AwsEc2Subnet": {
```

```
          "AssignIpv6AddressOnCreation": false,
          "AvailabilityZone": "eu-central-1b",
          "AvailabilityZoneId": "euc1-az3",
          "AvailableIpAddressCount": 4091,
          "CidrBlock": "10.24.34.0/23",
          "DefaultForAz": true,
          "MapPublicIpOnLaunch": true,
          "OwnerId": "123456789012",
          "State": "available",
          "SubnetArn": "arn:aws:ec2:eu-central-1:123456789012:subnet/
subnet-1234567890abcdef0",
          "SubnetId": "subnet-1234567890abcdef0",
          "VpcId": "vpc-021345abcdef6789"
        }
      }
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "SecurityControlId": "EC2.44",
    "AssociatedStandards": [
      {
        "StandardsId": "standards/aws-resource-tagging-standard/v/1.0.0"
      }
    ],
    "SecurityControlParameters": [
      {
        "Name": "requiredTagKeys",
        "Value": [
          "peepoo"
        ]
      }
    ],
            },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "LOW",
      "Original": "LOW"
    },
```

```
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards"
    ]
  },
  "ProcessedAt": "2024-04-29T13:02:03.259Z"
}
```

Temuan sampel untuk Standar yang Dikelola Layanan: AWS Control Tower

> **Note**
>
> Standar ini tersedia untuk Anda hanya jika Anda adalah AWS Control Tower pengguna yang telah membuat standar di AWS Control Tower. Untuk informasi selengkapnya, lihat Standar yang Dikelola Layanan: AWS Control Tower.

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-1:123456789012:subscription/service-managed-aws-
control-tower/v/1.0.0/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/securityhub",
  "ProductName": "Security Hub",
  "CompanyName": "AWS",
  "Region": "us-east-1",
  "GeneratorId": "service-managed-aws-control-tower/v/1.0.0/CloudTrail.2",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards"
  ],
  "FirstObservedAt": "2022-11-17T01:25:30.296Z",
  "LastObservedAt": "2022-11-17T01:25:45.805Z",
  "CreatedAt": "2022-11-17T01:25:30.296Z",
  "UpdatedAt": "2022-11-17T01:25:30.296Z",
  "Severity": {
    "Product": 40,
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
  },
  "Title": "CT.CloudTrail.2 CloudTrail should have encryption at-rest enabled",
```

```
  "Description": "This AWS control checks whether AWS CloudTrail is configured to use
 the server side encryption (SSE) AWS Key Management Service (AWS KMS) customer master
 key (CMK) encryption. The check will pass if the KmsKeyId is defined.",
  "Remediation": {
    "Recommendation": {
      "Text": "For information on how to correct this issue, consult the AWS Security
 Hub controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
    }
  },
  "ProductFields": {
    "StandardsArn": "arn:aws:securityhub:::standards/service-managed-aws-control-tower/
v/1.0.0",
    "StandardsSubscriptionArn": "arn:aws:securityhub:us-
east-1:123456789012:subscription/service-managed-aws-control-tower/v/1.0.0",
    "ControlId": "CT.CloudTrail.2",
    "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/
remediation",
    "RelatedAWSResources:0/name": "securityhub-cloud-trail-encryption-enabled-
fe95bf3f",
    "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
    "StandardsControlArn": "arn:aws:securityhub:us-east-1:123456789012:control/service-
managed-aws-control-tower/v/1.0.0/CloudTrail.2",
    "aws/securityhub/ProductName": "Security Hub",
    "aws/securityhub/CompanyName": "AWS",
    "Resources:0/Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWSMacieTrail-
DO-NOT-EDIT",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/
securityhub/arn:aws:securityhub:us-east-1:123456789012:subscription/service-managed-
aws-control-tower/v/1.0.0/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  },
  "Resources": [
    {
      "Type": "AwsAccount",
      "Id": "AWS::::Account:123456789012",
      "Partition": "aws",
      "Region": "us-east-1"
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "SecurityControlId": "CloudTrail.2",
    "AssociatedStandards": [{
      "StandardsId": "standards/service-managed-aws-control-tower/v/1.0.0"
```

```
    }]
  },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    },
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards"
    ]
  }
}
```

Temuan sampel di seluruh standar (ketika temuan kontrol terkonsolidasi diaktifkan)

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-2:123456789012:security-control/CloudTrail.2/
finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-2::product/aws/securityhub",
  "ProductName": "Security Hub",
  "CompanyName": "AWS",
  "Region": "us-east-2",
  "GeneratorId": "security-control/CloudTrail.2",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards"
  ],
  "FirstObservedAt": "2022-10-06T02:18:23.076Z",
  "LastObservedAt": "2022-10-28T16:10:06.956Z",
  "CreatedAt": "2022-10-06T02:18:23.076Z",
  "UpdatedAt": "2022-10-28T16:10:00.093Z",
  "Severity": {
    "Label": "MEDIUM",
    "Normalized": "40",
    "Original": "MEDIUM"
  },
  "Title": "CloudTrail should have encryption at-rest enabled",
```

```
  "Description": "This AWS control checks whether AWS CloudTrail is configured to use
 the server side encryption (SSE) AWS Key Management Service (AWS KMS) customer master
 key (CMK) encryption. The check will pass if the KmsKeyId is defined.",
  "Remediation": {
    "Recommendation": {
      "Text": "For directions on how to correct this issue, consult the AWS Security
 Hub controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
    }
  },
  "ProductFields": {
    "Related AWS Resources:0/name": "securityhub-cloud-trail-encryption-enabled-
fe95bf3f",
    "Related AWS Resources:0/type": "AWS::Config::ConfigRule",
    "aws/securityhub/ProductName": "Security Hub",
    "aws/securityhub/CompanyName": "AWS",
    "Resources:0/Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWS MacieTrail-
DO-NOT-EDIT",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-2::product/aws/
securityhub/arn:aws:securityhub:us-east-2:123456789012:security-control/CloudTrail.2/
finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  }
  "Resources": [
    {
      "Type": "AwsCloudTrailTrail",
      "Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWS MacieTrail-DO-NOT-
EDIT",
      "Partition": "aws",
      "Region": "us-east-2"
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "RelatedRequirements": [
        "PCI DSS v3.2.1/3.4",
        "CIS AWS Foundations Benchmark v1.2.0/2.7",
        "CIS AWS Foundations Benchmark v1.4.0/3.7"
    ],
    "SecurityControlId": "CloudTrail.2",
    "AssociatedStandards": [
       { "StandardsId": "standards/aws-foundational-security-best-practices/v/1.0.0"},
       { "StandardsId": "standards/pci-dss/v/3.2.1"},
       { "StandardsId": "ruleset/cis-aws-foundations-benchmark/v/1.2.0"},
       { "StandardsId": "standards/cis-aws-foundations-benchmark/v/1.4.0"},
```

```
        { "StandardsId": "standards/service-managed-aws-control-tower/v/1.0.0"},
      ]
    },
    "WorkflowState": "NEW",
    "Workflow": {
      "Status": "NEW"
    },
    "RecordState": "ACTIVE",
    "FindingProviderFields": {
      "Severity": {
        "Label": "MEDIUM",
        "Original": "MEDIUM"
      },
      "Types": [
        "Software and Configuration Checks/Industry and Regulatory Standards"
      ]
    }
}
```

Memfilter, menyortir, dan mengunduh temuan kontrol

Anda dapat memfilter daftar temuan kontrol berdasarkan status kepatuhan dengan menggunakan tab pemfilteran. Anda juga dapat memfilter daftar berdasarkan nilai bidang temuan lainnya, dan mengunduh temuan dari daftar.

Memfilter dan menyortir daftar pencarian kontrol

Tab Semua pemeriksaan mencantumkan semua temuan aktif yang memiliki status alur kerja`NEW`,`NOTIFIED`, atau`RESOLVED`. Secara default, daftar diurutkan sehingga temuan yang gagal berada di bagian atas daftar. Urutan semacam ini membantu Anda memprioritaskan temuan yang perlu ditangani.

Daftar pada tab Gagal, Tidak Diketahui, dan Lulus difilter berdasarkan nilai. `Compliance.Status` Daftar ini juga hanya mencakup temuan aktif yang memiliki status alur kerja`NEW`,`NOTIFIED`, atau`RESOLVED`.

Tab yang Ditekan berisi daftar temuan aktif yang memiliki status alur kerja. `SUPPRESSED`

Selain filter bawaan pada setiap tab, Anda dapat memfilter daftar menggunakan nilai dari bidang berikut:

- account-id

- Status alur kerja
- Status kepatuhan
- ID Sumber Daya
- Jenis sumber daya

Anda dapat mengurutkan setiap daftar menggunakan salah satu kolom.

Mengunduh daftar pencarian kontrol

Jika Anda menavigasi ke Standar keamanan dan memilih standar, Anda akan melihat daftar kontrol untuk standar tersebut. Memilih kontrol dari daftar akan membawa Anda ke halaman detail kontrol dengan daftar temuan untuk kontrol. Dari sini, Anda dapat mengunduh temuan kontrol ke file.csv.

Jika Anda memfilter daftar temuan, maka unduhan hanya menyertakan kontrol yang cocok dengan filter.

Jika Anda memilih temuan spesifik dari daftar, maka unduhan hanya menyertakan temuan yang dipilih.

Untuk mengunduh temuan, pilih Unduh. Halaman temuan saat ini diunduh.

Mengambil tindakan atas temuan kontrol

Untuk mencerminkan status investigasi saat ini, Anda menetapkan status alur kerja. Untuk informasi selengkapnya, lihat the section called “Mengatur status alur kerja temuan”.

Di AWS Security Hub, Anda juga dapat mengirim temuan yang dipilih ke tindakan kustom di Amazon EventBridge. Untuk informasi selengkapnya, lihat the section called “Mengirim temuan ke tindakan khusus”.

Bekerja dengan dasbor Ringkasan

Di konsol AWS Security Hub, dasbor pada halaman Ringkasan dapat membantu Anda mengidentifikasi area yang menjadi perhatian keamanan di AWS lingkungan Anda, tanpa perlu alat analitik tambahan atau kueri yang rumit. Anda dapat menyesuaikan tata letak dasbor, menambah atau menghapus widget, dan memfilter data untuk fokus pada bidang minat tertentu. Anda juga dapat menyimpan kriteria filter Anda sebagai set filter untuk dengan cepat mengambil jenis data tertentu di masa mendatang.

Jika Anda menyesuaikan dasbor atau memfilter data, Security Hub secara otomatis menyimpan pengaturan Anda untuk penggunaan selanjutnya. Selain itu, pengaturan disimpan secara independen untuk setiap pengguna akun Security Hub Anda. Ini berarti bahwa pengguna yang berbeda dapat memiliki tata letak, widget, dan set filter yang berbeda untuk dasbor.

Setiap kali Anda membuka dasbor Ringkasan, Security Hub secara otomatis menyegarkan sebagian besar data dasbor. Namun, beberapa data diperbarui lebih jarang. Misalnya, skor keamanan dan status kontrol diperbarui setiap 24 jam.

Jika Anda mengonfigurasi Wilayah agregasi Lintas wilayah untuk Security Hub, data dasbor Anda menyertakan temuan dari Wilayah agregasi dan semua Wilayah yang ditautkan. Jika Anda administrator Security Hub yang didelegasikan untuk suatu organisasi, data tersebut mencakup temuan untuk akun administrator dan akun anggota Anda. Anda dapat secara opsional memfilter data berdasarkan akun. Jika Anda memiliki akun anggota atau akun mandiri, data hanya mencakup temuan untuk akun Anda.

Widget yang tersedia untuk dasbor Ringkasan

Dasbor Ringkasan mencakup widget yang mencerminkan lanskap ancaman keamanan cloud modern, dipandu oleh operasi keamanan dan pengalaman AWS pelanggan. Beberapa widget ditampilkan secara default sementara yang lain tidak. Anda dapat menyesuaikan tampilan dasbor dengan menambahkan atau menghapus widget.

Untuk menambahkannya, pilih Tambah widget di kanan atas halaman Ringkasan. Di bilah pencarian, masukkan judul widget. Seret dan jatuhkan widget ke dasbor.

Widget ditampilkan secara default

Secara default, dasbor Ringkasan mencakup widget berikut:

Standar keamanan

Menampilkan skor keamanan ringkasan terbaru Anda dan skor keamanan untuk setiap standar Security Hub. Skor keamanan, yang berkisar antara 0-100 persen, mewakili proporsi kontrol yang diteruskan relatif terhadap semua kontrol yang Anda aktifkan. Untuk informasi lebih lanjut tentang skor ini, lihatBagaimana skor keamanan dihitung. Widget ini membantu Anda memahami postur keamanan Anda secara keseluruhan.

Aset dengan temuan terbanyak

Memberikan gambaran umum tentang sumber daya, akun, dan aplikasi yang memiliki temuan paling banyak. Daftar ini diurutkan dalam urutan menurun berdasarkan jumlah temuan. Di widget, setiap tab menampilkan enam item teratas dalam kategori itu, dikelompokkan berdasarkan tingkat keparahan dan jenis sumber daya. Jika Anda memilih nomor di kolom Total temuan, Security Hub akan membuka halaman yang menampilkan temuan untuk aset tersebut. Widget ini membantu Anda dengan cepat mengidentifikasi aset inti mana yang memiliki potensi ancaman keamanan.

Temuan berdasarkan Wilayah

Menunjukkan jumlah total temuan, dikelompokkan berdasarkan tingkat keparahan, Wilayah AWS di masing-masing tempat Security Hub diaktifkan. Widget ini membantu Anda mengidentifikasi masalah keamanan yang berpotensi memengaruhi Wilayah tertentu. Jika Anda membuka dasbor di Wilayah agregasi Anda, widget ini membantu Anda memantau potensi masalah keamanan di setiap Wilayah yang ditautkan.

Jenis ancaman yang paling umum

Memberikan rincian dari 10 jenis ancaman paling umum di AWS lingkungan Anda. Ini termasuk ancaman seperti eskalasi hak istimewa, penggunaan kredensional yang terbuka, atau komunikasi dengan alamat IP berbahaya.

Untuk melihat data ini, Amazon GuardDuty harus diaktifkan. Jika ya, pilih jenis ancaman di widget ini untuk membuka GuardDuty konsol dan meninjau temuan yang terkait dengan ancaman ini. Widget ini membantu Anda mengevaluasi potensi ancaman dalam konteks masalah keamanan lainnya.

Kerentanan perangkat lunak dengan eksploitasi

Menyediakan ringkasan kerentanan perangkat lunak yang ada di AWS lingkungan Anda dan telah diketahui eksploitasi. Anda juga dapat meninjau rincian kerentanan yang melakukan dan tidak memiliki perbaikan yang tersedia.

Untuk melihat data ini, Amazon Inspector harus diaktifkan. Jika ya, pilih statistik di widget ini untuk membuka konsol Amazon Inspector dan tinjau detail lebih lanjut tentang kerentanan. Widget ini membantu Anda mengevaluasi kerentanan perangkat lunak dalam konteks masalah keamanan lainnya.

Temuan baru dari waktu ke waktu

Menunjukkan tren dalam jumlah temuan harian baru selama 90 hari terakhir. Anda dapat memecah data berdasarkan tingkat keparahan atau oleh penyedia untuk konteks tambahan. Widget ini membantu Anda memahami jika menemukan volume melonjak atau turun pada waktu tertentu selama 90 hari terakhir.

Sumber daya dengan temuan terbanyak

Memberikan ringkasan sumber daya yang paling banyak menghasilkan temuan, yang dipecah berdasarkan jenis sumber daya berikut: Bucket Amazon Simple Storage Service (Amazon S3), instans Amazon Elastic Compute Cloud (Amazon EC2), dan fungsi. AWS Lambda

Di widget, setiap tab berfokus pada salah satu jenis sumber daya sebelumnya, mencantumkan 10 contoh sumber daya yang menghasilkan temuan terbanyak. Untuk meninjau temuan untuk sumber daya tertentu, pilih contoh sumber daya. Widget ini membantu Anda melakukan triase temuan keamanan yang terkait dengan AWS sumber daya umum.

Widget tersembunyi secara default

Widget berikut juga tersedia untuk dasbor Ringkasan, tetapi mereka disembunyikan secara default:

AMI dengan temuan terbanyak

Menyediakan daftar 10 Amazon Machine Images (AMI) yang telah menghasilkan temuan terbanyak. Data ini hanya tersedia jika Amazon EC2 diaktifkan untuk akun Anda. Ini membantu Anda mengidentifikasi AMI mana yang menimbulkan risiko keamanan potensial.

Prinsipal IAM dengan temuan terbanyak

Menyediakan daftar 10 AWS Identity and Access Management (IAM) pengguna yang telah menghasilkan temuan terbanyak. Widget ini membantu Anda melakukan tugas administratif dan penagihan. Ini menunjukkan kepada Anda pengguna mana yang paling berkontribusi pada penggunaan Security Hub.

Akun dengan temuan terbanyak (berdasarkan tingkat keparahan)

Menunjukkan grafik dari 10 akun yang telah menghasilkan temuan terbanyak, dikelompokkan berdasarkan tingkat keparahan. Widget ini membantu Anda menentukan akun mana yang akan memfokuskan upaya analisis dan remediasi.

Akun dengan temuan terbanyak (berdasarkan jenis sumber daya)

Menampilkan grafik dari 10 akun yang telah menghasilkan temuan terbanyak, dikelompokkan berdasarkan jenis sumber daya. Widget ini membantu Anda menentukan jenis akun dan sumber daya mana yang akan diprioritaskan untuk analisis dan remediasi.

Wawasan

Daftar lima wawasan terkelola Security Hub dan jumlah temuan yang mereka hasilkan. Wawasan mengidentifikasi area keamanan tertentu yang membutuhkan perhatian.

Temuan terbaru dari AWS integrasi

Menunjukkan jumlah temuan yang Anda terima di Security Hub dari terintegrasi Layanan AWS. Ini juga menunjukkan kapan Anda baru-baru ini menerima temuan dari setiap layanan terintegrasi. Widget ini menyediakan data temuan terkonsolidasi dari beberapaLayanan AWS. Untuk menelusuri, pilih layanan terintegrasi. Security Hub kemudian membuka konsol untuk layanan itu.

Memfilter dasbor Ringkasan

Untuk mengkurasi data di dasbor Ringkasan dan hanya menyertakan data keamanan yang paling relevan bagi Anda, Anda dapat memfilter dasbor. Misalnya, jika Anda anggota tim aplikasi, Anda dapat membuat tampilan khusus untuk aplikasi penting di lingkungan produksi Anda. Jika Anda anggota tim keamanan, Anda dapat membuat tampilan khusus yang membantu Anda fokus pada temuan tingkat keparahan tinggi. Untuk memfilter data di dasbor Ringkasan, Anda memasukkan kriteria filter di kotak filter di atas dasbor. Jika Anda menerapkan kriteria filter, kriteria tersebut berlaku untuk semua data di dasbor kecuali data dalam widget standar Wawasan dan Keamanan.

Anda dapat memfilter data dengan menggunakan bidang berikut:

- Nama akun
- ID Akun
- Aplikasi Nama Sumber Daya Amazon (ARN)

- Nama aplikasi
- Nama produk (untuk produk Layanan AWS atau pihak ketiga yang mengirimkan temuan ke Security Hub)
- Rekam keadaan
- wilayah
- Tanda sumber daya
- Kepelikan
- Status alur kerja

Secara default, data dasbor disaring menggunakan kriteria berikut: `Workflow status` is `NOTIFIED` or`NEW`, and `Record state` is`ACTIVE`. Kriteria ini muncul di atas dasbor, di bawah kotak filter. Untuk menghapus kriteria ini, pilih X di token filter untuk kriteria yang ingin Anda hapus.

Jika Anda menerapkan kriteria filter yang ingin Anda gunakan lagi, Anda dapat menyimpannya sebagai set filter. Kumpulan filter adalah sekumpulan kriteria filter yang Anda buat dan simpan untuk diterapkan kembali saat Anda meninjau data di dasbor Ringkasan.

> **Note**
>
> Bidang berikut tidak dapat disimpan sebagai bagian dari kumpulan filter: ARN aplikasi, nama aplikasi, dan tag sumber daya.

Membuat dan menyimpan set filter

Ikuti langkah-langkah ini untuk membuat dan menyimpan set filter.

Untuk membuat dan menyimpan set filter

1. Buka konsol AWS Security Hub di https://console.aws.amazon.com/securityhub/.
2. Di panel navigasi, pilih Ringkasan.
3. Pada kotak filter di atas dasbor Ringkasan, masukkan kriteria filter untuk set filter.
4. Pada menu Hapus filter, pilih Simpan set filter baru.
5. Dalam kotak dialog Simpan set filter, masukkan nama untuk set filter.
6. (Opsional) Untuk menggunakan filter yang ditetapkan secara default setiap kali Anda membuka halaman Ringkasan, pilih opsi untuk mengaturnya sebagai tampilan default.

7. Pilih Simpan.

Untuk beralih di antara set filter yang telah Anda buat dan simpan, gunakan menu Pilih set filter di atas dasbor Ringkasan. Saat Anda memilih set filter, Security Hub menerapkan kriteria penyaringan yang disetel ke data di dasbor.

Memperbarui atau menghapus set filter

Ikuti langkah-langkah ini untuk memperbarui atau menghapus set filter yang ada. Jika Anda menghapus kumpulan filter yang saat ini ditetapkan sebagai tampilan default dasbor Ringkasan, tampilan default Anda disetel ulang ke tampilan Hub Keamanan default.

Untuk memperbarui atau menghapus set filter

1. Buka konsol AWS Security Hub di https://console.aws.amazon.com/securityhub/.
2. Di panel navigasi, pilih Ringkasan.
3. Dalam menu Pilih set filter di atas halaman Ringkasan, pilih set filter.
4. Pada menu Hapus filter, lakukan salah satu hal berikut:
   - Untuk memperbarui set filter, pilih Perbarui set filter saat ini. Kemudian, masukkan perubahan Anda di kotak dialog yang muncul.
   - Untuk menghapus set filter pilih Hapus set filter saat ini. Kemudian, pilih Hapus di kotak dialog yang muncul.

Menyesuaikan dasbor Ringkasan

Anda dapat menyesuaikan dasbor Ringkasan dengan beberapa cara. Anda dapat menambah dan menghapus widget dari dasbor. Anda juga dapat mengatur ulang dan mengubah ukuran widget di dasbor.

Jika Anda menyesuaikan dasbor, Security Hub segera menerapkan perubahan Anda dan menyimpan pengaturan dasbor baru Anda. Perubahan Anda berlaku untuk tampilan dasbor Anda di semua Wilayah AWS dan browser.

Untuk menyesuaikan dasbor Ringkasan

1. Buka konsol AWS Security Hub di https://console.aws.amazon.com/securityhub/.

2. Di panel navigasi, pilih Ringkasan.
3. Lakukan langkah-langkah berikut:

   - Untuk menambahkan widget, pilih Tambahkan widget di sudut kanan atas halaman. Di bilah pencarian, masukkan judul widget yang akan ditambahkan. Kemudian, seret widget ke lokasi yang Anda inginkan.
   - Untuk menghapus widget, pilih tiga titik di sudut kanan atas widget.
   - Untuk memindahkan widget, pilih pegangan di sudut kiri atas widget, lalu seret widget ke lokasi yang Anda inginkan.
   - Untuk mengubah ukuran widget, pilih pegangan pengubahan ukuran di sudut kanan bawah widget. Seret tepi widget hingga widget adalah ukuran pilihan Anda.

Untuk selanjutnya mengembalikan pengaturan asli, pilih Atur ulang ke tata letak default di bagian atas halaman.

Membuat sumber daya Security Hub dengan AWS CloudFormation

AWS Security Hub terintegrasi dengan AWS CloudFormation, yang merupakan layanan yang membantu Anda memodelkan dan mengatur AWS sumber daya Anda sehingga Anda dapat menghabiskan lebih sedikit waktu untuk membuat dan mengelola sumber daya dan infrastruktur Anda. Anda membuat templat yang menjelaskan semua AWS sumber daya yang Anda inginkan (seperti aturan otomatisasi), dan AWS CloudFormation ketentuan serta mengonfigurasi sumber daya tersebut untuk Anda.

Saat menggunakannya AWS CloudFormation, Anda dapat menggunakan kembali template untuk menyiapkan sumber daya Security Hub secara konsisten dan berulang kali. Jelaskan sumber daya Anda sekali, lalu sediakan sumber daya yang sama berulang-ulang di beberapa Akun AWS dan Wilayah.

Security Hub dan AWS CloudFormation template

Untuk menyediakan dan mengonfigurasi sumber daya untuk Security Hub dan layanan terkait, Anda harus memahami cara kerja AWS CloudFormation templat. Template adalah file teks dalam format JSON atau YAMAL. Template ini menjelaskan sumber daya yang ingin Anda sediakan di AWS CloudFormation tumpukan Anda.

Jika Anda tidak terbiasa dengan JSON atau YAMAL, Anda dapat menggunakan AWS CloudFormation Designer untuk membantu Anda memulai dengan template. AWS CloudFormation Untuk informasi lebih lanjut, lihat Apa itu AWS CloudFormation Desainer? dalam AWS CloudFormation User Guide.

Anda dapat membuat AWS CloudFormation templat untuk jenis sumber daya Security Hub berikut:

- Mengaktifkan Security Hub
- Menunjuk administrator Security Hub yang didelegasikan untuk organisasi
- Mengaktifkan standar keamanan
- Membuat wawasan khusus
- Membuat aturan otomatisasi
- Berlangganan integrasi produk pihak ketiga

Untuk informasi selengkapnya, termasuk contoh template JSON dan YAMAL untuk sumber daya, lihat referensi jenis AWS Security Hub sumber daya di AWS CloudFormation Panduan Pengguna.

Pelajari lebih lanjut tentang AWS CloudFormation

Untuk mempelajari selengkapnya AWS CloudFormation, lihat sumber daya berikut:

- AWS CloudFormation
- AWS CloudFormation Panduan Pengguna
- AWS CloudFormation Referensi API
- AWS CloudFormation Panduan Pengguna Antarmuka Baris Perintah

Berlangganan pengumuman Security Hub dengan Amazon Simple Notification Service

Bagian ini memberikan informasi tentang berlangganan pengumuman AWS Security Hub dengan Amazon Simple Notification Service (Amazon SNS) untuk menerima pemberitahuan tentang Security Hub.

Setelah berlangganan, Anda akan menerima pemberitahuan tentang acara berikut (perhatikan yang sesuai `AnnouncementType` untuk setiap acara):

- `GENERAL`— Pemberitahuan umum tentang layanan Security Hub.
- `UPCOMING_STANDARDS_CONTROLS`— Kontrol atau standar Security Hub yang ditentukan akan segera dirilis. Jenis pengumuman ini membantu Anda mempersiapkan alur kerja respons dan remediasi sebelum rilis.
- `NEW_REGIONS`— Support for Security Hub tersedia dalam versi baruWilayah AWS.
- `NEW_STANDARDS_CONTROLS`— Kontrol atau standar Security Hub baru telah ditambahkan.
- `UPDATED_STANDARDS_CONTROLS`— Kontrol atau standar Security Hub yang ada telah diperbarui.
- `RETIRED_STANDARDS_CONTROLS`— Kontrol atau standar Security Hub yang ada telah dihentikan.
- `UPDATED_ASFF`— Sintaks, bidang, atau nilai AWS Security Finding Format (ASFF) telah diperbarui.
- `NEW_INTEGRATION`Integrasi baru dengan AWS layanan lain atau produk pihak ketiga tersedia.
- `NEW_FEATURE`— Fitur Security Hub baru tersedia.
- `UPDATED_FEATURE`— Fitur Security Hub yang ada telah diperbarui.

Notifikasi tersedia dalam semua format yang didukung Amazon SNS. Anda dapat berlangganan pengumuman Security Hub di semua Wilayah AWS tempat Security Hub tersedia.

Pengguna harus memiliki `Subscribe` izin untuk berlangganan topik Amazon SNS. Anda dapat mencapai ini dengan kebijakan Amazon SNS, kebijakan IAM, atau keduanya. Untuk informasi selengkapnya, lihat kebijakan IAM dan Amazon SNS bersama-sama di Panduan Pengembang Layanan Pemberitahuan Sederhana Amazon.

> **Note**
>
> Security Hub mengirimkan pengumuman Amazon SNS tentang pembaruan ke layanan Security Hub ke semua yang berlangganan. Akun AWS Untuk menerima pemberitahuan tentang temuan Security Hub, lihatMengelola dan meninjau detail dan riwayat penemuan.

Anda dapat berlangganan antrian Amazon Simple Queue Service (Amazon SQS) untuk topik Amazon SNS, tetapi Anda harus menggunakan topik Amazon SNS Nama Sumber Daya Amazon (ARN) yang ada di Wilayah yang sama. Untuk informasi selengkapnya, lihat Tutorial: Berlangganan antrian Amazon SQS ke topik Amazon SNS di Panduan Pengembang Layanan Antrian Sederhana Amazon.

Anda juga dapat menggunakan AWS Lambda fungsi untuk memanggil acara saat Anda menerima pemberitahuan. Untuk informasi selengkapnya, termasuk kode fungsi contoh, lihat Tutorial: Menggunakan AWS Lambda dengan Amazon Simple Notification Service di Panduan AWS Lambda Pengembang.

ARN topik Amazon SNS untuk setiap Wilayah adalah sebagai berikut.

Wilayah AWS	ARN topik Amazon SNS
AS Timur (Ohio)	`arn:aws:sns:us-east-2:291342846459:SecurityHubAnnouncements`
AS Timur (Virginia Utara)	`arn:aws:sns:us-east-1:088139225913:SecurityHubAnnouncements`
AS Barat (California Utara)	`arn:aws:sns:us-west-1:137690824926:SecurityHubAnnouncements`
AS Barat (Oregon)	`arn:aws:sns:us-west-2:393883065485:SecurityHubAnnouncements`

Wilayah AWS	ARN topik Amazon SNS
Afrika (Cape Town)	`arn:aws:sns:af-south-1:463142546776:SecurityHubAnnouncements`
Asia Pasifik (Hong Kong)	`arn:aws:sns:ap-east-1:464812404305:SecurityHubAnnouncements`
Asia Pasifik (Hyderabad)	`arn:aws:sns:ap-south-2:849907286123:SecurityHubAnnouncements`
Asia Pasifik (Jakarta)	`arn:aws:sns:ap-southeast-3:627843640627:SecurityHubAnnouncements`
Asia Pasifik (Mumbai)	`arn:aws:sns:ap-south-1:707356269775:SecurityHubAnnouncements`
Asia Pasifik (Osaka)	`arn:aws:sns:ap-northeast-3:633550238216:SecurityHubAnnouncements`
Asia Pasifik (Seoul)	`arn:aws:sns:ap-northeast-2:374299265323:SecurityHubAnnouncements`
Asia Pasifik (Singapura)	`arn:aws:sns:ap-southeast-1:512267288502:SecurityHubAnnouncements`
Asia Pasifik (Sydney)	`arn:aws:sns:ap-southeast-2:475730049140:SecurityHubAnnouncements`

Wilayah AWS	ARN topik Amazon SNS
Asia Pasifik (Tokyo)	`arn:aws:sns:ap-northeast-1:592469075483:SecurityHubAnnouncements`
Kanada (Pusat)	`arn:aws:sns:ca-central-1:137749997395:SecurityHubAnnouncements`
Tiongkok (Beijing)	`arn:aws-cn:sns:cn-north-1:672341567257:SecurityHubAnnouncements`
Tiongkok (Ningxia)	`arn:aws-cn:sns:cn-northwest-1:672534482217:SecurityHubAnnouncements`
Eropa (Frankfurt)	`arn:aws:sns:eu-central-1:871975303681:SecurityHubAnnouncements`
Eropa (Irlandia)	`arn:aws:sns:eu-west-1:705756202095:SecurityHubAnnouncements`
Eropa (London)	`arn:aws:sns:eu-west-2:883600840440:SecurityHubAnnouncements`
Eropa (Milan)	`arn:aws:sns:eu-south-1:151363035580:SecurityHubAnnouncements`
Eropa (Paris)	`arn:aws:sns:eu-west-3:313420042571:SecurityHubAnnouncements`

Wilayah AWS	ARN topik Amazon SNS
Eropa (Spanyol)	`arn:aws:sns:eu-south-2:777487947751:SecurityHubAnnouncements`
Eropa (Stockholm)	`arn:aws:sns:eu-north-1:191971010772:SecurityHubAnnouncements`
Eropa (Zürich)	`arn:aws:sns:eu-central-2:704347005078:SecurityHubAnnouncements`
Israel (Tel Aviv)	`arn:aws:sns:il-central-1:726652212146:SecurityHubAnnouncements`
Timur Tengah (Bahrain)	`arn:aws:sns:me-south-1:585146626860:SecurityHubAnnouncements`
Timur Tengah (UEA)	`arn:aws:sns:me-central-1:431548502100:SecurityHubAnnouncements`
Amerika Selatan (Sao Paulo)	`arn:aws:sns:sa-east-1:359811883282:SecurityHubAnnouncements`
AWS GovCloud (AS-Timur)	`arn:aws-us-gov:sns:us-gov-east-1:239368469855:SecurityHubAnnouncements`
AWS GovCloud (AS-Barat)	`arn:aws-us-gov:sns:us-gov-west-1:239334163374:SecurityHubAnnouncements`

Pesan biasanya sama di seluruh Wilayah dalam partisi, sehingga Anda dapat berlangganan satu Wilayah di setiap partisi untuk menerima pengumuman yang memengaruhi semua Wilayah di partisi tersebut. Pengumuman yang terkait dengan akun anggota tidak direplikasi di akun administrator. Akibatnya, setiap akun, termasuk akun administrator, hanya akan memiliki satu salinan dari setiap pengumuman. Anda dapat memutuskan akun mana yang ingin Anda gunakan untuk berlangganan pengumuman Security Hub.

Untuk informasi tentang biaya berlangganan pengumuman Security Hub, lihat harga Amazon SNS.

Berlangganan pengumuman Security Hub (konsol)

1. Buka konsol Amazon SNS di https://console.aws.amazon.com/sns/v3/home.
2. Dalam daftar Wilayah, pilih Wilayah tempat Anda ingin berlangganan pengumuman Security Hub. Contoh ini menggunakan Wilayah `us-west-2`.
3. Di panel navigasi, pilih Langganan, lalu pilih Buat langganan.
4. Masukkan topik ARN ke dalam topik ARN kotak. Sebagai contoh, `arn:aws:sns:us-west-2:393883065485:SecurityHubAnnouncements`.
5. Untuk Protokol, pilih cara Anda ingin menerima pengumuman Security Hub. Jika Anda memilih Email, untuk Endpoint, masukkan alamat email yang ingin Anda gunakan untuk menerima pengumuman.
6. Pilih Buat langganan.
7. Konfirmasi langganan. Misalnya, jika Anda memilih protokol email, Amazon SNS akan mengirim pesan konfirmasi berlangganan ke email yang Anda berikan.

Berlangganan pengumuman Security Hub () AWS CLI

1. Jalankan perintah berikut:

```
 aws  sns --region us-west-2 subscribe --topic-arn arn:aws:sns:us-
west-2:393883065485:SecurityHubAnnouncements --protocol email --notification-
endpoint your_email@your_domain.com
```

2. Konfirmasi langganan. Misalnya, jika Anda memilih protokol email, Amazon SNS akan mengirim pesan konfirmasi berlangganan ke email yang Anda berikan.

Format pesan Amazon SNS

Contoh berikut menunjukkan pengumuman Security Hub dari Amazon SNS tentang pengenalan kontrol keamanan baru. Konten pesan bervariasi berdasarkan jenis pengumuman, tetapi formatnya sama untuk semua jenis pengumuman. Secara opsional, `Link` bidang yang memberikan rincian tentang pengumuman dapat disertakan.

Contoh: Pengumuman Security Hub untuk kontrol baru (protokol email)

```
{
"AnnouncementType":"NEW_STANDARDS_CONTROLS",
"Title":"[New Controls] 36 new Security Hub controls added to the AWS Foundational
 Security Best Practices standard",
"Description":"We have added 36 new controls to the AWS Foundational Security Best
 Practices standard. These include controls for Amazon Auto Scaling (AutoScaling.3,
 AutoScaling.4, AutoScaling.6), AWS CloudFormation (CloudFormation.1), Amazon
 CloudFront (CloudFront.10), Amazon Elastic Compute Cloud (Amazon EC2) (EC2.23,
 EC2.24, EC2.27), Amazon Elastic Container Registry (Amazon ECR) (ECR.1, ECR.2), Amazon
 Elastic Container Service (Amazon ECS) (ECS.3, ECS.4, ECS.5, ECS.8, ECS.10, ECS.12),
 Amazon Elastic File System (Amazon EFS) (EFS.3, EFS.4), Amazon Elastic Kubernetes
 Service (Amazon EKS) (EKS.2), Elastic Load Balancing (ELB.12, ELB.13, ELB.14), Amazon
 Kinesis (Kinesis.1), AWS Network Firewall (NetworkFirewall.3, NetworkFirewall.4,
 NetworkFirewall.5), Amazon OpenSearch Service (OpenSearch.7), Amazon Redshift
 (Redshift.9),
Amazon Simple Storage Service (Amazon S3) (S3.13), Amazon Simple Notification Service
 (SNS.2), AWS WAF (WAF.2, WAF.3, WAF.4, WAF.6, WAF.7, WAF.8). If you enabled the AWS
 Foundational Security Best Practices standard in an account and configured Security
 Hub to automatically enable new controls, these controls are enabled by default.
 Availability of controls can vary by Region. "
}
```

Contoh: Pengumuman Security Hub untuk kontrol baru (protokol Email-JSON)

```
{
  "Type" : "Notification",
  "MessageId" : "d124c9cf-326a-5931-9263-92a92e7af49f",
  "TopicArn" : "arn:aws:sns:us-west-2:393883065485:SecurityHubAnnouncements",
  "Message" : "{\"AnnouncementType\":\"NEW_STANDARDS_CONTROLS\",\"Title\":\"[New
 Controls] 36 new Security Hub controls added to the AWS Foundational Security Best
 Practices standard\",\"Description\":\"We have added 36 new controls to the AWS
 Foundational Security Best Practices standard. These include controls for Amazon
 Auto Scaling (AutoScaling.3, AutoScaling.4, AutoScaling.6), AWS CloudFormation
```

```
 (CloudFormation.1), Amazon CloudFront (CloudFront.10), Amazon Elastic Compute Cloud
 (Amazon EC2) (EC2.23, EC2.24, EC2.27), Amazon Elastic Container Registry (Amazon ECR)
 (ECR.1, ECR.2), Amazon Elastic Container Service (Amazon ECS) (ECS.3, ECS.4, ECS.5,
 ECS.8, ECS.10, ECS.12), Amazon Elastic File System (Amazon EFS) (EFS.3, EFS.4), Amazon
 Elastic Kubernetes Service (Amazon EKS) (EKS.2), Elastic Load Balancing (ELB.12,
 ELB.13, ELB.14), Amazon Kinesis (Kinesis.1), AWS Network Firewall (NetworkFirewall.3,
 NetworkFirewall.4, NetworkFirewall.5), Amazon OpenSearch Service (OpenSearch.7),
 Amazon Redshift (Redshift.9),
Amazon Simple Storage Service (Amazon S3) (S3.13), Amazon Simple Notification Service
 (SNS.2), AWS WAF (WAF.2, WAF.3, WAF.4, WAF.6, WAF.7, WAF.8). If you enabled the AWS
 Foundational Security Best Practices standard in an account and configured SSecurity
 Hub to automatically enable new controls, these controls are enabled by default.
 Availability of controls can vary by Region. \"}",
  "Timestamp" : "2022-08-04T19:11:12.652Z",
  "SignatureVersion" : "1",
  "Signature" :
 "HTHgNFRYMetCvisulgLM4CVySvK9qCXFPHQDxYl9tuCFQuIrd7YO4m4YFR28XKMgzqrF20YP
+EilipUm2SOTpEEtOTekU5bn74+YmNZfwr4aPFx0vUuQCVOshmHl37hjkiLjhCg/t53QQiLfP7MH
+MTXIUPR37k5SuFCXvjpRQ8ynV532AH3Wpv0HmojDLMg+eg51V1fUsOG8yiJVCBEJhJ1yS
+gkwJdhRk2UQab9RcAmE6COK3hRWcjDwqTXz5nR6Ywv1ZqZfLIl7gYKslt+jsyd/k+7kOqGmOJRDr7qhE7H
+7vaGRLOptsQnbW8VmeYnDbahEO8FV+Mp1rpV+7Qg==",
  "SigningCertURL" : "https://sns.us-west-2.amazonaws.com/
SimpleNotificationService-56e67fcb41f6fec09b0196692625d385.pem",
  "UnsubscribeURL" : "https://sns.us-west-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-
west-2:393883065485:SecurityHubAnnouncements:9d0230d7-d582-451d-9f15-0c32818bf61f"
}
```

Keamanan di AWS Security Hub

Keamanan cloud di AWS merupakan prioritas tertinggi. Sebagai pelanggan AWS, Anda mendapatkan manfaat dari pusat data dan arsitektur jaringan yang dibangun untuk memenuhi persyaratan organisasi yang paling sensitif terhadap keamanan.

Keamanan adalah tanggung jawab bersama antara AWS dan Anda. Model tanggung jawab bersama menjelaskan hal ini sebagai keamanan dari cloud dan keamanan di cloud:

- Keamanan cloud – AWS bertanggung jawab untuk melindungi infrastruktur yang menjalankan layanan AWS di Cloud AWS. AWS juga memberikan Anda layanan yang dapat digunakan dengan aman. Auditor pihak ketiga menguji dan memverifikasi efektivitas keamanan kami sebagai bagian dari program kepatuhan AWS. Untuk mempelajari program kepatuhan yang berlaku di AWS Security Hub, lihat Cakupan Layanan Menurut Program Kepatuhan AWS.
- Keamanan di cloud – Tanggung jawab Anda ditentukan menurut layanan AWS yang Anda gunakan. Anda juga bertanggung jawab atas faktor lain, yang mencakup sensitivitas data Anda, persyaratan perusahaan Anda, serta undang-undang dan peraturan yang berlaku.

Dokumentasi ini membantu Anda memahami cara menerapkan model tanggung jawab bersama saat menggunakan Security Hub. Topik berikut menunjukkan cara mengonfigurasi Security Hub untuk memenuhi tujuan keamanan dan kepatuhan Anda. Anda juga mempelajari cara menggunakan AWS layanan lain yang membantu Anda memantau dan mengamankan sumber daya Security Hub Anda.

Topik

Perlindungan data di AWS Security Hub

Model tanggung jawab bersama AWS diterapkan untuk perlindungan data AWS Security Hub. Sebagaimana dijelaskan dalam model ini, AWS bertanggung jawab untuk melindungi infrastruktur

global yang menjalankan semua AWS Cloud. Anda harus bertanggung jawab untuk memelihara kendali terhadap konten yang di-hosting pada infrastruktur ini. Anda juga bertanggung jawab atas tugas konfigurasi dan manajemen keamanan untuk Layanan AWS yang Anda gunakan. Untuk informasi selengkapnya tentang privasi data, lihat FAQ Privasi Data. Untuk informasi tentang perlindungan data di Eropa, silakan lihat postingan blog Model Tanggung Jawab Bersama AWS dan GDPR di Blog Keamanan AWS.

Untuk tujuan perlindungan data, sebaiknya Anda melindungi kredensial Akun AWS dan menyiapkan AWS IAM Identity Center atau AWS Identity and Access Management (IAM) untuk pengguna individu. Dengan cara seperti itu, setiap pengguna hanya diberi izin yang diperlukan untuk memenuhi tanggung jawab tugas mereka. Kami juga merekomendasikan agar Anda mengamankan data Anda dengan cara-cara berikut:

- Gunakan autentikasi multi-faktor (MFA) pada setiap akun.
- Gunakan SSL/TLS untuk melakukan komunikasi dengan sumber daya AWS. Kami membutuhkan TLS 1.2 dan merekomendasikan TLS 1.3.
- Siapkan API dan log aktivitas pengguna dengan AWS CloudTrail.
- Gunakan solusi enkripsi AWS, bersama dengan semua kontrol keamanan default dalam Layanan AWS.
- Gunakan layanan keamanan terkelola lanjutan seperti Amazon Macie, yang membantu menemukan dan mengamankan data sensitif yang disimpan di Amazon S3.
- Jika Anda memerlukan modul kriptografi tervalidasi FIPS 140-2 ketika mengakses AWS melalui antarmuka baris perintah atau API, gunakan titik akhir FIPS. Untuk informasi selengkapnya tentang titik akhir FIPS yang tersedia, silakan lihat Standar Pemrosesan Informasi Federal (FIPS) 140-2.

Sebaiknya Anda tidak memasukkan informasi rahasia atau sensitif, seperti alamat email pelanggan, ke dalam tanda atau bidang teks bebas seperti bidang Nama. Ini termasuk saat Anda bekerja dengan Security Hub atau lainnya Layanan AWS menggunakan konsol, APIAWS CLI, atau AWS SDK. Data apa pun yang Anda masukkan ke dalam tanda atau bidang teks bebas yang digunakan untuk nama dapat digunakan untuk log penagihan atau diagnostik. Saat Anda memberikan URL ke server eksternal, sebaiknya Anda tidak menyertakan informasi kredensial di URL untuk memvalidasi permintaan Anda ke server tersebut.

Security Hub adalah penawaran layanan multi-tenant. Untuk memastikan perlindungan data, Security Hub mengenkripsi data saat istirahat dan data dalam perjalanan antar layanan komponen.

AWS Identity and Access Management untuk AWS Security Hub

AWS Identity and Access Management (IAM) adalah Layanan AWS yang membantu administrator mengontrol akses ke AWS sumber daya dengan aman. Administrator IAM mengontrol siapa yang dapat diautentikasi (masuk) dan diberi wewenang (memiliki izin) untuk menggunakan sumber daya Security Hub. IAM adalah Layanan AWS yang dapat Anda gunakan tanpa biaya tambahan.

Topik

Audiens

Cara Anda menggunakan AWS Identity and Access Management (IAM) berbeda, tergantung pada pekerjaan yang Anda lakukan di Security Hub.

Pengguna layanan — Jika Anda menggunakan layanan Security Hub untuk melakukan pekerjaan Anda, administrator Anda memberi Anda kredensi dan izin yang Anda butuhkan. Saat Anda menggunakan lebih banyak fitur Security Hub untuk melakukan pekerjaan Anda, Anda mungkin memerlukan izin tambahan. Memahami cara akses dikelola dapat membantu Anda meminta izin yang tepat dari administrator Anda. Jika Anda tidak dapat mengakses fitur di Security Hub, lihatMemecahkan masalah AWS Security Hub identitas dan akses.

Administrator layanan - Jika Anda bertanggung jawab atas sumber daya Security Hub di perusahaan Anda, Anda mungkin memiliki akses penuh ke Security Hub. Tugas Anda adalah menentukan fitur dan sumber daya Security Hub mana yang harus diakses pengguna layanan Anda. Kemudian, Anda harus mengirimkan permintaan kepada administrator IAM untuk mengubah izin pengguna layanan Anda. Tinjau informasi di halaman ini untuk memahami konsep Basic IAM. Untuk mempelajari lebih lanjut tentang cara perusahaan Anda dapat menggunakan IAM dengan Security Hub, lihatBagaimana AWS Security Hub bekerja dengan IAM.

Administrator IAM — Jika Anda administrator IAM, Anda mungkin ingin mempelajari detail tentang cara menulis kebijakan untuk mengelola akses ke Security Hub. Untuk melihat contoh kebijakan berbasis identitas Security Hub yang dapat Anda gunakan di IAM, lihat. Contoh kebijakan berbasis identitas untuk Security Hub

Mengautentikasi dengan identitas

Otentikasi adalah cara Anda masuk AWS menggunakan kredensyal 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 kredensyal 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 kredensil Anda. Jika Anda tidak menggunakan AWS alat, Anda harus menandatangani permintaan sendiri. Untuk informasi selengkapnya tentang penggunaan metode yang disarankan untuk menandatangani permintaan sendiri, lihat Menandatangani permintaan AWS API di 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 Menggunakan autentikasi multi-faktor (MFA) dalam AWS 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 kredensil yang disediakan melalui sumber identitas. Ketika identitas federasi mengakses Akun AWS, mereka mengambil peran, dan peran memberikan kredensyal 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 memiliki grup yang bernama IAMAdmins dan memberikan izin ke grup tersebut untuk mengelola sumber daya IAM.

Pengguna berbeda dari peran. Pengguna secara unik terkait dengan satu orang atau aplikasi, tetapi peran dimaksudkan untuk dapat digunakan oleh siapa pun yang membutuhkannya. Pengguna memiliki kredensial jangka panjang permanen, tetapi peran memberikan kredensial sementara. Untuk mempelajari selengkapnya, lihat Kapan harus membuat pengguna IAM (bukan peran) dalam Panduan Pengguna IAM.

Peran IAM

Peran IAM adalah identitas dalam diri Anda Akun AWS yang memiliki izin khusus. Peran ini mirip dengan pengguna IAM, tetapi tidak terkait dengan orang tertentu. Anda dapat mengambil peran IAM untuk sementara AWS Management Console dengan beralih peran. 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 Menggunakan peran IAM dalam Panduan Pengguna IAM.

Peran IAM dengan kredensial sementara berguna dalam situasi berikut:

- Akses pengguna terfederasi – Untuk menetapkan izin ke identitas terfederasi, Anda membuat peran dan menentukan izin untuk peran tersebut. Ketika identitas terfederasi mengautentikasi, identitas tersebut terhubung dengan peran dan diberi izin yang ditentukan oleh peran. Untuk informasi tentang peran untuk federasi, lihat Membuat peran untuk Penyedia Identitas pihak ketiga dalam Panduan Pengguna IAM. Jika menggunakan Pusat Identitas IAM, Anda harus mengonfigurasi set izin. Untuk mengontrol apa yang dapat diakses identitas Anda setelah identitas tersebut diautentikasi, Pusat Identitas IAM akan mengorelasikan set izin ke peran dalam IAM. Untuk informasi tentang set izin, lihat Set izin 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 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 di Panduan Pengguna IAM.
- Akses lintas layanan — Beberapa Layanan AWS menggunakan fitur lain Layanan AWS. Sebagai contoh, ketika Anda memanggil suatu layanan, biasanya layanan tersebut menjalankan aplikasi di Amazon EC2 atau menyimpan objek di Amazon S3. Sebuah layanan mungkin melakukannya

menggunakan izin 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 Membuat 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. 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 instans EC2 dan membuat atau permintaan API. AWS CLI AWS Cara ini lebih dianjurkan daripada menyimpan kunci akses dalam instans EC2. Untuk menetapkan AWS peran ke instans EC2 dan membuatnya tersedia untuk semua aplikasinya, Anda membuat profil instance yang dilampirkan ke instance. Profil instans berisi peran dan memungkinkan program yang berjalan di instans EC2 mendapatkan kredensial sementara. Untuk informasi selengkapnya, lihat Menggunakan peran IAM untuk memberikan izin ke aplikasi yang berjalan dalam instans Amazon EC2 dalam Panduan Pengguna IAM.

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

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 Membuat kebijakan IAM 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 dilampirkan 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 Memilih 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 (ACL)

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

Amazon S3, AWS WAF, dan Amazon VPC adalah contoh layanan yang mendukung ACL. Untuk mempelajari ACL selengkapnya, lihat Gambaran umum daftar kontrol akses (ACL) dalam Panduan Developer Amazon Simple Storage Service.

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 (SCP) — SCP 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 di organisasi, Anda dapat menerapkan kebijakan kontrol layanan (SCP) 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 Organisasi dan SCP, lihat Cara kerja SCP dalam Panduan Pengguna AWS Organizations .

- 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 AWS Security Hub bekerja dengan IAM

Sebelum Anda menggunakan AWS Identity and Access Management (IAM) untuk mengelola akses AWS Security Hub, pelajari fitur IAM mana yang tersedia untuk digunakan dengan Security Hub.

Fitur IAM yang dapat Anda gunakan AWS Security Hub

Fitur IAM	Dukungan Security Hub
Kebijakan berbasis identitas	Ya
Kebijakan berbasis sumber daya	Tidak
Tindakan kebijakan	Ya
Sumber daya kebijakan	Tidak
Kunci kondisi kebijakan	Ya
Daftar kontrol akses (ACL)	Tidak
Kontrol akses berbasis atribut (ABAC) — tag dalam kebijakan	Ya
Kredensial sementara	Ya
Sesi akses teruskan (FAS)	Ya

Fitur IAM	Dukungan Security Hub
Peran layanan	Tidak
Peran terkait layanan	Ya

Untuk tampilan tingkat tinggi tentang cara Layanan AWS kerja Security Hub dan fitur lainnya dengan sebagian besar fitur IAM, lihat fitur Layanan AWS tersebut bekerja dengan IAM di Panduan Pengguna IAM.

Kebijakan berbasis identitas untuk Security Hub

Mendukung kebijakan berbasis identitas	Ya

Kebijakan berbasis identitas adalah dokumen kebijakan izin JSON yang dapat Anda lampirkan ke sebuah identitas, seperti pengguna IAM, grup pengguna IAM, atau peran IAM. Kebijakan ini mengontrol jenis tindakan yang dapat dilakukan oleh pengguna dan peran, di sumber daya mana, dan berdasarkan kondisi seperti apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, lihat Membuat kebijakan IAM dalam Panduan Pengguna IAM.

Dengan kebijakan berbasis identitas IAM, Anda dapat menentukan secara spesifik apakah tindakan dan sumber daya diizinkan atau ditolak, serta kondisi yang menjadi dasar dikabulkan atau ditolaknya tindakan tersebut. Anda tidak dapat menentukan secara spesifik prinsipal dalam sebuah kebijakan berbasis identitas karena prinsipal berlaku bagi pengguna atau peran yang melekat kepadanya. Untuk mempelajari semua elemen yang dapat Anda gunakan dalam kebijakan JSON, lihat Referensi elemen kebijakan JSON IAM dalam Panduan Pengguna IAM.

Security Hub mendukung kebijakan berbasis identitas. Untuk informasi selengkapnya, lihat Contoh kebijakan berbasis identitas untuk Security Hub.

resource=Kebijakan berbasis untuk Security Hub

Mendukung kebijakan berbasis sumber daya	Tidak

Kebijakan berbasis sumber daya adalah dokumen kebijakan JSON yang Anda lampirkan ke sumber daya. Contoh kebijakan berbasis sumber daya adalah kebijakan kepercayaan peran IAM dan

kebijakan bucket Amazon S3. Dalam layanan yang mendukung kebijakan berbasis sumber daya, administrator layanan dapat menggunakannya untuk mengontrol akses ke sumber daya tertentu. Untuk sumber daya tempat kebijakan dilampirkan, kebijakan menentukan tindakan apa yang dapat dilakukan oleh prinsipal tertentu pada sumber daya tersebut dan dalam kondisi apa. Anda harus menentukan prinsipal dalam kebijakan berbasis sumber daya. Prinsipal dapat mencakup akun, pengguna, peran, pengguna federasi, atau. Layanan AWS

Untuk mengaktifkan akses lintas akun, Anda dapat menentukan secara spesifik seluruh akun atau entitas IAM di akun lain sebagai prinsipal dalam kebijakan berbasis sumber daya. Menambahkan prinsipal akun silang ke kebijakan berbasis sumber daya hanya setengah dari membangun hubungan kepercayaan. Ketika prinsipal dan sumber daya berbeda Akun AWS, administrator IAM di akun tepercaya juga harus memberikan izin entitas utama (pengguna atau peran) untuk mengakses sumber daya. Mereka memberikan izin dengan melampirkan kebijakan berbasis identitas kepada entitas. Namun, jika kebijakan berbasis sumber daya memberikan akses ke prinsipal dalam akun yang sama, tidak diperlukan kebijakan berbasis identitas tambahan. Untuk informasi selengkapnya, lihat Akses sumber daya lintas akun di IAM di Panduan Pengguna IAM.

Security Hub tidak mendukung kebijakan berbasis sumber daya. Anda tidak dapat melampirkan kebijakan IAM secara langsung ke sumber daya Security Hub.

Tindakan kebijakan untuk Security Hub

Mendukung tindakan kebijakan	Ya

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Artinya, prinsipal manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan kondisi apa.

Elemen `Action` dari kebijakan JSON menjelaskan tindakan yang dapat Anda gunakan untuk mengizinkan atau menolak akses dalam sebuah kebijakan. Tindakan kebijakan biasanya memiliki nama yang sama dengan operasi AWS API terkait. Ada beberapa pengecualian, misalnya tindakan hanya izin yang tidak memiliki operasi API yang cocok. Ada juga beberapa operasi yang memerlukan beberapa tindakan dalam suatu kebijakan. Tindakan tambahan ini disebut tindakan dependen.

Menyertakan tindakan dalam kebijakan untuk memberikan izin untuk melakukan operasi terkait.

Tindakan kebijakan di Security Hub menggunakan awalan berikut sebelum tindakan:

```
securityhub:
```

Misalnya, untuk memberikan izin kepada pengguna untuk mengaktifkan Security Hub, yang merupakan tindakan yang sesuai dengan `EnableSecurityHub` pengoperasian API Security Hub, sertakan `securityhub:EnableSecurityHub` tindakan tersebut dalam kebijakan mereka. Pernyataan kebijakan harus memuat elemen `Action` atau `NotAction`. Security Hub mendefinisikan serangkaian tindakannya sendiri yang menjelaskan tugas yang dapat Anda lakukan dengan layanan ini.

```
"Action": "securityhub:EnableSecurityHub"
```

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

```
"Action": [
      "securityhub:EnableSecurityHub",
      "securityhub:BatchEnableStandards"
```

Anda juga dapat menentukan beberapa tindakan menggunakan wildcard (*). Sebagai contoh, untuk menentukan semua tindakan yang dimulai dengan kata `Get`, sertakan tindakan berikut:

```
"Action": "securityhub:Get*"
```

Namun, sebagai praktik terbaik, Anda harus membuat kebijakan yang mengikuti prinsip hak istimewa paling sedikit. Dengan kata lain, Anda harus membuat kebijakan yang hanya menyertakan izin yang diperlukan untuk melakukan tugas tertentu.

Pengguna harus memiliki akses ke `DescribeStandardsControl` operasi untuk memiliki akses ke`BatchGetSecurityControls`,`BatchGetStandardsControlAssociations`, dan`ListStandardsControlAssociations`.

Pengguna harus memiliki akses ke `UpdateStandardsControls` operasi untuk memiliki akses ke`BatchUpdateStandardsControlAssociations`, dan`UpdateSecurityControl`.

Untuk daftar tindakan Security Hub, lihat Tindakan yang ditentukan oleh AWS Security Hub dalam Referensi Otorisasi Layanan. Untuk contoh kebijakan yang menentukan tindakan Security Hub, lihatContoh kebijakan berbasis identitas untuk Security Hub.

Sumber daya

Mendukung sumber daya kebijakan	Tidak

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Artinya, prinsipal manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan kondisi apa.

Elemen kebijakan JSON `Resource` menentukan objek yang menjadi target penerapan tindakan. Pernyataan harus menyertakan elemen `Resource` atau `NotResource`. Praktik terbaiknya, tentukan sumber daya menggunakan Amazon Resource Name (ARN). Anda dapat melakukan ini untuk tindakan yang mendukung jenis sumber daya tertentu, yang dikenal sebagai izin tingkat sumber daya.

Untuk tindakan yang tidak mendukung izin di tingkat sumber daya, misalnya operasi pencantuman, gunakan wildcard (*) untuk menunjukkan bahwa pernyataan tersebut berlaku untuk semua sumber daya.

```
"Resource": "*"
```

Security Hub mendefinisikan jenis sumber daya berikut:

- Hub
- Produk
- Menemukan agregator, juga disebut sebagai agregator lintas wilayah
- Aturan otomatisasi
- Kebijakan konfigurasi

Anda dapat menentukan jenis sumber daya ini dalam kebijakan dengan menggunakan ARN.

Untuk daftar jenis sumber daya Security Hub dan sintaks ARN untuk masing-masing, lihat Jenis sumber daya yang ditentukan oleh AWS Security Hub dalam Referensi Otorisasi Layanan. Untuk mempelajari tindakan yang dapat Anda tentukan untuk setiap jenis sumber daya, lihat Tindakan yang ditentukan oleh AWS Security Hub dalam Referensi Otorisasi Layanan. Untuk contoh kebijakan yang menentukan sumber daya, lihatContoh kebijakan berbasis identitas untuk Security Hub.

Kunci kondisi kebijakan untuk Security Hub

Mendukung kunci kondisi kebijakan khusus layanan	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 `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 tag yang sesuai dengan nama pengguna IAM mereka. Untuk informasi selengkapnya, lihat Elemen kebijakan IAM: variabel dan tag dalam Panduan Pengguna IAM.

AWS mendukung kunci kondisi global dan kunci kondisi khusus layanan. Untuk melihat semua kunci kondisi AWS global, lihat kunci konteks kondisi AWS global di Panduan Pengguna IAM.

Untuk daftar kunci kondisi Security Hub, lihat Kunci kondisi untuk AWS Security Hub Referensi Otorisasi Layanan. Untuk mempelajari tindakan dan sumber daya yang dapat digunakan untuk menggunakan kunci kondisi, lihat Tindakan yang ditentukan oleh AWS Security Hub. Untuk contoh kebijakan yang menggunakan kunci kondisi, lihatContoh kebijakan berbasis identitas untuk Security Hub.

Daftar kontrol akses (ACL) di Security Hub

Mendukung ACL	Tidak

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

Security Hub tidak mendukung ACL, yang berarti Anda tidak dapat melampirkan ACL ke sumber daya Security Hub.

Kontrol akses berbasis atribut (ABAC) dengan Security Hub

Mendukung ABAC (tanda dalam kebijakan)	Ya

Kontrol akses berbasis atribut (ABAC) adalah strategi otorisasi yang menentukan izin berdasarkan atribut. Dalam AWS, atribut ini disebut tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke banyak AWS sumber daya. Penandaan ke entitas dan sumber daya adalah langkah pertama dari ABAC. Kemudian rancanglah kebijakan ABAC untuk mengizinkan operasi ketika tag milik prinsipal cocok dengan tag 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 tag, berikan informasi tentang tag di elemen kondisi dari kebijakan menggunakan kunci kondisi `aws:ResourceTag/key-name`, `aws:RequestTag/key-name`, atau `aws:TagKeys`.

Jika sebuah layanan mendukung ketiga kunci kondisi untuk setiap jenis sumber daya, nilainya adalah Ya untuk layanan tersebut. Jika suatu layanan mendukung ketiga kunci kondisi untuk hanya beberapa jenis sumber daya, nilainya adalah Parsial.

Untuk informasi selengkapnya tentang ABAC, lihat Apa itu ABAC? dalam Panduan Pengguna IAM. Untuk melihat tutorial yang menguraikan langkah-langkah pengaturan ABAC, lihat Menggunakan kontrol akses berbasis atribut (ABAC) dalam Panduan Pengguna IAM.

Anda dapat melampirkan tag ke sumber daya Security Hub. Anda juga dapat mengontrol akses ke sumber daya dengan memberikan informasi tag dalam `Condition` elemen kebijakan.

Untuk informasi tentang menandai sumber daya Security Hub, lihatMenandai sumber daya AWS Security Hub. Untuk contoh kebijakan berbasis identitas yang mengontrol akses ke sumber daya berdasarkan tag, lihat. Contoh kebijakan berbasis identitas untuk Security Hub

Menggunakan kredensyal sementara dengan Security Hub

Mendukung penggunaan kredensial sementara	Ya

Beberapa Layanan AWS tidak berfungsi saat Anda masuk menggunakan kredensyal 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 kredensyal 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 kredensyal sementara. Anda juga akan secara otomatis membuat kredensial sementara ketika Anda masuk ke konsol sebagai seorang pengguna lalu beralih peran. Untuk informasi selengkapnya tentang peralihan peran, lihat Peralihan peran (konsol) dalam Panduan Pengguna IAM.

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

Anda dapat menggunakan kredensial sementara untuk masuk dengan gabungan, menjalankan IAM role, atau menjalankan peran lintas akun. Anda memperoleh kredensyal keamanan sementara dengan memanggil operasi AWS STS API seperti AssumeRoleatau. GetFederationToken

Security Hub mendukung penggunaan kredensyal sementara.

Teruskan sesi akses untuk Security Hub

Mendukung sesi akses maju (FAS)	Ya

Saat Anda menggunakan pengguna atau peran IAM untuk melakukan tindakan AWS, Anda dianggap sebagai prinsipal. Ketika Anda menggunakan beberapa layanan, Anda mungkin melakukan sebuah tindakan yang kemudian menginisiasi tindakan lain di layanan yang berbeda. FAS menggunakan izin dari pemanggilan utama Layanan AWS, dikombinasikan dengan permintaan Layanan AWS

untuk membuat permintaan ke layanan hilir. Permintaan FAS hanya dibuat ketika layanan menerima permintaan yang memerlukan interaksi dengan orang lain Layanan AWS atau sumber daya untuk menyelesaikannya. Dalam hal ini, Anda harus memiliki izin untuk melakukan kedua tindakan tersebut. Untuk detail kebijakan ketika mengajukan permintaan FAS, lihat Sesi akses maju.

Misalnya, Security Hub membuat permintaan FAS ke hilir Layanan AWS saat Anda mengintegrasikan Security Hub dengan AWS Organizations dan saat Anda menunjuk akun administrator Security Hub yang didelegasikan untuk organisasi di Organizations..

Untuk tugas lain, Security Hub menggunakan peran terkait layanan untuk melakukan tindakan atas nama Anda. Untuk detail tentang peran ini, lihatPeran terkait layanan untuk Security Hub.

Peran layanan untuk Security Hub

Security Hub tidak mengasumsikan atau menggunakan peran layanan. Untuk melakukan tindakan atas nama Anda, Security Hub menggunakan peran terkait layanan. Untuk detail tentang peran ini, lihatPeran terkait layanan untuk Security Hub.

> **Warning**
>
> Mengubah izin untuk peran layanan dapat menimbulkan masalah operasional dengan penggunaan Security Hub. Edit peran layanan hanya jika Security Hub memberikan panduan untuk melakukannya.

Peran terkait layanan untuk Security Hub

Mendukung peran terkait layanan	Ya

Peran terkait layanan adalah jenis peran layanan yang ditautkan ke. Layanan AWS Layanan tersebut dapat menjalankan peran untuk melakukan tindakan atas nama Anda. Peran terkait layanan muncul di Anda Akun AWS dan dimiliki oleh layanan. Administrator IAM dapat melihat, tetapi tidak dapat mengedit izin untuk peran terkait layanan.

Security Hub menggunakan peran terkait layanan untuk melakukan tindakan atas nama Anda. Untuk detail tentang peran ini, lihatPeran terkait layanan untuk Security Hub.

Contoh kebijakan berbasis identitas untuk Security Hub

Secara default, pengguna dan peran tidak memiliki izin untuk membuat atau memodifikasi sumber daya Security Hub. Mereka juga tidak dapat melakukan tugas dengan menggunakan AWS Management Console, AWS CLI, atau API AWS. Administrator harus membuat kebijakan IAM yang memberikan izin kepada pengguna dan peran untuk melakukan operasi API tertentu pada sumber daya tertentu yang mereka butuhkan. Administrator kemudian harus melampirkan kebijakan tersebut ke pengguna atau grup yang memerlukan izin tersebut.

Untuk mempelajari cara membuat kebijakan berbasis identitas IAM menggunakan contoh dokumen kebijakan JSON ini, lihat Membuat Kebijakan pada Tab JSON dalam Panduan Pengguna IAM.

Topik

Praktik terbaik kebijakan

Kebijakan berbasis identitas menentukan apakah seseorang dapat membuat, mengakses, atau menghapus sumber daya Security Hub di akun Anda. Tindakan ini dikenai biaya untuk Akun AWS Anda. Ketika Anda membuat atau mengedit kebijakan berbasis identitas, ikuti panduan dan rekomendasi ini:

- Mulai menggunakan kebijakan yang dikelola AWS dan beralih ke izin dengan hak akses paling rendah – Untuk mulai memberikan izin kepada pengguna dan beban kerja Anda, gunakan kebijakan yang dikelola AWS yang memberikan izin untuk banyak kasus penggunaan umum. Kebijakan ini ada di Akun AWS Anda. Sebaiknya Anda mengurangi izin lebih lanjut dengan menentukan kebijakan yang dikelola pelanggan AWS yang khusus untuk kasus penggunaan Anda. Untuk informasi selengkapnya, lihat kebijakan yang dikelola AWS atau kebijakan yang dikelola AWS untuk fungsi pekerjaan di 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 melakukan

ini dengan menentukan tindakan yang dapat diambil pada sumber daya tertentu dalam kondisi tertentu, juga dikenal sebagai izin hak akses paling rendah. Untuk informasi selengkapnya tentang cara menggunakan IAM untuk menerapkan izin, lihat Kebijakan dan izin di IAM di Panduan Pengguna IAM.

- Gunakan kondisi dalam kebijakan IAM untuk membatasi akses lebih lanjut – Anda dapat menambahkan kondisi ke kebijakan Anda untuk membatasi akses ke tindakan dan sumber daya. Misalnya, Anda dapat menulis syarat kebijakan untuk menentukan bahwa semua pengajuan harus dikirim menggunakan SSL. Anda juga dapat menggunakan kondisi untuk memberi akses ke tindakan layanan jika digunakan melalui Layanan AWS yang spesifk, seperti AWS CloudFormation. Untuk informasi selengkapnya, lihat Elemen kebijakan JSON IAM: Syarat di Panduan Pengguna IAM.
- Menggunakan IAM Access Analyzer untuk memvalidasi kebijakan IAM Anda guna memastikan izin yang aman dan berfungsi – 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 Analizer Akses IAM di Panduan Pengguna IAM.
- Wajibkan autentikasi multi-faktor (MFA) – Jika Anda memiliki skenario yang mengharuskan pengguna IAM atau pengguna root di Akun AWS Anda, aktifkan MFA untuk keamanan tambahan. Untuk mewajibkan MFA saat operasi API dipanggil, tambahkan kondisi MFA pada kebijakan Anda. Untuk informasi selengkapnya, lihat Mengonfigurasi akses API yang dilindungi MFA di Panduan Pengguna IAM.

Untuk informasi selengkapnya tentang praktik terbaik dalam IAM, lihat Praktik terbaik keamanan di IAM di Panduan Pengguna IAM.

Menggunakan konsol Security Hub

Untuk mengakses konsol AWS Security Hub tersebut, Anda harus memiliki rangkaian izin minimum. Izin ini harus memungkinkan Anda untuk membuat daftar dan melihat detail tentang sumber daya Security Hub di situs AndaAkun 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 memberikan izin konsol minimum untuk pengguna yang melakukan panggilan hanya ke AWS CLI atau API AWS. Sebaliknya, izinkan akses hanya ke tindakan yang cocok dengan operasi API yang coba dilakukan.

Untuk memastikan bahwa pengguna dan peran tersebut dapat menggunakan konsol Security Hub, lampirkan juga kebijakan AWS terkelola berikut ke entitas. Untuk informasi selengkapnya, lihat Menambahkan izin ke pengguna dalam Panduan Pengguna IAM:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "securityhub:*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "securityhub.amazonaws.com"
                }
            }
        }
    ]
}
```

Contoh: Izinkan pengguna untuk melihat izin mereka sendiri

Contoh ini menunjukkan cara membuat kebijakan yang mengizinkan para pengguna IAM melihat kebijakan inline dan terkelola yang dilampirkan ke identitas pengguna mereka. Kebijakan ini mencakup izin untuk menyelesaikan tindakan pada konsol atau menggunakan AWS CLI atau AWS API secara terprogram.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
```

```
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Contoh: Izinkan pengguna membuat dan mengelola kebijakan konfigurasi

Contoh ini menunjukkan cara membuat kebijakan IAM yang memungkinkan pengguna membuat, melihat, memperbarui, dan menghapus kebijakan konfigurasi. Kebijakan contoh ini juga memungkinkan pengguna untuk memulai, menghentikan, dan melihat asosiasi kebijakan. Agar kebijakan IAM ini berfungsi, pengguna harus menjadi administrator Security Hub yang didelegasikan untuk organisasi.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "CreateAndUpdateConfigurationPolicy",
            "Effect": "Allow",
            "Action": [
                "securityhub:CreateConfigurationPolicy",
                "securityhub:UpdateConfigurationPolicy"
            ],
            "Resource": "*"
        },
```

```
        {
            "Sid": "ViewConfigurationPolicy",
            "Effect": "Allow",
            "Action": [
                "securityhub:GetConfigurationPolicy",
                "securityhub:ListConfigurationPolicies"
            ],
            "Resource": "*"
        },
        {
            "Sid": "DeleteConfigurationPolicy",
            "Effect": "Allow",
            "Action": [
                "securityhub:DeleteConfigurationPolicy"
            ],
            "Resource": "*"
        },
        {
            "Sid": "ViewConfigurationPolicyAssociation",
            "Effect": "Allow",
            "Action": [
                "securityhub:BatchGetConfigurationPolicyAssociations",
                "securityhub:GetConfigurationPolicyAssociation",
                "securityhub:ListConfigurationPolicyAssociations"
            ],
            "Resource": "*"
        },
        {
            "Sid": "UpdateConfigurationPolicyAssociation",
            "Effect": "Allow",
            "Action": [
                "securityhub:StartConfigurationPolicyAssociation",
                "securityhub:StartConfigurationPolicyDisassociation"
            ],
            "Resource": "*"
        }
    ]
}
```

Contoh: Izinkan pengguna untuk melihat temuan

Contoh ini menunjukkan cara membuat kebijakan IAM yang memungkinkan pengguna melihat temuan Security Hub.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ReviewFindings",
            "Effect": "Allow",
            "Action": [
                "securityhub:GetFindings"
            ],
            "Resource": "*"
        }
    ]
}
```

Contoh: Izinkan pengguna membuat dan mengelola aturan otomatisasi

Contoh ini menunjukkan cara membuat kebijakan IAM yang memungkinkan pengguna membuat, melihat, memperbarui, dan menghapus aturan otomatisasi Security Hub. Agar kebijakan IAM ini berfungsi, pengguna harus menjadi administrator Security Hub. Untuk membatasi izin — misalnya, untuk mengizinkan pengguna hanya melihat aturan otomatisasi — Anda dapat menghapus izin buat, perbarui, dan hapus.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "CreateAndUpdateAutomationRules",
            "Effect": "Allow",
            "Action": [
                "securityhub:CreateAutomationRule",
                "securityhub:BatchUpdateAutomationRules"
            ],
            "Resource": "*"
        },
        {
            "Sid": "ViewAutomationRules",
            "Effect": "Allow",
            "Action": [
                "securityhub:BatchGetAutomationRules",
                "securityhub:ListAutomationRules"
            ],
            "Resource": "*"
```

```
        },
        {
            "Sid": "DeleteAutomationRules",
            "Effect": "Allow",
            "Action": [
                "securityhub:BatchDeleteAutomationRules"
            ],
            "Resource": "*"
        }
    ]
}
```

Peran terkait layanan untuk Security Hub

AWS Security Hubmenggunakan peran terkait layanan AWS Identity and Access Management (IAM) bernama. `AWSServiceRoleForSecurityHub` Peran terkait layanan ini adalah peran IAM yang ditautkan langsung ke Security Hub. Ini telah ditentukan sebelumnya oleh Security Hub, dan mencakup semua izin yang diperlukan Security Hub untuk memanggil sumber daya lain Layanan AWS dan memantau AWS sumber daya atas nama Anda. Security Hub menggunakan peran terkait layanan ini di semua Wilayah AWS tempat Security Hub tersedia.

Peran terkait layanan membuat pengaturan Security Hub lebih mudah karena Anda tidak perlu menambahkan izin yang diperlukan secara manual. Security Hub mendefinisikan izin peran terkait layanan, dan kecuali izin ditentukan sebaliknya, hanya Security Hub yang dapat mengambil peran tersebut. Izin yang ditentukan mencakup kebijakan kepercayaan dan kebijakan izin, dan Anda tidak dapat melampirkan kebijakan izin tersebut ke entitas IAM lainnya.

Untuk melihat detail peran terkait layanan, pada halaman Pengaturan konsol Security Hub, pilih Umum, lalu Lihat izin layanan.

Anda dapat menghapus peran terkait layanan Security Hub hanya setelah pertama kali menonaktifkan Security Hub di semua Wilayah yang diaktifkan. Ini melindungi sumber daya Security Hub karena Anda tidak dapat secara tidak sengaja menghapus izin untuk mengaksesnya.

Untuk informasi tentang layanan lain yang mendukung peran terkait layanan, lihat AWSlayanan yang bekerja dengan IAM di Panduan Pengguna IAM dan temukan layanan yang memiliki Ya di kolom Peran Tertaut Layanan. Pilih Ya dengan sebuah tautan untuk melihat dokumentasi peran terkait layanan untuk layanan tersebut.

Topik

Izin peran terkait layanan untuk Security Hub

Security Hub menggunakan nama peran terkait layanan. `AWSServiceRoleForSecurityHub` Ini adalah peran terkait layanan yang diperlukan AWS Security Hub untuk mengakses sumber daya Anda. Peran terkait layanan memungkinkan Security Hub menerima temuan dari yang lain Layanan AWS dan mengonfigurasi AWS Config infrastruktur yang diperlukan untuk menjalankan pemeriksaan keamanan untuk kontrol.

Peran tertaut layanan `AWSServiceRoleForSecurityHub` memercayai layanan berikut untuk mengambil peran tersebut:

- `securityhub.amazonaws.com`

`AWSServiceRoleForSecurityHub`Peran terkait layanan menggunakan kebijakan terkelola. `AWSSecurityHubServiceRolePolicy`

Anda harus memberikan izin untuk mengizinkan identitas IAM (seperti peran, grup, atau pengguna) untuk membuat, mengedit, atau menghapus peran terkait layanan. Agar peran `AWSServiceRoleForSecurityHub` terkait layanan berhasil dibuat, identitas IAM yang Anda gunakan untuk mengakses Security Hub harus memiliki izin yang diperlukan. Untuk memberikan izin yang diperlukan, lampirkan kebijakan berikut ke peran, grup, atau pengguna.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "securityhub:*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
```

```
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "securityhub.amazonaws.com"
                }
            }
        }
    ]
}
```

Membuat peran terkait layanan untuk Security Hub

Peran `AWSServiceRoleForSecurityHub` terkait layanan dibuat secara otomatis saat Anda mengaktifkan Security Hub untuk pertama kalinya atau mengaktifkan Security Hub di Wilayah yang didukung yang sebelumnya tidak mengaktifkannya. Anda juga dapat membuat peran tertaut layanan `AWSServiceRoleForSecurityHub` secara manual menggunakan konsol IAM, CLI IAM, atau API IAM.

> **Important**
>
> Peran terkait layanan yang dibuat untuk akun administrator Security Hub tidak berlaku untuk akun anggota Security Hub.

Untuk informasi selengkapnya tentang membuat peran secara manual, lihat Membuat peran tertaut layanan dalam Panduan Pengguna IAM.

Mengedit peran terkait layanan untuk Security Hub

Security Hub tidak mengizinkan Anda mengedit peran `AWSServiceRoleForSecurityHub` terkait layanan. Setelah membuat peran terkait layanan, Anda tidak dapat mengubah nama peran karena berbagai entitas mungkin mereferensikan peran tersebut. Namun, Anda dapat mengubah deskripsi peran dengan menggunakan IAM. Untuk informasi selengkapnya, silakan lihat Menyunting peran terkait layanan dalam Panduan Pengguna IAM.

Menghapus peran terkait layanan untuk Security Hub

Jika Anda tidak perlu lagi menggunakan fitur atau layanan yang memerlukan peran tertaut layanan, sebaiknya Anda menghapus peran tersebut. Dengan begitu, Anda tidak memiliki entitas yang tidak terpakai yang tidak dipantau atau dipelihara secara aktif.

> **Important**
>
> Untuk menghapus peran `AWSServiceRoleForSecurityHub` terkait layanan, Anda harus menonaktifkan Security Hub terlebih dahulu di semua Wilayah yang diaktifkan.
> Jika Security Hub tidak dinonaktifkan saat Anda mencoba menghapus peran terkait layanan, penghapusan akan gagal. Untuk informasi selengkapnya, lihat Menonaktifkan Security Hub.

Saat Anda menonaktifkan Security Hub, peran `AWSServiceRoleForSecurityHub` terkait layanan tidak akan dihapus secara otomatis. Jika Anda mengaktifkan Security Hub lagi, Security Hub akan mulai menggunakan peran `AWSServiceRoleForSecurityHub` terkait layanan yang ada.

Cara menghapus peran tertaut layanan secara manual menggunakan IAM

Gunakan konsol IAM, CLI IAM, atau API CLI untuk menghapus peran tertaut layanan `AWSServiceRoleForSecurityHub`. Untuk informasi selengkapnya, lihat Menghapus peran tertaut layanan dalam Panduan Pengguna IAM.

AWS kebijakan terkelola untuk AWS Security Hub

Kebijakan AWS terkelola adalah kebijakan mandiri yang dibuat dan dikelola oleh AWS. AWS Kebijakan terkelola dirancang untuk memberikan izin bagi banyak kasus penggunaan umum sehingga Anda dapat mulai menetapkan izin kepada pengguna, grup, dan peran.

Perlu diingat bahwa kebijakan AWS terkelola mungkin tidak memberikan izin hak istimewa paling sedikit untuk kasus penggunaan spesifik Anda karena tersedia untuk digunakan semua pelanggan. AWS Kami menyarankan Anda untuk mengurangi izin lebih lanjut dengan menentukan kebijakan yang dikelola pelanggan yang khusus untuk kasus penggunaan Anda.

Anda tidak dapat mengubah izin yang ditentukan dalam kebijakan AWS terkelola. Jika AWS memperbarui izin yang ditentukan dalam kebijakan AWS terkelola, pemutakhiran akan memengaruhi semua identitas utama (pengguna, grup, dan peran) yang dilampirkan kebijakan tersebut. AWS kemungkinan besar akan memperbarui kebijakan AWS terkelola saat baru Layanan AWS diluncurkan atau operasi API baru tersedia untuk layanan yang ada.

Untuk informasi selengkapnya, lihat AWS kebijakan yang dikelola dalam Panduan Pengguna IAM.

AWS kebijakan terkelola: AWSSecurityHubFullAccess

Anda dapat melampirkan kebijakan `AWSSecurityHubFullAccess` ke identitas IAM Anda.

Kebijakan ini memberikan izin administratif yang memungkinkan akses penuh utama ke semua tindakan Security Hub. Kebijakan ini harus dilampirkan ke prinsipal sebelum mengaktifkan Security Hub secara manual untuk akun mereka. Misalnya, kepala sekolah dengan izin ini dapat melihat dan memperbarui status temuan. Mereka dapat mengonfigurasi wawasan khusus, dan mengaktifkan integrasi. Mereka dapat mengaktifkan dan menonaktifkan standar dan kontrol. Prinsipal untuk akun administrator juga dapat mengelola akun anggota.

Detail izin

Kebijakan ini mencakup izin berikut.

- `securityhub`— Memungkinkan kepala sekolah akses penuh ke semua tindakan Security Hub.
- `guardduty`— Memungkinkan kepala sekolah untuk mendapatkan informasi tentang status akun di Amazon. GuardDuty
- `iam`— Memungkinkan kepala sekolah untuk membuat peran terkait layanan.
- `inspector`— Memungkinkan kepala sekolah untuk mendapatkan informasi tentang status akun di Amazon Inspector.
- `pricing`— Memungkinkan kepala sekolah untuk mendapatkan daftar harga dan produk. Layanan AWS

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "SecurityHubAllowAll",
            "Effect": "Allow",
            "Action": "securityhub:*",
            "Resource": "*"
        },
        {
            "Sid": "SecurityHubServiceLinkedRole",
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "securityhub.amazonaws.com"
                }
            }
```

```
        },
        {
            "Sid": "OtherServicePermission",
            "Effect": "Allow",
            "Action": [
                "guardduty:GetDetector",
                "guardduty:ListDetectors",
                "inspector2:BatchGetAccountStatus",
                "pricing:GetProducts"
            ],
            "Resource": "*",
        }
    ]
}
```

Kebijakan terkelola Security Hub: AWSSecurityHubReadOnlyAccess

Anda dapat melampirkan kebijakan `AWSSecurityHubReadOnlyAccess` ke identitas IAM Anda.

Kebijakan ini memberikan izin hanya-baca yang memungkinkan pengguna melihat informasi di Security Hub. Prinsipal dengan kebijakan ini terlampir tidak dapat melakukan pembaruan apa pun di Security Hub. Misalnya, kepala sekolah dengan izin ini dapat melihat daftar temuan yang terkait dengan akun mereka, tetapi tidak dapat mengubah status temuan. Mereka dapat melihat hasil wawasan, tetapi tidak dapat membuat atau mengonfigurasi wawasan khusus. Mereka tidak dapat mengonfigurasi kontrol atau integrasi produk.

Detail izin

Kebijakan ini mencakup izin berikut.

- `securityhub` – Mengizinkan pengguna melakukan tindakan yang mengembalikan daftar item atau detail tentang item. Ini termasuk operasi API yang dimulai dengan`Get`,`List`, atau`Describe`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSSecurityHubReadOnlyAccess",
            "Effect": "Allow",
            "Action": [
                "securityhub:Get*",
```

```
                "securityhub:List*",
                "securityhub:BatchGet*",
                "securityhub:Describe*"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS kebijakan terkelola: AWSSecurityHubOrganizationsAccess

Anda dapat melampirkan kebijakan `AWSSecurityHubOrganizationsAccess` ke identitas IAM Anda.

Kebijakan ini memberikan izin administratif AWS Organizations yang diperlukan untuk mendukung integrasi Security Hub dengan Organizations.

Izin ini memungkinkan akun manajemen organisasi menunjuk akun administrator yang didelegasikan untuk Security Hub. Mereka juga mengizinkan akun administrator Security Hub yang didelegasikan untuk mengaktifkan akun organisasi sebagai akun anggota.

Kebijakan ini hanya memberikan izin untuk Organizations. Akun manajemen organisasi dan akun administrator Security Hub yang didelegasikan juga memerlukan izin untuk tindakan terkait di Security Hub. Izin ini dapat diberikan menggunakan kebijakan `AWSSecurityHubFullAccess` terkelola.

Detail izin

Kebijakan ini mencakup izin berikut.

- `organizations:ListAccounts`— Memungkinkan kepala sekolah untuk mengambil daftar akun yang merupakan bagian dari organisasi.
- `organizations:DescribeOrganization`— Memungkinkan kepala sekolah untuk mengambil informasi tentang organisasi.
- `organizations:ListRoots`— Memungkinkan kepala sekolah untuk membuat daftar akar organisasi.
- `organizations:ListDelegatedAdministrators`— Memungkinkan kepala sekolah untuk membuat daftar administrator yang didelegasikan dari suatu organisasi.
- `organizations:ListAWSServiceAccessForOrganization`— Memungkinkan kepala sekolah untuk membuat daftar Layanan AWS yang digunakan organisasi.

- `organizations:ListOrganizationalUnitsForParent`— Memungkinkan kepala sekolah untuk membuat daftar unit organisasi anak (OU) dari OU orang tua.
- `organizations:ListAccountsForParent`— Memungkinkan kepala sekolah untuk membuat daftar akun anak dari OU orang tua.
- `organizations:DescribeAccount`— Memungkinkan kepala sekolah untuk mengambil informasi tentang akun di organisasi.
- `organizations:DescribeOrganizationalUnit`— Memungkinkan kepala sekolah untuk mengambil informasi tentang OU dalam organisasi.
- `organizations:DescribeOrganization`— Memungkinkan kepala sekolah untuk mengambil informasi tentang konfigurasi organisasi.
- `organizations:EnableAWSServiceAccess`— Memungkinkan prinsipal untuk mengaktifkan integrasi Security Hub dengan Organizations.
- `organizations:RegisterDelegatedAdministrator`— Memungkinkan kepala sekolah untuk menunjuk akun administrator yang didelegasikan untuk Security Hub.
- `organizations:DeregisterDelegatedAdministrator`— Memungkinkan kepala sekolah untuk menghapus akun administrator yang didelegasikan untuk Security Hub.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "OrganizationPermissions",
            "Effect": "Allow",
            "Action": [
                "organizations:ListAccounts",
                "organizations:DescribeOrganization",
                "organizations:ListRoots",
                "organizations:ListDelegatedAdministrators",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:ListOrganizationalUnitsForParent",
                "organizations:ListAccountsForParent",
                "organizations:DescribeAccount",
                "organizations:DescribeOrganizationalUnit"
            ],
            "Resource": "*"
        },
        {
            "Sid": "OrganizationPermissionsEnable",
```

```
            "Effect": "Allow",
            "Action": "organizations:EnableAWSServiceAccess",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "organizations:ServicePrincipal": "securityhub.amazonaws.com"
                }
            }
        },
        {
            "Sid": "OrganizationPermissionsDelegatedAdmin",
            "Effect": "Allow",
            "Action": [
                "organizations:RegisterDelegatedAdministrator",
                "organizations:DeregisterDelegatedAdministrator"
            ],
            "Resource": "arn:aws:organizations::*:account/o-*/*",
            "Condition": {
            "StringEquals": {
                "organizations:ServicePrincipal": "securityhub.amazonaws.com"
                }
            }
        }
    ]
}
```

AWS kebijakan terkelola: AWSSecurityHubServiceRolePolicy

Anda tidak dapat melampirkan `AWSSecurityHubServiceRolePolicy` ke entitas IAM Anda. Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan Security Hub melakukan tindakan atas nama Anda. Untuk informasi selengkapnya, lihat the section called “Peran terkait layanan”.

Kebijakan ini memberikan izin administratif yang memungkinkan peran terkait layanan untuk melakukan pemeriksaan keamanan untuk kontrol Security Hub.

Detail izin

Kebijakan ini mencakup izin untuk melakukan hal berikut:

- `cloudtrail`— Ambil informasi tentang jalan CloudTrail setapak.
- `cloudwatch`— Ambil CloudWatch alarm saat ini.

- `logs`— Ambil filter metrik untuk CloudWatch log.
- `sns`— Ambil daftar langganan ke topik SNS.
- `config`— Mengambil informasi tentang perekam konfigurasi, sumber daya, dan AWS Config aturan. Juga memungkinkan peran terkait layanan untuk membuat dan menghapus AWS Config aturan, dan menjalankan evaluasi terhadap aturan.
- `iam`— Dapatkan dan buat laporan kredensi untuk akun.
- `organizations`— Mengambil informasi akun dan unit organisasi (OU) untuk suatu organisasi.
- `securityhub`— Mengambil informasi tentang bagaimana layanan, standar, dan kontrol Security Hub dikonfigurasi.
- `tag`— Mengambil informasi tentang tag sumber daya.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "SecurityHubServiceRolePermissions",
            "Effect": "Allow",
            "Action": [
                "cloudtrail:DescribeTrails",
                "cloudtrail:GetTrailStatus",
                "cloudtrail:GetEventSelectors",
                "cloudwatch:DescribeAlarms",
                "cloudwatch:DescribeAlarmsForMetric",
                "logs:DescribeMetricFilters",
                "sns:ListSubscriptionsByTopic",
                "config:DescribeConfigurationRecorders",
                "config:DescribeConfigurationRecorderStatus",
                "config:DescribeConfigRules",
                "config:DescribeConfigRuleEvaluationStatus",
                "config:BatchGetResourceConfig",
                "config:SelectResourceConfig",
                "iam:GenerateCredentialReport",
                "organizations:ListAccounts",
                "config:PutEvaluations",
                "tag:GetResources",
                "iam:GetCredentialReport",
                "organizations:DescribeAccount",
                "organizations:DescribeOrganization",
                "organizations:ListChildren",
```

```
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:DescribeOrganizationalUnit",
                "securityhub:BatchDisableStandards",
                "securityhub:BatchEnableStandards",
                "securityhub:BatchUpdateStandardsControlAssociations",
                "securityhub:BatchGetSecurityControls",
                "securityhub:BatchGetStandardsControlAssociations",
                "securityhub:CreateMembers",
                "securityhub:DeleteMembers",
                "securityhub:DescribeHub",
                "securityhub:DescribeOrganizationConfiguration",
                "securityhub:DescribeStandards",
                "securityhub:DescribeStandardsControls",
                "securityhub:DisassociateFromAdministratorAccount",
                "securityhub:DisassociateMembers",
                "securityhub:DisableSecurityHub",
                "securityhub:EnableSecurityHub",
                "securityhub:GetEnabledStandards",
                "securityhub:ListStandardsControlAssociations",
                "securityhub:ListSecurityControlDefinitions",
                "securityhub:UpdateOrganizationConfiguration",
                "securityhub:UpdateSecurityControl",
                "securityhub:UpdateSecurityHubConfiguration",
                "securityhub:UpdateStandardsControl",
                "tag:GetResources"
            ],
            "Resource": "*"
        },
        {
            "Sid": "SecurityHubServiceRoleConfigPermissions",
            "Effect": "Allow",
            "Action": [
                "config:PutConfigRule",
                "config:DeleteConfigRule",
                "config:GetComplianceDetailsByConfigRule"
            ],
            "Resource": "arn:aws:config:*:*:config-rule/aws-service-rule/*securityhub*"
        },
        {
            "Sid": "SecurityHubServiceRoleOrganizationsPermissions",
            "Effect": "Allow",
            "Action": [
                "organizations:ListDelegatedAdministrators"
            ],
```

```
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "organizations:ServicePrincipal": [
                        "securityhub.amazonaws.com"
                    ]
                }
            }
        }
    ]
}
```

Pembaruan Security Hub ke kebijakan AWS terkelola

Lihat detail tentang pembaruan kebijakan AWS terkelola untuk Security Hub sejak layanan ini mulai melacak perubahan ini. Untuk peringatan otomatis tentang perubahan pada halaman ini, berlangganan umpan RSS di halaman riwayat Dokumen Security Hub.

Perubahan	Deskripsi	Tanggal
AWSSecurityHubFullAccess— Perbarui ke kebijakan yang ada	Security Hub memperbarui kebijakan untuk mendapatk an detail harga Layanan AWS dan produk.	April 24, 2024
AWSSecurityHubRead OnlyAccess— Perbarui ke kebijakan yang ada	Security Hub memperbarui kebijakan terkelola ini dengan menambahkan `Sid` bidang.	Februari 22, 2024
AWSSecurityHubFullAccess— Perbarui ke kebijakan yang ada	Security Hub memperbarui kebijakan sehingga dapat menentukan apakah Amazon GuardDuty dan Amazon Inspector diaktifkan di akun. Ini membantu pelanggan menyatukan informasi terkait	16 November 2023

Perubahan	Deskripsi	Tanggal
	keamanan dari beberapa. Layanan AWS	
AWSSecurityHubOrganizationsAccess— Perbarui ke kebijakan yang ada	Security Hub memperbarui kebijakan untuk memberikan izin tambahan guna mengizinkan akses hanya-baca ke fungsionalitas administrator yang AWS Organizations didelegasikan. Ini termasuk detail seperti root, unit organisasi (OU), akun, struktur organisasi, dan akses layanan.	16 November 2023
AWSSecurityHubServiceRolePolicy – Pembaruan ke kebijakan yang ada	Security Hub menambahkan `BatchGetSecurityControls` ,`DisassociateFromAdministratorAccount` , dan `UpdateSecurityControl` izin untuk membaca dan memperbarui properti kontrol keamanan yang dapat disesuaikan.	26 November 2023
AWSSecurityHubServiceRolePolicy – Pembaruan ke kebijakan yang ada	Security Hub menambahkan `tag:GetResources` izin untuk membaca tag sumber daya yang terkait dengan temuan.	7 November 2023

Perubahan	Deskripsi	Tanggal
AWSSecurityHubServiceRolePolicy – Pembaruan ke kebijakan yang ada	Security Hub menambahkan `BatchGetStandardsControlAssociations` izin untuk mendapatkan informasi tentang status pemberdayaan kontrol dalam standar.	27 September 2023
AWSSecurityHubServiceRolePolicy – Pembaruan ke kebijakan yang ada	Security Hub menambahkan izin baru untuk mendapatkan AWS Organizations data dan membaca serta memperbarui konfigurasi Security Hub, termasuk standar dan kontrol.	20 September 2023
AWSSecurityHubServiceRolePolicy – Pembaruan ke kebijakan yang ada	Security Hub memindahkan `config:DescribeConfigRuleEvaluationStatus` izin yang ada ke pernyataan lain dalam kebijakan. `config:DescribeConfigRuleEvaluationStatus` Izin sekarang diterapkan ke semua sumber daya.	Maret 17, 2023
AWSSecurityHubServiceRolePolicy – Pembaruan ke kebijakan yang ada	Security Hub memindahkan `config:PutEvaluations` izin yang ada ke pernyataan lain dalam kebijakan. `config:PutEvaluations` Izin sekarang diterapkan ke semua sumber daya.	14 Juli 2021

Perubahan	Deskripsi	Tanggal
AWSSecurityHubServiceRolePolicy – Pembaruan ke kebijakan yang ada	Security Hub menambahkan izin baru untuk memungkinkan peran terkait layanan memberikan hasil evaluasi. AWS Config	29 Juni 2021
AWSSecurityHubServiceRolePolicy— Ditambahkan ke daftar kebijakan terkelola	Menambahkan informasi tentang kebijakan terkelola AWSSecurityHubServiceRolePolicy, yang digunakan oleh peran terkait layanan Security Hub.	11 Juni 2021
AWSSecurityHubOrganizationsAccess— Kebijakan baru	Security Hub menambahkan kebijakan baru yang memberikan izin yang diperlukan untuk integrasi Security Hub dengan Organizations.	15 Maret 2021
Security Hub mulai melacak perubahan	Security Hub mulai melacak perubahan untuk kebijakan AWS terkelolanya.	15 Maret 2021

Memecahkan masalah AWS Security Hub identitas dan akses

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

Topik

- Saya tidak berwenang untuk melakukan tindakan di Security Hub
- Saya tidak berwenang untuk melakukan iam: PassRole
- Saya ingin akses terprogram ke Security Hub
- Saya seorang administrator dan ingin mengizinkan orang lain mengakses Security Hub

- Saya ingin mengizinkan orang di luar saya Akun AWS untuk mengakses sumber daya Security Hub saya

Saya tidak berwenang untuk melakukan tindakan di Security Hub

Jika AWS Management Console memberitahu Anda bahwa Anda tidak berwenang untuk melakukan tindakan, maka Anda harus menghubungi administrator Anda untuk bantuan. Administrator Anda adalah orang yang memberi Anda kredensial masuk.

Contoh kesalahan berikut terjadi ketika pengguna `mateojackson` mencoba menggunakan konsol untuk melihat detail tentang *`widget`* tetapi tidak memiliki `securityhub:`*`GetWidget`* izin.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 securityhub:GetWidget on resource: my-example-widget
```

Dalam hal ini, Mateo meminta administratornya untuk memperbarui kebijakannya untuk mengizinkan dia mengakses sumber daya *`my-example-widget`* menggunakan tindakan `securityhub:`*`GetWidget`*.

Saya tidak berwenang untuk melakukan iam: PassRole

Jika Anda menerima kesalahan yang tidak diizinkan untuk melakukan `iam:PassRole` tindakan, kebijakan Anda harus diperbarui agar Anda dapat meneruskan peran ke Security Hub.

Beberapa Layanan AWS memungkinkan Anda untuk meneruskan peran yang ada ke layanan tersebut alih-alih membuat peran layanan baru atau peran terkait layanan. Untuk melakukannya, Anda harus memiliki izin untuk meneruskan peran ke layanan.

Contoh kesalahan berikut terjadi ketika pengguna IAM bernama `marymajor` mencoba menggunakan konsol untuk melakukan tindakan di Security Hub. Namun, tindakan tersebut memerlukan layanan untuk mendapatkan izin yang diberikan oleh peran layanan. Mary tidak memiliki izin untuk meneruskan peran tersebut pada layanan.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

Dalam kasus ini, kebijakan Mary harus diperbarui agar dia mendapatkan izin untuk melakukan tindakan `iam:PassRole` tersebut.

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

Saya ingin akses terprogram ke Security Hub

Pengguna membutuhkan akses terprogram jika mereka ingin berinteraksi dengan AWS luar. AWS Management Console Cara untuk memberikan akses terprogram tergantung pada jenis pengguna yang mengakses AWS.

Untuk memberi pengguna akses programatis, pilih salah satu opsi berikut.

Pengguna mana yang membutuhkan akses programatis?	Untuk	Oleh
Identitas tenaga kerja (Pengguna yang dikelola di Pusat Identitas IAM)	Gunakan kredenal sementara untuk menandatangani permintaan terprogram ke AWS CLI, AWS SDK, atau API. AWS	Mengikuti petunjuk untuk antarmuka yang ingin Anda gunakan. • Untuk AWS CLI, lihat Mengkonfigurasi yang akan AWS CLI digunakan AWS IAM Identity Center dalam Panduan AWS Command Line Interface Pengguna. • Untuk AWS SDK, alat, dan AWS API, lihat autentikasi Pusat Identitas IAM di Panduan Referensi AWS SDK dan Alat.
IAM	Gunakan kredenal sementara untuk menandatangani permintaan terprogram ke AWS CLI, AWS SDK, atau API. AWS	Mengikuti petunjuk dalam Menggunakan kredensi sementara dengan AWS sumber daya di Panduan Pengguna IAM.

Pengguna mana yang membutuhkan akses programatis?	Untuk	Oleh
IAM	(Tidak direkomendasikan) Gunakan kredenal jangka panjang untuk menandata ngani permintaan terprogram ke AWS CLI, AWS SDK, atau API. AWS	Mengikuti petunjuk untuk antarmuka yang ingin Anda gunakan. • Untuk mengetahui AWS CLI, lihat Mengautentikasi menggunakan kredensi pengguna IAM di Panduan Pengguna.AWS Command Line Interface • Untuk AWS SDK dan alat bantu, lihat Mengautentikasi menggunakan kredensi jangka panjang di Panduan Referensi AWS SDK dan Alat. • Untuk AWS API, lihat Mengelola kunci akses untuk pengguna IAM di Panduan Pengguna IAM.

Saya seorang administrator dan ingin mengizinkan orang lain mengakses Security Hub

Untuk memberikan akses, menambahkan izin ke pengguna, grup, atau peran Anda:

- Pengguna dan grup di AWS IAM Identity Center:

  Buat rangkaian izin. Ikuti instruksi di Buat rangkaian izin di Panduan Pengguna AWS IAM Identity Center .
- Pengguna yang dikelola di IAM melalui penyedia identitas:

  Buat peran untuk federasi identitas. Ikuti instruksi dalam Membuat peran untuk penyedia identitas pihak ketiga (federasi) di Panduan Pengguna IAM.

- Pengguna IAM:
  - Buat peran yang dapat diambil pengguna Anda. Ikuti instruksi dalam Membuat peran untuk pengguna IAM dalam Panduan Pengguna IAM.
  - (Tidak disarankan) Pasang kebijakan langsung ke pengguna atau tambahkan pengguna ke grup pengguna. Ikuti instruksi dalam Menambahkan izin ke pengguna (konsol) dalam Panduan Pengguna IAM.

Saya ingin mengizinkan orang di luar saya Akun AWS untuk mengakses sumber daya Security Hub saya

Anda dapat membuat peran yang dapat digunakan pengguna di akun lain atau orang-orang di luar organisasi Anda untuk mengakses sumber daya Anda. Anda dapat menentukan siapa saja yang dipercaya untuk mengambil peran tersebut. Untuk layanan yang mendukung kebijakan berbasis sumber daya atau daftar kontrol akses (ACL), Anda dapat menggunakan kebijakan tersebut untuk memberi orang akses ke sumber daya Anda.

Untuk mempelajari selengkapnya, periksa referensi berikut:

- Untuk mengetahui apakah Security Hub mendukung fitur ini, lihatBagaimana AWS Security Hub bekerja dengan IAM.
- Untuk mempelajari cara menyediakan akses ke sumber daya Anda di seluruh sumber daya Akun AWS yang Anda miliki, lihat Menyediakan akses ke pengguna IAM di pengguna lain Akun AWS yang Anda miliki di Panduan Pengguna IAM.
- Untuk mempelajari cara menyediakan akses ke sumber daya Anda kepada pihak ketiga Akun AWS, lihat Menyediakan akses yang Akun AWS dimiliki oleh pihak ketiga dalam Panduan Pengguna IAM.
- Untuk mempelajari cara memberikan akses melalui federasi identitas, lihat Menyediakan akses ke pengguna terautentikasi eksternal (federasi identitas) dalam Panduan Pengguna IAM.
- Untuk mempelajari perbedaan antara menggunakan peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat Akses sumber daya lintas akun di IAM di Panduan Pengguna IAM.

Validasi kepatuhan untuk AWS Security Hub

Auditor pihak ketiga melakukan penilaian pada keamanan dan kepatuhan AWS Security Hub sebagai bagian dari beberapa program kepatuhan AWS. Mencakup SOC, PCI, FedRAMP, HIPAA, dan lainnya.

Untuk daftar layanan AWS dalam cakupan program kepatuhan spesifik, lihat Layanan AWS dalam Cakupan berdasarkan Program Kepatuhan. Untuk informasi umum, lihat AWS Program Kepatuhan.

Anda bisa mengunduh laporan audit pihak ke tiga menggunakan AWS Artifact. Untuk informasi selengkapnya, lihat Mengunduh Laporan di AWS Artifact.

Tanggung jawab kepatuhan Anda saat menggunakan Security Hub ditentukan oleh sensitivitas data Anda, tujuan kepatuhan perusahaan Anda, serta undang-undang dan peraturan yang berlaku. AWSmenyediakan sumber daya berikut untuk membantu kepatuhan:

- Panduan Quick Start Keamanan dan Kepatuhan – Panduan deployment ini membahas pertimbangan arsitektur dan memberikan langkah untuk menerapkan lingkungan dasar yang berfokus pada keamanan dan kepatuhan di AWS.
- Sumber Daya Kepatuhan AWS – Kumpulan buku kerja dan panduan ini mungkin berlaku untuk industri dan lokasi Anda.
- AWS Config – Layanan AWS ini menilai seberapa baik konfigurasi sumber daya Anda mematuhi praktik internal, pedoman industri, dan peraturan.
- AWS Security Hub – Layanan AWS ini akan menyediakan tampilan komprehensif dari status keamanan Anda dalam AWS yang akan membantu Anda memeriksa kepatuhan Anda terhadap standar dan praktik terbaik industri.

Ketahanan di Security Hub AWS

Infrastruktur AWS global dibangun di sekitar Wilayah AWS dan Availability Zones. Wilayah memberikan beberapa Zona Ketersediaan yang terpisah dan terisolasi secara fisik, yang terkoneksi melalui jaringan latensi rendah, throughput tinggi, dan sangat redundan. Dengan Zona Ketersediaan, Anda dapat merancang serta mengoperasikan aplikasi dan basis data yang secara otomatis melakukan fail over di antara zona tanpa gangguan. Availability Zone memiliki ketersediaan yang lebih baik, toleran terhadap kegagalan, dan dapat diukur skalanya jika dibandingkan dengan satu atau beberapa infrastruktur pusat data tradisional.

Untuk informasi selengkapnya tentang Wilayah AWS dan Availability Zone, lihat Infrastruktur Global AWS.

Keamanan infrastruktur dalam AWS Security Hub

Sebagai layanan terkelola, AWS Security Hub dilindungi oleh keamanan jaringan AWS global. Untuk informasi tentang layanan keamanan AWS dan cara AWS melindungi infrastruktur, lihat Keamanan Cloud AWS. Guna mendesain lingkungan AWS Anda menggunakan praktik terbaik untuk keamanan infrastruktur, lihat Perlindungan Infrastruktur dalam Kerangka Kerja AWS Well-Architected Pilar Keamanan.

Anda menggunakan panggilan API yang AWS dipublikasikan untuk mengakses Security Hub melalui jaringan. Klien harus mendukung hal-hal berikut:

- Keamanan Lapisan Pengangkutan (TLS). Kami membutuhkan TLS 1.2 dan merekomendasikan TLS 1.3.
- Cipher cocok dengan perfect forward secrecy (PFS) seperti DHE (Ephemeral Diffie-Hellman) atau ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Sebagian besar sistem modern seperti Java 7 dan sistem yang lebih baru mendukung mode ini.

Selain itu, permintaan harus ditandatangani menggunakan ID kunci akses dan kunci akses rahasia yang terkait dengan pengguna utama IAM. Atau Anda bisa menggunakan AWS Security Token Service (AWS STS) untuk membuat kredensial keamanan sementara guna menandatangani permintaan.

AWS Security Hub dan titik akhir VPC antarmuka (AWS PrivateLink)

Anda dapat membangun hubungan privat antara VPC Anda dan AWS Security Hub dengan membuat VPC endpoint antarmuka. Endpoint antarmuka didukung oleh AWS PrivateLink, teknologi yang memungkinkan Anda mengakses API Hub Keamanan secara pribadi tanpa gateway internet, perangkat NAT, koneksi VPN, atau koneksi AWS Direct Connect. Instans di VPC Anda tidak memerlukan alamat IP publik untuk berkomunikasi dengan API Hub Keamanan. Lalu lintas antara VPC dan Hub Keamanan Anda tidak meninggalkan jaringan Amazon.

Setiap titik akhir antarmuka diwakili oleh satu atau beberapa Antarmuka Jaringan Elastis di subnet Anda.

Untuk informasi selengkapnya, lihat Endpoint (AWS PrivateLink) Interface VPC di Panduan. AWS PrivateLink

Pertimbangan untuk titik akhir VPC Hub Keamanan

Sebelum menyiapkan endpoint VPC antarmuka untuk Hub Keamanan, pastikan Anda meninjau properti endpoint antarmuka dan batasan dalam Panduan. AWS PrivateLink

Security Hub mendukung melakukan panggilan ke semua tindakan API-nya dari VPC Anda.

> **Note**
>
> Security Hub tidak mendukung titik akhir VPC di Wilayah Asia Pasifik (Osaka).

Membuat endpoint VPC antarmuka untuk Hub Keamanan

Anda dapat membuat titik akhir VPC untuk layanan Hub Keamanan menggunakan konsol Amazon VPC atau (). AWS Command Line Interface AWS CLI Untuk informasi selengkapnya, lihat Membuat titik akhir antarmuka di AWS PrivateLinkPanduan.

Buat endpoint VPC untuk Hub Keamanan menggunakan nama layanan berikut:

- com.amazonaw. *wilayah.securityhub*

Jika Anda mengaktifkan DNS pribadi untuk titik akhir, Anda dapat membuat permintaan API ke Hub Keamanan menggunakan nama DNS default untuk Wilayah, misalnya,. `securityhub.us-east-1.amazonaws.com`

Untuk informasi selengkapnya, lihat Mengakses layanan melalui titik akhir antarmuka di AWS PrivateLinkPanduan.

Membuat kebijakan endpoint VPC untuk Hub Keamanan

Anda dapat melampirkan kebijakan endpoint ke endpoint VPC Anda yang mengontrol akses ke Hub Keamanan. Kebijakan menentukan informasi berikut ini:

- Prinsip-prinsip yang dapat melakukan tindakan.
- Tindakan yang dapat dilakukan.
- Sumber daya yang dapat digunakan untuk mengambil tindakan.

Untuk informasi selengkapnya, lihat Mengontrol akses ke layanan dengan titik akhir VPC di AWS PrivateLink Panduan.

Contoh: Kebijakan endpoint VPC untuk tindakan Hub Keamanan

Berikut ini adalah contoh kebijakan endpoint untuk Security Hub. Saat dilampirkan ke titik akhir, kebijakan ini memberikan akses ke tindakan Hub Keamanan yang terdaftar untuk semua prinsipal di semua sumber daya.

```
{
   "Statement":[
      {
         "Principal":"*",
         "Effect":"Allow",
         "Action":[
            "securityhub:getFindings",
            "securityhub:getEnabledStandards",
            "securityhub:getInsights"
         ],
         "Resource":"*"
      }
   ]
}
```

Subnet bersama

Anda tidak dapat membuat, menjelaskan, 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 Berbagi VPC Anda dengan akun lain di Panduan Pengguna Amazon VPC.

Mencatat panggilan API AWS Security Hub dengan AWS CloudTrail

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

Untuk mempelajari selengkapnya CloudTrail, termasuk cara mengonfigurasi dan mengaktifkannya, lihat Panduan AWS CloudTrail Pengguna.

Informasi Security Hub di CloudTrail

CloudTrail diaktifkan pada Akun AWS saat Anda membuat akun. Ketika aktivitas peristiwa yang didukung terjadi di Security Hub, aktivitas tersebut direkam dalam suatu CloudTrail peristiwa bersama dengan peristiwa AWS layanan lainnya dalam riwayat Acara. Anda dapat melihat, mencari, dan mengunduh peristiwa terbaru di akun . Untuk informasi selengkapnya, lihat Melihat peristiwa dengan riwayat CloudTrail acara.

Untuk catatan peristiwa yang sedang berlangsung di akun Anda, termasuk acara untuk Security Hub, buat jejak. Jejak memungkinkan CloudTrail untuk mengirimkan file log ke bucket Amazon S3. Secara default, ketika Anda membuat jejak di konsol, jejak akan diterapkan ke semua Wilayah AWS. Jejak mencatat peristiwa dari semua Wilayah di partisi AWS dan mengirimkan file log ke bucket Amazon S3 yang Anda tentukan. Selain itu, Anda dapat mengonfigurasi AWS layanan lain untuk menganalisis lebih lanjut dan menindaklanjuti data peristiwa yang dikumpulkan dalam CloudTrail log. Untuk informasi selengkapnya, lihat berikut:

- Gambaran umum untuk membuat jejak
- CloudTrail layanan dan integrasi yang didukung
- Mengonfigurasi notifikasi Amazon SNS untuk CloudTrail

- Menerima file CloudTrail log dari beberapa wilayah dan Menerima file CloudTrail log dari beberapa akun

Security Hub mendukung pencatatan semua tindakan Security Hub API sebagai peristiwa dalam CloudTrail log. Untuk melihat daftar operasi Security Hub, lihat Referensi API Security Hub.

Saat aktivitas untuk tindakan berikut dicatat CloudTrail, nilai untuk `responseElements` disetel ke`null`. Ini memastikan bahwa informasi sensitif tidak disertakan dalam CloudTrail log.

- `BatchImportFindings`
- `GetFindings`
- `GetInsights`
- `GetMembers`
- `UpdateFindings`

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

- Jika permintaan tersebut dibuat dengan kredensial pengguna root atau AWS Identity and Access Management (IAM)
- Jika permintaan tersebut dibuat dengan kredensial keamanan sementara untuk peran atau pengguna gabungan
- Jika permintaan tersebut dibuat oleh layanan AWS lainnya

Untuk informasi selengkapnya, lihat Elemen userIdentity CloudTrail .

Contoh: Entri file log Security Hub

Trail adalah konfigurasi yang memungkinkan pengiriman peristiwa sebagai file log ke bucket Amazon S3 yang Anda tentukan. CloudTrail file log berisi satu atau lebih entri log. Peristiwa mewakili permintaan tunggal dari sumber manapun dan mencakup informasi tentang tindakan yang diminta, tanggal dan waktu tindakan, parameter permintaan, dan sebagainya. CloudTrail file log bukanlah jejak tumpukan yang diurutkan dari panggilan API publik, jadi file tersebut tidak muncul dalam urutan tertentu.

Contoh berikut menunjukkan entri CloudTrail log yang menunjukkan `CreateInsight` tindakan. Dalam contoh ini, wawasan yang `Test Insight` disebut dibuat. `ResourceId`Atribut ditetapkan sebagai Grup menurut agregator, dan tidak ada filter opsional untuk wawasan ini yang ditentukan. Untuk informasi selengkapnya tentang wawasan, lihat Wawasan di AWS Security Hub.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAJK6U5DS22IAVUI7BW",
        "arn": "arn:aws:iam::012345678901:user/TestUser",
        "accountId": "012345678901",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "TestUser"
    },
    "eventTime": "2018-11-25T01:02:18Z",
    "eventSource": "securityhub.amazonaws.com",
    "eventName": "CreateInsight",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "205.251.233.179",
    "userAgent": "aws-cli/1.11.76 Python/2.7.10 Darwin/17.7.0 botocore/1.5.39",
    "requestParameters": {
        "Filters": {},
        "ResultField": "ResourceId",
        "Name": "Test Insight"
    },
    "responseElements": {
        "InsightArn": "arn:aws:securityhub:us-west-2:0123456789010:insight/custom/
f4c4890b-ac6b-4c26-95f9-e62cc46f3055"
    },
    "requestID": "c0fffccd-f04d-11e8-93fc-ddcd14710066",
    "eventID": "3dabcebf-35b0-443f-a1a2-26e186ce23bf",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "recipientAccountId": "012345678901"
}
```

Menandai sumber daya AWS Security Hub

Tag adalah label opsional yang dapat Anda tentukan dan tetapkan ke AWS sumber daya, termasuk jenis sumber daya AWS Security Hub tertentu. Tag dapat membantu Anda mengidentifikasi, mengkategorikan, dan mengelola sumber daya dengan cara yang berbeda, seperti berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Misalnya, Anda dapat menggunakan tag untuk membedakan sumber daya, mengidentifikasi sumber daya yang mendukung persyaratan kepatuhan atau alur kerja tertentu, atau mengalokasikan biaya.

Anda dapat menetapkan tag ke jenis sumber daya Security Hub berikut: aturan otomatisasi, kebijakan konfigurasi, dan Hub sumber daya.

Topik

Menandai dasar-dasar

Sumber daya dapat memiliki sebanyak 50 tag. Setiap tag terdiri dari kunci tag yang diperlukan dan nilai tag opsional, yang keduanya Anda tentukan. Kunci tag adalah label umum yang bertindak sebagai kategori untuk nilai tag yang lebih spesifik. Nilai tag bertindak sebagai deskriptor untuk kunci tag.

Misalnya, jika Anda membuat aturan otomatisasi yang berbeda untuk lingkungan yang berbeda (satu set aturan otomatisasi untuk akun pengujian dan satu lagi untuk akun produksi), Anda dapat menetapkan kunci `Environment` tag untuk aturan tersebut. Nilai tag terkait mungkin `Test` untuk aturan yang terkait dengan akun pengujian, dan `Prod` untuk aturan yang terkait dengan akun produksi dan OU.

Saat Anda menentukan dan menetapkan tag ke sumber daya AWS Security Hub, ingatlah hal berikut:

- Setiap sumber daya dapat memiliki maksimum 50 tag.

- Untuk setiap sumber daya, setiap kunci tag harus unik dan hanya dapat memiliki satu nilai tag.
- Kunci dan nilai tag peka huruf besar dan kecil. Sebagai praktik terbaik, kami menyarankan Anda menentukan strategi untuk memanfaatkan tag dan menerapkan strategi itu secara konsisten di seluruh sumber daya Anda.
- Tombol tag dapat memiliki maksimal 128 karakter UTF-8. Nilai tag dapat memiliki maksimal 256 karakter UTF-8. Karakter dapat berupa huruf, angka, spasi, atau simbol berikut: _.:/= + - @
- `aws:`Awalan dicadangkan untuk digunakan olehAWS. Anda tidak dapat menggunakannya dalam kunci tag atau nilai apa pun yang Anda tentukan. Selain itu, Anda tidak dapat mengubah atau menghapus kunci tag atau nilai yang menggunakan awalan ini. Tag yang menggunakan awalan ini tidak dihitung terhadap kuota 50 tag per sumber daya.
- Setiap tag yang Anda tetapkan hanya tersedia untuk Anda Akun AWS dan hanya Wilayah AWS di mana Anda menetapkannya.
- Jika Anda menetapkan tag ke sumber daya menggunakan Security Hub, tag hanya akan diterapkan ke sumber daya yang disimpan langsung di Security Hub di yang berlakuWilayah AWS. Mereka tidak diterapkan pada sumber daya pendukung terkait yang dibuat, digunakan, atau dikelola oleh Security Hub untuk Anda di tempat lainLayanan AWS. Misalnya, jika Anda menetapkan tag ke aturan otomatisasi yang memperbarui temuan yang terkait dengan Amazon Simple Storage Service (Amazon S3), tag hanya diterapkan ke aturan otomatisasi di Security Hub untuk Wilayah yang ditentukan. Mereka tidak diterapkan ke ember S3 Anda. Untuk juga menetapkan tag ke sumber daya terkait, Anda dapat menggunakan AWS Resource Groups atau Layanan AWS yang menyimpan sumber daya—misalnya, Amazon S3 untuk bucket S3. Menetapkan tag ke sumber daya terkait dapat membantu Anda mengidentifikasi sumber daya pendukung untuk sumber daya Security Hub Anda.
- Jika Anda menghapus sumber daya, tag apa pun yang ditetapkan ke sumber daya juga akan dihapus.

> **Important**
>
> Jangan menyimpan rahasia atau jenis data sensitif lainnya dalam tag. Tag dapat diakses dari banyak orangLayanan AWS, termasukAWS Billing and Cost Management. Mereka tidak dimaksudkan untuk digunakan untuk data sensitif.

Untuk menambahkan dan mengelola tag untuk sumber daya Security Hub, Anda dapat menggunakan konsol Security Hub, Security Hub API, atau API AWS Resource Groups Tagging.

Dengan Security Hub, Anda dapat menambahkan tag ke sumber daya saat membuat sumber daya. Anda juga dapat menambahkan dan mengelola tag untuk sumber daya individual yang ada. Dengan Resource Groups, Anda dapat menambahkan dan mengelola tag secara massal untuk beberapa sumber daya yang ada yang mencakup beberapaLayanan AWS, termasuk Security Hub.

Untuk tips penandaan tambahan dan praktik terbaik, lihat Menandai AWS sumber daya Anda di Panduan Pengguna Tagging AWS Resources.

Menggunakan tag dalam kebijakan IAM

Setelah Anda mulai menandai sumber daya, Anda dapat menentukan izin tingkat sumber daya berbasis tag dalam kebijakan (IAM). AWS Identity and Access Management Dengan menggunakan tag dengan cara ini, Anda dapat menerapkan kontrol terperinci tentang pengguna dan peran mana yang Akun AWS memiliki izin untuk membuat dan menandai sumber daya, dan pengguna dan peran mana yang memiliki izin untuk menambahkan, mengedit, dan menghapus tag secara lebih umum. Untuk mengontrol akses berdasarkan tag, Anda dapat menggunakan kunci kondisi terkait tag di elemen Kondisi kebijakan IAM.

Misalnya, Anda dapat membuat kebijakan IAM yang memungkinkan pengguna memiliki akses penuh ke semua sumber daya AWS Security Hub, jika `Owner` tag untuk sumber daya menentukan nama pengguna mereka:

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "ModifyResourceIfOwner",
            "Effect": "Allow",
            "Action": "securityhub:*",
            "Resource": "*",
            "Condition": {
                "StringEqualsIgnoreCase": {"aws:ResourceTag/Owner": "${aws:username}"}
            }
        }
    ]
}
```

Jika Anda menentukan izin tingkat sumber daya berbasis tag, izin akan segera berlaku. Ini berarti bahwa sumber daya Anda lebih aman segera setelah dibuat, dan Anda dapat dengan cepat mulai

menerapkan penggunaan tag untuk sumber daya baru. Anda juga dapat menggunakan izin tingkat sumber daya untuk mengontrol kunci dan nilai tag mana yang dapat dikaitkan dengan sumber daya baru dan yang sudah ada. Untuk informasi selengkapnya, lihat Mengontrol akses ke AWS sumber daya menggunakan tag di Panduan Pengguna IAM.

Menambahkan tag ke sumber daya AWS Security Hub

Untuk menambahkan tag ke sumber daya AWS Security Hub individual, Anda dapat menggunakan konsol Security Hub atau Security Hub API. Konsol tidak mendukung penambahan tag ke Hub sumber daya.

Untuk menambahkan tag ke beberapa sumber daya Security Hub secara bersamaan, gunakan operasi penandaan API AWS Resource GroupsPenandaan.

> **Important**
>
> Menambahkan tag ke sumber daya dapat memengaruhi akses ke sumber daya. Sebelum menambahkan tag ke sumber daya, tinjau kebijakan AWS Identity and Access Management (IAM) apa pun yang mungkin menggunakan tag untuk mengontrol akses ke sumber daya.

Console

Untuk menambahkan tag ke sumber daya

Saat Anda membuat aturan otomatisasi atau kebijakan konfigurasi, konsol Security Hub menyediakan opsi untuk menambahkan tag ke dalamnya. Anda dapat memberikan kunci tag dan nilai tag di bagian Tag.

Security Hub API & AWS CLI

Untuk menambahkan tag ke sumber daya

Untuk membuat sumber daya dan menambahkan satu atau beberapa tag ke dalamnya secara terprogram, gunakan operasi yang sesuai untuk jenis sumber daya yang ingin Anda buat:

- Untuk membuat kebijakan konfigurasi dan menambahkan satu atau beberapa tag ke dalamnya, panggil CreateConfigurationPolicyAPI atau, jika Anda menggunakanAWS CLI, jalankan create-configuration-policyperintah.

- Untuk membuat aturan otomatisasi dan menambahkan satu atau beberapa tag ke dalamnya, panggil CreateAutomationRuleAPI atau, jika Anda menggunakanAWS CLI, jalankan create-automation-ruleperintah.
- Untuk mengaktifkan Security Hub dan menambahkan satu atau beberapa tag ke Hub sumber daya Anda, jalankan EnableSecurityHubAPI atau, jika Anda menggunakan AWS Command Line Interface (AWS CLI), jalankan enable-security-hubperintah.

Dalam permintaan Anda, gunakan `tags` parameter untuk menentukan kunci tag dan nilai tag opsional untuk setiap tag untuk ditambahkan ke sumber daya. `tags`Parameter menentukan array objek. Setiap objek menentukan kunci tag dan nilai tag terkait.

Untuk menambahkan satu atau beberapa tag ke sumber daya yang ada, gunakan TagResourcepengoperasian Security Hub API atau, jika Anda menggunakanAWS CLI, jalankan perintah tag-resource. Dalam permintaan Anda, tentukan Nama Sumber Daya Amazon (ARN) dari sumber daya yang ingin Anda tambahkan tag. Gunakan `tags` parameter untuk menentukan kunci tag (`key`) dan nilai tag opsional (`value`) untuk setiap tag yang akan ditambahkan. `tags`Parameter menentukan array objek, satu objek untuk setiap kunci tag dan nilai tag terkait.

Misalnya, AWS CLI perintah berikut menambahkan kunci `Environment` tag dengan nilai `Prod` tag ke kebijakan konfigurasi yang ditentukan. Contoh ini diformat untuk Linux, macOS, atau Unix, dan menggunakan karakter garis miring terbalik (\) untuk meningkatkan keterbacaan.

Contoh perintah CLI:

```
$ aws securityhub tag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tags key=Environment,value=Prod
```

Di mana:

- `resource-arn`menentukan ARN dari kebijakan konfigurasi untuk menambahkan tag ke.
- *`Environment`*adalah kunci tag tag untuk ditambahkan ke aturan.
- *`Prod`*adalah nilai tag untuk kunci tag tertentu (*`Environment`*).

Dalam contoh berikut, perintah menambahkan beberapa tag ke kebijakan konfigurasi.

```
$ aws securityhub tag-resource \
```

```
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tags key=Environment,value=Prod key=CostCenter,value=12345 key=Owner,value=jane-
doe
```

Untuk setiap objek dalam `tags` array, kedua `value` argumen `key` dan argumen diperlukan. Namun, nilai untuk `value` argumen dapat berupa string kosong. Jika Anda tidak ingin mengaitkan nilai tag dengan kunci tag, jangan tentukan nilai untuk `value` argumen tersebut. Misalnya, perintah berikut menambahkan kunci `Owner` tag tanpa nilai tag terkait:

```
$ aws securityhub tag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tags key=Owner,value=
```

Jika operasi penandaan berhasil, Security Hub mengembalikan respons HTTP 200 kosong. Jika tidak, Security Hub mengembalikan respons HTTP 4 xx atau 500 yang menunjukkan mengapa operasi gagal.

Meninjau tag untuk sumber daya AWS Security Hub

Anda dapat meninjau tag (kunci tag dan nilai tag) untuk aturan otomatisasi Security Hub atau kebijakan konfigurasi menggunakan konsol Security Hub atau Security Hub API. Konsol tidak mendukung tag peninjauan untuk Hub sumber daya.

Untuk meninjau tag untuk beberapa sumber daya Security Hub secara bersamaan, gunakan operasi penandaan API AWS Resource GroupsPenandaan.

Console

Untuk meninjau tag untuk sumber daya

1. Menggunakan kredensi administrator Security Hub, buka konsol AWS Security Hub di https://console.aws.amazon.com/securityhub/.
2. Bergantung pada jenis sumber daya yang ingin Anda tambahkan tag, lakukan salah satu hal berikut:

   - Untuk meninjau tag untuk aturan otomatisasi, pilih Otomatisasi di panel navigasi. Kemudian, pilih aturan otomatisasi.

- Untuk meninjau tag untuk kebijakan konfigurasi, pilih Konfigurasi di panel navigasi. Kemudian, pada tab Kebijakan, pilih opsi di sebelah kebijakan konfigurasi. Panel samping terbuka yang menunjukkan jumlah tag yang ditetapkan ke kebijakan. Anda dapat memperluas header Tag untuk melihat kunci tag dan nilai tag.

Bagian Tag mencantumkan semua tag yang saat ini ditetapkan ke sumber daya.

Security Hub API & AWS CLI

Untuk meninjau tag untuk sumber daya

Untuk mengambil dan meninjau tag untuk sumber daya yang ada, panggil API. ListTagsForResource Dalam permintaan Anda, gunakan `resourceArn` parameter untuk menentukan Nama Sumber Daya Amazon (ARN) sumber daya.

Jika Anda menggunakanAWS CLI, jalankan list-tags-for-resourceperintah dan gunakan `resource-arn` parameter untuk menentukan ARN sumber daya. Sebagai contoh:

```
$ aws securityhub list-tags-for-resource --resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Jika operasi berhasil, Security Hub mengembalikan `tags` array. Setiap objek dalam array menentukan tag (baik kunci tag dan nilai tag) yang saat ini ditetapkan ke sumber daya. Sebagai contoh:

```
{
    "tags": [
        {
            "key": "Environment",
            "value": "Prod"
        },
        {
            "key": "CostCenter",
            "value": "12345"
        },
        {
            "key": "Owner",
            "value": ""
        }
    ]
}
```

Di mana `EnvironmentCostCenter`,, dan `Owner` merupakan kunci tag yang ditetapkan ke sumber daya. `Prod`adalah nilai tag yang terkait dengan kunci `Environment` tag. `12345`adalah nilai tag yang terkait dengan kunci `CostCenter` tag. Kunci `Owner` tag tidak memiliki nilai tag terkait.

Untuk mengambil daftar semua sumber daya Security Hub yang memiliki tag dan semua tag yang ditetapkan ke masing-masing sumber daya tersebut, gunakan GetResourcespengoperasian API AWS Resource Groups Tagging. Dalam permintaan Anda, tetapkan nilai untuk `ResourceTypeFilters` parameter ke`securityhub`. Untuk melakukan ini menggunakanAWS CLI, jalankan perintah get-resources dan atur nilai untuk `resource-type-filters` parameter ke. `securityhub` Sebagai contoh:

```
$ aws resourcegroupstaggingapi get-resources -\-resource-type-filters "securityhub"
```

Jika operasi berhasil, Resource Groups mengembalikan `ResourceTagMappingList` array. Array berisi satu objek untuk setiap sumber daya Security Hub yang memiliki tag. Setiap objek menentukan ARN sumber daya Security Hub, serta kunci tag serta nilai yang ditetapkan ke sumber daya.

Mengedit tag untuk sumber daya AWS Security Hub

Untuk mengedit tag (kunci tag atau nilai tag) untuk sumber daya AWS Security Hub, Anda dapat menggunakan Security Hub API. Konsol Security Hub saat ini tidak mendukung pengeditan tag.

Untuk mengedit tag untuk beberapa sumber daya Security Hub secara bersamaan, gunakan operasi penandaan API AWS Resource GroupsPenandaan.

> **Important**
>
> Mengedit tag untuk sumber daya dapat memengaruhi akses ke sumber daya. Sebelum Anda mengedit kunci tag atau nilai untuk sumber daya, tinjau kebijakan AWS Identity and Access Management (IAM) apa pun yang mungkin menggunakan tag untuk mengontrol akses ke sumber daya.

Security Hub API & AWS CLI

Untuk mengedit tag untuk sumber daya

Saat Anda mengedit tag untuk sumber daya secara terprogram, Anda menimpa tag yang ada dengan nilai baru. Oleh karena itu, cara terbaik untuk mengedit tag tergantung pada apakah Anda ingin mengedit kunci tag, nilai tag, atau keduanya. Untuk mengedit kunci tag, hapus tag saat ini dan tambahkan tag baru.

Untuk mengedit atau menghapus hanya nilai tag yang terkait dengan kunci tag, timpa nilai yang ada dengan menggunakan TagResourcepengoperasian Security Hub API. Jika Anda menggunakanAWS CLI, jalankan perintah tag-resource. Dalam permintaan Anda, tentukan Nama Sumber Daya Amazon (ARN) sumber daya yang nilai tagnya ingin Anda edit atau hapus.

Untuk mengedit nilai tag, gunakan `tags` parameter untuk menentukan kunci tag yang nilai tag yang ingin Anda ubah. Anda juga harus menentukan nilai tag baru untuk kunci tersebut. Misalnya, AWS CLI perintah berikut mengubah nilai tag dari `Prod` menjadi kunci `Test Environment` tag yang ditetapkan ke aturan otomatisasi yang ditentukan. Contoh ini diformat untuk Linux, macOS, atau Unix, dan menggunakan karakter garis miring terbalik (\) untuk meningkatkan keterbacaan.

```
$ aws securityhub tag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tags key=Environment,value=Test
```

Di mana:

- `resource-arn`menentukan ARN dari kebijakan konfigurasi.
- *`Environment`*adalah kunci tag yang terkait dengan nilai tag untuk diubah.
- *`Test`*adalah nilai tag baru untuk kunci tag tertentu (*`Environment`*).

Untuk menghapus nilai tag dari kunci tag, jangan tentukan nilai untuk `value` argumen kunci dalam `tags` parameter. Sebagai contoh:

```
$ aws securityhub tag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tags key=Owner,value=
```

Jika operasi berhasil, Security Hub mengembalikan respons HTTP 200 kosong. Jika tidak, Security Hub mengembalikan respons HTTP 4 xx atau 500 yang menunjukkan mengapa operasi gagal.

Menghapus tag dari sumber daya AWS Security Hub

Untuk menghapus tag dari sumber daya AWS Security Hub, Anda dapat menggunakan Security Hub API. Konsol Security Hub saat ini tidak mendukung penghapusan tag.

Untuk menghapus tag dari beberapa sumber daya Security Hub secara bersamaan, gunakan operasi penandaan API AWS Resource GroupsPenandaan.

> **Important**
>
> Menghapus tag dari sumber daya dapat memengaruhi akses ke sumber daya. Sebelum Anda menghapus tag, tinjau kebijakan AWS Identity and Access Management (IAM) apa pun yang mungkin menggunakan tag untuk mengontrol akses ke sumber daya.

Security Hub API & AWS CLI

Untuk menghapus tag dari sumber daya

Untuk menghapus satu atau beberapa tag dari sumber daya secara terprogram, gunakan UntagResourcepengoperasian Security Hub API. Dalam permintaan Anda, gunakan `resourceArn` parameter untuk menentukan Amazon Resource Name (ARN) sumber daya untuk menghapus tag dari. Gunakan `tagKeys` parameter untuk menentukan kunci tag tag yang akan dihapus. Untuk menghapus beberapa tag, tambahkan `tagKeys` parameter dan argumen untuk setiap tag yang akan dihapus, dipisahkan oleh ampersand (&) —misalnya,. `tagKeys=key1&tagKeys=key2` Untuk menghapus hanya nilai tag tertentu (bukan kunci tag) dari sumber daya, edit tag alih-alih menghapus tag.

Jika Anda menggunakanAWS CLI, jalankan perintah untag-resource untuk menghapus satu atau beberapa tag dari sumber daya. Untuk `resource-arn` parameter, tentukan ARN sumber daya untuk menghapus tag dari. Gunakan `tag-keys` parameter untuk menentukan kunci tag tag yang akan dihapus. Misalnya, perintah berikut menghapus `Environment` tag (kunci tag dan nilai tag) dari kebijakan konfigurasi yang ditentukan:

```
$ aws securityhub untag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tag-keys Environment
```

Di mana `resource-arn` menentukan ARN dari kebijakan konfigurasi untuk menghapus tag dari, *`Environment`* dan merupakan kunci tag tag untuk dihapus.

Untuk menghapus beberapa tag dari sumber daya, tambahkan setiap kunci tag tambahan sebagai argumen untuk `tag-keys` parameter. Sebagai contoh:

```
$ aws securityhub untag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tag-keys Environment Owner
```

Jika operasi berhasil, Security Hub mengembalikan respons HTTP 200 kosong. Jika tidak, Security Hub mengembalikan respons HTTP 4 xx atau 500 yang menunjukkan mengapa operasi gagal.

Kuota Security Hub

Akun Akun AWS Anda memiliki kuota default, yang sebelumnya disebut sebagai batasan, untuk setiap layanan Layanan AWS. Kuota ini merupakan jumlah maksimum layanan sumber daya atau operasi untuk akun Anda. Topik ini menautkan ke kuota yang berlaku untuk sumber daya dan operasi AWS Security Hub untuk akun Anda. Kecuali sebaliknya dinyatakan lain, setiap kuota berlaku untuk akun Anda di setiap Wilayah AWS.

Beberapa kuota dapat ditingkatkan, sementara yang lain tidak bisa. Untuk meminta peningkatan kuota, gunakan konsol Service Quotas. Untuk mempelajari selengkapnya cara menyampaikan permintaan kenaikan kuota, lihat Meminta kenaikan kuota dalam Panduan Pengguna Service Quotas. Jika kuota tidak tersedia di konsol Service Quotas, gunakan formulir peningkatan batas layanan untuk meminta kenaikan kuota. AWS Support Center Console

Kuota maksimum

Untuk daftar kuota yang berlaku untuk sumber daya Security Hub, lihat titik akhir dan kuota AWS Security Hub di. Referensi Umum AWS

Nilai kuota

Untuk daftar kuota yang berlaku untuk operasi Security Hub API, lihat Referensi API AWS Security Hub.

Jika Anda telah menyiapkanAgregasi Lintas Wilayah, satu panggilan ke `BatchImportFindings` dan `BatchUpdateFindings` memengaruhi Wilayah yang ditautkan dan Wilayah agregasi. `GetFindings`Operasi mengambil temuan dari Wilayah terkait dan Wilayah agregasi. Namun, `BatchEnableStandards` dan `UpdateStandardsControl` operasinya spesifik Wilayah.

Batas Regional Security Hub

Beberapa fitur AWS Security Hub hanya tersedia dalam beberapa hal Wilayah AWS. Bagian berikut menentukan batas Regional ini.

Untuk daftar Wilayah di mana Security Hub tersedia, lihat titik akhir dan kuota AWS Security Hub di. Referensi Umum AWS

Pembatasan agregasi Lintas Wilayah

Di AWS GovCloud (US), agregasi lintas wilayah tersedia untuk temuan, menemukan pembaruan, dan wawasan hanya di seluruh wilayah. AWS GovCloud (US) Secara khusus, Anda hanya dapat mengumpulkan temuan, menemukan pembaruan, dan wawasan antara AWS GovCloud (AS-Timur) dan AWS GovCloud (AS-Barat).

Di Wilayah China, agregasi lintas wilayah tersedia untuk temuan, menemukan pembaruan, dan wawasan di seluruh Wilayah China saja. Secara khusus, Anda hanya dapat mengumpulkan temuan, menemukan pembaruan, dan wawasan antara China (Beijing) dan China (Ningxia).

Anda tidak dapat menggunakan Wilayah yang dinonaktifkan secara default sebagai Wilayah agregasi Anda. Untuk daftar Wilayah yang dinonaktifkan secara default, lihat Mengaktifkan Wilayah di. Referensi Umum AWS

Ketersediaan integrasi menurut Wilayah

Beberapa integrasi tidak tersedia di semua Wilayah. Jika integrasi tidak tersedia di Wilayah tertentu, integrasi tidak tercantum di halaman Integrasi konsol Security Hub saat Anda memilih Wilayah tersebut.

Integrasi yang didukung di China (Beijing) dan China (Ningxia)

Wilayah China (Beijing) dan China (Ningxia) hanya mendukung integrasi berikut dengan AWS layanan:

- AWS Firewall Manager
- Amazon GuardDuty
- AWS Identity and Access Management Access Analyzer

- Amazon Inspector
- AWS IoT Device Defender
- AWS Systems Manager Explorer
- AWS Systems Manager OpsCenter
- AWS Systems Manager Manajer Patch

Wilayah China (Beijing) dan China (Ningxia) hanya mendukung integrasi pihak ketiga berikut:

- Cloud Custodian
- FireEye Helix
- Helecloud
- IBM QRadar
- PagerDuty
- Palo Alto Networks Cortex XSOAR
- Palo Alto Networks VM-Series
- Prowler
- RSA Archer
- Splunk Enterprise
- Splunk Phantom
- ThreatModeler

Integrasi yang didukung di AWS GovCloud (AS-Timur) dan AWS GovCloud (AS-Barat)

Wilayah AWS GovCloud (AS-Timur) dan AWS GovCloud (AS-Barat) hanya mendukung integrasi berikut dengan layanan: AWS

- AWS Config
- Amazon Detective
- AWS Firewall Manager
- Amazon GuardDuty
- AWS Health

- IAM Access Analyzer
- Amazon Inspector
- AWS IoT Device Defender

Wilayah AWS GovCloud (AS-Timur) dan AWS GovCloud (AS-Barat) hanya mendukung integrasi pihak ketiga berikut:

- Atlassian Jira Service Management
- Atlassian Jira Service Management Cloud
- Atlassian OpsGenie
- Caveonix Cloud
- Cloud Custodian
- Cloud Storage Security Antivirus for Amazon S3
- CrowdStrike Falcon
- FireEye Helix
- Forcepoint CASB
- Forcepoint DLP
- Forcepoint NGFW
- Fugue
- Kion
- MicroFocus ArcSight
- NETSCOUT Cyber Investigator
- PagerDuty
- Palo Alto Networks – Prisma Cloud Compute
- Palo Alto Networks – Prisma Cloud Enterprise
- Palo Alto Networks – VM-Series(hanya tersedia di AWS GovCloud (AS-Barat))
- Prowler
- Rackspace Technology – Cloud Native Security
- Rapid7 InsightConnect
- RSA Archer
- SecureCloudDb

- ServiceNow ITSM
- Slack
- ThreatModeler
- Vectra AI Cognito Detect

Ketersediaan standar menurut Wilayah

Standar yang Dikelola Layanan: hanya AWS Control Tower tersedia di Wilayah yang AWS Control Tower mendukung, termasuk. AWS GovCloud (US) Untuk daftar Wilayah yang AWS Control Tower mendukung, lihat Cara Wilayah AWS Bekerja Dengan AWS Control Tower di Panduan AWS Control Tower Pengguna.

Standar Penandaan AWS Sumber Daya tidak tersedia di Kanada Barat (Calgary), China, dan. AWS GovCloud (US)

Standar keamanan lainnya tersedia di semua Wilayah tempat Security Hub tersedia.

Ketersediaan kontrol berdasarkan Wilayah

Kontrol Security Hub mungkin tidak tersedia di semua Wilayah. Untuk melihat daftar kontrol yang tidak tersedia di setiap Wilayah, lihatBatas regional pada kontrol. Kontrol tidak akan muncul di daftar kontrol di konsol Security Hub jika tidak tersedia di Wilayah tempat Anda masuk. Pengecualiannya adalah jika Anda masuk ke Wilayah agregasi. Dalam hal ini, Anda dapat melihat kontrol yang tersedia di Wilayah agregasi atau di satu atau beberapa Wilayah tertaut.

Batas regional pada kontrol

AWS Kontrol Security Hub mungkin tidak tersedia di semua Wilayah AWS. Halaman ini menunjukkan kontrol mana yang tidak tersedia di Wilayah tertentu. Kontrol tidak akan muncul di daftar kontrol di konsol Security Hub jika tidak tersedia di Wilayah tempat Anda masuk. Pengecualiannya adalah jika Anda masuk ke Wilayah agregasi. Dalam hal ini, Anda dapat melihat kontrol yang tersedia di Wilayah agregasi atau di satu atau beberapa Wilayah tertaut.

Daftar Isi

- AS Barat (California Utara)
- AS Barat (Oregon)
- Afrika (Cape Town)
- Asia Pasifik (Hong Kong)
- Asia Pasifik (Hyderabad)
- Asia Pasifik (Jakarta)
- Asia Pasifik (Mumbai)
- Asia Pasifik (Melbourne)
- Asia Pasifik (Osaka)
- Asia Pasifik (Seoul)
- Asia Pasifik (Singapura)
- Asia Pasifik (Sydney)
- Asia Pasifik (Tokyo)
- Kanada (Pusat)
- Tiongkok (Beijing)
- Tiongkok (Ningxia)
- Eropa (Frankfurt)
- Eropa (Irlandia)
- Eropa (London)
- Eropa (Milan)
- Eropa (Paris)
- Eropa (Spanyol)
- Eropa (Stockholm)
- Eropa (Zürich)
- Israel (Tel Aviv)
- Timur Tengah (Bahrain)
- Timur Tengah (UEA)
- Amerika Selatan (Sao Paulo)
- AWS GovCloud (AS-Timur)
- AWS GovCloud (AS-Barat)

AS Timur (Virginia Utara)

Kontrol berikut tidak didukung di US East (Virginia N.).

- [DataFirehose.1] Aliran pengiriman Firehose harus dienkripsi saat istirahat
- [DMS.10] Titik akhir DMS untuk database Neptunus harus mengaktifkan otorisasi IAM
- [DMS.11] Titik akhir DMS untuk MongoDB harus mengaktifkan mekanisme otentikasi
- [DMS.12] Titik akhir DMS untuk Redis harus mengaktifkan TLS
- [DynamoDB.7] Cluster DynamoDB Accelerator harus dienkripsi saat transit
- [EFS.6] Target pemasangan EFS tidak boleh dikaitkan dengan subnet publik
- [EKS.3] Kluster EKS harus menggunakan rahasia Kubernetes terenkripsi
- [ElastiCache.4] ElastiCache untuk grup replikasi Redis harus dienkripsi saat istirahat
- [ElastiCache.5] ElastiCache untuk grup replikasi Redis harus dienkripsi saat transit
- [ElastiCache.6] ElastiCache untuk grup replikasi Redis sebelum versi 6.0 harus menggunakan Redis AUTH
- [ElastiCache.7] ElastiCache cluster tidak boleh menggunakan grup subnet default
- [FSX.2] Sistem file FSx for Lustre harus dikonfigurasi untuk menyalin tag ke cadangan
- [GlobalAccelerator.1] Akselerator Akselerator Global harus diberi tag
- [MQ.2] Broker ActiveMQ harus mengalirkan log audit ke CloudWatch
- [MQ.3] Broker Amazon MQ harus mengaktifkan peningkatan versi minor otomatis
- [Opensearch.11] OpenSearch domain harus memiliki setidaknya tiga node primer khusus
- [Redshift.15] Grup keamanan Redshift harus mengizinkan masuknya port cluster hanya dari asal yang dibatasi
- [SageMaker.4] varian produksi SageMaker titik akhir harus memiliki jumlah instance awal yang lebih besar dari 1
- [ServiceCatalog.1] Portofolio Service Catalog harus dibagikan hanya dalam suatu organisasi AWS
- [Transfer.2] Server Transfer Family tidak boleh menggunakan protokol FTP untuk koneksi titik akhir

AS Timur (Ohio)

Kontrol berikut tidak didukung di US East (Ohio).

- [CloudFront.1] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi

- [CloudFront.3] CloudFront distribusi harus memerlukan enkripsi dalam perjalanan
- [CloudFront.4] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi
- [CloudFront.5] CloudFront distribusi seharusnya mengaktifkan logging
- [CloudFront.6] CloudFront distribusi harus mengaktifkan WAF
- [CloudFront.7] CloudFront distribusi harus menggunakan sertifikat SSL/TLS khusus
- [CloudFront.8] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS
- [CloudFront.9] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus
- [CloudFront.10] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal khusus
- [CloudFront.12] CloudFront distribusi seharusnya tidak menunjukkan asal S3 yang tidak ada
- [CloudFront.13] CloudFront distribusi harus menggunakan kontrol akses asal
- [CloudFront.14] CloudFront distribusi harus ditandai
- [DataFirehose.1] Aliran pengiriman Firehose harus dienkripsi saat istirahat
- [DMS.10] Titik akhir DMS untuk database Neptunus harus mengaktifkan otorisasi IAM
- [DMS.11] Titik akhir DMS untuk MongoDB harus mengaktifkan mekanisme otentikasi
- [DMS.12] Titik akhir DMS untuk Redis harus mengaktifkan TLS
- [DynamoDB.7] Cluster DynamoDB Accelerator harus dienkripsi saat transit
- [EC2.24] Jenis instans paravirtual Amazon EC2 tidak boleh digunakan
- [ECR.4] Repositori publik ECR harus ditandai
- [EFS.6] Target pemasangan EFS tidak boleh dikaitkan dengan subnet publik
- [EKS.3] Kluster EKS harus menggunakan rahasia Kubernetes terenkripsi
- [FSX.2] Sistem file FSx for Lustre harus dikonfigurasi untuk menyalin tag ke cadangan
- [GlobalAccelerator.1] Akselerator Akselerator Global harus diberi tag
- [IAM.26] Sertifikat SSL/TLS kedaluwarsa yang dikelola di IAM harus dihapus
- [MQ.2] Broker ActiveMQ harus mengalirkan log audit ke CloudWatch
- [MQ.3] Broker Amazon MQ harus mengaktifkan peningkatan versi minor otomatis
- [Opensearch.11] OpenSearch domain harus memiliki setidaknya tiga node primer khusus
- [RDS.31] Grup keamanan RDS DB harus ditandai
- [Redshift.15] Grup keamanan Redshift harus mengizinkan masuknya port cluster hanya dari asal yang dibatasi
- [Route53.1] Pemeriksaan kesehatan rute 53 harus ditandai

- [Route53.2] Route 53 zona yang dihosting publik harus mencatat kueri DNS
- [SageMaker.4] varian produksi SageMaker titik akhir harus memiliki jumlah instance awal yang lebih besar dari 1
- [ServiceCatalog.1] Portofolio Service Catalog harus dibagikan hanya dalam suatu organisasi AWS
- [Transfer.2] Server Transfer Family tidak boleh menggunakan protokol FTP untuk koneksi titik akhir
- [WAF.1] Pencatatan ACL Web Global AWS WAF Klasik harus diaktifkan
- [WAF.6] Aturan global AWS WAF klasik harus memiliki setidaknya satu syarat
- [WAF.7] Kelompok aturan global AWS WAF klasik harus memiliki setidaknya satu aturan
- [WAF.8] ACL web global AWS WAF klasik harus memiliki setidaknya satu aturan atau kelompok aturan

AS Barat (California Utara)

Kontrol berikut tidak didukung di AS Barat (California Utara).

- [CloudFront.1] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi
- [CloudFront.3] CloudFront distribusi harus memerlukan enkripsi dalam perjalanan
- [CloudFront.4] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi
- [CloudFront.5] CloudFront distribusi seharusnya mengaktifkan logging
- [CloudFront.6] CloudFront distribusi harus mengaktifkan WAF
- [CloudFront.7] CloudFront distribusi harus menggunakan sertifikat SSL/TLS khusus
- [CloudFront.8] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS
- [CloudFront.9] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus
- [CloudFront.10] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal khusus
- [CloudFront.12] CloudFront distribusi seharusnya tidak menunjukkan asal S3 yang tidak ada
- [CloudFront.13] CloudFront distribusi harus menggunakan kontrol akses asal
- [CloudFront.14] CloudFront distribusi harus ditandai
- [CodeArtifact.1] CodeArtifact repositori harus diberi tag
- [DataFirehose.1] Aliran pengiriman Firehose harus dienkripsi saat istirahat
- [DMS.10] Titik akhir DMS untuk database Neptunus harus mengaktifkan otorisasi IAM
- [DMS.11] Titik akhir DMS untuk MongoDB harus mengaktifkan mekanisme otentikasi

- [DMS.12] Titik akhir DMS untuk Redis harus mengaktifkan TLS
- [DocumentDB.1] Cluster Amazon DocumentDB harus dienkripsi saat istirahat
- [DocumentDB.2] Cluster Amazon DocumentDB harus memiliki periode retensi cadangan yang memadai
- [DocumentDB.3] Cuplikan cluster manual Amazon DocumentDB seharusnya tidak bersifat publik
- [DocumentDB.4] Cluster Amazon DocumentDB harus mempublikasikan log audit ke Log CloudWatch
- [DocumentDB.5] Cluster Amazon DocumentDB harus mengaktifkan perlindungan penghapusan
- [DynamoDB.7] Cluster DynamoDB Accelerator harus dienkripsi saat transit
- [ECR.4] Repositori publik ECR harus ditandai
- [EFS.6] Target pemasangan EFS tidak boleh dikaitkan dengan subnet publik
- [EKS.1] Titik akhir klaster EKS seharusnya tidak dapat diakses publik
- [EKS.3] Kluster EKS harus menggunakan rahasia Kubernetes terenkripsi
- [FSX.1] FSx untuk sistem file OpenZFS harus dikonfigurasi untuk menyalin tag ke cadangan dan volume
- [FSX.2] Sistem file FSx for Lustre harus dikonfigurasi untuk menyalin tag ke cadangan
- [GlobalAccelerator.1] Akselerator Akselerator Global harus diberi tag
- [IAM.26] Sertifikat SSL/TLS kedaluwarsa yang dikelola di IAM harus dihapus
- [MQ.2] Broker ActiveMQ harus mengalirkan log audit ke CloudWatch
- [MQ.3] Broker Amazon MQ harus mengaktifkan peningkatan versi minor otomatis
- [Opensearch.11] OpenSearch domain harus memiliki setidaknya tiga node primer khusus
- [RDS.35] Cluster RDS DB harus mengaktifkan peningkatan versi minor otomatis
- [Redshift.15] Grup keamanan Redshift harus mengizinkan masuknya port cluster hanya dari asal yang dibatasi
- [Route53.1] Pemeriksaan kesehatan rute 53 harus ditandai
- [Route53.2] Route 53 zona yang dihosting publik harus mencatat kueri DNS
- [SageMaker.4] varian produksi SageMaker titik akhir harus memiliki jumlah instance awal yang lebih besar dari 1
- [ServiceCatalog.1] Portofolio Service Catalog harus dibagikan hanya dalam suatu organisasi AWS
- [Transfer.2] Server Transfer Family tidak boleh menggunakan protokol FTP untuk koneksi titik akhir
- [WAF.1] Pencatatan ACL Web Global AWS WAF Klasik harus diaktifkan

- [WAF.6] Aturan global AWS WAF klasik harus memiliki setidaknya satu syarat
- [WAF.7] Kelompok aturan global AWS WAF klasik harus memiliki setidaknya satu aturan
- [WAF.8] ACL web global AWS WAF klasik harus memiliki setidaknya satu aturan atau kelompok aturan

AS Barat (Oregon)

Kontrol berikut tidak didukung di US West (Oregon).

- [CloudFront.1] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi
- [CloudFront.3] CloudFront distribusi harus memerlukan enkripsi dalam perjalanan
- [CloudFront.4] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi
- [CloudFront.5] CloudFront distribusi seharusnya mengaktifkan logging
- [CloudFront.6] CloudFront distribusi harus mengaktifkan WAF
- [CloudFront.7] CloudFront distribusi harus menggunakan sertifikat SSL/TLS khusus
- [CloudFront.8] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS
- [CloudFront.9] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus
- [CloudFront.10] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal khusus
- [CloudFront.12] CloudFront distribusi seharusnya tidak menunjukkan asal S3 yang tidak ada
- [CloudFront.13] CloudFront distribusi harus menggunakan kontrol akses asal
- [CloudFront.14] CloudFront distribusi harus ditandai
- [DataFirehose.1] Aliran pengiriman Firehose harus dienkripsi saat istirahat
- [DMS.10] Titik akhir DMS untuk database Neptunus harus mengaktifkan otorisasi IAM
- [DMS.11] Titik akhir DMS untuk MongoDB harus mengaktifkan mekanisme otentikasi
- [DMS.12] Titik akhir DMS untuk Redis harus mengaktifkan TLS
- [DynamoDB.7] Cluster DynamoDB Accelerator harus dienkripsi saat transit
- [ECR.4] Repositori publik ECR harus ditandai
- [EFS.6] Target pemasangan EFS tidak boleh dikaitkan dengan subnet publik
- [EKS.3] Kluster EKS harus menggunakan rahasia Kubernetes terenkripsi
- [FSX.2] Sistem file FSx for Lustre harus dikonfigurasi untuk menyalin tag ke cadangan
- [IAM.26] Sertifikat SSL/TLS kedaluwarsa yang dikelola di IAM harus dihapus

- [MQ.2] Broker ActiveMQ harus mengalirkan log audit ke CloudWatch
- [MQ.3] Broker Amazon MQ harus mengaktifkan peningkatan versi minor otomatis
- [Opensearch.11] OpenSearch domain harus memiliki setidaknya tiga node primer khusus
- [Redshift.15] Grup keamanan Redshift harus mengizinkan masuknya port cluster hanya dari asal yang dibatasi
- [Route53.1] Pemeriksaan kesehatan rute 53 harus ditandai
- [Route53.2] Route 53 zona yang dihosting publik harus mencatat kueri DNS
- [SageMaker.4] varian produksi SageMaker titik akhir harus memiliki jumlah instance awal yang lebih besar dari 1
- [ServiceCatalog.1] Portofolio Service Catalog harus dibagikan hanya dalam suatu organisasi AWS
- [Transfer.2] Server Transfer Family tidak boleh menggunakan protokol FTP untuk koneksi titik akhir
- [WAF.1] Pencatatan ACL Web Global AWS WAF Klasik harus diaktifkan
- [WAF.6] Aturan global AWS WAF klasik harus memiliki setidaknya satu syarat
- [WAF.7] Kelompok aturan global AWS WAF klasik harus memiliki setidaknya satu aturan
- [WAF.8] ACL web global AWS WAF klasik harus memiliki setidaknya satu aturan atau kelompok aturan

Afrika (Cape Town)

Kontrol berikut tidak didukung di Afrika (Cape Town).

- [ACM.1] Sertifikat yang diimpor dan diterbitkan ACM harus diperbarui setelah jangka waktu tertentu
- [ApiGateway.1] API Gateway REST WebSocket dan pencatatan eksekusi API harus diaktifkan
- [AppSync.2] AWS AppSync harus mengaktifkan logging tingkat lapangan
- [AppSync.5] AWS AppSync GraphQL API tidak boleh diautentikasi dengan kunci API
- [CloudFront.1] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi
- [CloudFront.3] CloudFront distribusi harus memerlukan enkripsi dalam perjalanan
- [CloudFront.4] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi
- [CloudFront.5] CloudFront distribusi seharusnya mengaktifkan logging
- [CloudFront.6] CloudFront distribusi harus mengaktifkan WAF
- [CloudFront.7] CloudFront distribusi harus menggunakan sertifikat SSL/TLS khusus
- [CloudFront.8] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS

- [CloudFront.9] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus
- [CloudFront.10] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal khusus
- [CloudFront.12] CloudFront distribusi seharusnya tidak menunjukkan asal S3 yang tidak ada
- [CloudFront.13] CloudFront distribusi harus menggunakan kontrol akses asal
- [CloudFront.14] CloudFront distribusi harus ditandai
- [CodeArtifact.1] CodeArtifact repositori harus diberi tag
- [CodeBuild.1] URL repositori sumber CodeBuild Bitbucket tidak boleh berisi kredensyal sensitif
- [CodeBuild.2] variabel lingkungan CodeBuild proyek tidak boleh berisi kredensil teks yang jelas
- [DataFirehose.1] Aliran pengiriman Firehose harus dienkripsi saat istirahat
- [DMS.1] Instans replikasi Layanan Migrasi Database tidak boleh bersifat publik
- [DMS.10] Titik akhir DMS untuk database Neptunus harus mengaktifkan otorisasi IAM
- [DMS.11] Titik akhir DMS untuk MongoDB harus mengaktifkan mekanisme otentikasi
- [DMS.12] Titik akhir DMS untuk Redis harus mengaktifkan TLS
- [DocumentDB.1] Cluster Amazon DocumentDB harus dienkripsi saat istirahat
- [DocumentDB.2] Cluster Amazon DocumentDB harus memiliki periode retensi cadangan yang memadai
- [DocumentDB.3] Cuplikan cluster manual Amazon DocumentDB seharusnya tidak bersifat publik
- [DocumentDB.4] Cluster Amazon DocumentDB harus mempublikasikan log audit ke Log CloudWatch
- [DocumentDB.5] Cluster Amazon DocumentDB harus mengaktifkan perlindungan penghapusan
- [DynamoDB.3] Cluster DynamoDB Accelerator (DAX) harus dienkripsi saat istirahat
- [DynamoDB.7] Cluster DynamoDB Accelerator harus dienkripsi saat transit
- [EC2.3] Volume Amazon EBS yang terpasang harus dienkripsi saat istirahat
- [EC2.4] Instans EC2 yang dihentikan harus dihapus setelah periode waktu tertentu
- [EC2.8] Instans EC2 harus menggunakan Layanan Metadata Instance Versi 2 (IMDSv2)
- [EC2.12] EIP Amazon EC2 yang tidak digunakan harus dihapus
- [EC2.13] Grup keamanan tidak boleh mengizinkan masuknya dari 0.0.0.0/0 atau: :/0 ke port 22
- [EC2.14] Grup keamanan tidak boleh mengizinkan masuknya dari 0.0.0.0/0 atau: :/0 ke port 3389
- [EC2.24] Jenis instans paravirtual Amazon EC2 tidak boleh digunakan
- [ECR.4] Repositori publik ECR harus ditandai

- [EFS.1] Sistem File Elastis harus dikonfigurasi untuk mengenkripsi data file saat istirahat menggunakan AWS KMS
- [EFS.2] Volume Amazon EFS harus dalam rencana cadangan
- [EFS.6] Target pemasangan EFS tidak boleh dikaitkan dengan subnet publik
- [EKS.1] Titik akhir klaster EKS seharusnya tidak dapat diakses publik
- [EKS.3] Kluster EKS harus menggunakan rahasia Kubernetes terenkripsi
- [ELB.1] Application Load Balancer harus dikonfigurasi untuk mengalihkan semua permintaan HTTP ke HTTPS
- [ELB.2] Classic Load Balancer dengan pendengar SSL/HTTPS harus menggunakan sertifikat yang disediakan oleh AWS Certificate Manager
- [ELB.4] Application Load Balancer harus dikonfigurasi untuk menjatuhkan header http
- [ELB.8] Classic Load Balancer dengan pendengar SSL harus menggunakan kebijakan keamanan yang telah ditentukan sebelumnya yang memiliki urasi yang kuat AWS Config
- [ELB.16] Application Load Balancers harus dikaitkan dengan ACL web AWS WAF
- [EMR.1] Node primer cluster EMR Amazon seharusnya tidak memiliki alamat IP publik
- [ES.3] Domain Elasticsearch harus mengenkripsi data yang dikirim antar node
- [EventBridge.4] titik akhir EventBridge global harus mengaktifkan replikasi acara
- [FSX.1] FSx untuk sistem file OpenZFS harus dikonfigurasi untuk menyalin tag ke cadangan dan volume
- [FSX.2] Sistem file FSx for Lustre harus dikonfigurasi untuk menyalin tag ke cadangan
- [GlobalAccelerator.1] Akselerator Akselerator Global harus diberi tag
- [GuardDuty.1] GuardDuty harus diaktifkan
- [IAM.3] Kunci akses pengguna IAM harus diputar setiap 90 hari atau kurang
- [IAM.18] Memastikan peran dukungan telah dibuat untuk mengelola insiden dengan AWS Support
- [IAM.26] Sertifikat SSL/TLS kedaluwarsa yang dikelola di IAM harus dihapus
- [IoT.1] profil AWS IoT Core keamanan harus ditandai
- [IoT.2] tindakan AWS IoT Core mitigasi harus ditandai
- AWS IoT Core Dimensi [IoT.3] harus ditandai
- [IoT.4] AWS IoT Core otorisasi harus diberi tag
- [IoT.5] alias AWS IoT Core peran harus ditandai
- AWS IoT Core Kebijakan [IoT.6] harus ditandai

- [MQ.2] Broker ActiveMQ harus mengalirkan log audit ke CloudWatch
- [MQ.3] Broker Amazon MQ harus mengaktifkan peningkatan versi minor otomatis
- [Opensearch.1] OpenSearch domain harus mengaktifkan enkripsi saat istirahat
- [Opensearch.2] OpenSearch domain tidak boleh diakses publik
- [Opensearch.3] OpenSearch domain harus mengenkripsi data yang dikirim antar node
- [Opensearch.4] login kesalahan OpenSearch domain ke Log harus diaktifkan CloudWatch
- [Opensearch.5] OpenSearch domain harus mengaktifkan pencatatan audit
- [Opensearch.6] OpenSearch domain harus memiliki setidaknya tiga node data
- [Opensearch.7] OpenSearch domain harus mengaktifkan kontrol akses berbutir halus
- [Opensearch.8] Koneksi ke OpenSearch domain harus dienkripsi menggunakan kebijakan keamanan TLS terbaru
- [Opensearch.11] OpenSearch domain harus memiliki setidaknya tiga node primer khusus
- [RDS.1] Snapshot RDS harus pribadi
- [RDS.9] Instans RDS DB harus menerbitkan log ke Log CloudWatch
- [RDS.10] Otentikasi IAM harus dikonfigurasi untuk instance RDS
- [RDS.14] Cluster Amazon Aurora seharusnya mengaktifkan backtracking
- [RDS.31] Grup keamanan RDS DB harus ditandai
- [Redshift.3] Cluster Amazon Redshift harus mengaktifkan snapshot otomatis
- [Redshift.15] Grup keamanan Redshift harus mengizinkan masuknya port cluster hanya dari asal yang dibatasi
- [Route53.1] Pemeriksaan kesehatan rute 53 harus ditandai
- [Route53.2] Route 53 zona yang dihosting publik harus mencatat kueri DNS
- [SageMaker.1] Instans SageMaker notebook Amazon seharusnya tidak memiliki akses internet langsung
- [SageMaker.4] varian produksi SageMaker titik akhir harus memiliki jumlah instance awal yang lebih besar dari 1
- [ServiceCatalog.1] Portofolio Service Catalog harus dibagikan hanya dalam suatu organisasi AWS
- [SSM.2] Instans Amazon EC2 yang dikelola oleh Systems Manager harus memiliki status kepatuhan patch COMPLIANT setelah instalasi patch
- [SSM.3] Instans Amazon EC2 yang dikelola oleh Systems Manager harus memiliki status kepatuhan asosiasi COMPLIANT

- [Transfer.2] Server Transfer Family tidak boleh menggunakan protokol FTP untuk koneksi titik akhir
- [WAF.1] Pencatatan ACL Web Global AWS WAF Klasik harus diaktifkan
- [WAF.6] Aturan global AWS WAF klasik harus memiliki setidaknya satu syarat
- [WAF.7] Kelompok aturan global AWS WAF klasik harus memiliki setidaknya satu aturan
- [WAF.8] ACL web global AWS WAF klasik harus memiliki setidaknya satu aturan atau kelompok aturan
- [WAF.11] pencatatan ACL AWS WAF web harus diaktifkan

Asia Pasifik (Hong Kong)

Kontrol berikut tidak didukung di Asia Pasifik (Hong Kong).

- [CloudFront.1] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi
- [CloudFront.3] CloudFront distribusi harus memerlukan enkripsi dalam perjalanan
- [CloudFront.4] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi
- [CloudFront.5] CloudFront distribusi seharusnya mengaktifkan logging
- [CloudFront.6] CloudFront distribusi harus mengaktifkan WAF
- [CloudFront.7] CloudFront distribusi harus menggunakan sertifikat SSL/TLS khusus
- [CloudFront.8] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS
- [CloudFront.9] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus
- [CloudFront.10] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal khusus
- [CloudFront.12] CloudFront distribusi seharusnya tidak menunjukkan asal S3 yang tidak ada
- [CloudFront.13] CloudFront distribusi harus menggunakan kontrol akses asal
- [CloudFront.14] CloudFront distribusi harus ditandai
- [CodeArtifact.1] CodeArtifact repositori harus diberi tag
- [DataFirehose.1] Aliran pengiriman Firehose harus dienkripsi saat istirahat
- [DMS.10] Titik akhir DMS untuk database Neptunus harus mengaktifkan otorisasi IAM
- [DMS.11] Titik akhir DMS untuk MongoDB harus mengaktifkan mekanisme otentikasi
- [DMS.12] Titik akhir DMS untuk Redis harus mengaktifkan TLS
- [DocumentDB.1] Cluster Amazon DocumentDB harus dienkripsi saat istirahat

- [DocumentDB.2] Cluster Amazon DocumentDB harus memiliki periode retensi cadangan yang memadai
- [DocumentDB.3] Cuplikan cluster manual Amazon DocumentDB seharusnya tidak bersifat publik
- [DocumentDB.4] Cluster Amazon DocumentDB harus mempublikasikan log audit ke Log CloudWatch
- [DocumentDB.5] Cluster Amazon DocumentDB harus mengaktifkan perlindungan penghapusan
- [DynamoDB.3] Cluster DynamoDB Accelerator (DAX) harus dienkripsi saat istirahat
- [DynamoDB.7] Cluster DynamoDB Accelerator harus dienkripsi saat transit
- [EC2.23] Amazon EC2 Transit Gateways seharusnya tidak secara otomatis menerima permintaan lampiran VPC
- [EC2.24] Jenis instans paravirtual Amazon EC2 tidak boleh digunakan
- [ECR.4] Repositori publik ECR harus ditandai
- [EFS.6] Target pemasangan EFS tidak boleh dikaitkan dengan subnet publik
- [EKS.3] Kluster EKS harus menggunakan rahasia Kubernetes terenkripsi
- [EventBridge.4] titik akhir EventBridge global harus mengaktifkan replikasi acara
- [FSX.2] Sistem file FSx for Lustre harus dikonfigurasi untuk menyalin tag ke cadangan
- [GlobalAccelerator.1] Akselerator Akselerator Global harus diberi tag
- [IAM.26] Sertifikat SSL/TLS kedaluwarsa yang dikelola di IAM harus dihapus
- [MQ.2] Broker ActiveMQ harus mengalirkan log audit ke CloudWatch
- [MQ.3] Broker Amazon MQ harus mengaktifkan peningkatan versi minor otomatis
- [Opensearch.11] OpenSearch domain harus memiliki setidaknya tiga node primer khusus
- [RDS.10] Otentikasi IAM harus dikonfigurasi untuk instance RDS
- [RDS.14] Cluster Amazon Aurora seharusnya mengaktifkan backtracking
- [RDS.31] Grup keamanan RDS DB harus ditandai
- [Redshift.15] Grup keamanan Redshift harus mengizinkan masuknya port cluster hanya dari asal yang dibatasi
- [Route53.1] Pemeriksaan kesehatan rute 53 harus ditandai
- [Route53.2] Route 53 zona yang dihosting publik harus mencatat kueri DNS
- [SageMaker.4] varian produksi SageMaker titik akhir harus memiliki jumlah instance awal yang lebih besar dari 1
- [SES.1] Daftar kontak SES harus ditandai

- [SES.2] Set konfigurasi SES harus ditandai
- [ServiceCatalog.1] Portofolio Service Catalog harus dibagikan hanya dalam suatu organisasi AWS
- [Transfer.2] Server Transfer Family tidak boleh menggunakan protokol FTP untuk koneksi titik akhir
- [WAF.1] Pencatatan ACL Web Global AWS WAF Klasik harus diaktifkan
- [WAF.6] Aturan global AWS WAF klasik harus memiliki setidaknya satu syarat
- [WAF.7] Kelompok aturan global AWS WAF klasik harus memiliki setidaknya satu aturan
- [WAF.8] ACL web global AWS WAF klasik harus memiliki setidaknya satu aturan atau kelompok aturan

Asia Pasifik (Hyderabad)

Kontrol berikut tidak didukung di Asia Pasifik (Hyderabad).

- [ACM.1] Sertifikat yang diimpor dan diterbitkan ACM harus diperbarui setelah jangka waktu tertentu
- [ACM.2] Sertifikat RSA yang dikelola oleh ACM harus menggunakan panjang kunci minimal 2.048 bit
- [Akun.2] Akun AWS harus menjadi bagian dari organisasi AWS Organizations
- [ApiGateway.1] API Gateway REST WebSocket dan pencatatan eksekusi API harus diaktifkan
- [ApiGateway.2] Tahapan API Gateway REST API harus dikonfigurasi untuk menggunakan sertifikat SSL untuk otentikasi backend
- [ApiGateway.3] Tahapan API Gateway REST API harus mengaktifkan penelusuran AWS X-Ray
- [ApiGateway.4] API Gateway harus dikaitkan dengan ACL Web WAF
- [ApiGateway.8] Rute API Gateway harus menentukan jenis otorisasi
- [ApiGateway.9] Pencatatan akses harus dikonfigurasi untuk Tahapan API Gateway V2
- [AppSync.2] AWS AppSync harus mengaktifkan logging tingkat lapangan
- [AppSync.5] AWS AppSync GraphQL API tidak boleh diautentikasi dengan kunci API
- [Athena.2] Katalog data Athena harus diberi tag
- [Athena.3] Kelompok kerja Athena harus ditandai
- [AutoScaling.1] Grup Auto Scaling yang terkait dengan penyeimbang beban harus menggunakan pemeriksaan kesehatan ELB
- [Autoscaling.5] Instans Amazon EC2 yang diluncurkan menggunakan konfigurasi peluncuran grup Auto Scaling seharusnya tidak memiliki alamat IP Publik

- [Backup.1] titik AWS Backup pemulihan harus dienkripsi saat istirahat
- [Backup.2] poin AWS Backup pemulihan harus ditandai
- [Backup.3] AWS Backup brankas harus ditandai
- [Backup.4] rencana AWS Backup laporan harus ditandai
- [Backup.5] rencana AWS Backup cadangan harus ditandai
- [CloudFormation.2] CloudFormation tumpukan harus ditandai
- [CloudFront.1] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi
- [CloudFront.3] CloudFront distribusi harus memerlukan enkripsi dalam perjalanan
- [CloudFront.4] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi
- [CloudFront.5] CloudFront distribusi seharusnya mengaktifkan logging
- [CloudFront.6] CloudFront distribusi harus mengaktifkan WAF
- [CloudFront.7] CloudFront distribusi harus menggunakan sertifikat SSL/TLS khusus
- [CloudFront.8] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS
- [CloudFront.9] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus
- [CloudFront.10] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal khusus
- [CloudFront.12] CloudFront distribusi seharusnya tidak menunjukkan asal S3 yang tidak ada
- [CloudFront.13] CloudFront distribusi harus menggunakan kontrol akses asal
- [CloudFront.14] CloudFront distribusi harus ditandai
- [CloudTrail.6] Pastikan bucket S3 yang digunakan untuk menyimpan CloudTrail log tidak dapat diakses publik
- [CloudTrail.7] Pastikan pencatatan akses bucket S3 diaktifkan pada bucket CloudTrail S3
- [CodeArtifact.1] CodeArtifact repositori harus diberi tag
- [CodeBuild.1] URL repositori sumber CodeBuild Bitbucket tidak boleh berisi kredensyal sensitif
- [CodeBuild.2] variabel lingkungan CodeBuild proyek tidak boleh berisi kredensil teks yang jelas
- [CodeBuild.3] Log CodeBuild S3 harus dienkripsi
- [CodeBuild.4] lingkungan CodeBuild proyek harus memiliki urasi logging AWS Config
- [DataFirehose.1] Aliran pengiriman Firehose harus dienkripsi saat istirahat
- [Detective.1] Grafik perilaku detektif harus diberi tag
- [DMS.1] Instans replikasi Layanan Migrasi Database tidak boleh bersifat publik

- [DMS.2] Sertifikat DMS harus ditandai
- [DMS.3] Langganan acara DMS harus ditandai
- [DMS.4] Contoh replikasi DMS harus ditandai
- [DMS.5] Grup subnet replikasi DMS harus ditandai
- [DMS.6] Instans replikasi DMS harus mengaktifkan peningkatan versi minor otomatis
- [DMS.7] Tugas replikasi DMS untuk database target seharusnya mengaktifkan logging
- [DMS.8] Tugas replikasi DMS untuk database sumber seharusnya mengaktifkan logging
- [DMS.9] Titik akhir DMS harus menggunakan SSL
- [DMS.10] Titik akhir DMS untuk database Neptunus harus mengaktifkan otorisasi IAM
- [DMS.11] Titik akhir DMS untuk MongoDB harus mengaktifkan mekanisme otentikasi
- [DMS.12] Titik akhir DMS untuk Redis harus mengaktifkan TLS
- [DocumentDB.1] Cluster Amazon DocumentDB harus dienkripsi saat istirahat
- [DocumentDB.2] Cluster Amazon DocumentDB harus memiliki periode retensi cadangan yang memadai
- [DocumentDB.3] Cuplikan cluster manual Amazon DocumentDB seharusnya tidak bersifat publik
- [DocumentDB.4] Cluster Amazon DocumentDB harus mempublikasikan log audit ke Log CloudWatch
- [DocumentDB.5] Cluster Amazon DocumentDB harus mengaktifkan perlindungan penghapusan
- [DynamoDB.3] Cluster DynamoDB Accelerator (DAX) harus dienkripsi saat istirahat
- [DynamoDB.4] Tabel DynamoDB harus ada dalam rencana cadangan
- [DynamoDB.7] Cluster DynamoDB Accelerator harus dienkripsi saat transit
- [EC2.13] Grup keamanan tidak boleh mengizinkan masuknya dari 0.0.0.0/0 atau: :/0 ke port 22
- [EC2.14] Grup keamanan tidak boleh mengizinkan masuknya dari 0.0.0.0/0 atau: :/0 ke port 3389
- [EC2.18] Grup keamanan seharusnya hanya mengizinkan lalu lintas masuk yang tidak terbatas untuk port resmi
- [EC2.22] Grup keamanan Amazon EC2 yang tidak digunakan harus dihapus
- [EC2.23] Amazon EC2 Transit Gateways seharusnya tidak secara otomatis menerima permintaan lampiran VPC
- [EC2.24] Jenis instans paravirtual Amazon EC2 tidak boleh digunakan
- [EC2.25] Templat peluncuran Amazon EC2 tidak boleh menetapkan IP publik ke antarmuka jaringan

- [EC2.28] Volume EBS harus dicakup oleh rencana cadangan
- [EC2.34] Tabel rute gateway transit EC2 harus ditandai
- [EC2.40] Gerbang EC2 NAT harus ditandai
- [EC2.48] Log aliran VPC Amazon harus ditandai
- [EC2.51] Titik akhir EC2 Client VPN harus mengaktifkan pencatatan koneksi klien
- [ECR.1] Repositori pribadi ECR harus memiliki pemindaian gambar yang dikonfigurasi
- [ECR.2] Repositori pribadi ECR harus memiliki kekekalan tag yang dikonfigurasi
- [ECR.3] Repositori ECR harus memiliki setidaknya satu kebijakan siklus hidup yang dikonfigurasi
- [ECR.4] Repositori publik ECR harus ditandai
- [ECS.1] Definisi tugas Amazon ECS harus memiliki mode jaringan yang aman dan definisi pengguna.
- [ECS.9] Definisi tugas ECS harus memiliki konfigurasi logging
- [EFS.1] Sistem File Elastis harus dikonfigurasi untuk mengenkripsi data file saat istirahat menggunakan AWS KMS
- [EFS.2] Volume Amazon EFS harus dalam rencana cadangan
- [EFS.3] Titik akses EFS harus menegakkan direktori root
- [EFS.4] Titik akses EFS harus menegakkan identitas pengguna
- [EFS.5] Titik akses EFS harus ditandai
- [EFS.6] Target pemasangan EFS tidak boleh dikaitkan dengan subnet publik
- [EKS.1] Titik akhir klaster EKS seharusnya tidak dapat diakses publik
- [EKS.2] Kluster EKS harus berjalan pada versi Kubernetes yang didukung
- [EKS.3] Kluster EKS harus menggunakan rahasia Kubernetes terenkripsi
- [ELB.5] Pencatatan aplikasi dan Classic Load Balancer harus diaktifkan
- [ELB.13] Penyeimbang Beban Aplikasi, Jaringan, dan Gateway harus mencakup beberapa Availability Zone
- [ELB.14] Classic Load Balancer harus dikonfigurasi dengan mode mitigasi desync defensif atau paling ketat
- [ElastiCache.1] Cluster ElastiCache Redis harus mengaktifkan pencadangan otomatis
- [ElastiCache.6] ElastiCache untuk grup replikasi Redis sebelum versi 6.0 harus menggunakan Redis AUTH
- [ElastiCache.7] ElastiCache cluster tidak boleh menggunakan grup subnet default

- [ElasticBeanstalk.1] Lingkungan Elastic Beanstalk seharusnya mengaktifkan pelaporan kesehatan yang ditingkatkan
- [ElasticBeanstalk.2] Pembaruan platform yang dikelola Elastic Beanstalk harus diaktifkan
- [ElasticBeanstalk.3] Elastic Beanstalk harus mengalirkan log ke CloudWatch
- [EMR.1] Node primer cluster EMR Amazon seharusnya tidak memiliki alamat IP publik
- [ES.1] Domain Elasticsearch harus mengaktifkan enkripsi saat istirahat
- [ES.2] Domain Elasticsearch tidak boleh diakses publik
- [ES.3] Domain Elasticsearch harus mengenkripsi data yang dikirim antar node
- [ES.4] Kesalahan domain Elasticsearch yang masuk ke CloudWatch Log harus diaktifkan
- [EventBridge.2] bus EventBridge acara harus diberi tag
- [EventBridge.3] bus acara EventBridge khusus harus memiliki kebijakan berbasis sumber daya terlampir
- [EventBridge.4] titik akhir EventBridge global harus mengaktifkan replikasi acara
- [FSX.1] FSx untuk sistem file OpenZFS harus dikonfigurasi untuk menyalin tag ke cadangan dan volume
- [FSX.2] Sistem file FSx for Lustre harus dikonfigurasi untuk menyalin tag ke cadangan
- [GlobalAccelerator.1] Akselerator Akselerator Global harus diberi tag
- AWS Glue Pekerjaan [Glue.1] harus ditandai
- [GuardDuty.2] GuardDuty filter harus diberi tag
- [GuardDuty.3] GuardDuty IPset harus ditandai
- [GuardDuty.4] GuardDuty detektor harus ditandai
- [IAM.1] Kebijakan IAM seharusnya tidak mengizinkan hak administratif “*” penuh
- [IAM.2] Pengguna IAM seharusnya tidak memiliki kebijakan IAM yang dilampirkan
- [IAM.3] Kunci akses pengguna IAM harus diputar setiap 90 hari atau kurang
- [IAM.5] MFA harus diaktifkan untuk semua pengguna IAM yang memiliki kata sandi konsol
- [IAM.8] Kredensyal pengguna IAM yang tidak digunakan harus dihapus
- [IAM.18] Memastikan peran dukungan telah dibuat untuk mengelola insiden dengan AWS Support
- [IAM.19] MFA harus diaktifkan untuk semua pengguna IAM
- [IAM.21] Kebijakan terkelola pelanggan IAM yang Anda buat seharusnya tidak mengizinkan tindakan wildcard untuk layanan
- [IAM.22] Kredensyal pengguna IAM yang tidak digunakan selama 45 hari harus dihapus

- [IAM.24] Peran IAM harus ditandai
- [IAM.25] Pengguna IAM harus diberi tag
- [IAM.26] Sertifikat SSL/TLS kedaluwarsa yang dikelola di IAM harus dihapus
- [IAM.27] Identitas IAM seharusnya tidak memiliki kebijakan yang dilampirkan AWSCloudShellFullAccess
- [IoT.1] profil AWS IoT Core keamanan harus ditandai
- [IoT.2] tindakan AWS IoT Core mitigasi harus ditandai
- AWS IoT Core Dimensi [IoT.3] harus ditandai
- [IoT.4] AWS IoT Core otorisasi harus diberi tag
- [IoT.5] alias AWS IoT Core peran harus ditandai
- AWS IoT Core Kebijakan [IoT.6] harus ditandai
- [Kinesis.1] Aliran kinesis harus dienkripsi saat istirahat
- [KMS.1] Kebijakan yang dikelola pelanggan IAM tidak boleh mengizinkan tindakan dekripsi pada semua kunci KMS
- [KMS.2] Prinsipal IAM tidak boleh memiliki kebijakan inline IAM yang memungkinkan tindakan dekripsi pada semua kunci KMS
- [Lambda.5] Fungsi VPC Lambda harus beroperasi di beberapa Availability Zone
- [Macie.1] Amazon Macie harus diaktifkan
- [Macie.2] Penemuan data sensitif otomatis Macie harus diaktifkan
- [MQ.2] Broker ActiveMQ harus mengalirkan log audit ke CloudWatch
- [MQ.3] Broker Amazon MQ harus mengaktifkan peningkatan versi minor otomatis
- [MQ.4] Broker Amazon MQ harus diberi tag
- [MQ.5] Broker ActiveMQ harus menggunakan mode penerapan aktif/siaga
- [MQ.6] Broker RabbitMQ harus menggunakan mode penerapan cluster
- [MSK.1] Cluster MSK harus dienkripsi saat transit di antara node broker
- [MSK.2] Kluster MSK seharusnya telah meningkatkan pemantauan yang dikonfigurasi
- [Neptunus.1] Cluster DB Neptunus harus dienkripsi saat istirahat
- [Neptune.2] Cluster DB Neptunus harus menerbitkan log audit ke Log CloudWatch
- [Neptune.3] Snapshot cluster Neptunus DB seharusnya tidak publik
- [Neptunus.4] Cluster DB Neptunus harus mengaktifkan perlindungan penghapusan

- [Neptunus.5] Cluster DB Neptunus harus mengaktifkan cadangan otomatis
- [Neptune.6] Snapshot cluster Neptunus DB harus dienkripsi saat istirahat
- [Neptunus.7] Cluster DB Neptunus harus mengaktifkan otentikasi basis data IAM
- [Neptunus.8] Cluster DB Neptunus harus dikonfigurasi untuk menyalin tag ke snapshot
- [Neptunus.9] Cluster DB Neptunus harus digunakan di beberapa Availability Zone
- [NetworkFirewall.1] Firewall Firewall Jaringan harus digunakan di beberapa Availability Zone
- [NetworkFirewall.2] Pencatatan Firewall Jaringan harus diaktifkan
- [NetworkFirewall.3] Kebijakan Network Firewall harus memiliki setidaknya satu kelompok aturan yang terkait
- [NetworkFirewall.4] Tindakan stateless default untuk kebijakan Network Firewall harus drop atau forward untuk paket penuh
- [NetworkFirewall.5] Tindakan stateless default untuk kebijakan Network Firewall harus drop atau forward untuk paket yang terfragmentasi
- [NetworkFirewall.6] Grup aturan Stateless Network Firewall tidak boleh kosong
- [NetworkFirewall.9] Firewall Firewall Jaringan harus mengaktifkan perlindungan penghapusan
- [Opensearch.1] OpenSearch domain harus mengaktifkan enkripsi saat istirahat
- [Opensearch.2] OpenSearch domain tidak boleh diakses publik
- [Opensearch.3] OpenSearch domain harus mengenkripsi data yang dikirim antar node
- [Opensearch.4] login kesalahan OpenSearch domain ke Log harus diaktifkan CloudWatch
- [Opensearch.5] OpenSearch domain harus mengaktifkan pencatatan audit
- [Opensearch.6] OpenSearch domain harus memiliki setidaknya tiga node data
- [Opensearch.7] OpenSearch domain harus mengaktifkan kontrol akses berbutir halus
- [Opensearch.8] Koneksi ke OpenSearch domain harus dienkripsi menggunakan kebijakan keamanan TLS terbaru
- [Opensearch.9] domain harus ditandai OpenSearch
- [Opensearch.10] OpenSearch domain harus memiliki pembaruan perangkat lunak terbaru yang diinstal
- [Opensearch.11] OpenSearch domain harus memiliki setidaknya tiga node primer khusus
- [RDS.2] Instans RDS DB harus melarang akses publik, sebagaimana ditentukan oleh urasi PubliclyAccessible AWS Config
- [RDS.7] Cluster RDS harus mengaktifkan perlindungan penghapusan

- [RDS.9] Instans RDS DB harus menerbitkan log ke Log CloudWatch
- [RDS.12] Otentikasi IAM harus dikonfigurasi untuk cluster RDS
- [RDS.14] Cluster Amazon Aurora seharusnya mengaktifkan backtracking
- [RDS.15] Cluster RDS DB harus dikonfigurasi untuk beberapa Availability Zone
- [RDS.16] Cluster RDS DB harus dikonfigurasi untuk menyalin tag ke snapshot
- [RDS.24] Kluster Database RDS harus menggunakan nama pengguna administrator khusus
- [RDS.26] Instans RDS DB harus dilindungi oleh rencana cadangan
- [RDS.27] Cluster RDS DB harus dienkripsi saat istirahat
- [RDS.28] Cluster RDS DB harus ditandai
- [RDS.31] Grup keamanan RDS DB harus ditandai
- [RDS.34] Cluster Aurora MySQL DB harus menerbitkan log audit ke Log CloudWatch
- [RDS.35] Cluster RDS DB harus mengaktifkan peningkatan versi minor otomatis
- [Redshift.1] Cluster Amazon Redshift harus melarang akses publik
- [Redshift.2] Koneksi ke cluster Amazon Redshift harus dienkripsi saat transit
- [Redshift.3] Cluster Amazon Redshift harus mengaktifkan snapshot otomatis
- [Redshift.6] Amazon Redshift harus mengaktifkan peningkatan otomatis ke versi utama
- [Redshift.7] Cluster Redshift harus menggunakan perutean VPC yang ditingkatkan
- [Redshift.10] Cluster Redshift harus dienkripsi saat istirahat
- [Redshift.12] Langganan pemberitahuan acara Redshift harus ditandai
- [Redshift.15] Grup keamanan Redshift harus mengizinkan masuknya port cluster hanya dari asal yang dibatasi
- [Route53.1] Pemeriksaan kesehatan rute 53 harus ditandai
- [Route53.2] Route 53 zona yang dihosting publik harus mencatat kueri DNS
- [S3.6] Kebijakan bucket tujuan umum S3 harus membatasi akses ke yang lain Akun AWS
- [S3.17] Ember tujuan umum S3 harus dienkripsi saat istirahat AWS KMS keys
- [SageMaker.1] Instans SageMaker notebook Amazon seharusnya tidak memiliki akses internet langsung
- [SageMaker.2] instance SageMaker notebook harus diluncurkan dalam VPC khusus
- [SageMaker.3] Pengguna seharusnya tidak memiliki akses root ke instance SageMaker notebook
- [SageMaker.4] varian produksi SageMaker titik akhir harus memiliki jumlah instance awal yang lebih besar dari 1

- [SES.1] Daftar kontak SES harus ditandai
- [SES.2] Set konfigurasi SES harus ditandai
- [ServiceCatalog.1] Portofolio Service Catalog harus dibagikan hanya dalam suatu organisasi AWS
- [SNS.3] Topik SNS harus ditandai
- [SQS.1] Antrian Amazon SQS harus dienkripsi saat istirahat
- [SQS.2] Antrian SQS harus ditandai
- [SSM.1] Instans Amazon EC2 harus dikelola oleh AWS Systems Manager
- [SSM.2] Instans Amazon EC2 yang dikelola oleh Systems Manager harus memiliki status kepatuhan patch COMPLIANT setelah instalasi patch
- [SSM.3] Instans Amazon EC2 yang dikelola oleh Systems Manager harus memiliki status kepatuhan asosiasi COMPLIANT
- [StepFunctions.1] Mesin status Step Functions seharusnya mengaktifkan logging
- [Transfer.1] AWS Transfer Family alur kerja harus ditandai
- [Transfer.2] Server Transfer Family tidak boleh menggunakan protokol FTP untuk koneksi titik akhir
- [WAF.1] Pencatatan ACL Web Global AWS WAF Klasik harus diaktifkan
- [WAF.2] Aturan Regional AWS WAF Klasik harus memiliki setidaknya satu syarat
- [WAF.3] Kelompok aturan Regional AWS WAF Klasik harus memiliki setidaknya satu aturan
- [WAF.4] ACL web Regional AWS WAF klasik harus memiliki setidaknya satu aturan atau kelompok aturan
- [WAF.6] Aturan global AWS WAF klasik harus memiliki setidaknya satu syarat
- [WAF.7] Kelompok aturan global AWS WAF klasik harus memiliki setidaknya satu aturan
- [WAF.8] ACL web global AWS WAF klasik harus memiliki setidaknya satu aturan atau kelompok aturan
- [WAF.10] ACL AWS WAF web harus memiliki setidaknya satu aturan atau kelompok aturan
- [WAF.11] pencatatan ACL AWS WAF web harus diaktifkan

Asia Pasifik (Jakarta)

Kontrol berikut tidak didukung di Asia Pasifik (Jakarta).

- [Akun.2] Akun AWS harus menjadi bagian dari organisasi AWS Organizations
- [ApiGateway.1] API Gateway REST WebSocket dan pencatatan eksekusi API harus diaktifkan

- [ApiGateway.2] Tahapan API Gateway REST API harus dikonfigurasi untuk menggunakan sertifikat SSL untuk otentikasi backend
- [ApiGateway.3] Tahapan API Gateway REST API harus mengaktifkan penelusuran AWS X-Ray
- [ApiGateway.4] API Gateway harus dikaitkan dengan ACL Web WAF
- [ApiGateway.8] Rute API Gateway harus menentukan jenis otorisasi
- [ApiGateway.9] Pencatatan akses harus dikonfigurasi untuk Tahapan API Gateway V2
- [AppSync.2] AWS AppSync harus mengaktifkan logging tingkat lapangan
- [AppSync.5] AWS AppSync GraphQL API tidak boleh diautentikasi dengan kunci API
- [AutoScaling.3] Konfigurasi peluncuran grup Auto Scaling harus mengonfigurasi instans EC2 agar memerlukan Layanan Metadata Instans Versi 2 (IMDSv2)
- [AutoScaling.6] Grup Auto Scaling harus menggunakan beberapa jenis instance di beberapa Availability Zone
- [AutoScaling.9] Grup Auto Scaling Amazon EC2 harus menggunakan templat peluncuran Amazon EC2
- [Autoscaling.5] Instans Amazon EC2 yang diluncurkan menggunakan konfigurasi peluncuran grup Auto Scaling seharusnya tidak memiliki alamat IP Publik
- [Backup.1] titik AWS Backup pemulihan harus dienkripsi saat istirahat
- [Backup.2] poin AWS Backup pemulihan harus ditandai
- [Backup.4] rencana AWS Backup laporan harus ditandai
- [Backup.5] rencana AWS Backup cadangan harus ditandai
- [CloudFormation.2] CloudFormation tumpukan harus ditandai
- [CloudFront.1] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi
- [CloudFront.3] CloudFront distribusi harus memerlukan enkripsi dalam perjalanan
- [CloudFront.4] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi
- [CloudFront.5] CloudFront distribusi seharusnya mengaktifkan logging
- [CloudFront.6] CloudFront distribusi harus mengaktifkan WAF
- [CloudFront.7] CloudFront distribusi harus menggunakan sertifikat SSL/TLS khusus
- [CloudFront.8] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS
- [CloudFront.9] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus
- [CloudFront.10] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal khusus

- [CloudFront.12] CloudFront distribusi seharusnya tidak menunjukkan asal S3 yang tidak ada
- [CloudFront.13] CloudFront distribusi harus menggunakan kontrol akses asal
- [CloudFront.14] CloudFront distribusi harus ditandai
- [CloudWatch.17] tindakan CloudWatch alarm harus diaktifkan
- [CodeArtifact.1] CodeArtifact repositori harus diberi tag
- [CodeBuild.1] URL repositori sumber CodeBuild Bitbucket tidak boleh berisi kredensyal sensitif
- [CodeBuild.2] variabel lingkungan CodeBuild proyek tidak boleh berisi kredensil teks yang jelas
- [CodeBuild.3] Log CodeBuild S3 harus dienkripsi
- [CodeBuild.4] lingkungan CodeBuild proyek harus memiliki urasi logging AWS Config
- [DataFirehose.1] Aliran pengiriman Firehose harus dienkripsi saat istirahat
- [Detective.1] Grafik perilaku detektif harus diberi tag
- [DMS.1] Instans replikasi Layanan Migrasi Database tidak boleh bersifat publik
- [DMS.2] Sertifikat DMS harus ditandai
- [DMS.3] Langganan acara DMS harus ditandai
- [DMS.4] Contoh replikasi DMS harus ditandai
- [DMS.5] Grup subnet replikasi DMS harus ditandai
- [DMS.6] Instans replikasi DMS harus mengaktifkan peningkatan versi minor otomatis
- [DMS.7] Tugas replikasi DMS untuk database target seharusnya mengaktifkan logging
- [DMS.8] Tugas replikasi DMS untuk database sumber seharusnya mengaktifkan logging
- [DMS.9] Titik akhir DMS harus menggunakan SSL
- [DMS.10] Titik akhir DMS untuk database Neptunus harus mengaktifkan otorisasi IAM
- [DMS.11] Titik akhir DMS untuk MongoDB harus mengaktifkan mekanisme otentikasi
- [DMS.12] Titik akhir DMS untuk Redis harus mengaktifkan TLS
- [DocumentDB.1] Cluster Amazon DocumentDB harus dienkripsi saat istirahat
- [DocumentDB.2] Cluster Amazon DocumentDB harus memiliki periode retensi cadangan yang memadai
- [DocumentDB.3] Cuplikan cluster manual Amazon DocumentDB seharusnya tidak bersifat publik
- [DocumentDB.4] Cluster Amazon DocumentDB harus mempublikasikan log audit ke Log CloudWatch
- [DocumentDB.5] Cluster Amazon DocumentDB harus mengaktifkan perlindungan penghapusan
- [DynamoDB.3] Cluster DynamoDB Accelerator (DAX) harus dienkripsi saat istirahat

- [DynamoDB.4] Tabel DynamoDB harus ada dalam rencana cadangan
- [DynamoDB.7] Cluster DynamoDB Accelerator harus dienkripsi saat transit
- [EC2.13] Grup keamanan tidak boleh mengizinkan masuknya dari 0.0.0.0/0 atau: :/0 ke port 22
- [EC2.14] Grup keamanan tidak boleh mengizinkan masuknya dari 0.0.0.0/0 atau: :/0 ke port 3389
- [EC2.18] Grup keamanan seharusnya hanya mengizinkan lalu lintas masuk yang tidak terbatas untuk port resmi
- [EC2.22] Grup keamanan Amazon EC2 yang tidak digunakan harus dihapus
- [EC2.23] Amazon EC2 Transit Gateways seharusnya tidak secara otomatis menerima permintaan lampiran VPC
- [EC2.24] Jenis instans paravirtual Amazon EC2 tidak boleh digunakan
- [EC2.28] Volume EBS harus dicakup oleh rencana cadangan
- [EC2.51] Titik akhir EC2 Client VPN harus mengaktifkan pencatatan koneksi klien
- [ECR.1] Repositori pribadi ECR harus memiliki pemindaian gambar yang dikonfigurasi
- [ECR.2] Repositori pribadi ECR harus memiliki kekekalan tag yang dikonfigurasi
- [ECR.3] Repositori ECR harus memiliki setidaknya satu kebijakan siklus hidup yang dikonfigurasi
- [ECR.4] Repositori publik ECR harus ditandai
- [ECS.2] Layanan ECS seharusnya tidak memiliki alamat IP publik yang ditetapkan kepadanya secara otomatis
- [ECS.3] Definisi tugas ECS tidak boleh membagikan namespace proses host
- [ECS.4] Kontainer ECS harus berjalan sebagai non-hak istimewa
- [ECS.5] Wadah ECS harus dibatasi pada akses hanya-baca ke sistem file root
- [ECS.8] Rahasia tidak boleh diteruskan sebagai variabel lingkungan kontainer
- [ECS.9] Definisi tugas ECS harus memiliki konfigurasi logging
- [ECS.10] Layanan ECS Fargate harus berjalan pada versi platform Fargate terbaru
- [ECS.12] Cluster ECS harus menggunakan Wawasan Kontainer
- [EFS.1] Sistem File Elastis harus dikonfigurasi untuk mengenkripsi data file saat istirahat menggunakan AWS KMS
- [EFS.2] Volume Amazon EFS harus dalam rencana cadangan
- [EFS.3] Titik akses EFS harus menegakkan direktori root
- [EFS.4] Titik akses EFS harus menegakkan identitas pengguna
- [EFS.6] Target pemasangan EFS tidak boleh dikaitkan dengan subnet publik

- [EKS.1] Titik akhir klaster EKS seharusnya tidak dapat diakses publik
- [EKS.2] Kluster EKS harus berjalan pada versi Kubernetes yang didukung
- [EKS.3] Kluster EKS harus menggunakan rahasia Kubernetes terenkripsi
- [ELB.12] Application Load Balancer harus dikonfigurasi dengan mode mitigasi desync defensif atau paling ketat
- [ELB.13] Penyeimbang Beban Aplikasi, Jaringan, dan Gateway harus mencakup beberapa Availability Zone
- [ELB.14] Classic Load Balancer harus dikonfigurasi dengan mode mitigasi desync defensif atau paling ketat
- [ElastiCache.1] Cluster ElastiCache Redis harus mengaktifkan pencadangan otomatis
- [ElastiCache.6] ElastiCache untuk grup replikasi Redis sebelum versi 6.0 harus menggunakan Redis AUTH
- [ElastiCache.7] ElastiCache cluster tidak boleh menggunakan grup subnet default
- [ElasticBeanstalk.1] Lingkungan Elastic Beanstalk seharusnya mengaktifkan pelaporan kesehatan yang ditingkatkan
- [ElasticBeanstalk.2] Pembaruan platform yang dikelola Elastic Beanstalk harus diaktifkan
- [EMR.1] Node primer cluster EMR Amazon seharusnya tidak memiliki alamat IP publik
- [ES.1] Domain Elasticsearch harus mengaktifkan enkripsi saat istirahat
- [ES.2] Domain Elasticsearch tidak boleh diakses publik
- [ES.3] Domain Elasticsearch harus mengenkripsi data yang dikirim antar node
- [EventBridge.4] titik akhir EventBridge global harus mengaktifkan replikasi acara
- [FSX.1] FSx untuk sistem file OpenZFS harus dikonfigurasi untuk menyalin tag ke cadangan dan volume
- [FSX.2] Sistem file FSx for Lustre harus dikonfigurasi untuk menyalin tag ke cadangan
- [GlobalAccelerator.1] Akselerator Akselerator Global harus diberi tag
- AWS Glue Pekerjaan [Glue.1] harus ditandai
- [GuardDuty.2] GuardDuty filter harus diberi tag
- [GuardDuty.3] GuardDuty IPset harus ditandai
- [GuardDuty.4] GuardDuty detektor harus ditandai
- [IAM.18] Memastikan peran dukungan telah dibuat untuk mengelola insiden dengan AWS Support
- [IAM.26] Sertifikat SSL/TLS kedaluwarsa yang dikelola di IAM harus dihapus

- [IoT.1] profil AWS IoT Core keamanan harus ditandai
- [IoT.2] tindakan AWS IoT Core mitigasi harus ditandai
- AWS IoT Core Dimensi [IoT.3] harus ditandai
- [IoT.4] AWS IoT Core otorisasi harus diberi tag
- [IoT.5] alias AWS IoT Core peran harus ditandai
- AWS IoT Core Kebijakan [IoT.6] harus ditandai
- [Kinesis.1] Aliran kinesis harus dienkripsi saat istirahat
- [Lambda.5] Fungsi VPC Lambda harus beroperasi di beberapa Availability Zone
- [Macie.1] Amazon Macie harus diaktifkan
- [Macie.2] Penemuan data sensitif otomatis Macie harus diaktifkan
- [MQ.2] Broker ActiveMQ harus mengalirkan log audit ke CloudWatch
- [MQ.3] Broker Amazon MQ harus mengaktifkan peningkatan versi minor otomatis
- [MSK.1] Cluster MSK harus dienkripsi saat transit di antara node broker
- [MSK.2] Kluster MSK seharusnya telah meningkatkan pemantauan yang dikonfigurasi
- [Neptunus.1] Cluster DB Neptunus harus dienkripsi saat istirahat
- [Neptune.2] Cluster DB Neptunus harus menerbitkan log audit ke Log CloudWatch
- [Neptune.3] Snapshot cluster Neptunus DB seharusnya tidak publik
- [Neptunus.4] Cluster DB Neptunus harus mengaktifkan perlindungan penghapusan
- [Neptunus.5] Cluster DB Neptunus harus mengaktifkan cadangan otomatis
- [Neptune.6] Snapshot cluster Neptunus DB harus dienkripsi saat istirahat
- [Neptunus.7] Cluster DB Neptunus harus mengaktifkan otentikasi basis data IAM
- [Neptunus.8] Cluster DB Neptunus harus dikonfigurasi untuk menyalin tag ke snapshot
- [Neptunus.9] Cluster DB Neptunus harus digunakan di beberapa Availability Zone
- [NetworkFirewall.1] Firewall Firewall Jaringan harus digunakan di beberapa Availability Zone
- [NetworkFirewall.3] Kebijakan Network Firewall harus memiliki setidaknya satu kelompok aturan yang terkait
- [NetworkFirewall.4] Tindakan stateless default untuk kebijakan Network Firewall harus drop atau forward untuk paket penuh
- [NetworkFirewall.5] Tindakan stateless default untuk kebijakan Network Firewall harus drop atau forward untuk paket yang terfragmentasi
- [NetworkFirewall.6] Grup aturan Stateless Network Firewall tidak boleh kosong

- [Opensearch.1] OpenSearch domain harus mengaktifkan enkripsi saat istirahat
- [Opensearch.2] OpenSearch domain tidak boleh diakses publik
- [Opensearch.3] OpenSearch domain harus mengenkripsi data yang dikirim antar node
- [Opensearch.4] login kesalahan OpenSearch domain ke Log harus diaktifkan CloudWatch
- [Opensearch.5] OpenSearch domain harus mengaktifkan pencatatan audit
- [Opensearch.6] OpenSearch domain harus memiliki setidaknya tiga node data
- [Opensearch.7] OpenSearch domain harus mengaktifkan kontrol akses berbutir halus
- [Opensearch.8] Koneksi ke OpenSearch domain harus dienkripsi menggunakan kebijakan keamanan TLS terbaru
- [Opensearch.11] OpenSearch domain harus memiliki setidaknya tiga node primer khusus
- [RDS.9] Instans RDS DB harus menerbitkan log ke Log CloudWatch
- [RDS.14] Cluster Amazon Aurora seharusnya mengaktifkan backtracking
- [RDS.16] Cluster RDS DB harus dikonfigurasi untuk menyalin tag ke snapshot
- [RDS.24] Kluster Database RDS harus menggunakan nama pengguna administrator khusus
- [RDS.26] Instans RDS DB harus dilindungi oleh rencana cadangan
- [RDS.31] Grup keamanan RDS DB harus ditandai
- [Redshift.1] Cluster Amazon Redshift harus melarang akses publik
- [Redshift.2] Koneksi ke cluster Amazon Redshift harus dienkripsi saat transit
- [Redshift.3] Cluster Amazon Redshift harus mengaktifkan snapshot otomatis
- [Redshift.7] Cluster Redshift harus menggunakan perutean VPC yang ditingkatkan
- [Redshift.9] Cluster Redshift tidak boleh menggunakan nama database default
- [Redshift.10] Cluster Redshift harus dienkripsi saat istirahat
- [Redshift.12] Langganan pemberitahuan acara Redshift harus ditandai
- [Redshift.15] Grup keamanan Redshift harus mengizinkan masuknya port cluster hanya dari asal yang dibatasi
- [Route53.1] Pemeriksaan kesehatan rute 53 harus ditandai
- [Route53.2] Route 53 zona yang dihosting publik harus mencatat kueri DNS
- [S3.11] Bucket tujuan umum S3 harus mengaktifkan pemberitahuan acara
- [S3.13] Bucket tujuan umum S3 harus memiliki konfigurasi Siklus Hidup
- [SageMaker.1] Instans SageMaker notebook Amazon seharusnya tidak memiliki akses internet langsung

- [SageMaker.2] instance SageMaker notebook harus diluncurkan dalam VPC khusus
- [SageMaker.3] Pengguna seharusnya tidak memiliki akses root ke instance SageMaker notebook
- [SageMaker.4] varian produksi SageMaker titik akhir harus memiliki jumlah instance awal yang lebih besar dari 1
- [ServiceCatalog.1] Portofolio Service Catalog harus dibagikan hanya dalam suatu organisasi AWS
- [SNS.3] Topik SNS harus ditandai
- [SQS.1] Antrian Amazon SQS harus dienkripsi saat istirahat
- [SQS.2] Antrian SQS harus ditandai
- [SSM.1] Instans Amazon EC2 harus dikelola oleh AWS Systems Manager
- [SSM.2] Instans Amazon EC2 yang dikelola oleh Systems Manager harus memiliki status kepatuhan patch COMPLIANT setelah instalasi patch
- [SSM.3] Instans Amazon EC2 yang dikelola oleh Systems Manager harus memiliki status kepatuhan asosiasi COMPLIANT
- [Transfer.2] Server Transfer Family tidak boleh menggunakan protokol FTP untuk koneksi titik akhir
- [WAF.1] Pencatatan ACL Web Global AWS WAF Klasik harus diaktifkan
- [WAF.2] Aturan Regional AWS WAF Klasik harus memiliki setidaknya satu syarat
- [WAF.3] Kelompok aturan Regional AWS WAF Klasik harus memiliki setidaknya satu aturan
- [WAF.4] ACL web Regional AWS WAF klasik harus memiliki setidaknya satu aturan atau kelompok aturan
- [WAF.6] Aturan global AWS WAF klasik harus memiliki setidaknya satu syarat
- [WAF.7] Kelompok aturan global AWS WAF klasik harus memiliki setidaknya satu aturan
- [WAF.8] ACL web global AWS WAF klasik harus memiliki setidaknya satu aturan atau kelompok aturan
- [WAF.10] ACL AWS WAF web harus memiliki setidaknya satu aturan atau kelompok aturan
- [WAF.11] pencatatan ACL AWS WAF web harus diaktifkan

Asia Pasifik (Mumbai)

Kontrol berikut tidak didukung di Asia Pasifik (Mumbai).

- [CloudFront.1] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi
- [CloudFront.3] CloudFront distribusi harus memerlukan enkripsi dalam perjalanan

- [CloudFront.4] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi
- [CloudFront.5] CloudFront distribusi seharusnya mengaktifkan logging
- [CloudFront.6] CloudFront distribusi harus mengaktifkan WAF
- [CloudFront.7] CloudFront distribusi harus menggunakan sertifikat SSL/TLS khusus
- [CloudFront.8] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS
- [CloudFront.9] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus
- [CloudFront.10] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal khusus
- [CloudFront.12] CloudFront distribusi seharusnya tidak menunjukkan asal S3 yang tidak ada
- [CloudFront.13] CloudFront distribusi harus menggunakan kontrol akses asal
- [CloudFront.14] CloudFront distribusi harus ditandai
- [DataFirehose.1] Aliran pengiriman Firehose harus dienkripsi saat istirahat
- [DMS.10] Titik akhir DMS untuk database Neptunus harus mengaktifkan otorisasi IAM
- [DMS.11] Titik akhir DMS untuk MongoDB harus mengaktifkan mekanisme otentikasi
- [DMS.12] Titik akhir DMS untuk Redis harus mengaktifkan TLS
- [DynamoDB.7] Cluster DynamoDB Accelerator harus dienkripsi saat transit
- [EC2.23] Amazon EC2 Transit Gateways seharusnya tidak secara otomatis menerima permintaan lampiran VPC
- [EC2.24] Jenis instans paravirtual Amazon EC2 tidak boleh digunakan
- [ECR.4] Repositori publik ECR harus ditandai
- [EFS.6] Target pemasangan EFS tidak boleh dikaitkan dengan subnet publik
- [EKS.3] Kluster EKS harus menggunakan rahasia Kubernetes terenkripsi
- [FSX.2] Sistem file FSx for Lustre harus dikonfigurasi untuk menyalin tag ke cadangan
- [GlobalAccelerator.1] Akselerator Akselerator Global harus diberi tag
- [IAM.26] Sertifikat SSL/TLS kedaluwarsa yang dikelola di IAM harus dihapus
- [MQ.2] Broker ActiveMQ harus mengalirkan log audit ke CloudWatch
- [MQ.3] Broker Amazon MQ harus mengaktifkan peningkatan versi minor otomatis
- [Opensearch.11] OpenSearch domain harus memiliki setidaknya tiga node primer khusus
- [RDS.31] Grup keamanan RDS DB harus ditandai
- [Redshift.15] Grup keamanan Redshift harus mengizinkan masuknya port cluster hanya dari asal yang dibatasi

- [Route53.1] Pemeriksaan kesehatan rute 53 harus ditandai
- [Route53.2] Route 53 zona yang dihosting publik harus mencatat kueri DNS
- [SageMaker.4] varian produksi SageMaker titik akhir harus memiliki jumlah instance awal yang lebih besar dari 1
- [ServiceCatalog.1] Portofolio Service Catalog harus dibagikan hanya dalam suatu organisasi AWS
- [Transfer.2] Server Transfer Family tidak boleh menggunakan protokol FTP untuk koneksi titik akhir
- [WAF.1] Pencatatan ACL Web Global AWS WAF Klasik harus diaktifkan
- [WAF.6] Aturan global AWS WAF klasik harus memiliki setidaknya satu syarat
- [WAF.7] Kelompok aturan global AWS WAF klasik harus memiliki setidaknya satu aturan
- [WAF.8] ACL web global AWS WAF klasik harus memiliki setidaknya satu aturan atau kelompok aturan

Asia Pasifik (Melbourne)

Kontrol berikut tidak didukung di Asia Pasifik (Melbourne).

- [ACM.1] Sertifikat yang diimpor dan diterbitkan ACM harus diperbarui setelah jangka waktu tertentu
- [ACM.2] Sertifikat RSA yang dikelola oleh ACM harus menggunakan panjang kunci minimal 2.048 bit
- [ApiGateway.4] API Gateway harus dikaitkan dengan ACL Web WAF
- [ApiGateway.8] Rute API Gateway harus menentukan jenis otorisasi
- [ApiGateway.9] Pencatatan akses harus dikonfigurasi untuk Tahapan API Gateway V2
- [AppSync.2] AWS AppSync harus mengaktifkan logging tingkat lapangan
- [AppSync.4] AWS AppSync GraphQL API harus diberi tag
- [AppSync.5] AWS AppSync GraphQL API tidak boleh diautentikasi dengan kunci API
- [Athena.2] Katalog data Athena harus diberi tag
- [Athena.3] Kelompok kerja Athena harus ditandai
- [AutoScaling.1] Grup Auto Scaling yang terkait dengan penyeimbang beban harus menggunakan pemeriksaan kesehatan ELB
- [Autoscaling.5] Instans Amazon EC2 yang diluncurkan menggunakan konfigurasi peluncuran grup Auto Scaling seharusnya tidak memiliki alamat IP Publik
- [Backup.1] titik AWS Backup pemulihan harus dienkripsi saat istirahat

- [Backup.2] poin AWS Backup pemulihan harus ditandai
- [Backup.3] AWS Backup brankas harus ditandai
- [Backup.4] rencana AWS Backup laporan harus ditandai
- [Backup.5] rencana AWS Backup cadangan harus ditandai
- [CloudFormation.2] CloudFormation tumpukan harus ditandai
- [CloudFront.1] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi
- [CloudFront.3] CloudFront distribusi harus memerlukan enkripsi dalam perjalanan
- [CloudFront.4] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi
- [CloudFront.5] CloudFront distribusi seharusnya mengaktifkan logging
- [CloudFront.6] CloudFront distribusi harus mengaktifkan WAF
- [CloudFront.7] CloudFront distribusi harus menggunakan sertifikat SSL/TLS khusus
- [CloudFront.8] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS
- [CloudFront.9] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus
- [CloudFront.10] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal khusus
- [CloudFront.12] CloudFront distribusi seharusnya tidak menunjukkan asal S3 yang tidak ada
- [CloudFront.13] CloudFront distribusi harus menggunakan kontrol akses asal
- [CloudFront.14] CloudFront distribusi harus ditandai
- [CodeArtifact.1] CodeArtifact repositori harus diberi tag
- [CodeBuild.1] URL repositori sumber CodeBuild Bitbucket tidak boleh berisi kredensyal sensitif
- [CodeBuild.2] variabel lingkungan CodeBuild proyek tidak boleh berisi kredensil teks yang jelas
- [CodeBuild.3] Log CodeBuild S3 harus dienkripsi
- [CodeBuild.4] lingkungan CodeBuild proyek harus memiliki urasi logging AWS Config
- [DataFirehose.1] Aliran pengiriman Firehose harus dienkripsi saat istirahat
- [Detective.1] Grafik perilaku detektif harus diberi tag
- [DMS.1] Instans replikasi Layanan Migrasi Database tidak boleh bersifat publik
- [DMS.2] Sertifikat DMS harus ditandai
- [DMS.3] Langganan acara DMS harus ditandai
- [DMS.4] Contoh replikasi DMS harus ditandai
- [DMS.5] Grup subnet replikasi DMS harus ditandai
- [DMS.6] Instans replikasi DMS harus mengaktifkan peningkatan versi minor otomatis

- [DMS.7] Tugas replikasi DMS untuk database target seharusnya mengaktifkan logging
- [DMS.8] Tugas replikasi DMS untuk database sumber seharusnya mengaktifkan logging
- [DMS.9] Titik akhir DMS harus menggunakan SSL
- [DMS.10] Titik akhir DMS untuk database Neptunus harus mengaktifkan otorisasi IAM
- [DMS.11] Titik akhir DMS untuk MongoDB harus mengaktifkan mekanisme otentikasi
- [DMS.12] Titik akhir DMS untuk Redis harus mengaktifkan TLS
- [DocumentDB.1] Cluster Amazon DocumentDB harus dienkripsi saat istirahat
- [DocumentDB.2] Cluster Amazon DocumentDB harus memiliki periode retensi cadangan yang memadai
- [DocumentDB.3] Cuplikan cluster manual Amazon DocumentDB seharusnya tidak bersifat publik
- [DocumentDB.4] Cluster Amazon DocumentDB harus mempublikasikan log audit ke Log CloudWatch
- [DocumentDB.5] Cluster Amazon DocumentDB harus mengaktifkan perlindungan penghapusan
- [DynamoDB.3] Cluster DynamoDB Accelerator (DAX) harus dienkripsi saat istirahat
- [DynamoDB.4] Tabel DynamoDB harus ada dalam rencana cadangan
- [DynamoDB.7] Cluster DynamoDB Accelerator harus dienkripsi saat transit
- [EC2.1] Snapshot Amazon EBS tidak boleh dipulihkan secara publik
- [EC2.4] Instans EC2 yang dihentikan harus dihapus setelah periode waktu tertentu
- [EC2.8] Instans EC2 harus menggunakan Layanan Metadata Instance Versi 2 (IMDSv2)
- [EC2.9] Instans Amazon EC2 seharusnya tidak memiliki alamat IPv4 publik
- [EC2.13] Grup keamanan tidak boleh mengizinkan masuknya dari 0.0.0.0/0 atau: :/0 ke port 22
- [EC2.14] Grup keamanan tidak boleh mengizinkan masuknya dari 0.0.0.0/0 atau: :/0 ke port 3389
- [EC2.18] Grup keamanan seharusnya hanya mengizinkan lalu lintas masuk yang tidak terbatas untuk port resmi
- [EC2.22] Grup keamanan Amazon EC2 yang tidak digunakan harus dihapus
- [EC2.23] Amazon EC2 Transit Gateways seharusnya tidak secara otomatis menerima permintaan lampiran VPC
- [EC2.24] Jenis instans paravirtual Amazon EC2 tidak boleh digunakan
- [EC2.25] Templat peluncuran Amazon EC2 tidak boleh menetapkan IP publik ke antarmuka jaringan
- [EC2.28] Volume EBS harus dicakup oleh rencana cadangan

- [EC2.33] Lampiran gateway transit EC2 harus ditandai
- [EC2.34] Tabel rute gateway transit EC2 harus ditandai
- [EC2.40] Gerbang EC2 NAT harus ditandai
- [EC2.48] Log aliran VPC Amazon harus ditandai
- [EC2.51] Titik akhir EC2 Client VPN harus mengaktifkan pencatatan koneksi klien
- [EC2.52] Gerbang transit EC2 harus ditandai
- [ECR.1] Repositori pribadi ECR harus memiliki pemindaian gambar yang dikonfigurasi
- [ECR.4] Repositori publik ECR harus ditandai
- [ECS.1] Definisi tugas Amazon ECS harus memiliki mode jaringan yang aman dan definisi pengguna.
- [ECS.9] Definisi tugas ECS harus memiliki konfigurasi logging
- [EFS.1] Sistem File Elastis harus dikonfigurasi untuk mengenkripsi data file saat istirahat menggunakan AWS KMS
- [EFS.2] Volume Amazon EFS harus dalam rencana cadangan
- [EFS.3] Titik akses EFS harus menegakkan direktori root
- [EFS.4] Titik akses EFS harus menegakkan identitas pengguna
- [EFS.5] Titik akses EFS harus ditandai
- [EFS.6] Target pemasangan EFS tidak boleh dikaitkan dengan subnet publik
- [EKS.1] Titik akhir klaster EKS seharusnya tidak dapat diakses publik
- [EKS.2] Kluster EKS harus berjalan pada versi Kubernetes yang didukung
- [EKS.3] Kluster EKS harus menggunakan rahasia Kubernetes terenkripsi
- [EKS.6] Kluster EKS harus ditandai
- [EKS.7] Konfigurasi penyedia identitas EKS harus ditandai
- [EKS.8] Kluster EKS harus mengaktifkan pencatatan audit
- [ELB.13] Penyeimbang Beban Aplikasi, Jaringan, dan Gateway harus mencakup beberapa Availability Zone
- [ELB.14] Classic Load Balancer harus dikonfigurasi dengan mode mitigasi desync defensif atau paling ketat
- [ElastiCache.1] Cluster ElastiCache Redis harus mengaktifkan pencadangan otomatis
- [ElastiCache.2] ElastiCache untuk kluster cache Redis harus mengaktifkan peningkatan versi minor otomatis

- [ElastiCache.3] ElastiCache untuk grup replikasi Redis harus mengaktifkan failover otomatis
- [ElastiCache.4] ElastiCache untuk grup replikasi Redis harus dienkripsi saat istirahat
- [ElastiCache.5] ElastiCache untuk grup replikasi Redis harus dienkripsi saat transit
- [ElastiCache.6] ElastiCache untuk grup replikasi Redis sebelum versi 6.0 harus menggunakan Redis AUTH
- [ElastiCache.7] ElastiCache cluster tidak boleh menggunakan grup subnet default
- [ElasticBeanstalk.1] Lingkungan Elastic Beanstalk seharusnya mengaktifkan pelaporan kesehatan yang ditingkatkan
- [ElasticBeanstalk.2] Pembaruan platform yang dikelola Elastic Beanstalk harus diaktifkan
- [ElasticBeanstalk.3] Elastic Beanstalk harus mengalirkan log ke CloudWatch
- [EMR.1] Node primer cluster EMR Amazon seharusnya tidak memiliki alamat IP publik
- [ES.1] Domain Elasticsearch harus mengaktifkan enkripsi saat istirahat
- [ES.2] Domain Elasticsearch tidak boleh diakses publik
- [ES.3] Domain Elasticsearch harus mengenkripsi data yang dikirim antar node
- [ES.4] Kesalahan domain Elasticsearch yang masuk ke CloudWatch Log harus diaktifkan
- [EventBridge.2] bus EventBridge acara harus diberi tag
- [EventBridge.3] bus acara EventBridge khusus harus memiliki kebijakan berbasis sumber daya terlampir
- [EventBridge.4] titik akhir EventBridge global harus mengaktifkan replikasi acara
- [FSX.1] FSx untuk sistem file OpenZFS harus dikonfigurasi untuk menyalin tag ke cadangan dan volume
- [FSX.2] Sistem file FSx for Lustre harus dikonfigurasi untuk menyalin tag ke cadangan
- [GlobalAccelerator.1] Akselerator Akselerator Global harus diberi tag
- AWS Glue Pekerjaan [Glue.1] harus ditandai
- [GuardDuty.2] GuardDuty filter harus diberi tag
- [GuardDuty.3] GuardDuty IPset harus ditandai
- [GuardDuty.4] GuardDuty detektor harus ditandai
- [IAM.1] Kebijakan IAM seharusnya tidak mengizinkan hak administratif “*” penuh
- [IAM.2] Pengguna IAM seharusnya tidak memiliki kebijakan IAM yang dilampirkan
- [IAM.3] Kunci akses pengguna IAM harus diputar setiap 90 hari atau kurang

- [IAM.5] MFA harus diaktifkan untuk semua pengguna IAM yang memiliki kata sandi konsol
- [IAM.6] MFA perangkat keras harus diaktifkan untuk pengguna root
- [IAM.7] Kebijakan kata sandi untuk pengguna IAM harus memiliki konfigurasi yang kuat
- [IAM.8] Kredensyal pengguna IAM yang tidak digunakan harus dihapus
- [IAM.10] Kebijakan kata sandi untuk pengguna IAM harus memiliki urasi yang kuat AWS Config
- [IAM.11] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu huruf besar
- [IAM.12] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu huruf kecil
- [IAM.13] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu simbol
- [IAM.14] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu nomor
- [IAM.15] Pastikan kebijakan kata sandi IAM membutuhkan panjang kata sandi minimum 14 atau lebih
- [IAM.16] Pastikan kebijakan kata sandi IAM mencegah penggunaan kembali kata sandi
- [IAM.17] Pastikan kebijakan kata sandi IAM kedaluwarsa kata sandi dalam waktu 90 hari atau kurang
- [IAM.18] Memastikan peran dukungan telah dibuat untuk mengelola insiden dengan AWS Support
- [IAM.19] MFA harus diaktifkan untuk semua pengguna IAM
- [IAM.21] Kebijakan terkelola pelanggan IAM yang Anda buat seharusnya tidak mengizinkan tindakan wildcard untuk layanan
- [IAM.22] Kredensyal pengguna IAM yang tidak digunakan selama 45 hari harus dihapus
- [IAM.24] Peran IAM harus ditandai
- [IAM.25] Pengguna IAM harus diberi tag
- [IAM.26] Sertifikat SSL/TLS kedaluwarsa yang dikelola di IAM harus dihapus
- [IAM.27] Identitas IAM seharusnya tidak memiliki kebijakan yang dilampirkan AWSCloudShellFullAccess
- [IoT.1] profil AWS IoT Core keamanan harus ditandai
- [IoT.2] tindakan AWS IoT Core mitigasi harus ditandai
- AWS IoT Core Dimensi [IoT.3] harus ditandai
- [IoT.4] AWS IoT Core otorisasi harus diberi tag
- [IoT.5] alias AWS IoT Core peran harus ditandai
- AWS IoT Core Kebijakan [IoT.6] harus ditandai
- [Kinesis.1] Aliran kinesis harus dienkripsi saat istirahat

- [KMS.1] Kebijakan yang dikelola pelanggan IAM tidak boleh mengizinkan tindakan dekripsi pada semua kunci KMS
- [KMS.2] Prinsipal IAM tidak boleh memiliki kebijakan inline IAM yang memungkinkan tindakan dekripsi pada semua kunci KMS
- [Lambda.5] Fungsi VPC Lambda harus beroperasi di beberapa Availability Zone
- [Macie.1] Amazon Macie harus diaktifkan
- [Macie.2] Penemuan data sensitif otomatis Macie harus diaktifkan
- [MQ.2] Broker ActiveMQ harus mengalirkan log audit ke CloudWatch
- [MQ.3] Broker Amazon MQ harus mengaktifkan peningkatan versi minor otomatis
- [MQ.4] Broker Amazon MQ harus diberi tag
- [MQ.5] Broker ActiveMQ harus menggunakan mode penerapan aktif/siaga
- [MQ.6] Broker RabbitMQ harus menggunakan mode penerapan cluster
- [MSK.1] Cluster MSK harus dienkripsi saat transit di antara node broker
- [MSK.2] Kluster MSK seharusnya telah meningkatkan pemantauan yang dikonfigurasi
- [Neptunus.1] Cluster DB Neptunus harus dienkripsi saat istirahat
- [Neptune.2] Cluster DB Neptunus harus menerbitkan log audit ke Log CloudWatch
- [Neptune.3] Snapshot cluster Neptunus DB seharusnya tidak publik
- [Neptunus.4] Cluster DB Neptunus harus mengaktifkan perlindungan penghapusan
- [Neptunus.5] Cluster DB Neptunus harus mengaktifkan cadangan otomatis
- [Neptune.6] Snapshot cluster Neptunus DB harus dienkripsi saat istirahat
- [Neptunus.7] Cluster DB Neptunus harus mengaktifkan otentikasi basis data IAM
- [Neptunus.8] Cluster DB Neptunus harus dikonfigurasi untuk menyalin tag ke snapshot
- [Neptunus.9] Cluster DB Neptunus harus digunakan di beberapa Availability Zone
- [NetworkFirewall.1] Firewall Firewall Jaringan harus digunakan di beberapa Availability Zone
- [NetworkFirewall.2] Pencatatan Firewall Jaringan harus diaktifkan
- [NetworkFirewall.3] Kebijakan Network Firewall harus memiliki setidaknya satu kelompok aturan yang terkait
- [NetworkFirewall.4] Tindakan stateless default untuk kebijakan Network Firewall harus drop atau forward untuk paket penuh
- [NetworkFirewall.5] Tindakan stateless default untuk kebijakan Network Firewall harus drop atau forward untuk paket yang terfragmentasi

- [NetworkFirewall.6] Grup aturan Stateless Network Firewall tidak boleh kosong
- [NetworkFirewall.9] Firewall Firewall Jaringan harus mengaktifkan perlindungan penghapusan
- [Opensearch.1] OpenSearch domain harus mengaktifkan enkripsi saat istirahat
- [Opensearch.2] OpenSearch domain tidak boleh diakses publik
- [Opensearch.3] OpenSearch domain harus mengenkripsi data yang dikirim antar node
- [Opensearch.4] login kesalahan OpenSearch domain ke Log harus diaktifkan CloudWatch
- [Opensearch.5] OpenSearch domain harus mengaktifkan pencatatan audit
- [Opensearch.6] OpenSearch domain harus memiliki setidaknya tiga node data
- [Opensearch.7] OpenSearch domain harus mengaktifkan kontrol akses berbutir halus
- [Opensearch.8] Koneksi ke OpenSearch domain harus dienkripsi menggunakan kebijakan keamanan TLS terbaru
- [Opensearch.9] domain harus ditandai OpenSearch
- [Opensearch.10] OpenSearch domain harus memiliki pembaruan perangkat lunak terbaru yang diinstal
- [Opensearch.11] OpenSearch domain harus memiliki setidaknya tiga node primer khusus
- [RDS.1] Snapshot RDS harus pribadi
- [RDS.3] Instans RDS DB harus mengaktifkan enkripsi saat istirahat
- [RDS.7] Cluster RDS harus mengaktifkan perlindungan penghapusan
- [RDS.12] Otentikasi IAM harus dikonfigurasi untuk cluster RDS
- [RDS.14] Cluster Amazon Aurora seharusnya mengaktifkan backtracking
- [RDS.15] Cluster RDS DB harus dikonfigurasi untuk beberapa Availability Zone
- [RDS.16] Cluster RDS DB harus dikonfigurasi untuk menyalin tag ke snapshot
- [RDS.24] Kluster Database RDS harus menggunakan nama pengguna administrator khusus
- [RDS.26] Instans RDS DB harus dilindungi oleh rencana cadangan
- [RDS.27] Cluster RDS DB harus dienkripsi saat istirahat
- [RDS.28] Cluster RDS DB harus ditandai
- [RDS.31] Grup keamanan RDS DB harus ditandai
- [RDS.34] Cluster Aurora MySQL DB harus menerbitkan log audit ke Log CloudWatch
- [RDS.35] Cluster RDS DB harus mengaktifkan peningkatan versi minor otomatis
- [Redshift.12] Langganan pemberitahuan acara Redshift harus ditandai

- [Redshift.15] Grup keamanan Redshift harus mengizinkan masuknya port cluster hanya dari asal yang dibatasi
- [Route53.1] Pemeriksaan kesehatan rute 53 harus ditandai
- [Route53.2] Route 53 zona yang dihosting publik harus mencatat kueri DNS
- [S3.14] Bucket tujuan umum S3 harus mengaktifkan versi
- [S3.15] Bucket tujuan umum S3 harus mengaktifkan Object Lock
- [SageMaker.1] Instans SageMaker notebook Amazon seharusnya tidak memiliki akses internet langsung
- [SageMaker.2] instance SageMaker notebook harus diluncurkan dalam VPC khusus
- [SageMaker.3] Pengguna seharusnya tidak memiliki akses root ke instance SageMaker notebook
- [SageMaker.4] varian produksi SageMaker titik akhir harus memiliki jumlah instance awal yang lebih besar dari 1
- [SES.1] Daftar kontak SES harus ditandai
- [SES.2] Set konfigurasi SES harus ditandai
- [ServiceCatalog.1] Portofolio Service Catalog harus dibagikan hanya dalam suatu organisasi AWS
- [SNS.1] Topik SNS harus dienkripsi saat istirahat menggunakan AWS KMS
- [SNS.3] Topik SNS harus ditandai
- [SQS.1] Antrian Amazon SQS harus dienkripsi saat istirahat
- [SQS.2] Antrian SQS harus ditandai
- [SSM.2] Instans Amazon EC2 yang dikelola oleh Systems Manager harus memiliki status kepatuhan patch COMPLIANT setelah instalasi patch
- [SSM.3] Instans Amazon EC2 yang dikelola oleh Systems Manager harus memiliki status kepatuhan asosiasi COMPLIANT
- [SSM.4] Dokumen SSM seharusnya tidak bersifat publik
- [StepFunctions.1] Mesin status Step Functions seharusnya mengaktifkan logging
- [StepFunctions.2] Aktivitas Step Functions harus diberi tag
- [Transfer.1] AWS Transfer Family alur kerja harus ditandai
- [Transfer.2] Server Transfer Family tidak boleh menggunakan protokol FTP untuk koneksi titik akhir
- [WAF.1] Pencatatan ACL Web Global AWS WAF Klasik harus diaktifkan
- [WAF.6] Aturan global AWS WAF klasik harus memiliki setidaknya satu syarat
- [WAF.7] Kelompok aturan global AWS WAF klasik harus memiliki setidaknya satu aturan

- [WAF.8] ACL web global AWS WAF klasik harus memiliki setidaknya satu aturan atau kelompok aturan
- [WAF.11] pencatatan ACL AWS WAF web harus diaktifkan

Asia Pasifik (Osaka)

Kontrol berikut tidak didukung di Asia Pasifik (Osaka).

- [ACM.1] Sertifikat yang diimpor dan diterbitkan ACM harus diperbarui setelah jangka waktu tertentu
- [Akun.2] Akun AWS harus menjadi bagian dari organisasi AWS Organizations
- [ApiGateway.1] API Gateway REST WebSocket dan pencatatan eksekusi API harus diaktifkan
- [ApiGateway.2] Tahapan API Gateway REST API harus dikonfigurasi untuk menggunakan sertifikat SSL untuk otentikasi backend
- [ApiGateway.3] Tahapan API Gateway REST API harus mengaktifkan penelusuran AWS X-Ray
- [ApiGateway.4] API Gateway harus dikaitkan dengan ACL Web WAF
- [Autoscaling.5] Instans Amazon EC2 yang diluncurkan menggunakan konfigurasi peluncuran grup Auto Scaling seharusnya tidak memiliki alamat IP Publik
- [Backup.1] titik AWS Backup pemulihan harus dienkripsi saat istirahat
- [Backup.4] rencana AWS Backup laporan harus ditandai
- [CloudFormation.2] CloudFormation tumpukan harus ditandai
- [CloudFront.1] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi
- [CloudFront.3] CloudFront distribusi harus memerlukan enkripsi dalam perjalanan
- [CloudFront.4] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi
- [CloudFront.5] CloudFront distribusi seharusnya mengaktifkan logging
- [CloudFront.6] CloudFront distribusi harus mengaktifkan WAF
- [CloudFront.7] CloudFront distribusi harus menggunakan sertifikat SSL/TLS khusus
- [CloudFront.8] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS
- [CloudFront.9] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus
- [CloudFront.10] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal khusus
- [CloudFront.12] CloudFront distribusi seharusnya tidak menunjukkan asal S3 yang tidak ada
- [CloudFront.13] CloudFront distribusi harus menggunakan kontrol akses asal

- [CloudFront.14] CloudFront distribusi harus ditandai
- [CloudWatch.15] CloudWatch alarm harus memiliki tindakan tertentu yang dikonfigurasi
- [CloudWatch.16] grup CloudWatch log harus dipertahankan untuk jangka waktu tertentu
- [CodeArtifact.1] CodeArtifact repositori harus diberi tag
- [CodeBuild.1] URL repositori sumber CodeBuild Bitbucket tidak boleh berisi kredensyal sensitif
- [CodeBuild.2] variabel lingkungan CodeBuild proyek tidak boleh berisi kredensil teks yang jelas
- [CodeBuild.3] Log CodeBuild S3 harus dienkripsi
- [CodeBuild.4] lingkungan CodeBuild proyek harus memiliki urasi logging AWS Config
- [DataFirehose.1] Aliran pengiriman Firehose harus dienkripsi saat istirahat
- [Detective.1] Grafik perilaku detektif harus diberi tag
- [DMS.1] Instans replikasi Layanan Migrasi Database tidak boleh bersifat publik
- [DMS.7] Tugas replikasi DMS untuk database target seharusnya mengaktifkan logging
- [DMS.8] Tugas replikasi DMS untuk database sumber seharusnya mengaktifkan logging
- [DMS.10] Titik akhir DMS untuk database Neptunus harus mengaktifkan otorisasi IAM
- [DMS.11] Titik akhir DMS untuk MongoDB harus mengaktifkan mekanisme otentikasi
- [DMS.12] Titik akhir DMS untuk Redis harus mengaktifkan TLS
- [DocumentDB.1] Cluster Amazon DocumentDB harus dienkripsi saat istirahat
- [DocumentDB.2] Cluster Amazon DocumentDB harus memiliki periode retensi cadangan yang memadai
- [DocumentDB.3] Cuplikan cluster manual Amazon DocumentDB seharusnya tidak bersifat publik
- [DocumentDB.4] Cluster Amazon DocumentDB harus mempublikasikan log audit ke Log CloudWatch
- [DocumentDB.5] Cluster Amazon DocumentDB harus mengaktifkan perlindungan penghapusan
- [DynamoDB.2] Tabel DynamoDB harus mengaktifkan pemulihan point-in-time
- [DynamoDB.3] Cluster DynamoDB Accelerator (DAX) harus dienkripsi saat istirahat
- [DynamoDB.4] Tabel DynamoDB harus ada dalam rencana cadangan
- [DynamoDB.7] Cluster DynamoDB Accelerator harus dienkripsi saat transit
- [EC2.1] Snapshot Amazon EBS tidak boleh dipulihkan secara publik
- [EC2.3] Volume Amazon EBS yang terpasang harus dienkripsi saat istirahat
- [EC2.4] Instans EC2 yang dihentikan harus dihapus setelah periode waktu tertentu

- [EC2.7] Enkripsi default EBS harus diaktifkan
- [EC2.8] Instans EC2 harus menggunakan Layanan Metadata Instance Versi 2 (IMDSv2)
- [EC2.9] Instans Amazon EC2 seharusnya tidak memiliki alamat IPv4 publik
- [EC2.10] Amazon EC2 harus dikonfigurasi untuk menggunakan titik akhir VPC yang dibuat untuk layanan Amazon EC2
- [EC2.13] Grup keamanan tidak boleh mengizinkan masuknya dari 0.0.0.0/0 atau: :/0 ke port 22
- [EC2.14] Grup keamanan tidak boleh mengizinkan masuknya dari 0.0.0.0/0 atau: :/0 ke port 3389
- [EC2.15] Subnet Amazon EC2 seharusnya tidak secara otomatis menetapkan alamat IP publik
- [EC2.16] Daftar Kontrol Akses Jaringan yang Tidak Digunakan harus dihapus
- [EC2.17] Instans Amazon EC2 tidak boleh menggunakan beberapa ENI
- [EC2.18] Grup keamanan seharusnya hanya mengizinkan lalu lintas masuk yang tidak terbatas untuk port resmi
- [EC2.20] Kedua terowongan VPN untuk koneksi VPN Site-to-Site harus AWS aktif
- [EC2.22] Grup keamanan Amazon EC2 yang tidak digunakan harus dihapus
- [EC2.23] Amazon EC2 Transit Gateways seharusnya tidak secara otomatis menerima permintaan lampiran VPC
- [EC2.24] Jenis instans paravirtual Amazon EC2 tidak boleh digunakan
- [EC2.28] Volume EBS harus dicakup oleh rencana cadangan
- [EC2.51] Titik akhir EC2 Client VPN harus mengaktifkan pencatatan koneksi klien
- [EC2.52] Gerbang transit EC2 harus ditandai
- [ECR.1] Repositori pribadi ECR harus memiliki pemindaian gambar yang dikonfigurasi
- [ECR.2] Repositori pribadi ECR harus memiliki kekekalan tag yang dikonfigurasi
- [ECR.4] Repositori publik ECR harus ditandai
- [ECS.1] Definisi tugas Amazon ECS harus memiliki mode jaringan yang aman dan definisi pengguna.
- [ECS.2] Layanan ECS seharusnya tidak memiliki alamat IP publik yang ditetapkan kepadanya secara otomatis
- [ECS.3] Definisi tugas ECS tidak boleh membagikan namespace proses host
- [ECS.4] Kontainer ECS harus berjalan sebagai non-hak istimewa
- [ECS.8] Rahasia tidak boleh diteruskan sebagai variabel lingkungan kontainer
- [ECS.9] Definisi tugas ECS harus memiliki konfigurasi logging

- [ECS.10] Layanan ECS Fargate harus berjalan pada versi platform Fargate terbaru
- [ECS.12] Cluster ECS harus menggunakan Wawasan Kontainer
- [EFS.1] Sistem File Elastis harus dikonfigurasi untuk mengenkripsi data file saat istirahat menggunakan AWS KMS
- [EFS.2] Volume Amazon EFS harus dalam rencana cadangan
- [EFS.6] Target pemasangan EFS tidak boleh dikaitkan dengan subnet publik
- [EKS.1] Titik akhir klaster EKS seharusnya tidak dapat diakses publik
- [EKS.2] Kluster EKS harus berjalan pada versi Kubernetes yang didukung
- [EKS.3] Kluster EKS harus menggunakan rahasia Kubernetes terenkripsi
- [ELB.1] Application Load Balancer harus dikonfigurasi untuk mengalihkan semua permintaan HTTP ke HTTPS
- [ELB.2] Classic Load Balancer dengan pendengar SSL/HTTPS harus menggunakan sertifikat yang disediakan oleh AWS Certificate Manager
- [ELB.3] Pendengar Classic Load Balancer harus dikonfigurasi dengan penghentian HTTPS atau TLS
- [ELB.4] Application Load Balancer harus dikonfigurasi untuk menjatuhkan header http
- [ELB.6] Aplikasi, Gateway, dan Network Load Balancer harus mengaktifkan perlindungan penghapusan
- [ELB.8] Classic Load Balancer dengan pendengar SSL harus menggunakan kebijakan keamanan yang telah ditentukan sebelumnya yang memiliki urasi yang kuat AWS Config
- [ELB.9] Classic Load Balancer harus mengaktifkan penyeimbangan beban lintas zona
- [ELB.16] Application Load Balancers harus dikaitkan dengan ACL web AWS WAF
- [ElastiCache.1] Cluster ElastiCache Redis harus mengaktifkan pencadangan otomatis
- [ElastiCache.7] ElastiCache cluster tidak boleh menggunakan grup subnet default
- [ElasticBeanstalk.1] Lingkungan Elastic Beanstalk seharusnya mengaktifkan pelaporan kesehatan yang ditingkatkan
- [ElasticBeanstalk.2] Pembaruan platform yang dikelola Elastic Beanstalk harus diaktifkan
- [ElasticBeanstalk.3] Elastic Beanstalk harus mengalirkan log ke CloudWatch
- [EMR.1] Node primer cluster EMR Amazon seharusnya tidak memiliki alamat IP publik
- [ES.1] Domain Elasticsearch harus mengaktifkan enkripsi saat istirahat
- [ES.2] Domain Elasticsearch tidak boleh diakses publik
- [ES.3] Domain Elasticsearch harus mengenkripsi data yang dikirim antar node

- [FSX.1] FSx untuk sistem file OpenZFS harus dikonfigurasi untuk menyalin tag ke cadangan dan volume
- [FSX.2] Sistem file FSx for Lustre harus dikonfigurasi untuk menyalin tag ke cadangan
- [GlobalAccelerator.1] Akselerator Akselerator Global harus diberi tag
- [GuardDuty.1] GuardDuty harus diaktifkan
- [IAM.4] Kunci akses pengguna root IAM seharusnya tidak ada
- [IAM.18] Memastikan peran dukungan telah dibuat untuk mengelola insiden dengan AWS Support
- [IAM.21] Kebijakan terkelola pelanggan IAM yang Anda buat seharusnya tidak mengizinkan tindakan wildcard untuk layanan
- [IAM.26] Sertifikat SSL/TLS kedaluwarsa yang dikelola di IAM harus dihapus
- [IoT.1] profil AWS IoT Core keamanan harus ditandai
- [IoT.2] tindakan AWS IoT Core mitigasi harus ditandai
- AWS IoT Core Dimensi [IoT.3] harus ditandai
- [IoT.4] AWS IoT Core otorisasi harus diberi tag
- [IoT.5] alias AWS IoT Core peran harus ditandai
- AWS IoT Core Kebijakan [IoT.6] harus ditandai
- [Kinesis.1] Aliran kinesis harus dienkripsi saat istirahat
- [KMS.1] Kebijakan yang dikelola pelanggan IAM tidak boleh mengizinkan tindakan dekripsi pada semua kunci KMS
- [KMS.2] Prinsipal IAM tidak boleh memiliki kebijakan inline IAM yang memungkinkan tindakan dekripsi pada semua kunci KMS
- [KMS.3] tidak AWS KMS keys boleh dihapus secara tidak sengaja
- [Lambda.1] Kebijakan fungsi Lambda harus melarang akses publik
- [Lambda.2] Fungsi Lambda harus menggunakan runtime yang didukung
- [Lambda.3] Fungsi Lambda harus dalam VPC
- [Lambda.5] Fungsi VPC Lambda harus beroperasi di beberapa Availability Zone
- [MQ.2] Broker ActiveMQ harus mengalirkan log audit ke CloudWatch
- [MQ.3] Broker Amazon MQ harus mengaktifkan peningkatan versi minor otomatis
- [Neptunus.1] Cluster DB Neptunus harus dienkripsi saat istirahat
- [Neptune.2] Cluster DB Neptunus harus menerbitkan log audit ke Log CloudWatch
- [Neptune.3] Snapshot cluster Neptunus DB seharusnya tidak publik

- [Neptunus.4] Cluster DB Neptunus harus mengaktifkan perlindungan penghapusan
- [Neptunus.5] Cluster DB Neptunus harus mengaktifkan cadangan otomatis
- [Neptune.6] Snapshot cluster Neptunus DB harus dienkripsi saat istirahat
- [Neptunus.7] Cluster DB Neptunus harus mengaktifkan otentikasi basis data IAM
- [Neptunus.8] Cluster DB Neptunus harus dikonfigurasi untuk menyalin tag ke snapshot
- [Neptunus.9] Cluster DB Neptunus harus digunakan di beberapa Availability Zone
- [Opensearch.1] OpenSearch domain harus mengaktifkan enkripsi saat istirahat
- [Opensearch.2] OpenSearch domain tidak boleh diakses publik
- [Opensearch.3] OpenSearch domain harus mengenkripsi data yang dikirim antar node
- [Opensearch.4] login kesalahan OpenSearch domain ke Log harus diaktifkan CloudWatch
- [Opensearch.5] OpenSearch domain harus mengaktifkan pencatatan audit
- [Opensearch.6] OpenSearch domain harus memiliki setidaknya tiga node data
- [Opensearch.7] OpenSearch domain harus mengaktifkan kontrol akses berbutir halus
- [Opensearch.8] Koneksi ke OpenSearch domain harus dienkripsi menggunakan kebijakan keamanan TLS terbaru
- [Opensearch.11] OpenSearch domain harus memiliki setidaknya tiga node primer khusus
- [RDS.1] Snapshot RDS harus pribadi
- [RDS.4] Snapshot cluster RDS dan snapshot database harus dienkripsi saat istirahat
- [RDS.6] Pemantauan yang ditingkatkan harus dikonfigurasi untuk instans RDS DB
- [RDS.7] Cluster RDS harus mengaktifkan perlindungan penghapusan
- [RDS.8] Instans RDS DB harus mengaktifkan perlindungan penghapusan
- [RDS.9] Instans RDS DB harus menerbitkan log ke Log CloudWatch
- [RDS.10] Otentikasi IAM harus dikonfigurasi untuk instance RDS
- [RDS.12] Otentikasi IAM harus dikonfigurasi untuk cluster RDS
- [RDS.13] Peningkatan versi minor otomatis RDS harus diaktifkan
- [RDS.14] Cluster Amazon Aurora seharusnya mengaktifkan backtracking
- [RDS.15] Cluster RDS DB harus dikonfigurasi untuk beberapa Availability Zone
- [RDS.26] Instans RDS DB harus dilindungi oleh rencana cadangan
- [RDS.31] Grup keamanan RDS DB harus ditandai
- [RDS.35] Cluster RDS DB harus mengaktifkan peningkatan versi minor otomatis
- [Redshift.1] Cluster Amazon Redshift harus melarang akses publik

- [Redshift.2] Koneksi ke cluster Amazon Redshift harus dienkripsi saat transit
- [Redshift.3] Cluster Amazon Redshift harus mengaktifkan snapshot otomatis
- [Redshift.7] Cluster Redshift harus menggunakan perutean VPC yang ditingkatkan
- [Redshift.10] Cluster Redshift harus dienkripsi saat istirahat
- [Redshift.15] Grup keamanan Redshift harus mengizinkan masuknya port cluster hanya dari asal yang dibatasi
- [Route53.1] Pemeriksaan kesehatan rute 53 harus ditandai
- [Route53.2] Route 53 zona yang dihosting publik harus mencatat kueri DNS
- [S3.8] Bucket tujuan umum S3 harus memblokir akses publik
- [S3.15] Bucket tujuan umum S3 harus mengaktifkan Object Lock
- [S3.17] Ember tujuan umum S3 harus dienkripsi saat istirahat AWS KMS keys
- [SageMaker.1] Instans SageMaker notebook Amazon seharusnya tidak memiliki akses internet langsung
- [SageMaker.4] varian produksi SageMaker titik akhir harus memiliki jumlah instance awal yang lebih besar dari 1
- [SecretsManager.1] Rahasia Secrets Manager harus mengaktifkan rotasi otomatis
- [SecretsManager.2] Rahasia Secrets Manager yang dikonfigurasi dengan rotasi otomatis harus berhasil diputar
- [SecretsManager.3] Hapus rahasia Secrets Manager yang tidak digunakan
- [SecretsManager.4] Rahasia Secrets Manager harus diputar dalam jumlah hari tertentu
- [ServiceCatalog.1] Portofolio Service Catalog harus dibagikan hanya dalam suatu organisasi AWS
- [SNS.1] Topik SNS harus dienkripsi saat istirahat menggunakan AWS KMS
- [SSM.2] Instans Amazon EC2 yang dikelola oleh Systems Manager harus memiliki status kepatuhan patch COMPLIANT setelah instalasi patch
- [SSM.3] Instans Amazon EC2 yang dikelola oleh Systems Manager harus memiliki status kepatuhan asosiasi COMPLIANT
- [Transfer.2] Server Transfer Family tidak boleh menggunakan protokol FTP untuk koneksi titik akhir
- [WAF.1] Pencatatan ACL Web Global AWS WAF Klasik harus diaktifkan
- [WAF.3] Kelompok aturan Regional AWS WAF Klasik harus memiliki setidaknya satu aturan
- [WAF.6] Aturan global AWS WAF klasik harus memiliki setidaknya satu syarat
- [WAF.7] Kelompok aturan global AWS WAF klasik harus memiliki setidaknya satu aturan

- [WAF.8] ACL web global AWS WAF klasik harus memiliki setidaknya satu aturan atau kelompok aturan
- [WAF.10] ACL AWS WAF web harus memiliki setidaknya satu aturan atau kelompok aturan
- [WAF.11] pencatatan ACL AWS WAF web harus diaktifkan

Asia Pasifik (Seoul)

Kontrol berikut tidak didukung di Asia Pasifik (Seoul).

- [CloudFront.1] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi
- [CloudFront.3] CloudFront distribusi harus memerlukan enkripsi dalam perjalanan
- [CloudFront.4] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi
- [CloudFront.5] CloudFront distribusi seharusnya mengaktifkan logging
- [CloudFront.6] CloudFront distribusi harus mengaktifkan WAF
- [CloudFront.7] CloudFront distribusi harus menggunakan sertifikat SSL/TLS khusus
- [CloudFront.8] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS
- [CloudFront.9] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus
- [CloudFront.10] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal khusus
- [CloudFront.12] CloudFront distribusi seharusnya tidak menunjukkan asal S3 yang tidak ada
- [CloudFront.13] CloudFront distribusi harus menggunakan kontrol akses asal
- [CloudFront.14] CloudFront distribusi harus ditandai
- [CodeArtifact.1] CodeArtifact repositori harus diberi tag
- [DataFirehose.1] Aliran pengiriman Firehose harus dienkripsi saat istirahat
- [DMS.10] Titik akhir DMS untuk database Neptunus harus mengaktifkan otorisasi IAM
- [DMS.11] Titik akhir DMS untuk MongoDB harus mengaktifkan mekanisme otentikasi
- [DMS.12] Titik akhir DMS untuk Redis harus mengaktifkan TLS
- [DynamoDB.3] Cluster DynamoDB Accelerator (DAX) harus dienkripsi saat istirahat
- [DynamoDB.7] Cluster DynamoDB Accelerator harus dienkripsi saat transit
- [EC2.24] Jenis instans paravirtual Amazon EC2 tidak boleh digunakan
- [ECR.4] Repositori publik ECR harus ditandai
- [EFS.6] Target pemasangan EFS tidak boleh dikaitkan dengan subnet publik

- [EKS.3] Kluster EKS harus menggunakan rahasia Kubernetes terenkripsi
- [FSX.2] Sistem file FSx for Lustre harus dikonfigurasi untuk menyalin tag ke cadangan
- [GlobalAccelerator.1] Akselerator Akselerator Global harus diberi tag
- [IAM.26] Sertifikat SSL/TLS kedaluwarsa yang dikelola di IAM harus dihapus
- [MQ.2] Broker ActiveMQ harus mengalirkan log audit ke CloudWatch
- [MQ.3] Broker Amazon MQ harus mengaktifkan peningkatan versi minor otomatis
- [Opensearch.11] OpenSearch domain harus memiliki setidaknya tiga node primer khusus
- [RDS.31] Grup keamanan RDS DB harus ditandai
- [Redshift.15] Grup keamanan Redshift harus mengizinkan masuknya port cluster hanya dari asal yang dibatasi
- [Route53.1] Pemeriksaan kesehatan rute 53 harus ditandai
- [Route53.2] Route 53 zona yang dihosting publik harus mencatat kueri DNS
- [SageMaker.4] varian produksi SageMaker titik akhir harus memiliki jumlah instance awal yang lebih besar dari 1
- [ServiceCatalog.1] Portofolio Service Catalog harus dibagikan hanya dalam suatu organisasi AWS
- [Transfer.2] Server Transfer Family tidak boleh menggunakan protokol FTP untuk koneksi titik akhir
- [WAF.1] Pencatatan ACL Web Global AWS WAF Klasik harus diaktifkan
- [WAF.6] Aturan global AWS WAF klasik harus memiliki setidaknya satu syarat
- [WAF.7] Kelompok aturan global AWS WAF klasik harus memiliki setidaknya satu aturan
- [WAF.8] ACL web global AWS WAF klasik harus memiliki setidaknya satu aturan atau kelompok aturan

Asia Pasifik (Singapura)

Kontrol berikut tidak didukung di Asia Pasifik (Singapura).

- [CloudFront.1] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi
- [CloudFront.3] CloudFront distribusi harus memerlukan enkripsi dalam perjalanan
- [CloudFront.4] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi
- [CloudFront.5] CloudFront distribusi seharusnya mengaktifkan logging
- [CloudFront.6] CloudFront distribusi harus mengaktifkan WAF
- [CloudFront.7] CloudFront distribusi harus menggunakan sertifikat SSL/TLS khusus

- [CloudFront.8] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS
- [CloudFront.9] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus
- [CloudFront.10] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal khusus
- [CloudFront.12] CloudFront distribusi seharusnya tidak menunjukkan asal S3 yang tidak ada
- [CloudFront.13] CloudFront distribusi harus menggunakan kontrol akses asal
- [CloudFront.14] CloudFront distribusi harus ditandai
- [DataFirehose.1] Aliran pengiriman Firehose harus dienkripsi saat istirahat
- [DMS.10] Titik akhir DMS untuk database Neptunus harus mengaktifkan otorisasi IAM
- [DMS.11] Titik akhir DMS untuk MongoDB harus mengaktifkan mekanisme otentikasi
- [DMS.12] Titik akhir DMS untuk Redis harus mengaktifkan TLS
- [DynamoDB.7] Cluster DynamoDB Accelerator harus dienkripsi saat transit
- [ECR.4] Repositori publik ECR harus ditandai
- [EFS.6] Target pemasangan EFS tidak boleh dikaitkan dengan subnet publik
- [EKS.3] Kluster EKS harus menggunakan rahasia Kubernetes terenkripsi
- [FSX.2] Sistem file FSx for Lustre harus dikonfigurasi untuk menyalin tag ke cadangan
- [GlobalAccelerator.1] Akselerator Akselerator Global harus diberi tag
- [IAM.26] Sertifikat SSL/TLS kedaluwarsa yang dikelola di IAM harus dihapus
- [MQ.2] Broker ActiveMQ harus mengalirkan log audit ke CloudWatch
- [MQ.3] Broker Amazon MQ harus mengaktifkan peningkatan versi minor otomatis
- [Opensearch.11] OpenSearch domain harus memiliki setidaknya tiga node primer khusus
- [Redshift.15] Grup keamanan Redshift harus mengizinkan masuknya port cluster hanya dari asal yang dibatasi
- [Route53.1] Pemeriksaan kesehatan rute 53 harus ditandai
- [Route53.2] Route 53 zona yang dihosting publik harus mencatat kueri DNS
- [SageMaker.4] varian produksi SageMaker titik akhir harus memiliki jumlah instance awal yang lebih besar dari 1
- [ServiceCatalog.1] Portofolio Service Catalog harus dibagikan hanya dalam suatu organisasi AWS
- [Transfer.2] Server Transfer Family tidak boleh menggunakan protokol FTP untuk koneksi titik akhir
- [WAF.1] Pencatatan ACL Web Global AWS WAF Klasik harus diaktifkan
- [WAF.6] Aturan global AWS WAF klasik harus memiliki setidaknya satu syarat

- [WAF.7] Kelompok aturan global AWS WAF klasik harus memiliki setidaknya satu aturan
- [WAF.8] ACL web global AWS WAF klasik harus memiliki setidaknya satu aturan atau kelompok aturan

Asia Pasifik (Sydney)

Kontrol berikut tidak didukung di Asia Pasifik (Sydney).

- [CloudFront.1] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi
- [CloudFront.3] CloudFront distribusi harus memerlukan enkripsi dalam perjalanan
- [CloudFront.4] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi
- [CloudFront.5] CloudFront distribusi seharusnya mengaktifkan logging
- [CloudFront.6] CloudFront distribusi harus mengaktifkan WAF
- [CloudFront.7] CloudFront distribusi harus menggunakan sertifikat SSL/TLS khusus
- [CloudFront.8] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS
- [CloudFront.9] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus
- [CloudFront.10] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal khusus
- [CloudFront.12] CloudFront distribusi seharusnya tidak menunjukkan asal S3 yang tidak ada
- [CloudFront.13] CloudFront distribusi harus menggunakan kontrol akses asal
- [CloudFront.14] CloudFront distribusi harus ditandai
- [DataFirehose.1] Aliran pengiriman Firehose harus dienkripsi saat istirahat
- [DMS.10] Titik akhir DMS untuk database Neptunus harus mengaktifkan otorisasi IAM
- [DMS.11] Titik akhir DMS untuk MongoDB harus mengaktifkan mekanisme otentikasi
- [DMS.12] Titik akhir DMS untuk Redis harus mengaktifkan TLS
- [DynamoDB.7] Cluster DynamoDB Accelerator harus dienkripsi saat transit
- [ECR.4] Repositori publik ECR harus ditandai
- [EFS.6] Target pemasangan EFS tidak boleh dikaitkan dengan subnet publik
- [EKS.3] Kluster EKS harus menggunakan rahasia Kubernetes terenkripsi
- [FSX.2] Sistem file FSx for Lustre harus dikonfigurasi untuk menyalin tag ke cadangan
- [GlobalAccelerator.1] Akselerator Akselerator Global harus diberi tag
- [IAM.26] Sertifikat SSL/TLS kedaluwarsa yang dikelola di IAM harus dihapus

- [MQ.2] Broker ActiveMQ harus mengalirkan log audit ke CloudWatch
- [MQ.3] Broker Amazon MQ harus mengaktifkan peningkatan versi minor otomatis
- [Opensearch.11] OpenSearch domain harus memiliki setidaknya tiga node primer khusus
- [Redshift.3] Cluster Amazon Redshift harus mengaktifkan snapshot otomatis
- [Redshift.15] Grup keamanan Redshift harus mengizinkan masuknya port cluster hanya dari asal yang dibatasi
- [Route53.1] Pemeriksaan kesehatan rute 53 harus ditandai
- [Route53.2] Route 53 zona yang dihosting publik harus mencatat kueri DNS
- [SageMaker.4] varian produksi SageMaker titik akhir harus memiliki jumlah instance awal yang lebih besar dari 1
- [ServiceCatalog.1] Portofolio Service Catalog harus dibagikan hanya dalam suatu organisasi AWS
- [Transfer.2] Server Transfer Family tidak boleh menggunakan protokol FTP untuk koneksi titik akhir
- [WAF.1] Pencatatan ACL Web Global AWS WAF Klasik harus diaktifkan
- [WAF.6] Aturan global AWS WAF klasik harus memiliki setidaknya satu syarat
- [WAF.7] Kelompok aturan global AWS WAF klasik harus memiliki setidaknya satu aturan
- [WAF.8] ACL web global AWS WAF klasik harus memiliki setidaknya satu aturan atau kelompok aturan

Asia Pasifik (Tokyo)

Kontrol berikut tidak didukung di Asia Pasifik (Tokyo).

- [CloudFront.1] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi
- [CloudFront.3] CloudFront distribusi harus memerlukan enkripsi dalam perjalanan
- [CloudFront.4] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi
- [CloudFront.5] CloudFront distribusi seharusnya mengaktifkan logging
- [CloudFront.6] CloudFront distribusi harus mengaktifkan WAF
- [CloudFront.7] CloudFront distribusi harus menggunakan sertifikat SSL/TLS khusus
- [CloudFront.8] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS
- [CloudFront.9] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus
- [CloudFront.10] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal khusus

- [CloudFront.12] CloudFront distribusi seharusnya tidak menunjukkan asal S3 yang tidak ada
- [CloudFront.13] CloudFront distribusi harus menggunakan kontrol akses asal
- [CloudFront.14] CloudFront distribusi harus ditandai
- [DataFirehose.1] Aliran pengiriman Firehose harus dienkripsi saat istirahat
- [DMS.10] Titik akhir DMS untuk database Neptunus harus mengaktifkan otorisasi IAM
- [DMS.11] Titik akhir DMS untuk MongoDB harus mengaktifkan mekanisme otentikasi
- [DMS.12] Titik akhir DMS untuk Redis harus mengaktifkan TLS
- [DynamoDB.7] Cluster DynamoDB Accelerator harus dienkripsi saat transit
- [ECR.4] Repositori publik ECR harus ditandai
- [EFS.6] Target pemasangan EFS tidak boleh dikaitkan dengan subnet publik
- [EKS.3] Kluster EKS harus menggunakan rahasia Kubernetes terenkripsi
- [FSX.2] Sistem file FSx for Lustre harus dikonfigurasi untuk menyalin tag ke cadangan
- [GlobalAccelerator.1] Akselerator Akselerator Global harus diberi tag
- [IAM.26] Sertifikat SSL/TLS kedaluwarsa yang dikelola di IAM harus dihapus
- [MQ.2] Broker ActiveMQ harus mengalirkan log audit ke CloudWatch
- [MQ.3] Broker Amazon MQ harus mengaktifkan peningkatan versi minor otomatis
- [Opensearch.11] OpenSearch domain harus memiliki setidaknya tiga node primer khusus
- [Redshift.15] Grup keamanan Redshift harus mengizinkan masuknya port cluster hanya dari asal yang dibatasi
- [Route53.1] Pemeriksaan kesehatan rute 53 harus ditandai
- [Route53.2] Route 53 zona yang dihosting publik harus mencatat kueri DNS
- [SageMaker.4] varian produksi SageMaker titik akhir harus memiliki jumlah instance awal yang lebih besar dari 1
- [ServiceCatalog.1] Portofolio Service Catalog harus dibagikan hanya dalam suatu organisasi AWS
- [Transfer.2] Server Transfer Family tidak boleh menggunakan protokol FTP untuk koneksi titik akhir
- [WAF.1] Pencatatan ACL Web Global AWS WAF Klasik harus diaktifkan
- [WAF.6] Aturan global AWS WAF klasik harus memiliki setidaknya satu syarat
- [WAF.7] Kelompok aturan global AWS WAF klasik harus memiliki setidaknya satu aturan
- [WAF.8] ACL web global AWS WAF klasik harus memiliki setidaknya satu aturan atau kelompok aturan

Kanada (Pusat)

Kontrol berikut tidak didukung di Kanada (Tengah).

- [CloudFront.1] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi
- [CloudFront.3] CloudFront distribusi harus memerlukan enkripsi dalam perjalanan
- [CloudFront.4] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi
- [CloudFront.5] CloudFront distribusi seharusnya mengaktifkan logging
- [CloudFront.6] CloudFront distribusi harus mengaktifkan WAF
- [CloudFront.7] CloudFront distribusi harus menggunakan sertifikat SSL/TLS khusus
- [CloudFront.8] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS
- [CloudFront.9] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus
- [CloudFront.10] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal khusus
- [CloudFront.12] CloudFront distribusi seharusnya tidak menunjukkan asal S3 yang tidak ada
- [CloudFront.13] CloudFront distribusi harus menggunakan kontrol akses asal
- [CloudFront.14] CloudFront distribusi harus ditandai
- [CodeArtifact.1] CodeArtifact repositori harus diberi tag
- [DataFirehose.1] Aliran pengiriman Firehose harus dienkripsi saat istirahat
- [DMS.10] Titik akhir DMS untuk database Neptunus harus mengaktifkan otorisasi IAM
- [DMS.11] Titik akhir DMS untuk MongoDB harus mengaktifkan mekanisme otentikasi
- [DMS.12] Titik akhir DMS untuk Redis harus mengaktifkan TLS
- [DynamoDB.3] Cluster DynamoDB Accelerator (DAX) harus dienkripsi saat istirahat
- [DynamoDB.7] Cluster DynamoDB Accelerator harus dienkripsi saat transit
- [EC2.24] Jenis instans paravirtual Amazon EC2 tidak boleh digunakan
- [ECR.4] Repositori publik ECR harus ditandai
- [EFS.6] Target pemasangan EFS tidak boleh dikaitkan dengan subnet publik
- [EKS.3] Kluster EKS harus menggunakan rahasia Kubernetes terenkripsi
- [FSX.2] Sistem file FSx for Lustre harus dikonfigurasi untuk menyalin tag ke cadangan
- [GlobalAccelerator.1] Akselerator Akselerator Global harus diberi tag
- [IAM.26] Sertifikat SSL/TLS kedaluwarsa yang dikelola di IAM harus dihapus
- [MQ.2] Broker ActiveMQ harus mengalirkan log audit ke CloudWatch

- [MQ.3] Broker Amazon MQ harus mengaktifkan peningkatan versi minor otomatis
- [Opensearch.11] OpenSearch domain harus memiliki setidaknya tiga node primer khusus
- [RDS.31] Grup keamanan RDS DB harus ditandai
- [Redshift.15] Grup keamanan Redshift harus mengizinkan masuknya port cluster hanya dari asal yang dibatasi
- [Route53.1] Pemeriksaan kesehatan rute 53 harus ditandai
- [Route53.2] Route 53 zona yang dihosting publik harus mencatat kueri DNS
- [SageMaker.4] varian produksi SageMaker titik akhir harus memiliki jumlah instance awal yang lebih besar dari 1
- [ServiceCatalog.1] Portofolio Service Catalog harus dibagikan hanya dalam suatu organisasi AWS
- [Transfer.2] Server Transfer Family tidak boleh menggunakan protokol FTP untuk koneksi titik akhir
- [WAF.1] Pencatatan ACL Web Global AWS WAF Klasik harus diaktifkan
- [WAF.6] Aturan global AWS WAF klasik harus memiliki setidaknya satu syarat
- [WAF.7] Kelompok aturan global AWS WAF klasik harus memiliki setidaknya satu aturan
- [WAF.8] ACL web global AWS WAF klasik harus memiliki setidaknya satu aturan atau kelompok aturan

Tiongkok (Beijing)

Kontrol berikut tidak didukung di China (Beijing).

- [ACM.1] Sertifikat yang diimpor dan diterbitkan ACM harus diperbarui setelah jangka waktu tertentu
- [ACM.2] Sertifikat RSA yang dikelola oleh ACM harus menggunakan panjang kunci minimal 2.048 bit
- [ACM.3] Sertifikat ACM harus ditandai
- [Akun.2] Akun AWS harus menjadi bagian dari organisasi AWS Organizations
- [ApiGateway.2] Tahapan API Gateway REST API harus dikonfigurasi untuk menggunakan sertifikat SSL untuk otentikasi backend
- [ApiGateway.3] Tahapan API Gateway REST API harus mengaktifkan penelusuran AWS X-Ray
- [ApiGateway.4] API Gateway harus dikaitkan dengan ACL Web WAF
- [AppSync.4] AWS AppSync GraphQL API harus diberi tag
- [Athena.2] Katalog data Athena harus diberi tag

- [Athena.3] Kelompok kerja Athena harus ditandai
- [AutoScaling.10] Grup Penskalaan Otomatis EC2 harus diberi tag
- [Backup.1] titik AWS Backup pemulihan harus dienkripsi saat istirahat
- [Backup.2] poin AWS Backup pemulihan harus ditandai
- [Backup.3] AWS Backup brankas harus ditandai
- [Backup.4] rencana AWS Backup laporan harus ditandai
- [Backup.5] rencana AWS Backup cadangan harus ditandai
- [CloudFormation.2] CloudFormation tumpukan harus ditandai
- [CloudFront.1] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi
- [CloudFront.3] CloudFront distribusi harus memerlukan enkripsi dalam perjalanan
- [CloudFront.4] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi
- [CloudFront.5] CloudFront distribusi seharusnya mengaktifkan logging
- [CloudFront.6] CloudFront distribusi harus mengaktifkan WAF
- [CloudFront.7] CloudFront distribusi harus menggunakan sertifikat SSL/TLS khusus
- [CloudFront.8] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS
- [CloudFront.9] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus
- [CloudFront.10] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal khusus
- [CloudFront.13] CloudFront distribusi harus menggunakan kontrol akses asal
- [CloudFront.14] CloudFront distribusi harus ditandai
- [CloudTrail.9] CloudTrail jejak harus ditandai
- [CloudWatch.15] CloudWatch alarm harus memiliki tindakan tertentu yang dikonfigurasi
- [CloudWatch.16] grup CloudWatch log harus dipertahankan untuk jangka waktu tertentu
- [CodeArtifact.1] CodeArtifact repositori harus diberi tag
- [DataFirehose.1] Aliran pengiriman Firehose harus dienkripsi saat istirahat
- [Detective.1] Grafik perilaku detektif harus diberi tag
- [DMS.2] Sertifikat DMS harus ditandai
- [DMS.3] Langganan acara DMS harus ditandai
- [DMS.4] Contoh replikasi DMS harus ditandai
- [DMS.5] Grup subnet replikasi DMS harus ditandai
- [DMS.10] Titik akhir DMS untuk database Neptunus harus mengaktifkan otorisasi IAM

- [DMS.11] Titik akhir DMS untuk MongoDB harus mengaktifkan mekanisme otentikasi
- [DMS.12] Titik akhir DMS untuk Redis harus mengaktifkan TLS
- [DocumentDB.1] Cluster Amazon DocumentDB harus dienkripsi saat istirahat
- [DocumentDB.2] Cluster Amazon DocumentDB harus memiliki periode retensi cadangan yang memadai
- [DocumentDB.3] Cuplikan cluster manual Amazon DocumentDB seharusnya tidak bersifat publik
- [DocumentDB.4] Cluster Amazon DocumentDB harus mempublikasikan log audit ke Log CloudWatch
- [DocumentDB.5] Cluster Amazon DocumentDB harus mengaktifkan perlindungan penghapusan
- [DynamoDB.3] Cluster DynamoDB Accelerator (DAX) harus dienkripsi saat istirahat
- [DynamoDB.4] Tabel DynamoDB harus ada dalam rencana cadangan
- [DynamoDB.5] Tabel DynamoDB harus diberi tag
- [DynamoDB.7] Cluster DynamoDB Accelerator harus dienkripsi saat transit
- [EC2.15] Subnet Amazon EC2 seharusnya tidak secara otomatis menetapkan alamat IP publik
- [EC2.16] Daftar Kontrol Akses Jaringan yang Tidak Digunakan harus dihapus
- [EC2.20] Kedua terowongan VPN untuk koneksi VPN Site-to-Site harus AWS aktif
- [EC2.22] Grup keamanan Amazon EC2 yang tidak digunakan harus dihapus
- [EC2.23] Amazon EC2 Transit Gateways seharusnya tidak secara otomatis menerima permintaan lampiran VPC
- [EC2.28] Volume EBS harus dicakup oleh rencana cadangan
- [EC2.33] Lampiran gateway transit EC2 harus ditandai
- [EC2.34] Tabel rute gateway transit EC2 harus ditandai
- [EC2.35] Antarmuka jaringan EC2 harus ditandai
- [EC2.36] Gateway pelanggan EC2 harus ditandai
- [EC2.37] Alamat IP Elastis EC2 harus ditandai
- [EC2.38] Instans EC2 harus ditandai
- [EC2.39] Gerbang internet EC2 harus ditandai
- [EC2.40] Gerbang EC2 NAT harus ditandai
- [EC2.41] ACL jaringan EC2 harus ditandai
- [EC2.42] Tabel rute EC2 harus ditandai
- [EC2.43] Grup keamanan EC2 harus ditandai

- [EC2.44] Subnet EC2 harus ditandai
- [EC2.45] Volume EC2 harus ditandai
- [EC2.46] VPC Amazon harus ditandai
- [EC2.47] Layanan titik akhir Amazon VPC harus ditandai
- [EC2.48] Log aliran VPC Amazon harus ditandai
- [EC2.49] Koneksi peering VPC Amazon harus ditandai
- [EC2.50] Gateway EC2 VPN harus ditandai
- [EC2.51] Titik akhir EC2 Client VPN harus mengaktifkan pencatatan koneksi klien
- [EC2.52] Gerbang transit EC2 harus ditandai
- [EC2.53] Grup keamanan EC2 tidak boleh mengizinkan masuknya dari 0.0.0.0/0 ke port administrasi server jarak jauh
- [EC2.54] Grup keamanan EC2 tidak boleh mengizinkan masuknya dari: :/0 ke port administrasi server jarak jauh
- [ECR.1] Repositori pribadi ECR harus memiliki pemindaian gambar yang dikonfigurasi
- [ECR.4] Repositori publik ECR harus ditandai
- [ECS.1] Definisi tugas Amazon ECS harus memiliki mode jaringan yang aman dan definisi pengguna.
- [ECS.13] Layanan ECS harus ditandai
- [ECS.14] Cluster ECS harus ditandai
- [ECS.15] Definisi tugas ECS harus ditandai
- [EFS.5] Titik akses EFS harus ditandai
- [EFS.6] Target pemasangan EFS tidak boleh dikaitkan dengan subnet publik
- [EKS.3] Kluster EKS harus menggunakan rahasia Kubernetes terenkripsi
- [EKS.6] Kluster EKS harus ditandai
- [EKS.7] Konfigurasi penyedia identitas EKS harus ditandai
- [ELB.2] Classic Load Balancer dengan pendengar SSL/HTTPS harus menggunakan sertifikat yang disediakan oleh AWS Certificate Manager
- [ELB.16] Application Load Balancers harus dikaitkan dengan ACL web AWS WAF
- [ElastiCache.1] Cluster ElastiCache Redis harus mengaktifkan pencadangan otomatis
- [ElasticBeanstalk.1] Lingkungan Elastic Beanstalk seharusnya mengaktifkan pelaporan kesehatan yang ditingkatkan

- [ElasticBeanstalk.2] Pembaruan platform yang dikelola Elastic Beanstalk harus diaktifkan
- [ElasticBeanstalk.3] Elastic Beanstalk harus mengalirkan log ke CloudWatch
- [EMR.2] Pengaturan akses publik blok EMR Amazon harus diaktifkan
- [ES.3] Domain Elasticsearch harus mengenkripsi data yang dikirim antar node
- [ES.4] Kesalahan domain Elasticsearch yang masuk ke CloudWatch Log harus diaktifkan
- [ES.9] Domain Elasticsearch harus diberi tag
- [EventBridge.2] bus EventBridge acara harus diberi tag
- [EventBridge.4] titik akhir EventBridge global harus mengaktifkan replikasi acara
- [FSX.1] FSx untuk sistem file OpenZFS harus dikonfigurasi untuk menyalin tag ke cadangan dan volume
- [FSX.2] Sistem file FSx for Lustre harus dikonfigurasi untuk menyalin tag ke cadangan
- [GlobalAccelerator.1] Akselerator Akselerator Global harus diberi tag
- AWS Glue Pekerjaan [Glue.1] harus ditandai
- [GuardDuty.1] GuardDuty harus diaktifkan
- [GuardDuty.2] GuardDuty filter harus diberi tag
- [GuardDuty.3] GuardDuty IPset harus ditandai
- [GuardDuty.4] GuardDuty detektor harus ditandai
- [IAM.6] MFA perangkat keras harus diaktifkan untuk pengguna root
- [IAM.9] MFA harus diaktifkan untuk pengguna root
- [IAM.21] Kebijakan terkelola pelanggan IAM yang Anda buat seharusnya tidak mengizinkan tindakan wildcard untuk layanan
- [IAM.23] Penganalisis Akses IAM harus ditandai
- [IAM.24] Peran IAM harus ditandai
- [IAM.25] Pengguna IAM harus diberi tag
- [IAM.26] Sertifikat SSL/TLS kedaluwarsa yang dikelola di IAM harus dihapus
- [IAM.27] Identitas IAM seharusnya tidak memiliki kebijakan yang dilampirkan AWSCloudShellFullAccess
- [IAM.28] IAM Access Analyzer penganalisis akses eksternal harus diaktifkan
- [IoT.1] profil AWS IoT Core keamanan harus ditandai
- [IoT.2] tindakan AWS IoT Core mitigasi harus ditandai
- AWS IoT Core Dimensi [IoT.3] harus ditandai

- [IoT.4] AWS IoT Core otorisasi harus diberi tag
- [IoT.5] alias AWS IoT Core peran harus ditandai
- AWS IoT Core Kebijakan [IoT.6] harus ditandai
- [Kinesis.2] Aliran kinesis harus ditandai
- [Lambda.6] Fungsi Lambda harus ditandai
- [Macie.1] Amazon Macie harus diaktifkan
- [Macie.2] Penemuan data sensitif otomatis Macie harus diaktifkan
- [MQ.2] Broker ActiveMQ harus mengalirkan log audit ke CloudWatch
- [MQ.3] Broker Amazon MQ harus mengaktifkan peningkatan versi minor otomatis
- [MQ.4] Broker Amazon MQ harus diberi tag
- [Neptunus.1] Cluster DB Neptunus harus dienkripsi saat istirahat
- [Neptune.2] Cluster DB Neptunus harus menerbitkan log audit ke Log CloudWatch
- [Neptune.3] Snapshot cluster Neptunus DB seharusnya tidak publik
- [Neptunus.4] Cluster DB Neptunus harus mengaktifkan perlindungan penghapusan
- [Neptunus.5] Cluster DB Neptunus harus mengaktifkan cadangan otomatis
- [Neptune.6] Snapshot cluster Neptunus DB harus dienkripsi saat istirahat
- [Neptunus.7] Cluster DB Neptunus harus mengaktifkan otentikasi basis data IAM
- [Neptunus.8] Cluster DB Neptunus harus dikonfigurasi untuk menyalin tag ke snapshot
- [Neptunus.9] Cluster DB Neptunus harus digunakan di beberapa Availability Zone
- [NetworkFirewall.1] Firewall Firewall Jaringan harus digunakan di beberapa Availability Zone
- [NetworkFirewall.2] Pencatatan Firewall Jaringan harus diaktifkan
- [NetworkFirewall.3] Kebijakan Network Firewall harus memiliki setidaknya satu kelompok aturan yang terkait
- [NetworkFirewall.4] Tindakan stateless default untuk kebijakan Network Firewall harus drop atau forward untuk paket penuh
- [NetworkFirewall.5] Tindakan stateless default untuk kebijakan Network Firewall harus drop atau forward untuk paket yang terfragmentasi
- [NetworkFirewall.6] Grup aturan Stateless Network Firewall tidak boleh kosong
- [NetworkFirewall.7] Firewall Firewall Jaringan harus diberi tag
- [NetworkFirewall.8] Kebijakan firewall Network Firewall harus ditandai
- [NetworkFirewall.9] Firewall Firewall Jaringan harus mengaktifkan perlindungan penghapusan

- [Opensearch.1] OpenSearch domain harus mengaktifkan enkripsi saat istirahat
- [Opensearch.2] OpenSearch domain tidak boleh diakses publik
- [Opensearch.3] OpenSearch domain harus mengenkripsi data yang dikirim antar node
- [Opensearch.4] login kesalahan OpenSearch domain ke Log harus diaktifkan CloudWatch
- [Opensearch.5] OpenSearch domain harus mengaktifkan pencatatan audit
- [Opensearch.6] OpenSearch domain harus memiliki setidaknya tiga node data
- [Opensearch.7] OpenSearch domain harus mengaktifkan kontrol akses berbutir halus
- [Opensearch.8] Koneksi ke OpenSearch domain harus dienkripsi menggunakan kebijakan keamanan TLS terbaru
- [Opensearch.9] domain harus ditandai OpenSearch
- [Opensearch.11] OpenSearch domain harus memiliki setidaknya tiga node primer khusus
- [PCA.1] otoritas sertifikat AWS Private CA root harus dinonaktifkan
- [RDS.7] Cluster RDS harus mengaktifkan perlindungan penghapusan
- [RDS.10] Otentikasi IAM harus dikonfigurasi untuk instance RDS
- [RDS.12] Otentikasi IAM harus dikonfigurasi untuk cluster RDS
- [RDS.13] Peningkatan versi minor otomatis RDS harus diaktifkan
- [RDS.14] Cluster Amazon Aurora seharusnya mengaktifkan backtracking
- [RDS.15] Cluster RDS DB harus dikonfigurasi untuk beberapa Availability Zone
- [RDS.16] Cluster RDS DB harus dikonfigurasi untuk menyalin tag ke snapshot
- [RDS.24] Kluster Database RDS harus menggunakan nama pengguna administrator khusus
- [RDS.25] Instans database RDS harus menggunakan nama pengguna administrator khusus
- [RDS.26] Instans RDS DB harus dilindungi oleh rencana cadangan
- [RDS.27] Cluster RDS DB harus dienkripsi saat istirahat
- [RDS.28] Cluster RDS DB harus ditandai
- [RDS.29] Snapshot cluster RDS DB harus ditandai
- [RDS.30] Instans RDS DB harus ditandai
- [RDS.31] Grup keamanan RDS DB harus ditandai
- [RDS.32] Snapshot RDS DB harus ditandai
- [RDS.33] Grup subnet RDS DB harus ditandai
- [RDS.34] Cluster Aurora MySQL DB harus menerbitkan log audit ke Log CloudWatch
- [RDS.35] Cluster RDS DB harus mengaktifkan peningkatan versi minor otomatis

- [Redshift.7] Cluster Redshift harus menggunakan perutean VPC yang ditingkatkan
- [Redshift.10] Cluster Redshift harus dienkripsi saat istirahat
- [Redshift.11] Cluster Redshift harus ditandai
- [Redshift.12] Langganan pemberitahuan acara Redshift harus ditandai
- [Redshift.13] Snapshot cluster Redshift harus ditandai
- [Redshift.14] Grup subnet cluster Redshift harus ditandai
- [Redshift.15] Grup keamanan Redshift harus mengizinkan masuknya port cluster hanya dari asal yang dibatasi
- [Route53.1] Pemeriksaan kesehatan rute 53 harus ditandai
- [Route53.2] Route 53 zona yang dihosting publik harus mencatat kueri DNS
- [S3.1] Bucket tujuan umum S3 harus mengaktifkan pengaturan akses publik blok
- [S3.8] Bucket tujuan umum S3 harus memblokir akses publik
- [S3.14] Bucket tujuan umum S3 harus mengaktifkan versi
- [S3.22] Bucket tujuan umum S3 harus mencatat peristiwa penulisan tingkat objek
- [S3.23] Bucket tujuan umum S3 harus mencatat peristiwa pembacaan tingkat objek
- [SageMaker.1] Instans SageMaker notebook Amazon seharusnya tidak memiliki akses internet langsung
- [SageMaker.4] varian produksi SageMaker titik akhir harus memiliki jumlah instance awal yang lebih besar dari 1
- [SES.1] Daftar kontak SES harus ditandai
- [SES.2] Set konfigurasi SES harus ditandai
- [SecretsManager.3] Hapus rahasia Secrets Manager yang tidak digunakan
- [SecretsManager.4] Rahasia Secrets Manager harus diputar dalam jumlah hari tertentu
- [SecretsManager.5] Rahasia Secrets Manager harus diberi tag
- [ServiceCatalog.1] Portofolio Service Catalog harus dibagikan hanya dalam suatu organisasi AWS
- [SNS.3] Topik SNS harus ditandai
- [SQS.2] Antrian SQS harus ditandai
- [StepFunctions.2] Aktivitas Step Functions harus diberi tag
- [Transfer.1] AWS Transfer Family alur kerja harus ditandai
- [Transfer.2] Server Transfer Family tidak boleh menggunakan protokol FTP untuk koneksi titik akhir
- [WAF.1] Pencatatan ACL Web Global AWS WAF Klasik harus diaktifkan

- [WAF.3] Kelompok aturan Regional AWS WAF Klasik harus memiliki setidaknya satu aturan
- [WAF.6] Aturan global AWS WAF klasik harus memiliki setidaknya satu syarat
- [WAF.7] Kelompok aturan global AWS WAF klasik harus memiliki setidaknya satu aturan
- [WAF.8] ACL web global AWS WAF klasik harus memiliki setidaknya satu aturan atau kelompok aturan
- [WAF.11] pencatatan ACL AWS WAF web harus diaktifkan

Tiongkok (Ningxia)

Kontrol berikut tidak didukung di China (Ningxia).

- [ACM.1] Sertifikat yang diimpor dan diterbitkan ACM harus diperbarui setelah jangka waktu tertentu
- [ACM.2] Sertifikat RSA yang dikelola oleh ACM harus menggunakan panjang kunci minimal 2.048 bit
- [ACM.3] Sertifikat ACM harus ditandai
- [Akun.2] Akun AWS harus menjadi bagian dari organisasi AWS Organizations
- [ApiGateway.2] Tahapan API Gateway REST API harus dikonfigurasi untuk menggunakan sertifikat SSL untuk otentikasi backend
- [ApiGateway.3] Tahapan API Gateway REST API harus mengaktifkan penelusuran AWS X-Ray
- [ApiGateway.4] API Gateway harus dikaitkan dengan ACL Web WAF
- [AppSync.4] AWS AppSync GraphQL API harus diberi tag
- [Athena.2] Katalog data Athena harus diberi tag
- [Athena.3] Kelompok kerja Athena harus ditandai
- [AutoScaling.10] Grup Penskalaan Otomatis EC2 harus diberi tag
- [Backup.1] titik AWS Backup pemulihan harus dienkripsi saat istirahat
- [Backup.2] poin AWS Backup pemulihan harus ditandai
- [Backup.3] AWS Backup brankas harus ditandai
- [Backup.4] rencana AWS Backup laporan harus ditandai
- [Backup.5] rencana AWS Backup cadangan harus ditandai
- [CloudFormation.2] CloudFormation tumpukan harus ditandai
- [CloudFront.1] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi
- [CloudFront.3] CloudFront distribusi harus memerlukan enkripsi dalam perjalanan

- [CloudFront.4] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi
- [CloudFront.5] CloudFront distribusi seharusnya mengaktifkan logging
- [CloudFront.6] CloudFront distribusi harus mengaktifkan WAF
- [CloudFront.7] CloudFront distribusi harus menggunakan sertifikat SSL/TLS khusus
- [CloudFront.8] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS
- [CloudFront.9] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus
- [CloudFront.10] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal khusus
- [CloudFront.12] CloudFront distribusi seharusnya tidak menunjukkan asal S3 yang tidak ada
- [CloudFront.13] CloudFront distribusi harus menggunakan kontrol akses asal
- [CloudFront.14] CloudFront distribusi harus ditandai
- [CloudTrail.9] CloudTrail jejak harus ditandai
- [CloudWatch.15] CloudWatch alarm harus memiliki tindakan tertentu yang dikonfigurasi
- [CloudWatch.16] grup CloudWatch log harus dipertahankan untuk jangka waktu tertentu
- [CodeArtifact.1] CodeArtifact repositori harus diberi tag
- [DataFirehose.1] Aliran pengiriman Firehose harus dienkripsi saat istirahat
- [Detective.1] Grafik perilaku detektif harus diberi tag
- [DMS.2] Sertifikat DMS harus ditandai
- [DMS.3] Langganan acara DMS harus ditandai
- [DMS.4] Contoh replikasi DMS harus ditandai
- [DMS.5] Grup subnet replikasi DMS harus ditandai
- [DMS.10] Titik akhir DMS untuk database Neptunus harus mengaktifkan otorisasi IAM
- [DMS.11] Titik akhir DMS untuk MongoDB harus mengaktifkan mekanisme otentikasi
- [DMS.12] Titik akhir DMS untuk Redis harus mengaktifkan TLS
- [DocumentDB.3] Cuplikan cluster manual Amazon DocumentDB seharusnya tidak bersifat publik
- [DynamoDB.3] Cluster DynamoDB Accelerator (DAX) harus dienkripsi saat istirahat
- [DynamoDB.4] Tabel DynamoDB harus ada dalam rencana cadangan
- [DynamoDB.5] Tabel DynamoDB harus diberi tag
- [DynamoDB.7] Cluster DynamoDB Accelerator harus dienkripsi saat transit
- [EC2.15] Subnet Amazon EC2 seharusnya tidak secara otomatis menetapkan alamat IP publik
- [EC2.16] Daftar Kontrol Akses Jaringan yang Tidak Digunakan harus dihapus

- [EC2.20] Kedua terowongan VPN untuk koneksi VPN Site-to-Site harus AWS aktif
- [EC2.22] Grup keamanan Amazon EC2 yang tidak digunakan harus dihapus
- [EC2.23] Amazon EC2 Transit Gateways seharusnya tidak secara otomatis menerima permintaan lampiran VPC
- [EC2.24] Jenis instans paravirtual Amazon EC2 tidak boleh digunakan
- [EC2.28] Volume EBS harus dicakup oleh rencana cadangan
- [EC2.33] Lampiran gateway transit EC2 harus ditandai
- [EC2.34] Tabel rute gateway transit EC2 harus ditandai
- [EC2.35] Antarmuka jaringan EC2 harus ditandai
- [EC2.36] Gateway pelanggan EC2 harus ditandai
- [EC2.37] Alamat IP Elastis EC2 harus ditandai
- [EC2.38] Instans EC2 harus ditandai
- [EC2.39] Gerbang internet EC2 harus ditandai
- [EC2.40] Gerbang EC2 NAT harus ditandai
- [EC2.41] ACL jaringan EC2 harus ditandai
- [EC2.42] Tabel rute EC2 harus ditandai
- [EC2.43] Grup keamanan EC2 harus ditandai
- [EC2.44] Subnet EC2 harus ditandai
- [EC2.45] Volume EC2 harus ditandai
- [EC2.46] VPC Amazon harus ditandai
- [EC2.47] Layanan titik akhir Amazon VPC harus ditandai
- [EC2.48] Log aliran VPC Amazon harus ditandai
- [EC2.49] Koneksi peering VPC Amazon harus ditandai
- [EC2.50] Gateway EC2 VPN harus ditandai
- [EC2.51] Titik akhir EC2 Client VPN harus mengaktifkan pencatatan koneksi klien
- [EC2.52] Gerbang transit EC2 harus ditandai
- [ECR.1] Repositori pribadi ECR harus memiliki pemindaian gambar yang dikonfigurasi
- [ECR.4] Repositori publik ECR harus ditandai
- [ECS.1] Definisi tugas Amazon ECS harus memiliki mode jaringan yang aman dan definisi pengguna.
- [ECS.13] Layanan ECS harus ditandai

- [ECS.14] Cluster ECS harus ditandai
- [ECS.15] Definisi tugas ECS harus ditandai
- [EFS.3] Titik akses EFS harus menegakkan direktori root
- [EFS.4] Titik akses EFS harus menegakkan identitas pengguna
- [EFS.5] Titik akses EFS harus ditandai
- [EFS.6] Target pemasangan EFS tidak boleh dikaitkan dengan subnet publik
- [EKS.3] Kluster EKS harus menggunakan rahasia Kubernetes terenkripsi
- [EKS.6] Kluster EKS harus ditandai
- [EKS.7] Konfigurasi penyedia identitas EKS harus ditandai
- [ELB.2] Classic Load Balancer dengan pendengar SSL/HTTPS harus menggunakan sertifikat yang disediakan oleh AWS Certificate Manager
- [ELB.16] Application Load Balancers harus dikaitkan dengan ACL web AWS WAF
- [ElastiCache.1] Cluster ElastiCache Redis harus mengaktifkan pencadangan otomatis
- [ElasticBeanstalk.1] Lingkungan Elastic Beanstalk seharusnya mengaktifkan pelaporan kesehatan yang ditingkatkan
- [ElasticBeanstalk.2] Pembaruan platform yang dikelola Elastic Beanstalk harus diaktifkan
- [ElasticBeanstalk.3] Elastic Beanstalk harus mengalirkan log ke CloudWatch
- [EMR.2] Pengaturan akses publik blok EMR Amazon harus diaktifkan
- [ES.1] Domain Elasticsearch harus mengaktifkan enkripsi saat istirahat
- [ES.3] Domain Elasticsearch harus mengenkripsi data yang dikirim antar node
- [ES.4] Kesalahan domain Elasticsearch yang masuk ke CloudWatch Log harus diaktifkan
- [ES.9] Domain Elasticsearch harus diberi tag
- [EventBridge.2] bus EventBridge acara harus diberi tag
- [EventBridge.4] titik akhir EventBridge global harus mengaktifkan replikasi acara
- [FSX.1] FSx untuk sistem file OpenZFS harus dikonfigurasi untuk menyalin tag ke cadangan dan volume
- [FSX.2] Sistem file FSx for Lustre harus dikonfigurasi untuk menyalin tag ke cadangan
- [GlobalAccelerator.1] Akselerator Akselerator Global harus diberi tag
- AWS Glue Pekerjaan [Glue.1] harus ditandai
- [GuardDuty.1] GuardDuty harus diaktifkan
- [GuardDuty.2] GuardDuty filter harus diberi tag

- [GuardDuty.3] GuardDuty IPset harus ditandai
- [GuardDuty.4] GuardDuty detektor harus ditandai
- [IAM.6] MFA perangkat keras harus diaktifkan untuk pengguna root
- [IAM.9] MFA harus diaktifkan untuk pengguna root
- [IAM.21] Kebijakan terkelola pelanggan IAM yang Anda buat seharusnya tidak mengizinkan tindakan wildcard untuk layanan
- [IAM.23] Penganalisis Akses IAM harus ditandai
- [IAM.24] Peran IAM harus ditandai
- [IAM.25] Pengguna IAM harus diberi tag
- [IAM.26] Sertifikat SSL/TLS kedaluwarsa yang dikelola di IAM harus dihapus
- [IAM.27] Identitas IAM seharusnya tidak memiliki kebijakan yang dilampirkan AWSCloudShellFullAccess
- [IAM.28] IAM Access Analyzer penganalisis akses eksternal harus diaktifkan
- [IoT.1] profil AWS IoT Core keamanan harus ditandai
- [IoT.2] tindakan AWS IoT Core mitigasi harus ditandai
- AWS IoT Core Dimensi [IoT.3] harus ditandai
- [IoT.4] AWS IoT Core otorisasi harus diberi tag
- [IoT.5] alias AWS IoT Core peran harus ditandai
- AWS IoT Core Kebijakan [IoT.6] harus ditandai
- [Kinesis.2] Aliran kinesis harus ditandai
- [Lambda.1] Kebijakan fungsi Lambda harus melarang akses publik
- [Lambda.2] Fungsi Lambda harus menggunakan runtime yang didukung
- [Lambda.3] Fungsi Lambda harus dalam VPC
- [Lambda.5] Fungsi VPC Lambda harus beroperasi di beberapa Availability Zone
- [Lambda.6] Fungsi Lambda harus ditandai
- [Macie.1] Amazon Macie harus diaktifkan
- [Macie.2] Penemuan data sensitif otomatis Macie harus diaktifkan
- [MQ.2] Broker ActiveMQ harus mengalirkan log audit ke CloudWatch
- [MQ.3] Broker Amazon MQ harus mengaktifkan peningkatan versi minor otomatis
- [MQ.4] Broker Amazon MQ harus diberi tag
- [Neptune.3] Snapshot cluster Neptunus DB seharusnya tidak publik

- [NetworkFirewall.1] Firewall Firewall Jaringan harus digunakan di beberapa Availability Zone
- [NetworkFirewall.2] Pencatatan Firewall Jaringan harus diaktifkan
- [NetworkFirewall.3] Kebijakan Network Firewall harus memiliki setidaknya satu kelompok aturan yang terkait
- [NetworkFirewall.4] Tindakan stateless default untuk kebijakan Network Firewall harus drop atau forward untuk paket penuh
- [NetworkFirewall.5] Tindakan stateless default untuk kebijakan Network Firewall harus drop atau forward untuk paket yang terfragmentasi
- [NetworkFirewall.6] Grup aturan Stateless Network Firewall tidak boleh kosong
- [NetworkFirewall.7] Firewall Firewall Jaringan harus diberi tag
- [NetworkFirewall.8] Kebijakan firewall Network Firewall harus ditandai
- [NetworkFirewall.9] Firewall Firewall Jaringan harus mengaktifkan perlindungan penghapusan
- [Opensearch.1] OpenSearch domain harus mengaktifkan enkripsi saat istirahat
- [Opensearch.2] OpenSearch domain tidak boleh diakses publik
- [Opensearch.3] OpenSearch domain harus mengenkripsi data yang dikirim antar node
- [Opensearch.4] login kesalahan OpenSearch domain ke Log harus diaktifkan CloudWatch
- [Opensearch.5] OpenSearch domain harus mengaktifkan pencatatan audit
- [Opensearch.6] OpenSearch domain harus memiliki setidaknya tiga node data
- [Opensearch.7] OpenSearch domain harus mengaktifkan kontrol akses berbutir halus
- [Opensearch.8] Koneksi ke OpenSearch domain harus dienkripsi menggunakan kebijakan keamanan TLS terbaru
- [Opensearch.9] domain harus ditandai OpenSearch
- [Opensearch.11] OpenSearch domain harus memiliki setidaknya tiga node primer khusus
- [PCA.1] otoritas sertifikat AWS Private CA root harus dinonaktifkan
- [RDS.7] Cluster RDS harus mengaktifkan perlindungan penghapusan
- [RDS.9] Instans RDS DB harus menerbitkan log ke Log CloudWatch
- [RDS.10] Otentikasi IAM harus dikonfigurasi untuk instance RDS
- [RDS.12] Otentikasi IAM harus dikonfigurasi untuk cluster RDS
- [RDS.13] Peningkatan versi minor otomatis RDS harus diaktifkan
- [RDS.14] Cluster Amazon Aurora seharusnya mengaktifkan backtracking
- [RDS.15] Cluster RDS DB harus dikonfigurasi untuk beberapa Availability Zone

- [RDS.24] Kluster Database RDS harus menggunakan nama pengguna administrator khusus
- [RDS.25] Instans database RDS harus menggunakan nama pengguna administrator khusus
- [RDS.26] Instans RDS DB harus dilindungi oleh rencana cadangan
- [RDS.28] Cluster RDS DB harus ditandai
- [RDS.29] Snapshot cluster RDS DB harus ditandai
- [RDS.30] Instans RDS DB harus ditandai
- [RDS.31] Grup keamanan RDS DB harus ditandai
- [RDS.32] Snapshot RDS DB harus ditandai
- [RDS.33] Grup subnet RDS DB harus ditandai
- [RDS.34] Cluster Aurora MySQL DB harus menerbitkan log audit ke Log CloudWatch
- [RDS.35] Cluster RDS DB harus mengaktifkan peningkatan versi minor otomatis
- [Redshift.3] Cluster Amazon Redshift harus mengaktifkan snapshot otomatis
- [Redshift.7] Cluster Redshift harus menggunakan perutean VPC yang ditingkatkan
- [Redshift.10] Cluster Redshift harus dienkripsi saat istirahat
- [Redshift.11] Cluster Redshift harus ditandai
- [Redshift.12] Langganan pemberitahuan acara Redshift harus ditandai
- [Redshift.13] Snapshot cluster Redshift harus ditandai
- [Redshift.14] Grup subnet cluster Redshift harus ditandai
- [Redshift.15] Grup keamanan Redshift harus mengizinkan masuknya port cluster hanya dari asal yang dibatasi
- [Route53.1] Pemeriksaan kesehatan rute 53 harus ditandai
- [Route53.2] Route 53 zona yang dihosting publik harus mencatat kueri DNS
- [S3.1] Bucket tujuan umum S3 harus mengaktifkan pengaturan akses publik blok
- [S3.8] Bucket tujuan umum S3 harus memblokir akses publik
- [S3.14] Bucket tujuan umum S3 harus mengaktifkan versi
- [SageMaker.1] Instans SageMaker notebook Amazon seharusnya tidak memiliki akses internet langsung
- [SageMaker.4] varian produksi SageMaker titik akhir harus memiliki jumlah instance awal yang lebih besar dari 1
- [SES.1] Daftar kontak SES harus ditandai
- [SES.2] Set konfigurasi SES harus ditandai

- [SecretsManager.3] Hapus rahasia Secrets Manager yang tidak digunakan
- [SecretsManager.4] Rahasia Secrets Manager harus diputar dalam jumlah hari tertentu
- [SecretsManager.5] Rahasia Secrets Manager harus diberi tag
- [ServiceCatalog.1] Portofolio Service Catalog harus dibagikan hanya dalam suatu organisasi AWS
- [SNS.3] Topik SNS harus ditandai
- [SQS.2] Antrian SQS harus ditandai
- [StepFunctions.2] Aktivitas Step Functions harus diberi tag
- [Transfer.1] AWS Transfer Family alur kerja harus ditandai
- [Transfer.2] Server Transfer Family tidak boleh menggunakan protokol FTP untuk koneksi titik akhir
- [WAF.1] Pencatatan ACL Web Global AWS WAF Klasik harus diaktifkan
- [WAF.3] Kelompok aturan Regional AWS WAF Klasik harus memiliki setidaknya satu aturan
- [WAF.6] Aturan global AWS WAF klasik harus memiliki setidaknya satu syarat
- [WAF.7] Kelompok aturan global AWS WAF klasik harus memiliki setidaknya satu aturan
- [WAF.8] ACL web global AWS WAF klasik harus memiliki setidaknya satu aturan atau kelompok aturan
- [WAF.11] pencatatan ACL AWS WAF web harus diaktifkan

Eropa (Frankfurt)

Kontrol berikut tidak didukung di Eropa (Frankfurt).

- [CloudFront.1] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi
- [CloudFront.3] CloudFront distribusi harus memerlukan enkripsi dalam perjalanan
- [CloudFront.4] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi
- [CloudFront.5] CloudFront distribusi seharusnya mengaktifkan logging
- [CloudFront.6] CloudFront distribusi harus mengaktifkan WAF
- [CloudFront.7] CloudFront distribusi harus menggunakan sertifikat SSL/TLS khusus
- [CloudFront.8] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS
- [CloudFront.9] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus
- [CloudFront.10] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal khusus
- [CloudFront.12] CloudFront distribusi seharusnya tidak menunjukkan asal S3 yang tidak ada

- [CloudFront.13] CloudFront distribusi harus menggunakan kontrol akses asal
- [CloudFront.14] CloudFront distribusi harus ditandai
- [ECR.4] Repositori publik ECR harus ditandai
- [GlobalAccelerator.1] Akselerator Akselerator Global harus diberi tag
- [IAM.26] Sertifikat SSL/TLS kedaluwarsa yang dikelola di IAM harus dihapus
- [RDS.31] Grup keamanan RDS DB harus ditandai
- [Route53.1] Pemeriksaan kesehatan rute 53 harus ditandai
- [Route53.2] Route 53 zona yang dihosting publik harus mencatat kueri DNS
- [WAF.1] Pencatatan ACL Web Global AWS WAF Klasik harus diaktifkan
- [WAF.6] Aturan global AWS WAF klasik harus memiliki setidaknya satu syarat
- [WAF.7] Kelompok aturan global AWS WAF klasik harus memiliki setidaknya satu aturan
- [WAF.8] ACL web global AWS WAF klasik harus memiliki setidaknya satu aturan atau kelompok aturan

Eropa (Irlandia)

Kontrol berikut tidak didukung di Eropa (Irlandia).

- [CloudFront.1] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi
- [CloudFront.3] CloudFront distribusi harus memerlukan enkripsi dalam perjalanan
- [CloudFront.4] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi
- [CloudFront.5] CloudFront distribusi seharusnya mengaktifkan logging
- [CloudFront.6] CloudFront distribusi harus mengaktifkan WAF
- [CloudFront.7] CloudFront distribusi harus menggunakan sertifikat SSL/TLS khusus
- [CloudFront.8] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS
- [CloudFront.9] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus
- [CloudFront.10] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal khusus
- [CloudFront.12] CloudFront distribusi seharusnya tidak menunjukkan asal S3 yang tidak ada
- [CloudFront.13] CloudFront distribusi harus menggunakan kontrol akses asal
- [CloudFront.14] CloudFront distribusi harus ditandai
- [DataFirehose.1] Aliran pengiriman Firehose harus dienkripsi saat istirahat

- [DMS.10] Titik akhir DMS untuk database Neptunus harus mengaktifkan otorisasi IAM
- [DMS.11] Titik akhir DMS untuk MongoDB harus mengaktifkan mekanisme otentikasi
- [DMS.12] Titik akhir DMS untuk Redis harus mengaktifkan TLS
- [DynamoDB.7] Cluster DynamoDB Accelerator harus dienkripsi saat transit
- [ECR.4] Repositori publik ECR harus ditandai
- [EFS.6] Target pemasangan EFS tidak boleh dikaitkan dengan subnet publik
- [EKS.3] Kluster EKS harus menggunakan rahasia Kubernetes terenkripsi
- [FSX.2] Sistem file FSx for Lustre harus dikonfigurasi untuk menyalin tag ke cadangan
- [GlobalAccelerator.1] Akselerator Akselerator Global harus diberi tag
- [IAM.26] Sertifikat SSL/TLS kedaluwarsa yang dikelola di IAM harus dihapus
- [MQ.2] Broker ActiveMQ harus mengalirkan log audit ke CloudWatch
- [MQ.3] Broker Amazon MQ harus mengaktifkan peningkatan versi minor otomatis
- [Opensearch.11] OpenSearch domain harus memiliki setidaknya tiga node primer khusus
- [Redshift.15] Grup keamanan Redshift harus mengizinkan masuknya port cluster hanya dari asal yang dibatasi
- [Route53.1] Pemeriksaan kesehatan rute 53 harus ditandai
- [Route53.2] Route 53 zona yang dihosting publik harus mencatat kueri DNS
- [SageMaker.4] varian produksi SageMaker titik akhir harus memiliki jumlah instance awal yang lebih besar dari 1
- [ServiceCatalog.1] Portofolio Service Catalog harus dibagikan hanya dalam suatu organisasi AWS
- [Transfer.2] Server Transfer Family tidak boleh menggunakan protokol FTP untuk koneksi titik akhir
- [WAF.1] Pencatatan ACL Web Global AWS WAF Klasik harus diaktifkan
- [WAF.6] Aturan global AWS WAF klasik harus memiliki setidaknya satu syarat
- [WAF.7] Kelompok aturan global AWS WAF klasik harus memiliki setidaknya satu aturan
- [WAF.8] ACL web global AWS WAF klasik harus memiliki setidaknya satu aturan atau kelompok aturan

Eropa (London)

Kontrol berikut tidak didukung di Eropa (London).

- [CloudFront.1] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi

- [CloudFront.3] CloudFront distribusi harus memerlukan enkripsi dalam perjalanan
- [CloudFront.4] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi
- [CloudFront.5] CloudFront distribusi seharusnya mengaktifkan logging
- [CloudFront.6] CloudFront distribusi harus mengaktifkan WAF
- [CloudFront.7] CloudFront distribusi harus menggunakan sertifikat SSL/TLS khusus
- [CloudFront.8] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS
- [CloudFront.9] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus
- [CloudFront.10] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal khusus
- [CloudFront.12] CloudFront distribusi seharusnya tidak menunjukkan asal S3 yang tidak ada
- [CloudFront.13] CloudFront distribusi harus menggunakan kontrol akses asal
- [CloudFront.14] CloudFront distribusi harus ditandai
- [DataFirehose.1] Aliran pengiriman Firehose harus dienkripsi saat istirahat
- [DMS.10] Titik akhir DMS untuk database Neptunus harus mengaktifkan otorisasi IAM
- [DMS.11] Titik akhir DMS untuk MongoDB harus mengaktifkan mekanisme otentikasi
- [DMS.12] Titik akhir DMS untuk Redis harus mengaktifkan TLS
- [DynamoDB.7] Cluster DynamoDB Accelerator harus dienkripsi saat transit
- [EC2.24] Jenis instans paravirtual Amazon EC2 tidak boleh digunakan
- [ECR.4] Repositori publik ECR harus ditandai
- [EFS.6] Target pemasangan EFS tidak boleh dikaitkan dengan subnet publik
- [EKS.3] Kluster EKS harus menggunakan rahasia Kubernetes terenkripsi
- [FSX.2] Sistem file FSx for Lustre harus dikonfigurasi untuk menyalin tag ke cadangan
- [GlobalAccelerator.1] Akselerator Akselerator Global harus diberi tag
- [IAM.26] Sertifikat SSL/TLS kedaluwarsa yang dikelola di IAM harus dihapus
- [MQ.2] Broker ActiveMQ harus mengalirkan log audit ke CloudWatch
- [MQ.3] Broker Amazon MQ harus mengaktifkan peningkatan versi minor otomatis
- [Opensearch.11] OpenSearch domain harus memiliki setidaknya tiga node primer khusus
- [RDS.31] Grup keamanan RDS DB harus ditandai
- [Redshift.15] Grup keamanan Redshift harus mengizinkan masuknya port cluster hanya dari asal yang dibatasi
- [Route53.1] Pemeriksaan kesehatan rute 53 harus ditandai

- [Route53.2] Route 53 zona yang dihosting publik harus mencatat kueri DNS
- [SageMaker.4] varian produksi SageMaker titik akhir harus memiliki jumlah instance awal yang lebih besar dari 1
- [ServiceCatalog.1] Portofolio Service Catalog harus dibagikan hanya dalam suatu organisasi AWS
- [Transfer.2] Server Transfer Family tidak boleh menggunakan protokol FTP untuk koneksi titik akhir
- [WAF.1] Pencatatan ACL Web Global AWS WAF Klasik harus diaktifkan
- [WAF.6] Aturan global AWS WAF klasik harus memiliki setidaknya satu syarat
- [WAF.7] Kelompok aturan global AWS WAF klasik harus memiliki setidaknya satu aturan
- [WAF.8] ACL web global AWS WAF klasik harus memiliki setidaknya satu aturan atau kelompok aturan

Eropa (Milan)

Kontrol berikut tidak didukung di Eropa (Milan).

- [ACM.1] Sertifikat yang diimpor dan diterbitkan ACM harus diperbarui setelah jangka waktu tertentu
- [ApiGateway.1] API Gateway REST WebSocket dan pencatatan eksekusi API harus diaktifkan
- [CloudFront.1] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi
- [CloudFront.3] CloudFront distribusi harus memerlukan enkripsi dalam perjalanan
- [CloudFront.4] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi
- [CloudFront.5] CloudFront distribusi seharusnya mengaktifkan logging
- [CloudFront.6] CloudFront distribusi harus mengaktifkan WAF
- [CloudFront.7] CloudFront distribusi harus menggunakan sertifikat SSL/TLS khusus
- [CloudFront.8] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS
- [CloudFront.9] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus
- [CloudFront.10] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal khusus
- [CloudFront.12] CloudFront distribusi seharusnya tidak menunjukkan asal S3 yang tidak ada
- [CloudFront.13] CloudFront distribusi harus menggunakan kontrol akses asal
- [CloudFront.14] CloudFront distribusi harus ditandai
- [CodeBuild.1] URL repositori sumber CodeBuild Bitbucket tidak boleh berisi kredensyal sensitif
- [CodeBuild.2] variabel lingkungan CodeBuild proyek tidak boleh berisi kredensil teks yang jelas

- [DataFirehose.1] Aliran pengiriman Firehose harus dienkripsi saat istirahat
- [DMS.1] Instans replikasi Layanan Migrasi Database tidak boleh bersifat publik
- [DMS.10] Titik akhir DMS untuk database Neptunus harus mengaktifkan otorisasi IAM
- [DMS.11] Titik akhir DMS untuk MongoDB harus mengaktifkan mekanisme otentikasi
- [DMS.12] Titik akhir DMS untuk Redis harus mengaktifkan TLS
- [DynamoDB.3] Cluster DynamoDB Accelerator (DAX) harus dienkripsi saat istirahat
- [DynamoDB.7] Cluster DynamoDB Accelerator harus dienkripsi saat transit
- [EC2.3] Volume Amazon EBS yang terpasang harus dienkripsi saat istirahat
- [EC2.4] Instans EC2 yang dihentikan harus dihapus setelah periode waktu tertentu
- [EC2.8] Instans EC2 harus menggunakan Layanan Metadata Instance Versi 2 (IMDSv2)
- [EC2.12] EIP Amazon EC2 yang tidak digunakan harus dihapus
- [EC2.13] Grup keamanan tidak boleh mengizinkan masuknya dari 0.0.0.0/0 atau: :/0 ke port 22
- [EC2.14] Grup keamanan tidak boleh mengizinkan masuknya dari 0.0.0.0/0 atau: :/0 ke port 3389
- [EC2.24] Jenis instans paravirtual Amazon EC2 tidak boleh digunakan
- [ECR.4] Repositori publik ECR harus ditandai
- [ECS.12] Cluster ECS harus menggunakan Wawasan Kontainer
- [EFS.1] Sistem File Elastis harus dikonfigurasi untuk mengenkripsi data file saat istirahat menggunakan AWS KMS
- [EFS.2] Volume Amazon EFS harus dalam rencana cadangan
- [EFS.6] Target pemasangan EFS tidak boleh dikaitkan dengan subnet publik
- [EKS.1] Titik akhir klaster EKS seharusnya tidak dapat diakses publik
- [EKS.3] Kluster EKS harus menggunakan rahasia Kubernetes terenkripsi
- [ELB.1] Application Load Balancer harus dikonfigurasi untuk mengalihkan semua permintaan HTTP ke HTTPS
- [ELB.2] Classic Load Balancer dengan pendengar SSL/HTTPS harus menggunakan sertifikat yang disediakan oleh AWS Certificate Manager
- [ELB.4] Application Load Balancer harus dikonfigurasi untuk menjatuhkan header http
- [ELB.8] Classic Load Balancer dengan pendengar SSL harus menggunakan kebijakan keamanan yang telah ditentukan sebelumnya yang memiliki urasi yang kuat AWS Config
- [ELB.16] Application Load Balancers harus dikaitkan dengan ACL web AWS WAF
- [EMR.1] Node primer cluster EMR Amazon seharusnya tidak memiliki alamat IP publik

- [ES.3] Domain Elasticsearch harus mengenkripsi data yang dikirim antar node
- [EventBridge.4] titik akhir EventBridge global harus mengaktifkan replikasi acara
- [FSX.1] FSx untuk sistem file OpenZFS harus dikonfigurasi untuk menyalin tag ke cadangan dan volume
- [FSX.2] Sistem file FSx for Lustre harus dikonfigurasi untuk menyalin tag ke cadangan
- [GlobalAccelerator.1] Akselerator Akselerator Global harus diberi tag
- [GuardDuty.1] GuardDuty harus diaktifkan
- [IAM.3] Kunci akses pengguna IAM harus diputar setiap 90 hari atau kurang
- [IAM.18] Memastikan peran dukungan telah dibuat untuk mengelola insiden dengan AWS Support
- [IAM.26] Sertifikat SSL/TLS kedaluwarsa yang dikelola di IAM harus dihapus
- [IoT.1] profil AWS IoT Core keamanan harus ditandai
- [IoT.2] tindakan AWS IoT Core mitigasi harus ditandai
- AWS IoT Core Dimensi [IoT.3] harus ditandai
- [IoT.4] AWS IoT Core otorisasi harus diberi tag
- [IoT.5] alias AWS IoT Core peran harus ditandai
- AWS IoT Core Kebijakan [IoT.6] harus ditandai
- [KMS.3] tidak AWS KMS keys boleh dihapus secara tidak sengaja
- [MQ.2] Broker ActiveMQ harus mengalirkan log audit ke CloudWatch
- [MQ.3] Broker Amazon MQ harus mengaktifkan peningkatan versi minor otomatis
- [Neptunus.1] Cluster DB Neptunus harus dienkripsi saat istirahat
- [Neptune.2] Cluster DB Neptunus harus menerbitkan log audit ke Log CloudWatch
- [Neptune.3] Snapshot cluster Neptunus DB seharusnya tidak publik
- [Neptunus.4] Cluster DB Neptunus harus mengaktifkan perlindungan penghapusan
- [Neptunus.5] Cluster DB Neptunus harus mengaktifkan cadangan otomatis
- [Neptune.6] Snapshot cluster Neptunus DB harus dienkripsi saat istirahat
- [Neptunus.7] Cluster DB Neptunus harus mengaktifkan otentikasi basis data IAM
- [Neptunus.8] Cluster DB Neptunus harus dikonfigurasi untuk menyalin tag ke snapshot
- [Neptunus.9] Cluster DB Neptunus harus digunakan di beberapa Availability Zone
- [Opensearch.1] OpenSearch domain harus mengaktifkan enkripsi saat istirahat
- [Opensearch.2] OpenSearch domain tidak boleh diakses publik
- [Opensearch.3] OpenSearch domain harus mengenkripsi data yang dikirim antar node

- [Opensearch.4] login kesalahan OpenSearch domain ke Log harus diaktifkan CloudWatch
- [Opensearch.5] OpenSearch domain harus mengaktifkan pencatatan audit
- [Opensearch.6] OpenSearch domain harus memiliki setidaknya tiga node data
- [Opensearch.7] OpenSearch domain harus mengaktifkan kontrol akses berbutir halus
- [Opensearch.8] Koneksi ke OpenSearch domain harus dienkripsi menggunakan kebijakan keamanan TLS terbaru
- [Opensearch.11] OpenSearch domain harus memiliki setidaknya tiga node primer khusus
- [RDS.1] Snapshot RDS harus pribadi
- [RDS.4] Snapshot cluster RDS dan snapshot database harus dienkripsi saat istirahat
- [RDS.9] Instans RDS DB harus menerbitkan log ke Log CloudWatch
- [RDS.14] Cluster Amazon Aurora seharusnya mengaktifkan backtracking
- [RDS.31] Grup keamanan RDS DB harus ditandai
- [Redshift.2] Koneksi ke cluster Amazon Redshift harus dienkripsi saat transit
- [Redshift.3] Cluster Amazon Redshift harus mengaktifkan snapshot otomatis
- [Redshift.15] Grup keamanan Redshift harus mengizinkan masuknya port cluster hanya dari asal yang dibatasi
- [Route53.1] Pemeriksaan kesehatan rute 53 harus ditandai
- [Route53.2] Route 53 zona yang dihosting publik harus mencatat kueri DNS
- [SageMaker.1] Instans SageMaker notebook Amazon seharusnya tidak memiliki akses internet langsung
- [SageMaker.4] varian produksi SageMaker titik akhir harus memiliki jumlah instance awal yang lebih besar dari 1
- [ServiceCatalog.1] Portofolio Service Catalog harus dibagikan hanya dalam suatu organisasi AWS
- [SSM.2] Instans Amazon EC2 yang dikelola oleh Systems Manager harus memiliki status kepatuhan patch COMPLIANT setelah instalasi patch
- [SSM.3] Instans Amazon EC2 yang dikelola oleh Systems Manager harus memiliki status kepatuhan asosiasi COMPLIANT
- [Transfer.2] Server Transfer Family tidak boleh menggunakan protokol FTP untuk koneksi titik akhir
- [WAF.1] Pencatatan ACL Web Global AWS WAF Klasik harus diaktifkan
- [WAF.6] Aturan global AWS WAF klasik harus memiliki setidaknya satu syarat
- [WAF.7] Kelompok aturan global AWS WAF klasik harus memiliki setidaknya satu aturan

- [WAF.8] ACL web global AWS WAF klasik harus memiliki setidaknya satu aturan atau kelompok aturan
- [WAF.11] pencatatan ACL AWS WAF web harus diaktifkan

Eropa (Paris)

Kontrol berikut tidak didukung di Eropa (Paris).

- [CloudFront.1] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi
- [CloudFront.3] CloudFront distribusi harus memerlukan enkripsi dalam perjalanan
- [CloudFront.4] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi
- [CloudFront.5] CloudFront distribusi seharusnya mengaktifkan logging
- [CloudFront.6] CloudFront distribusi harus mengaktifkan WAF
- [CloudFront.7] CloudFront distribusi harus menggunakan sertifikat SSL/TLS khusus
- [CloudFront.8] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS
- [CloudFront.9] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus
- [CloudFront.10] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal khusus
- [CloudFront.12] CloudFront distribusi seharusnya tidak menunjukkan asal S3 yang tidak ada
- [CloudFront.13] CloudFront distribusi harus menggunakan kontrol akses asal
- [CloudFront.14] CloudFront distribusi harus ditandai
- [DataFirehose.1] Aliran pengiriman Firehose harus dienkripsi saat istirahat
- [DMS.10] Titik akhir DMS untuk database Neptunus harus mengaktifkan otorisasi IAM
- [DMS.11] Titik akhir DMS untuk MongoDB harus mengaktifkan mekanisme otentikasi
- [DMS.12] Titik akhir DMS untuk Redis harus mengaktifkan TLS
- [DynamoDB.7] Cluster DynamoDB Accelerator harus dienkripsi saat transit
- [EC2.24] Jenis instans paravirtual Amazon EC2 tidak boleh digunakan
- [ECR.4] Repositori publik ECR harus ditandai
- [EFS.6] Target pemasangan EFS tidak boleh dikaitkan dengan subnet publik
- [EKS.3] Kluster EKS harus menggunakan rahasia Kubernetes terenkripsi
- [FSX.1] FSx untuk sistem file OpenZFS harus dikonfigurasi untuk menyalin tag ke cadangan dan volume

- [FSX.2] Sistem file FSx for Lustre harus dikonfigurasi untuk menyalin tag ke cadangan
- [GlobalAccelerator.1] Akselerator Akselerator Global harus diberi tag
- [IAM.26] Sertifikat SSL/TLS kedaluwarsa yang dikelola di IAM harus dihapus
- [MQ.2] Broker ActiveMQ harus mengalirkan log audit ke CloudWatch
- [MQ.3] Broker Amazon MQ harus mengaktifkan peningkatan versi minor otomatis
- [Opensearch.11] OpenSearch domain harus memiliki setidaknya tiga node primer khusus
- [RDS.31] Grup keamanan RDS DB harus ditandai
- [Redshift.15] Grup keamanan Redshift harus mengizinkan masuknya port cluster hanya dari asal yang dibatasi
- [Route53.1] Pemeriksaan kesehatan rute 53 harus ditandai
- [Route53.2] Route 53 zona yang dihosting publik harus mencatat kueri DNS
- [SageMaker.4] varian produksi SageMaker titik akhir harus memiliki jumlah instance awal yang lebih besar dari 1
- [ServiceCatalog.1] Portofolio Service Catalog harus dibagikan hanya dalam suatu organisasi AWS
- [Transfer.2] Server Transfer Family tidak boleh menggunakan protokol FTP untuk koneksi titik akhir
- [WAF.1] Pencatatan ACL Web Global AWS WAF Klasik harus diaktifkan
- [WAF.6] Aturan global AWS WAF klasik harus memiliki setidaknya satu syarat
- [WAF.7] Kelompok aturan global AWS WAF klasik harus memiliki setidaknya satu aturan
- [WAF.8] ACL web global AWS WAF klasik harus memiliki setidaknya satu aturan atau kelompok aturan

Eropa (Spanyol)

Kontrol berikut tidak didukung di Eropa (Spanyol).

- [ACM.1] Sertifikat yang diimpor dan diterbitkan ACM harus diperbarui setelah jangka waktu tertentu
- [ACM.2] Sertifikat RSA yang dikelola oleh ACM harus menggunakan panjang kunci minimal 2.048 bit
- [Akun.2] Akun AWS harus menjadi bagian dari organisasi AWS Organizations
- [ApiGateway.1] API Gateway REST WebSocket dan pencatatan eksekusi API harus diaktifkan
- [ApiGateway.2] Tahapan API Gateway REST API harus dikonfigurasi untuk menggunakan sertifikat SSL untuk otentikasi backend

- [ApiGateway.3] Tahapan API Gateway REST API harus mengaktifkan penelusuran AWS X-Ray
- [ApiGateway.4] API Gateway harus dikaitkan dengan ACL Web WAF
- [ApiGateway.8] Rute API Gateway harus menentukan jenis otorisasi
- [ApiGateway.9] Pencatatan akses harus dikonfigurasi untuk Tahapan API Gateway V2
- [AppSync.2] AWS AppSync harus mengaktifkan logging tingkat lapangan
- [AppSync.5] AWS AppSync GraphQL API tidak boleh diautentikasi dengan kunci API
- [Athena.2] Katalog data Athena harus diberi tag
- [Athena.3] Kelompok kerja Athena harus ditandai
- [AutoScaling.1] Grup Auto Scaling yang terkait dengan penyeimbang beban harus menggunakan pemeriksaan kesehatan ELB
- [Autoscaling.5] Instans Amazon EC2 yang diluncurkan menggunakan konfigurasi peluncuran grup Auto Scaling seharusnya tidak memiliki alamat IP Publik
- [Backup.1] titik AWS Backup pemulihan harus dienkripsi saat istirahat
- [Backup.2] poin AWS Backup pemulihan harus ditandai
- [Backup.3] AWS Backup brankas harus ditandai
- [Backup.4] rencana AWS Backup laporan harus ditandai
- [Backup.5] rencana AWS Backup cadangan harus ditandai
- [CloudFormation.2] CloudFormation tumpukan harus ditandai
- [CloudFront.1] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi
- [CloudFront.3] CloudFront distribusi harus memerlukan enkripsi dalam perjalanan
- [CloudFront.4] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi
- [CloudFront.5] CloudFront distribusi seharusnya mengaktifkan logging
- [CloudFront.6] CloudFront distribusi harus mengaktifkan WAF
- [CloudFront.7] CloudFront distribusi harus menggunakan sertifikat SSL/TLS khusus
- [CloudFront.8] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS
- [CloudFront.9] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus
- [CloudFront.10] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal khusus
- [CloudFront.12] CloudFront distribusi seharusnya tidak menunjukkan asal S3 yang tidak ada
- [CloudFront.13] CloudFront distribusi harus menggunakan kontrol akses asal
- [CloudFront.14] CloudFront distribusi harus ditandai

- [CloudTrail.6] Pastikan bucket S3 yang digunakan untuk menyimpan CloudTrail log tidak dapat diakses publik
- [CloudTrail.7] Pastikan pencatatan akses bucket S3 diaktifkan pada bucket CloudTrail S3
- [CloudWatch.16] grup CloudWatch log harus dipertahankan untuk jangka waktu tertentu
- [CodeArtifact.1] CodeArtifact repositori harus diberi tag
- [CodeBuild.1] URL repositori sumber CodeBuild Bitbucket tidak boleh berisi kredensyal sensitif
- [CodeBuild.2] variabel lingkungan CodeBuild proyek tidak boleh berisi kredensil teks yang jelas
- [CodeBuild.3] Log CodeBuild S3 harus dienkripsi
- [CodeBuild.4] lingkungan CodeBuild proyek harus memiliki urasi logging AWS Config
- [DataFirehose.1] Aliran pengiriman Firehose harus dienkripsi saat istirahat
- [Detective.1] Grafik perilaku detektif harus diberi tag
- [DMS.1] Instans replikasi Layanan Migrasi Database tidak boleh bersifat publik
- [DMS.2] Sertifikat DMS harus ditandai
- [DMS.3] Langganan acara DMS harus ditandai
- [DMS.4] Contoh replikasi DMS harus ditandai
- [DMS.5] Grup subnet replikasi DMS harus ditandai
- [DMS.6] Instans replikasi DMS harus mengaktifkan peningkatan versi minor otomatis
- [DMS.7] Tugas replikasi DMS untuk database target seharusnya mengaktifkan logging
- [DMS.8] Tugas replikasi DMS untuk database sumber seharusnya mengaktifkan logging
- [DMS.9] Titik akhir DMS harus menggunakan SSL
- [DMS.10] Titik akhir DMS untuk database Neptunus harus mengaktifkan otorisasi IAM
- [DMS.11] Titik akhir DMS untuk MongoDB harus mengaktifkan mekanisme otentikasi
- [DMS.12] Titik akhir DMS untuk Redis harus mengaktifkan TLS
- [DocumentDB.1] Cluster Amazon DocumentDB harus dienkripsi saat istirahat
- [DocumentDB.2] Cluster Amazon DocumentDB harus memiliki periode retensi cadangan yang memadai
- [DocumentDB.3] Cuplikan cluster manual Amazon DocumentDB seharusnya tidak bersifat publik
- [DocumentDB.4] Cluster Amazon DocumentDB harus mempublikasikan log audit ke Log CloudWatch
- [DocumentDB.5] Cluster Amazon DocumentDB harus mengaktifkan perlindungan penghapusan
- [DynamoDB.1] Tabel DynamoDB harus secara otomatis menskalakan kapasitas sesuai permintaan

- [DynamoDB.2] Tabel DynamoDB harus mengaktifkan pemulihan point-in-time
- [DynamoDB.3] Cluster DynamoDB Accelerator (DAX) harus dienkripsi saat istirahat
- [DynamoDB.4] Tabel DynamoDB harus ada dalam rencana cadangan
- [DynamoDB.7] Cluster DynamoDB Accelerator harus dienkripsi saat transit
- [EC2.1] Snapshot Amazon EBS tidak boleh dipulihkan secara publik
- [EC2.2] Grup keamanan default VPC tidak boleh mengizinkan lalu lintas masuk atau keluar
- [EC2.3] Volume Amazon EBS yang terpasang harus dienkripsi saat istirahat
- [EC2.4] Instans EC2 yang dihentikan harus dihapus setelah periode waktu tertentu
- [EC2.6] Pencatatan aliran VPC harus diaktifkan di semua VPC
- [EC2.7] Enkripsi default EBS harus diaktifkan
- [EC2.8] Instans EC2 harus menggunakan Layanan Metadata Instance Versi 2 (IMDSv2)
- [EC2.9] Instans Amazon EC2 seharusnya tidak memiliki alamat IPv4 publik
- [EC2.10] Amazon EC2 harus dikonfigurasi untuk menggunakan titik akhir VPC yang dibuat untuk layanan Amazon EC2
- [EC2.13] Grup keamanan tidak boleh mengizinkan masuknya dari 0.0.0.0/0 atau: :/0 ke port 22
- [EC2.14] Grup keamanan tidak boleh mengizinkan masuknya dari 0.0.0.0/0 atau: :/0 ke port 3389
- [EC2.15] Subnet Amazon EC2 seharusnya tidak secara otomatis menetapkan alamat IP publik
- [EC2.16] Daftar Kontrol Akses Jaringan yang Tidak Digunakan harus dihapus
- [EC2.17] Instans Amazon EC2 tidak boleh menggunakan beberapa ENI
- [EC2.18] Grup keamanan seharusnya hanya mengizinkan lalu lintas masuk yang tidak terbatas untuk port resmi
- [EC2.20] Kedua terowongan VPN untuk koneksi VPN Site-to-Site harus AWS aktif
- [EC2.22] Grup keamanan Amazon EC2 yang tidak digunakan harus dihapus
- [EC2.23] Amazon EC2 Transit Gateways seharusnya tidak secara otomatis menerima permintaan lampiran VPC
- [EC2.24] Jenis instans paravirtual Amazon EC2 tidak boleh digunakan
- [EC2.25] Templat peluncuran Amazon EC2 tidak boleh menetapkan IP publik ke antarmuka jaringan
- [EC2.28] Volume EBS harus dicakup oleh rencana cadangan
- [EC2.34] Tabel rute gateway transit EC2 harus ditandai
- [EC2.40] Gerbang EC2 NAT harus ditandai

- [EC2.48] Log aliran VPC Amazon harus ditandai
- [EC2.51] Titik akhir EC2 Client VPN harus mengaktifkan pencatatan koneksi klien
- [ECR.1] Repositori pribadi ECR harus memiliki pemindaian gambar yang dikonfigurasi
- [ECR.2] Repositori pribadi ECR harus memiliki kekekalan tag yang dikonfigurasi
- [ECR.3] Repositori ECR harus memiliki setidaknya satu kebijakan siklus hidup yang dikonfigurasi
- [ECR.4] Repositori publik ECR harus ditandai
- [ECS.1] Definisi tugas Amazon ECS harus memiliki mode jaringan yang aman dan definisi pengguna.
- [ECS.9] Definisi tugas ECS harus memiliki konfigurasi logging
- [EFS.1] Sistem File Elastis harus dikonfigurasi untuk mengenkripsi data file saat istirahat menggunakan AWS KMS
- [EFS.2] Volume Amazon EFS harus dalam rencana cadangan
- [EFS.3] Titik akses EFS harus menegakkan direktori root
- [EFS.4] Titik akses EFS harus menegakkan identitas pengguna
- [EFS.5] Titik akses EFS harus ditandai
- [EFS.6] Target pemasangan EFS tidak boleh dikaitkan dengan subnet publik
- [EKS.1] Titik akhir klaster EKS seharusnya tidak dapat diakses publik
- [EKS.2] Kluster EKS harus berjalan pada versi Kubernetes yang didukung
- [EKS.3] Kluster EKS harus menggunakan rahasia Kubernetes terenkripsi
- [ELB.1] Application Load Balancer harus dikonfigurasi untuk mengalihkan semua permintaan HTTP ke HTTPS
- [ELB.2] Classic Load Balancer dengan pendengar SSL/HTTPS harus menggunakan sertifikat yang disediakan oleh AWS Certificate Manager
- [ELB.3] Pendengar Classic Load Balancer harus dikonfigurasi dengan penghentian HTTPS atau TLS
- [ELB.4] Application Load Balancer harus dikonfigurasi untuk menjatuhkan header http
- [ELB.5] Pencatatan aplikasi dan Classic Load Balancer harus diaktifkan
- [ELB.6] Aplikasi, Gateway, dan Network Load Balancer harus mengaktifkan perlindungan penghapusan
- [ELB.8] Classic Load Balancer dengan pendengar SSL harus menggunakan kebijakan keamanan yang telah ditentukan sebelumnya yang memiliki urasi yang kuat AWS Config
- [ELB.9] Classic Load Balancer harus mengaktifkan penyeimbangan beban lintas zona

- [ELB.14] Classic Load Balancer harus dikonfigurasi dengan mode mitigasi desync defensif atau paling ketat
- [ELB.16] Application Load Balancers harus dikaitkan dengan ACL web AWS WAF
- [ElastiCache.1] Cluster ElastiCache Redis harus mengaktifkan pencadangan otomatis
- [ElastiCache.6] ElastiCache untuk grup replikasi Redis sebelum versi 6.0 harus menggunakan Redis AUTH
- [ElastiCache.7] ElastiCache cluster tidak boleh menggunakan grup subnet default
- [ElasticBeanstalk.1] Lingkungan Elastic Beanstalk seharusnya mengaktifkan pelaporan kesehatan yang ditingkatkan
- [ElasticBeanstalk.2] Pembaruan platform yang dikelola Elastic Beanstalk harus diaktifkan
- [ElasticBeanstalk.3] Elastic Beanstalk harus mengalirkan log ke CloudWatch
- [EMR.1] Node primer cluster EMR Amazon seharusnya tidak memiliki alamat IP publik
- [ES.1] Domain Elasticsearch harus mengaktifkan enkripsi saat istirahat
- [ES.2] Domain Elasticsearch tidak boleh diakses publik
- [ES.3] Domain Elasticsearch harus mengenkripsi data yang dikirim antar node
- [ES.4] Kesalahan domain Elasticsearch yang masuk ke CloudWatch Log harus diaktifkan
- [EventBridge.2] bus EventBridge acara harus diberi tag
- [EventBridge.3] bus acara EventBridge khusus harus memiliki kebijakan berbasis sumber daya terlampir
- [EventBridge.4] titik akhir EventBridge global harus mengaktifkan replikasi acara
- [FSX.1] FSx untuk sistem file OpenZFS harus dikonfigurasi untuk menyalin tag ke cadangan dan volume
- [FSX.2] Sistem file FSx for Lustre harus dikonfigurasi untuk menyalin tag ke cadangan
- [GlobalAccelerator.1] Akselerator Akselerator Global harus diberi tag
- AWS Glue Pekerjaan [Glue.1] harus ditandai
- [GuardDuty.1] GuardDuty harus diaktifkan
- [GuardDuty.2] GuardDuty filter harus diberi tag
- [GuardDuty.3] GuardDuty IPset harus ditandai
- [GuardDuty.4] GuardDuty detektor harus ditandai
- [IAM.1] Kebijakan IAM seharusnya tidak mengizinkan hak administratif “*” penuh
- [IAM.2] Pengguna IAM seharusnya tidak memiliki kebijakan IAM yang dilampirkan

- [IAM.3] Kunci akses pengguna IAM harus diputar setiap 90 hari atau kurang
- [IAM.4] Kunci akses pengguna root IAM seharusnya tidak ada
- [IAM.5] MFA harus diaktifkan untuk semua pengguna IAM yang memiliki kata sandi konsol
- [IAM.8] Kredensyal pengguna IAM yang tidak digunakan harus dihapus
- [IAM.18] Memastikan peran dukungan telah dibuat untuk mengelola insiden dengan AWS Support
- [IAM.19] MFA harus diaktifkan untuk semua pengguna IAM
- [IAM.21] Kebijakan terkelola pelanggan IAM yang Anda buat seharusnya tidak mengizinkan tindakan wildcard untuk layanan
- [IAM.22] Kredensyal pengguna IAM yang tidak digunakan selama 45 hari harus dihapus
- [IAM.24] Peran IAM harus ditandai
- [IAM.25] Pengguna IAM harus diberi tag
- [IAM.26] Sertifikat SSL/TLS kedaluwarsa yang dikelola di IAM harus dihapus
- [IAM.27] Identitas IAM seharusnya tidak memiliki kebijakan yang dilampirkan AWSCloudShellFullAccess
- [IoT.1] profil AWS IoT Core keamanan harus ditandai
- [IoT.2] tindakan AWS IoT Core mitigasi harus ditandai
- AWS IoT Core Dimensi [IoT.3] harus ditandai
- [IoT.4] AWS IoT Core otorisasi harus diberi tag
- [IoT.5] alias AWS IoT Core peran harus ditandai
- AWS IoT Core Kebijakan [IoT.6] harus ditandai
- [Kinesis.1] Aliran kinesis harus dienkripsi saat istirahat
- [KMS.1] Kebijakan yang dikelola pelanggan IAM tidak boleh mengizinkan tindakan dekripsi pada semua kunci KMS
- [KMS.2] Prinsipal IAM tidak boleh memiliki kebijakan inline IAM yang memungkinkan tindakan dekripsi pada semua kunci KMS
- [KMS.4] rotasi AWS KMS tombol harus diaktifkan
- [Lambda.1] Kebijakan fungsi Lambda harus melarang akses publik
- [Lambda.2] Fungsi Lambda harus menggunakan runtime yang didukung
- [Lambda.3] Fungsi Lambda harus dalam VPC
- [Lambda.5] Fungsi VPC Lambda harus beroperasi di beberapa Availability Zone
- [Macie.1] Amazon Macie harus diaktifkan

- [Macie.2] Penemuan data sensitif otomatis Macie harus diaktifkan
- [MQ.2] Broker ActiveMQ harus mengalirkan log audit ke CloudWatch
- [MQ.3] Broker Amazon MQ harus mengaktifkan peningkatan versi minor otomatis
- [MQ.4] Broker Amazon MQ harus diberi tag
- [MQ.5] Broker ActiveMQ harus menggunakan mode penerapan aktif/siaga
- [MQ.6] Broker RabbitMQ harus menggunakan mode penerapan cluster
- [MSK.1] Cluster MSK harus dienkripsi saat transit di antara node broker
- [MSK.2] Kluster MSK seharusnya telah meningkatkan pemantauan yang dikonfigurasi
- [Neptunus.1] Cluster DB Neptunus harus dienkripsi saat istirahat
- [Neptune.2] Cluster DB Neptunus harus menerbitkan log audit ke Log CloudWatch
- [Neptune.3] Snapshot cluster Neptunus DB seharusnya tidak publik
- [Neptunus.4] Cluster DB Neptunus harus mengaktifkan perlindungan penghapusan
- [Neptunus.5] Cluster DB Neptunus harus mengaktifkan cadangan otomatis
- [Neptune.6] Snapshot cluster Neptunus DB harus dienkripsi saat istirahat
- [Neptunus.7] Cluster DB Neptunus harus mengaktifkan otentikasi basis data IAM
- [Neptunus.8] Cluster DB Neptunus harus dikonfigurasi untuk menyalin tag ke snapshot
- [Neptunus.9] Cluster DB Neptunus harus digunakan di beberapa Availability Zone
- [NetworkFirewall.1] Firewall Firewall Jaringan harus digunakan di beberapa Availability Zone
- [NetworkFirewall.2] Pencatatan Firewall Jaringan harus diaktifkan
- [NetworkFirewall.3] Kebijakan Network Firewall harus memiliki setidaknya satu kelompok aturan yang terkait
- [NetworkFirewall.4] Tindakan stateless default untuk kebijakan Network Firewall harus drop atau forward untuk paket penuh
- [NetworkFirewall.5] Tindakan stateless default untuk kebijakan Network Firewall harus drop atau forward untuk paket yang terfragmentasi
- [NetworkFirewall.6] Grup aturan Stateless Network Firewall tidak boleh kosong
- [NetworkFirewall.9] Firewall Firewall Jaringan harus mengaktifkan perlindungan penghapusan
- [Opensearch.1] OpenSearch domain harus mengaktifkan enkripsi saat istirahat
- [Opensearch.2] OpenSearch domain tidak boleh diakses publik
- [Opensearch.3] OpenSearch domain harus mengenkripsi data yang dikirim antar node
- [Opensearch.4] login kesalahan OpenSearch domain ke Log harus diaktifkan CloudWatch

- [Opensearch.5] OpenSearch domain harus mengaktifkan pencatatan audit
- [Opensearch.6] OpenSearch domain harus memiliki setidaknya tiga node data
- [Opensearch.7] OpenSearch domain harus mengaktifkan kontrol akses berbutir halus
- [Opensearch.8] Koneksi ke OpenSearch domain harus dienkripsi menggunakan kebijakan keamanan TLS terbaru
- [Opensearch.9] domain harus ditandai OpenSearch
- [Opensearch.10] OpenSearch domain harus memiliki pembaruan perangkat lunak terbaru yang diinstal
- [Opensearch.11] OpenSearch domain harus memiliki setidaknya tiga node primer khusus
- [RDS.1] Snapshot RDS harus pribadi
- [RDS.2] Instans RDS DB harus melarang akses publik, sebagaimana ditentukan oleh urasi PubliclyAccessible AWS Config
- [RDS.3] Instans RDS DB harus mengaktifkan enkripsi saat istirahat
- [RDS.4] Snapshot cluster RDS dan snapshot database harus dienkripsi saat istirahat
- [RDS.5] Instans RDS DB harus dikonfigurasi dengan beberapa Availability Zone
- [RDS.6] Pemantauan yang ditingkatkan harus dikonfigurasi untuk instans RDS DB
- [RDS.7] Cluster RDS harus mengaktifkan perlindungan penghapusan
- [RDS.8] Instans RDS DB harus mengaktifkan perlindungan penghapusan
- [RDS.9] Instans RDS DB harus menerbitkan log ke Log CloudWatch
- [RDS.10] Otentikasi IAM harus dikonfigurasi untuk instance RDS
- [RDS.11] Instans RDS harus mengaktifkan pencadangan otomatis
- [RDS.12] Otentikasi IAM harus dikonfigurasi untuk cluster RDS
- [RDS.13] Peningkatan versi minor otomatis RDS harus diaktifkan
- [RDS.14] Cluster Amazon Aurora seharusnya mengaktifkan backtracking
- [RDS.15] Cluster RDS DB harus dikonfigurasi untuk beberapa Availability Zone
- [RDS.16] Cluster RDS DB harus dikonfigurasi untuk menyalin tag ke snapshot
- [RDS.24] Kluster Database RDS harus menggunakan nama pengguna administrator khusus
- [RDS.26] Instans RDS DB harus dilindungi oleh rencana cadangan
- [RDS.27] Cluster RDS DB harus dienkripsi saat istirahat
- [RDS.28] Cluster RDS DB harus ditandai
- [RDS.31] Grup keamanan RDS DB harus ditandai

- [RDS.34] Cluster Aurora MySQL DB harus menerbitkan log audit ke Log CloudWatch
- [RDS.35] Cluster RDS DB harus mengaktifkan peningkatan versi minor otomatis
- [Redshift.1] Cluster Amazon Redshift harus melarang akses publik
- [Redshift.2] Koneksi ke cluster Amazon Redshift harus dienkripsi saat transit
- [Redshift.3] Cluster Amazon Redshift harus mengaktifkan snapshot otomatis
- [Redshift.6] Amazon Redshift harus mengaktifkan peningkatan otomatis ke versi utama
- [Redshift.7] Cluster Redshift harus menggunakan perutean VPC yang ditingkatkan
- [Redshift.10] Cluster Redshift harus dienkripsi saat istirahat
- [Redshift.12] Langganan pemberitahuan acara Redshift harus ditandai
- [Redshift.15] Grup keamanan Redshift harus mengizinkan masuknya port cluster hanya dari asal yang dibatasi
- [Route53.1] Pemeriksaan kesehatan rute 53 harus ditandai
- [Route53.2] Route 53 zona yang dihosting publik harus mencatat kueri DNS
- [S3.1] Bucket tujuan umum S3 harus mengaktifkan pengaturan akses publik blok
- [S3.5] Bucket tujuan umum S3 harus memerlukan permintaan untuk menggunakan SSL
- [S3.6] Kebijakan bucket tujuan umum S3 harus membatasi akses ke yang lain Akun AWS
- [S3.8] Bucket tujuan umum S3 harus memblokir akses publik
- [S3.9] Bucket tujuan umum S3 harus mengaktifkan pencatatan akses server
- [S3.15] Bucket tujuan umum S3 harus mengaktifkan Object Lock
- [S3.17] Ember tujuan umum S3 harus dienkripsi saat istirahat AWS KMS keys
- [SageMaker.1] Instans SageMaker notebook Amazon seharusnya tidak memiliki akses internet langsung
- [SageMaker.2] instance SageMaker notebook harus diluncurkan dalam VPC khusus
- [SageMaker.3] Pengguna seharusnya tidak memiliki akses root ke instance SageMaker notebook
- [SageMaker.4] varian produksi SageMaker titik akhir harus memiliki jumlah instance awal yang lebih besar dari 1
- [SES.1] Daftar kontak SES harus ditandai
- [SES.2] Set konfigurasi SES harus ditandai
- [SecretsManager.2] Rahasia Secrets Manager yang dikonfigurasi dengan rotasi otomatis harus berhasil diputar
- [ServiceCatalog.1] Portofolio Service Catalog harus dibagikan hanya dalam suatu organisasi AWS

- [SNS.1] Topik SNS harus dienkripsi saat istirahat menggunakan AWS KMS
- [SNS.3] Topik SNS harus ditandai
- [SQS.1] Antrian Amazon SQS harus dienkripsi saat istirahat
- [SQS.2] Antrian SQS harus ditandai
- [SSM.1] Instans Amazon EC2 harus dikelola oleh AWS Systems Manager
- [SSM.2] Instans Amazon EC2 yang dikelola oleh Systems Manager harus memiliki status kepatuhan patch COMPLIANT setelah instalasi patch
- [SSM.3] Instans Amazon EC2 yang dikelola oleh Systems Manager harus memiliki status kepatuhan asosiasi COMPLIANT
- [StepFunctions.1] Mesin status Step Functions seharusnya mengaktifkan logging
- [Transfer.1] AWS Transfer Family alur kerja harus ditandai
- [Transfer.2] Server Transfer Family tidak boleh menggunakan protokol FTP untuk koneksi titik akhir
- [WAF.1] Pencatatan ACL Web Global AWS WAF Klasik harus diaktifkan
- [WAF.2] Aturan Regional AWS WAF Klasik harus memiliki setidaknya satu syarat
- [WAF.3] Kelompok aturan Regional AWS WAF Klasik harus memiliki setidaknya satu aturan
- [WAF.4] ACL web Regional AWS WAF klasik harus memiliki setidaknya satu aturan atau kelompok aturan
- [WAF.6] Aturan global AWS WAF klasik harus memiliki setidaknya satu syarat
- [WAF.7] Kelompok aturan global AWS WAF klasik harus memiliki setidaknya satu aturan
- [WAF.8] ACL web global AWS WAF klasik harus memiliki setidaknya satu aturan atau kelompok aturan
- [WAF.10] ACL AWS WAF web harus memiliki setidaknya satu aturan atau kelompok aturan
- [WAF.11] pencatatan ACL AWS WAF web harus diaktifkan

Eropa (Stockholm)

Kontrol berikut tidak didukung di Eropa (Stockholm).

- [CloudFront.1] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi
- [CloudFront.3] CloudFront distribusi harus memerlukan enkripsi dalam perjalanan
- [CloudFront.4] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi
- [CloudFront.5] CloudFront distribusi seharusnya mengaktifkan logging

- [CloudFront.6] CloudFront distribusi harus mengaktifkan WAF
- [CloudFront.7] CloudFront distribusi harus menggunakan sertifikat SSL/TLS khusus
- [CloudFront.8] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS
- [CloudFront.9] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus
- [CloudFront.10] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal khusus
- [CloudFront.12] CloudFront distribusi seharusnya tidak menunjukkan asal S3 yang tidak ada
- [CloudFront.13] CloudFront distribusi harus menggunakan kontrol akses asal
- [CloudFront.14] CloudFront distribusi harus ditandai
- [DataFirehose.1] Aliran pengiriman Firehose harus dienkripsi saat istirahat
- [DMS.10] Titik akhir DMS untuk database Neptunus harus mengaktifkan otorisasi IAM
- [DMS.11] Titik akhir DMS untuk MongoDB harus mengaktifkan mekanisme otentikasi
- [DMS.12] Titik akhir DMS untuk Redis harus mengaktifkan TLS
- [DocumentDB.1] Cluster Amazon DocumentDB harus dienkripsi saat istirahat
- [DocumentDB.2] Cluster Amazon DocumentDB harus memiliki periode retensi cadangan yang memadai
- [DocumentDB.3] Cuplikan cluster manual Amazon DocumentDB seharusnya tidak bersifat publik
- [DocumentDB.4] Cluster Amazon DocumentDB harus mempublikasikan log audit ke Log CloudWatch
- [DocumentDB.5] Cluster Amazon DocumentDB harus mengaktifkan perlindungan penghapusan
- [DynamoDB.3] Cluster DynamoDB Accelerator (DAX) harus dienkripsi saat istirahat
- [DynamoDB.7] Cluster DynamoDB Accelerator harus dienkripsi saat transit
- [EC2.24] Jenis instans paravirtual Amazon EC2 tidak boleh digunakan
- [ECR.4] Repositori publik ECR harus ditandai
- [EFS.6] Target pemasangan EFS tidak boleh dikaitkan dengan subnet publik
- [EKS.3] Kluster EKS harus menggunakan rahasia Kubernetes terenkripsi
- [FSX.2] Sistem file FSx for Lustre harus dikonfigurasi untuk menyalin tag ke cadangan
- [GlobalAccelerator.1] Akselerator Akselerator Global harus diberi tag
- [IAM.26] Sertifikat SSL/TLS kedaluwarsa yang dikelola di IAM harus dihapus
- [MQ.2] Broker ActiveMQ harus mengalirkan log audit ke CloudWatch
- [MQ.3] Broker Amazon MQ harus mengaktifkan peningkatan versi minor otomatis

- [Opensearch.11] OpenSearch domain harus memiliki setidaknya tiga node primer khusus
- [RDS.14] Cluster Amazon Aurora seharusnya mengaktifkan backtracking
- [RDS.31] Grup keamanan RDS DB harus ditandai
- [Redshift.15] Grup keamanan Redshift harus mengizinkan masuknya port cluster hanya dari asal yang dibatasi
- [Route53.1] Pemeriksaan kesehatan rute 53 harus ditandai
- [Route53.2] Route 53 zona yang dihosting publik harus mencatat kueri DNS
- [SageMaker.4] varian produksi SageMaker titik akhir harus memiliki jumlah instance awal yang lebih besar dari 1
- [ServiceCatalog.1] Portofolio Service Catalog harus dibagikan hanya dalam suatu organisasi AWS
- [Transfer.2] Server Transfer Family tidak boleh menggunakan protokol FTP untuk koneksi titik akhir
- [WAF.1] Pencatatan ACL Web Global AWS WAF Klasik harus diaktifkan
- [WAF.6] Aturan global AWS WAF klasik harus memiliki setidaknya satu syarat
- [WAF.7] Kelompok aturan global AWS WAF klasik harus memiliki setidaknya satu aturan
- [WAF.8] ACL web global AWS WAF klasik harus memiliki setidaknya satu aturan atau kelompok aturan

Eropa (Zürich)

Kontrol berikut tidak didukung di Eropa (Zurich).

- [ACM.1] Sertifikat yang diimpor dan diterbitkan ACM harus diperbarui setelah jangka waktu tertentu
- [ACM.2] Sertifikat RSA yang dikelola oleh ACM harus menggunakan panjang kunci minimal 2.048 bit
- [ApiGateway.1] API Gateway REST WebSocket dan pencatatan eksekusi API harus diaktifkan
- [ApiGateway.2] Tahapan API Gateway REST API harus dikonfigurasi untuk menggunakan sertifikat SSL untuk otentikasi backend
- [ApiGateway.8] Rute API Gateway harus menentukan jenis otorisasi
- [ApiGateway.9] Pencatatan akses harus dikonfigurasi untuk Tahapan API Gateway V2
- [AppSync.2] AWS AppSync harus mengaktifkan logging tingkat lapangan
- [AppSync.5] AWS AppSync GraphQL API tidak boleh diautentikasi dengan kunci API
- [Athena.2] Katalog data Athena harus diberi tag

- [Athena.3] Kelompok kerja Athena harus ditandai
- [AutoScaling.1] Grup Auto Scaling yang terkait dengan penyeimbang beban harus menggunakan pemeriksaan kesehatan ELB
- [Autoscaling.5] Instans Amazon EC2 yang diluncurkan menggunakan konfigurasi peluncuran grup Auto Scaling seharusnya tidak memiliki alamat IP Publik
- [Backup.1] titik AWS Backup pemulihan harus dienkripsi saat istirahat
- [Backup.2] poin AWS Backup pemulihan harus ditandai
- [Backup.3] AWS Backup brankas harus ditandai
- [Backup.4] rencana AWS Backup laporan harus ditandai
- [Backup.5] rencana AWS Backup cadangan harus ditandai
- [CloudFormation.2] CloudFormation tumpukan harus ditandai
- [CloudFront.1] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi
- [CloudFront.3] CloudFront distribusi harus memerlukan enkripsi dalam perjalanan
- [CloudFront.4] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi
- [CloudFront.5] CloudFront distribusi seharusnya mengaktifkan logging
- [CloudFront.6] CloudFront distribusi harus mengaktifkan WAF
- [CloudFront.7] CloudFront distribusi harus menggunakan sertifikat SSL/TLS khusus
- [CloudFront.8] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS
- [CloudFront.9] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus
- [CloudFront.10] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal khusus
- [CloudFront.12] CloudFront distribusi seharusnya tidak menunjukkan asal S3 yang tidak ada
- [CloudFront.13] CloudFront distribusi harus menggunakan kontrol akses asal
- [CloudFront.14] CloudFront distribusi harus ditandai
- [CloudTrail.6] Pastikan bucket S3 yang digunakan untuk menyimpan CloudTrail log tidak dapat diakses publik
- [CloudTrail.7] Pastikan pencatatan akses bucket S3 diaktifkan pada bucket CloudTrail S3
- [CodeArtifact.1] CodeArtifact repositori harus diberi tag
- [CodeBuild.1] URL repositori sumber CodeBuild Bitbucket tidak boleh berisi kredensyal sensitif
- [CodeBuild.2] variabel lingkungan CodeBuild proyek tidak boleh berisi kredensil teks yang jelas
- [CodeBuild.3] Log CodeBuild S3 harus dienkripsi

- [CodeBuild.4] lingkungan CodeBuild proyek harus memiliki urasi logging AWS Config
- [DataFirehose.1] Aliran pengiriman Firehose harus dienkripsi saat istirahat
- [Detective.1] Grafik perilaku detektif harus diberi tag
- [DMS.1] Instans replikasi Layanan Migrasi Database tidak boleh bersifat publik
- [DMS.2] Sertifikat DMS harus ditandai
- [DMS.3] Langganan acara DMS harus ditandai
- [DMS.4] Contoh replikasi DMS harus ditandai
- [DMS.5] Grup subnet replikasi DMS harus ditandai
- [DMS.6] Instans replikasi DMS harus mengaktifkan peningkatan versi minor otomatis
- [DMS.7] Tugas replikasi DMS untuk database target seharusnya mengaktifkan logging
- [DMS.8] Tugas replikasi DMS untuk database sumber seharusnya mengaktifkan logging
- [DMS.9] Titik akhir DMS harus menggunakan SSL
- [DMS.10] Titik akhir DMS untuk database Neptunus harus mengaktifkan otorisasi IAM
- [DMS.11] Titik akhir DMS untuk MongoDB harus mengaktifkan mekanisme otentikasi
- [DMS.12] Titik akhir DMS untuk Redis harus mengaktifkan TLS
- [DocumentDB.1] Cluster Amazon DocumentDB harus dienkripsi saat istirahat
- [DocumentDB.2] Cluster Amazon DocumentDB harus memiliki periode retensi cadangan yang memadai
- [DocumentDB.3] Cuplikan cluster manual Amazon DocumentDB seharusnya tidak bersifat publik
- [DocumentDB.4] Cluster Amazon DocumentDB harus mempublikasikan log audit ke Log CloudWatch
- [DocumentDB.5] Cluster Amazon DocumentDB harus mengaktifkan perlindungan penghapusan
- [DynamoDB.1] Tabel DynamoDB harus secara otomatis menskalakan kapasitas sesuai permintaan
- [DynamoDB.2] Tabel DynamoDB harus mengaktifkan pemulihan point-in-time
- [DynamoDB.3] Cluster DynamoDB Accelerator (DAX) harus dienkripsi saat istirahat
- [DynamoDB.4] Tabel DynamoDB harus ada dalam rencana cadangan
- [DynamoDB.7] Cluster DynamoDB Accelerator harus dienkripsi saat transit
- [EC2.2] Grup keamanan default VPC tidak boleh mengizinkan lalu lintas masuk atau keluar
- [EC2.3] Volume Amazon EBS yang terpasang harus dienkripsi saat istirahat
- [EC2.4] Instans EC2 yang dihentikan harus dihapus setelah periode waktu tertentu

- [EC2.6] Pencatatan aliran VPC harus diaktifkan di semua VPC
- [EC2.8] Instans EC2 harus menggunakan Layanan Metadata Instance Versi 2 (IMDSv2)
- [EC2.9] Instans Amazon EC2 seharusnya tidak memiliki alamat IPv4 publik
- [EC2.10] Amazon EC2 harus dikonfigurasi untuk menggunakan titik akhir VPC yang dibuat untuk layanan Amazon EC2
- [EC2.13] Grup keamanan tidak boleh mengizinkan masuknya dari 0.0.0.0/0 atau: :/0 ke port 22
- [EC2.14] Grup keamanan tidak boleh mengizinkan masuknya dari 0.0.0.0/0 atau: :/0 ke port 3389
- [EC2.15] Subnet Amazon EC2 seharusnya tidak secara otomatis menetapkan alamat IP publik
- [EC2.16] Daftar Kontrol Akses Jaringan yang Tidak Digunakan harus dihapus
- [EC2.17] Instans Amazon EC2 tidak boleh menggunakan beberapa ENI
- [EC2.18] Grup keamanan seharusnya hanya mengizinkan lalu lintas masuk yang tidak terbatas untuk port resmi
- [EC2.20] Kedua terowongan VPN untuk koneksi VPN Site-to-Site harus AWS aktif
- [EC2.22] Grup keamanan Amazon EC2 yang tidak digunakan harus dihapus
- [EC2.23] Amazon EC2 Transit Gateways seharusnya tidak secara otomatis menerima permintaan lampiran VPC
- [EC2.24] Jenis instans paravirtual Amazon EC2 tidak boleh digunakan
- [EC2.25] Templat peluncuran Amazon EC2 tidak boleh menetapkan IP publik ke antarmuka jaringan
- [EC2.28] Volume EBS harus dicakup oleh rencana cadangan
- [EC2.51] Titik akhir EC2 Client VPN harus mengaktifkan pencatatan koneksi klien
- [ECR.1] Repositori pribadi ECR harus memiliki pemindaian gambar yang dikonfigurasi
- [ECR.2] Repositori pribadi ECR harus memiliki kekekalan tag yang dikonfigurasi
- [ECR.3] Repositori ECR harus memiliki setidaknya satu kebijakan siklus hidup yang dikonfigurasi
- [ECR.4] Repositori publik ECR harus ditandai
- [ECS.1] Definisi tugas Amazon ECS harus memiliki mode jaringan yang aman dan definisi pengguna.
- [ECS.9] Definisi tugas ECS harus memiliki konfigurasi logging
- [EFS.1] Sistem File Elastis harus dikonfigurasi untuk mengenkripsi data file saat istirahat menggunakan AWS KMS
- [EFS.2] Volume Amazon EFS harus dalam rencana cadangan

- [EFS.3] Titik akses EFS harus menegakkan direktori root
- [EFS.4] Titik akses EFS harus menegakkan identitas pengguna
- [EFS.5] Titik akses EFS harus ditandai
- [EFS.6] Target pemasangan EFS tidak boleh dikaitkan dengan subnet publik
- [EKS.1] Titik akhir klaster EKS seharusnya tidak dapat diakses publik
- [EKS.2] Kluster EKS harus berjalan pada versi Kubernetes yang didukung
- [EKS.3] Kluster EKS harus menggunakan rahasia Kubernetes terenkripsi
- [ELB.1] Application Load Balancer harus dikonfigurasi untuk mengalihkan semua permintaan HTTP ke HTTPS
- [ELB.2] Classic Load Balancer dengan pendengar SSL/HTTPS harus menggunakan sertifikat yang disediakan oleh AWS Certificate Manager
- [ELB.3] Pendengar Classic Load Balancer harus dikonfigurasi dengan penghentian HTTPS atau TLS
- [ELB.4] Application Load Balancer harus dikonfigurasi untuk menjatuhkan header http
- [ELB.8] Classic Load Balancer dengan pendengar SSL harus menggunakan kebijakan keamanan yang telah ditentukan sebelumnya yang memiliki urasi yang kuat AWS Config
- [ELB.9] Classic Load Balancer harus mengaktifkan penyeimbangan beban lintas zona
- [ELB.14] Classic Load Balancer harus dikonfigurasi dengan mode mitigasi desync defensif atau paling ketat
- [ELB.16] Application Load Balancers harus dikaitkan dengan ACL web AWS WAF
- [ElastiCache.1] Cluster ElastiCache Redis harus mengaktifkan pencadangan otomatis
- [ElastiCache.6] ElastiCache untuk grup replikasi Redis sebelum versi 6.0 harus menggunakan Redis AUTH
- [ElastiCache.7] ElastiCache cluster tidak boleh menggunakan grup subnet default
- [ElasticBeanstalk.1] Lingkungan Elastic Beanstalk seharusnya mengaktifkan pelaporan kesehatan yang ditingkatkan
- [ElasticBeanstalk.2] Pembaruan platform yang dikelola Elastic Beanstalk harus diaktifkan
- [ElasticBeanstalk.3] Elastic Beanstalk harus mengalirkan log ke CloudWatch
- [EMR.1] Node primer cluster EMR Amazon seharusnya tidak memiliki alamat IP publik
- [ES.1] Domain Elasticsearch harus mengaktifkan enkripsi saat istirahat
- [ES.2] Domain Elasticsearch tidak boleh diakses publik
- [ES.3] Domain Elasticsearch harus mengenkripsi data yang dikirim antar node

- [ES.4] Kesalahan domain Elasticsearch yang masuk ke CloudWatch Log harus diaktifkan
- [EventBridge.2] bus EventBridge acara harus diberi tag
- [EventBridge.3] bus acara EventBridge khusus harus memiliki kebijakan berbasis sumber daya terlampir
- [EventBridge.4] titik akhir EventBridge global harus mengaktifkan replikasi acara
- [FSX.1] FSx untuk sistem file OpenZFS harus dikonfigurasi untuk menyalin tag ke cadangan dan volume
- [FSX.2] Sistem file FSx for Lustre harus dikonfigurasi untuk menyalin tag ke cadangan
- [GlobalAccelerator.1] Akselerator Akselerator Global harus diberi tag
- AWS Glue Pekerjaan [Glue.1] harus ditandai
- [GuardDuty.1] GuardDuty harus diaktifkan
- [GuardDuty.2] GuardDuty filter harus diberi tag
- [GuardDuty.3] GuardDuty IPset harus ditandai
- [GuardDuty.4] GuardDuty detektor harus ditandai
- [IAM.1] Kebijakan IAM seharusnya tidak mengizinkan hak administratif “*” penuh
- [IAM.2] Pengguna IAM seharusnya tidak memiliki kebijakan IAM yang dilampirkan
- [IAM.3] Kunci akses pengguna IAM harus diputar setiap 90 hari atau kurang
- [IAM.4] Kunci akses pengguna root IAM seharusnya tidak ada
- [IAM.5] MFA harus diaktifkan untuk semua pengguna IAM yang memiliki kata sandi konsol
- [IAM.8] Kredensyal pengguna IAM yang tidak digunakan harus dihapus
- [IAM.18] Memastikan peran dukungan telah dibuat untuk mengelola insiden dengan AWS Support
- [IAM.19] MFA harus diaktifkan untuk semua pengguna IAM
- [IAM.21] Kebijakan terkelola pelanggan IAM yang Anda buat seharusnya tidak mengizinkan tindakan wildcard untuk layanan
- [IAM.22] Kredensyal pengguna IAM yang tidak digunakan selama 45 hari harus dihapus
- [IAM.24] Peran IAM harus ditandai
- [IAM.25] Pengguna IAM harus diberi tag
- [IAM.26] Sertifikat SSL/TLS kedaluwarsa yang dikelola di IAM harus dihapus
- [IAM.27] Identitas IAM seharusnya tidak memiliki kebijakan yang dilampirkan AWSCloudShellFullAccess
- [IoT.1] profil AWS IoT Core keamanan harus ditandai

- [IoT.2] tindakan AWS IoT Core mitigasi harus ditandai
- AWS IoT Core Dimensi [IoT.3] harus ditandai
- [IoT.4] AWS IoT Core otorisasi harus diberi tag
- [IoT.5] alias AWS IoT Core peran harus ditandai
- AWS IoT Core Kebijakan [IoT.6] harus ditandai
- [Kinesis.1] Aliran kinesis harus dienkripsi saat istirahat
- [KMS.1] Kebijakan yang dikelola pelanggan IAM tidak boleh mengizinkan tindakan dekripsi pada semua kunci KMS
- [KMS.2] Prinsipal IAM tidak boleh memiliki kebijakan inline IAM yang memungkinkan tindakan dekripsi pada semua kunci KMS
- [Lambda.5] Fungsi VPC Lambda harus beroperasi di beberapa Availability Zone
- [Macie.1] Amazon Macie harus diaktifkan
- [Macie.2] Penemuan data sensitif otomatis Macie harus diaktifkan
- [MQ.2] Broker ActiveMQ harus mengalirkan log audit ke CloudWatch
- [MQ.3] Broker Amazon MQ harus mengaktifkan peningkatan versi minor otomatis
- [MQ.4] Broker Amazon MQ harus diberi tag
- [MQ.5] Broker ActiveMQ harus menggunakan mode penerapan aktif/siaga
- [MQ.6] Broker RabbitMQ harus menggunakan mode penerapan cluster
- [MSK.1] Cluster MSK harus dienkripsi saat transit di antara node broker
- [MSK.2] Kluster MSK seharusnya telah meningkatkan pemantauan yang dikonfigurasi
- [Neptunus.1] Cluster DB Neptunus harus dienkripsi saat istirahat
- [Neptune.2] Cluster DB Neptunus harus menerbitkan log audit ke Log CloudWatch
- [Neptune.3] Snapshot cluster Neptunus DB seharusnya tidak publik
- [Neptunus.4] Cluster DB Neptunus harus mengaktifkan perlindungan penghapusan
- [Neptunus.5] Cluster DB Neptunus harus mengaktifkan cadangan otomatis
- [Neptune.6] Snapshot cluster Neptunus DB harus dienkripsi saat istirahat
- [Neptunus.7] Cluster DB Neptunus harus mengaktifkan otentikasi basis data IAM
- [Neptunus.8] Cluster DB Neptunus harus dikonfigurasi untuk menyalin tag ke snapshot
- [Neptunus.9] Cluster DB Neptunus harus digunakan di beberapa Availability Zone
- [NetworkFirewall.1] Firewall Firewall Jaringan harus digunakan di beberapa Availability Zone
- [NetworkFirewall.2] Pencatatan Firewall Jaringan harus diaktifkan

- [NetworkFirewall.3] Kebijakan Network Firewall harus memiliki setidaknya satu kelompok aturan yang terkait
- [NetworkFirewall.4] Tindakan stateless default untuk kebijakan Network Firewall harus drop atau forward untuk paket penuh
- [NetworkFirewall.5] Tindakan stateless default untuk kebijakan Network Firewall harus drop atau forward untuk paket yang terfragmentasi
- [NetworkFirewall.6] Grup aturan Stateless Network Firewall tidak boleh kosong
- [NetworkFirewall.9] Firewall Firewall Jaringan harus mengaktifkan perlindungan penghapusan
- [Opensearch.1] OpenSearch domain harus mengaktifkan enkripsi saat istirahat
- [Opensearch.2] OpenSearch domain tidak boleh diakses publik
- [Opensearch.3] OpenSearch domain harus mengenkripsi data yang dikirim antar node
- [Opensearch.4] login kesalahan OpenSearch domain ke Log harus diaktifkan CloudWatch
- [Opensearch.5] OpenSearch domain harus mengaktifkan pencatatan audit
- [Opensearch.6] OpenSearch domain harus memiliki setidaknya tiga node data
- [Opensearch.7] OpenSearch domain harus mengaktifkan kontrol akses berbutir halus
- [Opensearch.8] Koneksi ke OpenSearch domain harus dienkripsi menggunakan kebijakan keamanan TLS terbaru
- [Opensearch.9] domain harus ditandai OpenSearch
- [Opensearch.10] OpenSearch domain harus memiliki pembaruan perangkat lunak terbaru yang diinstal
- [Opensearch.11] OpenSearch domain harus memiliki setidaknya tiga node primer khusus
- [RDS.1] Snapshot RDS harus pribadi
- [RDS.3] Instans RDS DB harus mengaktifkan enkripsi saat istirahat
- [RDS.5] Instans RDS DB harus dikonfigurasi dengan beberapa Availability Zone
- [RDS.8] Instans RDS DB harus mengaktifkan perlindungan penghapusan
- [RDS.14] Cluster Amazon Aurora seharusnya mengaktifkan backtracking
- [RDS.16] Cluster RDS DB harus dikonfigurasi untuk menyalin tag ke snapshot
- [RDS.24] Kluster Database RDS harus menggunakan nama pengguna administrator khusus
- [RDS.26] Instans RDS DB harus dilindungi oleh rencana cadangan
- [RDS.31] Grup keamanan RDS DB harus ditandai
- [RDS.35] Cluster RDS DB harus mengaktifkan peningkatan versi minor otomatis

- [Redshift.3] Cluster Amazon Redshift harus mengaktifkan snapshot otomatis
- [Redshift.12] Langganan pemberitahuan acara Redshift harus ditandai
- [Redshift.15] Grup keamanan Redshift harus mengizinkan masuknya port cluster hanya dari asal yang dibatasi
- [Route53.1] Pemeriksaan kesehatan rute 53 harus ditandai
- [Route53.2] Route 53 zona yang dihosting publik harus mencatat kueri DNS
- [S3.1] Bucket tujuan umum S3 harus mengaktifkan pengaturan akses publik blok
- [S3.8] Bucket tujuan umum S3 harus memblokir akses publik
- [SageMaker.1] Instans SageMaker notebook Amazon seharusnya tidak memiliki akses internet langsung
- [SageMaker.2] instance SageMaker notebook harus diluncurkan dalam VPC khusus
- [SageMaker.3] Pengguna seharusnya tidak memiliki akses root ke instance SageMaker notebook
- [SageMaker.4] varian produksi SageMaker titik akhir harus memiliki jumlah instance awal yang lebih besar dari 1
- [SES.1] Daftar kontak SES harus ditandai
- [SES.2] Set konfigurasi SES harus ditandai
- [SecretsManager.2] Rahasia Secrets Manager yang dikonfigurasi dengan rotasi otomatis harus berhasil diputar
- [ServiceCatalog.1] Portofolio Service Catalog harus dibagikan hanya dalam suatu organisasi AWS
- [SNS.1] Topik SNS harus dienkripsi saat istirahat menggunakan AWS KMS
- [SNS.3] Topik SNS harus ditandai
- [SQS.1] Antrian Amazon SQS harus dienkripsi saat istirahat
- [SQS.2] Antrian SQS harus ditandai
- [SSM.2] Instans Amazon EC2 yang dikelola oleh Systems Manager harus memiliki status kepatuhan patch COMPLIANT setelah instalasi patch
- [SSM.3] Instans Amazon EC2 yang dikelola oleh Systems Manager harus memiliki status kepatuhan asosiasi COMPLIANT
- [StepFunctions.1] Mesin status Step Functions seharusnya mengaktifkan logging
- [Transfer.1] AWS Transfer Family alur kerja harus ditandai
- [Transfer.2] Server Transfer Family tidak boleh menggunakan protokol FTP untuk koneksi titik akhir
- [WAF.1] Pencatatan ACL Web Global AWS WAF Klasik harus diaktifkan

- [WAF.2] Aturan Regional AWS WAF Klasik harus memiliki setidaknya satu syarat
- [WAF.3] Kelompok aturan Regional AWS WAF Klasik harus memiliki setidaknya satu aturan
- [WAF.4] ACL web Regional AWS WAF klasik harus memiliki setidaknya satu aturan atau kelompok aturan
- [WAF.6] Aturan global AWS WAF klasik harus memiliki setidaknya satu syarat
- [WAF.7] Kelompok aturan global AWS WAF klasik harus memiliki setidaknya satu aturan
- [WAF.8] ACL web global AWS WAF klasik harus memiliki setidaknya satu aturan atau kelompok aturan
- [WAF.10] ACL AWS WAF web harus memiliki setidaknya satu aturan atau kelompok aturan
- [WAF.11] pencatatan ACL AWS WAF web harus diaktifkan

Israel (Tel Aviv)

Kontrol berikut tidak didukung di Israel (Tel Aviv).

- [ACM.1] Sertifikat yang diimpor dan diterbitkan ACM harus diperbarui setelah jangka waktu tertentu
- [ACM.2] Sertifikat RSA yang dikelola oleh ACM harus menggunakan panjang kunci minimal 2.048 bit
- [ApiGateway.8] Rute API Gateway harus menentukan jenis otorisasi
- [ApiGateway.9] Pencatatan akses harus dikonfigurasi untuk Tahapan API Gateway V2
- [AppSync.2] AWS AppSync harus mengaktifkan logging tingkat lapangan
- [AppSync.4] AWS AppSync GraphQL API harus diberi tag
- [AppSync.5] AWS AppSync GraphQL API tidak boleh diautentikasi dengan kunci API
- [Athena.2] Katalog data Athena harus diberi tag
- [Athena.3] Kelompok kerja Athena harus ditandai
- [Autoscaling.5] Instans Amazon EC2 yang diluncurkan menggunakan konfigurasi peluncuran grup Auto Scaling seharusnya tidak memiliki alamat IP Publik
- [Backup.1] titik AWS Backup pemulihan harus dienkripsi saat istirahat
- [Backup.2] poin AWS Backup pemulihan harus ditandai
- [Backup.3] AWS Backup brankas harus ditandai
- [Backup.4] rencana AWS Backup laporan harus ditandai
- [Backup.5] rencana AWS Backup cadangan harus ditandai

- [CloudFormation.2] CloudFormation tumpukan harus ditandai
- [CloudFront.1] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi
- [CloudFront.3] CloudFront distribusi harus memerlukan enkripsi dalam perjalanan
- [CloudFront.4] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi
- [CloudFront.5] CloudFront distribusi seharusnya mengaktifkan logging
- [CloudFront.6] CloudFront distribusi harus mengaktifkan WAF
- [CloudFront.7] CloudFront distribusi harus menggunakan sertifikat SSL/TLS khusus
- [CloudFront.8] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS
- [CloudFront.9] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus
- [CloudFront.10] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal khusus
- [CloudFront.12] CloudFront distribusi seharusnya tidak menunjukkan asal S3 yang tidak ada
- [CloudFront.13] CloudFront distribusi harus menggunakan kontrol akses asal
- [CloudFront.14] CloudFront distribusi harus ditandai
- [CodeArtifact.1] CodeArtifact repositori harus diberi tag
- [CodeBuild.1] URL repositori sumber CodeBuild Bitbucket tidak boleh berisi kredensyal sensitif
- [CodeBuild.2] variabel lingkungan CodeBuild proyek tidak boleh berisi kredensil teks yang jelas
- [CodeBuild.3] Log CodeBuild S3 harus dienkripsi
- [CodeBuild.4] lingkungan CodeBuild proyek harus memiliki urasi logging AWS Config
- [DataFirehose.1] Aliran pengiriman Firehose harus dienkripsi saat istirahat
- [Detective.1] Grafik perilaku detektif harus diberi tag
- [DMS.1] Instans replikasi Layanan Migrasi Database tidak boleh bersifat publik
- [DMS.2] Sertifikat DMS harus ditandai
- [DMS.3] Langganan acara DMS harus ditandai
- [DMS.4] Contoh replikasi DMS harus ditandai
- [DMS.5] Grup subnet replikasi DMS harus ditandai
- [DMS.6] Instans replikasi DMS harus mengaktifkan peningkatan versi minor otomatis
- [DMS.7] Tugas replikasi DMS untuk database target seharusnya mengaktifkan logging
- [DMS.8] Tugas replikasi DMS untuk database sumber seharusnya mengaktifkan logging
- [DMS.9] Titik akhir DMS harus menggunakan SSL

- [DMS.10] Titik akhir DMS untuk database Neptunus harus mengaktifkan otorisasi IAM
- [DMS.11] Titik akhir DMS untuk MongoDB harus mengaktifkan mekanisme otentikasi
- [DMS.12] Titik akhir DMS untuk Redis harus mengaktifkan TLS
- [DocumentDB.1] Cluster Amazon DocumentDB harus dienkripsi saat istirahat
- [DocumentDB.2] Cluster Amazon DocumentDB harus memiliki periode retensi cadangan yang memadai
- [DocumentDB.3] Cuplikan cluster manual Amazon DocumentDB seharusnya tidak bersifat publik
- [DocumentDB.4] Cluster Amazon DocumentDB harus mempublikasikan log audit ke Log CloudWatch
- [DocumentDB.5] Cluster Amazon DocumentDB harus mengaktifkan perlindungan penghapusan
- [DynamoDB.3] Cluster DynamoDB Accelerator (DAX) harus dienkripsi saat istirahat
- [DynamoDB.4] Tabel DynamoDB harus ada dalam rencana cadangan
- [DynamoDB.7] Cluster DynamoDB Accelerator harus dienkripsi saat transit
- [EC2.3] Volume Amazon EBS yang terpasang harus dienkripsi saat istirahat
- [EC2.4] Instans EC2 yang dihentikan harus dihapus setelah periode waktu tertentu
- [EC2.6] Pencatatan aliran VPC harus diaktifkan di semua VPC
- [EC2.10] Amazon EC2 harus dikonfigurasi untuk menggunakan titik akhir VPC yang dibuat untuk layanan Amazon EC2
- [EC2.13] Grup keamanan tidak boleh mengizinkan masuknya dari 0.0.0.0/0 atau: :/0 ke port 22
- [EC2.14] Grup keamanan tidak boleh mengizinkan masuknya dari 0.0.0.0/0 atau: :/0 ke port 3389
- [EC2.18] Grup keamanan seharusnya hanya mengizinkan lalu lintas masuk yang tidak terbatas untuk port resmi
- [EC2.20] Kedua terowongan VPN untuk koneksi VPN Site-to-Site harus AWS aktif
- [EC2.22] Grup keamanan Amazon EC2 yang tidak digunakan harus dihapus
- [EC2.23] Amazon EC2 Transit Gateways seharusnya tidak secara otomatis menerima permintaan lampiran VPC
- [EC2.24] Jenis instans paravirtual Amazon EC2 tidak boleh digunakan
- [EC2.25] Templat peluncuran Amazon EC2 tidak boleh menetapkan IP publik ke antarmuka jaringan
- [EC2.28] Volume EBS harus dicakup oleh rencana cadangan
- [EC2.33] Lampiran gateway transit EC2 harus ditandai

- [EC2.34] Tabel rute gateway transit EC2 harus ditandai
- [EC2.40] Gerbang EC2 NAT harus ditandai
- [EC2.48] Log aliran VPC Amazon harus ditandai
- [EC2.51] Titik akhir EC2 Client VPN harus mengaktifkan pencatatan koneksi klien
- [EC2.52] Gerbang transit EC2 harus ditandai
- [ECR.2] Repositori pribadi ECR harus memiliki kekekalan tag yang dikonfigurasi
- [ECR.3] Repositori ECR harus memiliki setidaknya satu kebijakan siklus hidup yang dikonfigurasi
- [ECR.4] Repositori publik ECR harus ditandai
- [ECS.1] Definisi tugas Amazon ECS harus memiliki mode jaringan yang aman dan definisi pengguna.
- [ECS.9] Definisi tugas ECS harus memiliki konfigurasi logging
- [EFS.1] Sistem File Elastis harus dikonfigurasi untuk mengenkripsi data file saat istirahat menggunakan AWS KMS
- [EFS.2] Volume Amazon EFS harus dalam rencana cadangan
- [EFS.3] Titik akses EFS harus menegakkan direktori root
- [EFS.4] Titik akses EFS harus menegakkan identitas pengguna
- [EFS.5] Titik akses EFS harus ditandai
- [EFS.6] Target pemasangan EFS tidak boleh dikaitkan dengan subnet publik
- [EKS.1] Titik akhir klaster EKS seharusnya tidak dapat diakses publik
- [EKS.2] Kluster EKS harus berjalan pada versi Kubernetes yang didukung
- [EKS.3] Kluster EKS harus menggunakan rahasia Kubernetes terenkripsi
- [EKS.6] Kluster EKS harus ditandai
- [EKS.7] Konfigurasi penyedia identitas EKS harus ditandai
- [EKS.8] Kluster EKS harus mengaktifkan pencatatan audit
- [ELB.1] Application Load Balancer harus dikonfigurasi untuk mengalihkan semua permintaan HTTP ke HTTPS
- [ELB.2] Classic Load Balancer dengan pendengar SSL/HTTPS harus menggunakan sertifikat yang disediakan oleh AWS Certificate Manager
- [ELB.4] Application Load Balancer harus dikonfigurasi untuk menjatuhkan header http
- [ELB.6] Aplikasi, Gateway, dan Network Load Balancer harus mengaktifkan perlindungan penghapusan

- [ELB.8] Classic Load Balancer dengan pendengar SSL harus menggunakan kebijakan keamanan yang telah ditentukan sebelumnya yang memiliki urasi yang kuat AWS Config
- [ELB.13] Penyeimbang Beban Aplikasi, Jaringan, dan Gateway harus mencakup beberapa Availability Zone
- [ELB.14] Classic Load Balancer harus dikonfigurasi dengan mode mitigasi desync defensif atau paling ketat
- [ELB.16] Application Load Balancers harus dikaitkan dengan ACL web AWS WAF
- [ElastiCache.1] Cluster ElastiCache Redis harus mengaktifkan pencadangan otomatis
- [ElastiCache.2] ElastiCache untuk kluster cache Redis harus mengaktifkan peningkatan versi minor otomatis
- [ElastiCache.3] ElastiCache untuk grup replikasi Redis harus mengaktifkan failover otomatis
- [ElastiCache.4] ElastiCache untuk grup replikasi Redis harus dienkripsi saat istirahat
- [ElastiCache.5] ElastiCache untuk grup replikasi Redis harus dienkripsi saat transit
- [ElastiCache.6] ElastiCache untuk grup replikasi Redis sebelum versi 6.0 harus menggunakan Redis AUTH
- [ElastiCache.7] ElastiCache cluster tidak boleh menggunakan grup subnet default
- [ElasticBeanstalk.1] Lingkungan Elastic Beanstalk seharusnya mengaktifkan pelaporan kesehatan yang ditingkatkan
- [ElasticBeanstalk.2] Pembaruan platform yang dikelola Elastic Beanstalk harus diaktifkan
- [ElasticBeanstalk.3] Elastic Beanstalk harus mengalirkan log ke CloudWatch
- [EMR.1] Node primer cluster EMR Amazon seharusnya tidak memiliki alamat IP publik
- [ES.1] Domain Elasticsearch harus mengaktifkan enkripsi saat istirahat
- [ES.2] Domain Elasticsearch tidak boleh diakses publik
- [ES.3] Domain Elasticsearch harus mengenkripsi data yang dikirim antar node
- [ES.4] Kesalahan domain Elasticsearch yang masuk ke CloudWatch Log harus diaktifkan
- [EventBridge.2] bus EventBridge acara harus diberi tag
- [EventBridge.3] bus acara EventBridge khusus harus memiliki kebijakan berbasis sumber daya terlampir
- [EventBridge.4] titik akhir EventBridge global harus mengaktifkan replikasi acara
- [FSX.1] FSx untuk sistem file OpenZFS harus dikonfigurasi untuk menyalin tag ke cadangan dan volume
- [FSX.2] Sistem file FSx for Lustre harus dikonfigurasi untuk menyalin tag ke cadangan

- [GlobalAccelerator.1] Akselerator Akselerator Global harus diberi tag
- [GuardDuty.1] GuardDuty harus diaktifkan
- [GuardDuty.2] GuardDuty filter harus diberi tag
- [GuardDuty.3] GuardDuty IPset harus ditandai
- [GuardDuty.4] GuardDuty detektor harus ditandai
- [IAM.1] Kebijakan IAM seharusnya tidak mengizinkan hak administratif “*” penuh
- [IAM.2] Pengguna IAM seharusnya tidak memiliki kebijakan IAM yang dilampirkan
- [IAM.3] Kunci akses pengguna IAM harus diputar setiap 90 hari atau kurang
- [IAM.4] Kunci akses pengguna root IAM seharusnya tidak ada
- [IAM.5] MFA harus diaktifkan untuk semua pengguna IAM yang memiliki kata sandi konsol
- [IAM.6] MFA perangkat keras harus diaktifkan untuk pengguna root
- [IAM.7] Kebijakan kata sandi untuk pengguna IAM harus memiliki konfigurasi yang kuat
- [IAM.8] Kredensyal pengguna IAM yang tidak digunakan harus dihapus
- [IAM.9] MFA harus diaktifkan untuk pengguna root
- [IAM.10] Kebijakan kata sandi untuk pengguna IAM harus memiliki urasi yang kuat AWS Config
- [IAM.11] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu huruf besar
- [IAM.12] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu huruf kecil
- [IAM.13] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu simbol
- [IAM.14] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu nomor
- [IAM.15] Pastikan kebijakan kata sandi IAM membutuhkan panjang kata sandi minimum 14 atau lebih
- [IAM.16] Pastikan kebijakan kata sandi IAM mencegah penggunaan kembali kata sandi
- [IAM.17] Pastikan kebijakan kata sandi IAM kedaluwarsa kata sandi dalam waktu 90 hari atau kurang
- [IAM.18] Memastikan peran dukungan telah dibuat untuk mengelola insiden dengan AWS Support
- [IAM.19] MFA harus diaktifkan untuk semua pengguna IAM
- [IAM.21] Kebijakan terkelola pelanggan IAM yang Anda buat seharusnya tidak mengizinkan tindakan wildcard untuk layanan
- [IAM.22] Kredensyal pengguna IAM yang tidak digunakan selama 45 hari harus dihapus
- [IAM.23] Penganalisis Akses IAM harus ditandai

- [IAM.24] Peran IAM harus ditandai
- [IAM.25] Pengguna IAM harus diberi tag
- [IAM.26] Sertifikat SSL/TLS kedaluwarsa yang dikelola di IAM harus dihapus
- [IAM.27] Identitas IAM seharusnya tidak memiliki kebijakan yang dilampirkan AWSCloudShellFullAccess
- [IAM.28] IAM Access Analyzer penganalisis akses eksternal harus diaktifkan
- [IoT.1] profil AWS IoT Core keamanan harus ditandai
- [IoT.2] tindakan AWS IoT Core mitigasi harus ditandai
- AWS IoT Core Dimensi [IoT.3] harus ditandai
- [IoT.4] AWS IoT Core otorisasi harus diberi tag
- [IoT.5] alias AWS IoT Core peran harus ditandai
- AWS IoT Core Kebijakan [IoT.6] harus ditandai
- [Kinesis.1] Aliran kinesis harus dienkripsi saat istirahat
- [Kinesis.2] Aliran kinesis harus ditandai
- [KMS.1] Kebijakan yang dikelola pelanggan IAM tidak boleh mengizinkan tindakan dekripsi pada semua kunci KMS
- [KMS.2] Prinsipal IAM tidak boleh memiliki kebijakan inline IAM yang memungkinkan tindakan dekripsi pada semua kunci KMS
- [Lambda.5] Fungsi VPC Lambda harus beroperasi di beberapa Availability Zone
- [Macie.1] Amazon Macie harus diaktifkan
- [MQ.2] Broker ActiveMQ harus mengalirkan log audit ke CloudWatch
- [MQ.3] Broker Amazon MQ harus mengaktifkan peningkatan versi minor otomatis
- [MQ.4] Broker Amazon MQ harus diberi tag
- [MQ.5] Broker ActiveMQ harus menggunakan mode penerapan aktif/siaga
- [MQ.6] Broker RabbitMQ harus menggunakan mode penerapan cluster
- [MSK.1] Cluster MSK harus dienkripsi saat transit di antara node broker
- [MSK.2] Kluster MSK seharusnya telah meningkatkan pemantauan yang dikonfigurasi
- [Neptunus.1] Cluster DB Neptunus harus dienkripsi saat istirahat
- [Neptune.2] Cluster DB Neptunus harus menerbitkan log audit ke Log CloudWatch
- [Neptune.3] Snapshot cluster Neptunus DB seharusnya tidak publik
- [Neptunus.4] Cluster DB Neptunus harus mengaktifkan perlindungan penghapusan

- [Neptunus.5] Cluster DB Neptunus harus mengaktifkan cadangan otomatis
- [Neptune.6] Snapshot cluster Neptunus DB harus dienkripsi saat istirahat
- [Neptunus.7] Cluster DB Neptunus harus mengaktifkan otentikasi basis data IAM
- [Neptunus.8] Cluster DB Neptunus harus dikonfigurasi untuk menyalin tag ke snapshot
- [Neptunus.9] Cluster DB Neptunus harus digunakan di beberapa Availability Zone
- [NetworkFirewall.1] Firewall Firewall Jaringan harus digunakan di beberapa Availability Zone
- [NetworkFirewall.2] Pencatatan Firewall Jaringan harus diaktifkan
- [NetworkFirewall.3] Kebijakan Network Firewall harus memiliki setidaknya satu kelompok aturan yang terkait
- [NetworkFirewall.4] Tindakan stateless default untuk kebijakan Network Firewall harus drop atau forward untuk paket penuh
- [NetworkFirewall.5] Tindakan stateless default untuk kebijakan Network Firewall harus drop atau forward untuk paket yang terfragmentasi
- [NetworkFirewall.6] Grup aturan Stateless Network Firewall tidak boleh kosong
- [NetworkFirewall.9] Firewall Firewall Jaringan harus mengaktifkan perlindungan penghapusan
- [Opensearch.1] OpenSearch domain harus mengaktifkan enkripsi saat istirahat
- [Opensearch.2] OpenSearch domain tidak boleh diakses publik
- [Opensearch.3] OpenSearch domain harus mengenkripsi data yang dikirim antar node
- [Opensearch.4] login kesalahan OpenSearch domain ke Log harus diaktifkan CloudWatch
- [Opensearch.5] OpenSearch domain harus mengaktifkan pencatatan audit
- [Opensearch.6] OpenSearch domain harus memiliki setidaknya tiga node data
- [Opensearch.7] OpenSearch domain harus mengaktifkan kontrol akses berbutir halus
- [Opensearch.8] Koneksi ke OpenSearch domain harus dienkripsi menggunakan kebijakan keamanan TLS terbaru
- [Opensearch.9] domain harus ditandai OpenSearch
- [Opensearch.10] OpenSearch domain harus memiliki pembaruan perangkat lunak terbaru yang diinstal
- [Opensearch.11] OpenSearch domain harus memiliki setidaknya tiga node primer khusus
- [PCA.1] otoritas sertifikat AWS Private CA root harus dinonaktifkan
- [RDS.1] Snapshot RDS harus pribadi
- [RDS.4] Snapshot cluster RDS dan snapshot database harus dienkripsi saat istirahat

- [RDS.7] Cluster RDS harus mengaktifkan perlindungan penghapusan
- [RDS.8] Instans RDS DB harus mengaktifkan perlindungan penghapusan
- [RDS.12] Otentikasi IAM harus dikonfigurasi untuk cluster RDS
- [RDS.14] Cluster Amazon Aurora seharusnya mengaktifkan backtracking
- [RDS.15] Cluster RDS DB harus dikonfigurasi untuk beberapa Availability Zone
- [RDS.16] Cluster RDS DB harus dikonfigurasi untuk menyalin tag ke snapshot
- [RDS.24] Kluster Database RDS harus menggunakan nama pengguna administrator khusus
- [RDS.26] Instans RDS DB harus dilindungi oleh rencana cadangan
- [RDS.27] Cluster RDS DB harus dienkripsi saat istirahat
- [RDS.28] Cluster RDS DB harus ditandai
- [RDS.29] Snapshot cluster RDS DB harus ditandai
- [RDS.31] Grup keamanan RDS DB harus ditandai
- [RDS.34] Cluster Aurora MySQL DB harus menerbitkan log audit ke Log CloudWatch
- [RDS.35] Cluster RDS DB harus mengaktifkan peningkatan versi minor otomatis
- [Redshift.3] Cluster Amazon Redshift harus mengaktifkan snapshot otomatis
- [Redshift.8] Cluster Amazon Redshift tidak boleh menggunakan nama pengguna Admin default
- [Redshift.9] Cluster Redshift tidak boleh menggunakan nama database default
- [Redshift.12] Langganan pemberitahuan acara Redshift harus ditandai
- [Redshift.15] Grup keamanan Redshift harus mengizinkan masuknya port cluster hanya dari asal yang dibatasi
- [Route53.1] Pemeriksaan kesehatan rute 53 harus ditandai
- [Route53.2] Route 53 zona yang dihosting publik harus mencatat kueri DNS
- [S3.1] Bucket tujuan umum S3 harus mengaktifkan pengaturan akses publik blok
- [S3.2] Bucket tujuan umum S3 harus memblokir akses baca publik
- [S3.3] Bucket tujuan umum S3 harus memblokir akses tulis publik
- [S3.8] Bucket tujuan umum S3 harus memblokir akses publik
- [S3.9] Bucket tujuan umum S3 harus mengaktifkan pencatatan akses server
- [SageMaker.1] Instans SageMaker notebook Amazon seharusnya tidak memiliki akses internet langsung
- [SageMaker.2] instance SageMaker notebook harus diluncurkan dalam VPC khusus

- [SageMaker.3] Pengguna seharusnya tidak memiliki akses root ke instance SageMaker notebook
- [SageMaker.4] varian produksi SageMaker titik akhir harus memiliki jumlah instance awal yang lebih besar dari 1
- [SES.1] Daftar kontak SES harus ditandai
- [SES.2] Set konfigurasi SES harus ditandai
- [SecretsManager.1] Rahasia Secrets Manager harus mengaktifkan rotasi otomatis
- [SecretsManager.2] Rahasia Secrets Manager yang dikonfigurasi dengan rotasi otomatis harus berhasil diputar
- [SecretsManager.3] Hapus rahasia Secrets Manager yang tidak digunakan
- [SecretsManager.4] Rahasia Secrets Manager harus diputar dalam jumlah hari tertentu
- [ServiceCatalog.1] Portofolio Service Catalog harus dibagikan hanya dalam suatu organisasi AWS
- [SNS.1] Topik SNS harus dienkripsi saat istirahat menggunakan AWS KMS
- [SNS.3] Topik SNS harus ditandai
- [SQS.1] Antrian Amazon SQS harus dienkripsi saat istirahat
- [SQS.2] Antrian SQS harus ditandai
- [SSM.1] Instans Amazon EC2 harus dikelola oleh AWS Systems Manager
- [SSM.2] Instans Amazon EC2 yang dikelola oleh Systems Manager harus memiliki status kepatuhan patch COMPLIANT setelah instalasi patch
- [SSM.3] Instans Amazon EC2 yang dikelola oleh Systems Manager harus memiliki status kepatuhan asosiasi COMPLIANT
- [SSM.4] Dokumen SSM seharusnya tidak bersifat publik
- [StepFunctions.1] Mesin status Step Functions seharusnya mengaktifkan logging
- [StepFunctions.2] Aktivitas Step Functions harus diberi tag
- [Transfer.1] AWS Transfer Family alur kerja harus ditandai
- [Transfer.2] Server Transfer Family tidak boleh menggunakan protokol FTP untuk koneksi titik akhir
- [WAF.1] Pencatatan ACL Web Global AWS WAF Klasik harus diaktifkan
- [WAF.2] Aturan Regional AWS WAF Klasik harus memiliki setidaknya satu syarat
- [WAF.3] Kelompok aturan Regional AWS WAF Klasik harus memiliki setidaknya satu aturan
- [WAF.4] ACL web Regional AWS WAF klasik harus memiliki setidaknya satu aturan atau kelompok aturan
- [WAF.6] Aturan global AWS WAF klasik harus memiliki setidaknya satu syarat

- [WAF.7] Kelompok aturan global AWS WAF klasik harus memiliki setidaknya satu aturan
- [WAF.8] ACL web global AWS WAF klasik harus memiliki setidaknya satu aturan atau kelompok aturan
- [WAF.11] pencatatan ACL AWS WAF web harus diaktifkan
- AWS WAF Aturan [WAF.12] harus mengaktifkan metrik CloudWatch

Timur Tengah (Bahrain)

Kontrol berikut tidak didukung di Timur Tengah (Bahrain).

- [CloudFront.1] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi
- [CloudFront.3] CloudFront distribusi harus memerlukan enkripsi dalam perjalanan
- [CloudFront.4] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi
- [CloudFront.5] CloudFront distribusi seharusnya mengaktifkan logging
- [CloudFront.6] CloudFront distribusi harus mengaktifkan WAF
- [CloudFront.7] CloudFront distribusi harus menggunakan sertifikat SSL/TLS khusus
- [CloudFront.8] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS
- [CloudFront.9] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus
- [CloudFront.10] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal khusus
- [CloudFront.12] CloudFront distribusi seharusnya tidak menunjukkan asal S3 yang tidak ada
- [CloudFront.13] CloudFront distribusi harus menggunakan kontrol akses asal
- [CloudFront.14] CloudFront distribusi harus ditandai
- [CodeArtifact.1] CodeArtifact repositori harus diberi tag
- [DataFirehose.1] Aliran pengiriman Firehose harus dienkripsi saat istirahat
- [DMS.10] Titik akhir DMS untuk database Neptunus harus mengaktifkan otorisasi IAM
- [DMS.11] Titik akhir DMS untuk MongoDB harus mengaktifkan mekanisme otentikasi
- [DMS.12] Titik akhir DMS untuk Redis harus mengaktifkan TLS
- [DocumentDB.1] Cluster Amazon DocumentDB harus dienkripsi saat istirahat
- [DocumentDB.2] Cluster Amazon DocumentDB harus memiliki periode retensi cadangan yang memadai
- [DocumentDB.3] Cuplikan cluster manual Amazon DocumentDB seharusnya tidak bersifat publik

- [DocumentDB.4] Cluster Amazon DocumentDB harus mempublikasikan log audit ke Log CloudWatch
- [DocumentDB.5] Cluster Amazon DocumentDB harus mengaktifkan perlindungan penghapusan
- [DynamoDB.3] Cluster DynamoDB Accelerator (DAX) harus dienkripsi saat istirahat
- [DynamoDB.7] Cluster DynamoDB Accelerator harus dienkripsi saat transit
- [EC2.20] Kedua terowongan VPN untuk koneksi VPN Site-to-Site harus AWS aktif
- [EC2.23] Amazon EC2 Transit Gateways seharusnya tidak secara otomatis menerima permintaan lampiran VPC
- [EC2.24] Jenis instans paravirtual Amazon EC2 tidak boleh digunakan
- [ECR.4] Repositori publik ECR harus ditandai
- [EFS.6] Target pemasangan EFS tidak boleh dikaitkan dengan subnet publik
- [EKS.3] Kluster EKS harus menggunakan rahasia Kubernetes terenkripsi
- [ElasticBeanstalk.1] Lingkungan Elastic Beanstalk seharusnya mengaktifkan pelaporan kesehatan yang ditingkatkan
- [ElasticBeanstalk.3] Elastic Beanstalk harus mengalirkan log ke CloudWatch
- [EventBridge.4] titik akhir EventBridge global harus mengaktifkan replikasi acara
- [FSX.1] FSx untuk sistem file OpenZFS harus dikonfigurasi untuk menyalin tag ke cadangan dan volume
- [FSX.2] Sistem file FSx for Lustre harus dikonfigurasi untuk menyalin tag ke cadangan
- [GlobalAccelerator.1] Akselerator Akselerator Global harus diberi tag
- [GuardDuty.1] GuardDuty harus diaktifkan
- [IAM.26] Sertifikat SSL/TLS kedaluwarsa yang dikelola di IAM harus dihapus
- [MQ.2] Broker ActiveMQ harus mengalirkan log audit ke CloudWatch
- [MQ.3] Broker Amazon MQ harus mengaktifkan peningkatan versi minor otomatis
- [Opensearch.11] OpenSearch domain harus memiliki setidaknya tiga node primer khusus
- [RDS.7] Cluster RDS harus mengaktifkan perlindungan penghapusan
- [RDS.12] Otentikasi IAM harus dikonfigurasi untuk cluster RDS
- [RDS.14] Cluster Amazon Aurora seharusnya mengaktifkan backtracking
- [RDS.15] Cluster RDS DB harus dikonfigurasi untuk beberapa Availability Zone
- [RDS.16] Cluster RDS DB harus dikonfigurasi untuk menyalin tag ke snapshot
- [RDS.24] Kluster Database RDS harus menggunakan nama pengguna administrator khusus

- [RDS.31] Grup keamanan RDS DB harus ditandai
- [Redshift.6] Amazon Redshift harus mengaktifkan peningkatan otomatis ke versi utama
- [Redshift.15] Grup keamanan Redshift harus mengizinkan masuknya port cluster hanya dari asal yang dibatasi
- [Route53.1] Pemeriksaan kesehatan rute 53 harus ditandai
- [Route53.2] Route 53 zona yang dihosting publik harus mencatat kueri DNS
- [SageMaker.4] varian produksi SageMaker titik akhir harus memiliki jumlah instance awal yang lebih besar dari 1
- [ServiceCatalog.1] Portofolio Service Catalog harus dibagikan hanya dalam suatu organisasi AWS
- [SSM.2] Instans Amazon EC2 yang dikelola oleh Systems Manager harus memiliki status kepatuhan patch COMPLIANT setelah instalasi patch
- [Transfer.2] Server Transfer Family tidak boleh menggunakan protokol FTP untuk koneksi titik akhir
- [WAF.1] Pencatatan ACL Web Global AWS WAF Klasik harus diaktifkan
- [WAF.6] Aturan global AWS WAF klasik harus memiliki setidaknya satu syarat
- [WAF.7] Kelompok aturan global AWS WAF klasik harus memiliki setidaknya satu aturan
- [WAF.8] ACL web global AWS WAF klasik harus memiliki setidaknya satu aturan atau kelompok aturan

Timur Tengah (UEA)

Kontrol berikut tidak didukung di Timur Tengah (UEA).

- [ACM.2] Sertifikat RSA yang dikelola oleh ACM harus menggunakan panjang kunci minimal 2.048 bit
- [ApiGateway.1] API Gateway REST WebSocket dan pencatatan eksekusi API harus diaktifkan
- [ApiGateway.8] Rute API Gateway harus menentukan jenis otorisasi
- [ApiGateway.9] Pencatatan akses harus dikonfigurasi untuk Tahapan API Gateway V2
- [AppSync.2] AWS AppSync harus mengaktifkan logging tingkat lapangan
- [AppSync.5] AWS AppSync GraphQL API tidak boleh diautentikasi dengan kunci API
- [Athena.2] Katalog data Athena harus diberi tag
- [Athena.3] Kelompok kerja Athena harus ditandai
- [AutoScaling.1] Grup Auto Scaling yang terkait dengan penyeimbang beban harus menggunakan pemeriksaan kesehatan ELB

- [Backup.1] titik AWS Backup pemulihan harus dienkripsi saat istirahat
- [Backup.2] poin AWS Backup pemulihan harus ditandai
- [Backup.4] rencana AWS Backup laporan harus ditandai
- [Backup.5] rencana AWS Backup cadangan harus ditandai
- [CloudFormation.2] CloudFormation tumpukan harus ditandai
- [CloudFront.1] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi
- [CloudFront.3] CloudFront distribusi harus memerlukan enkripsi dalam perjalanan
- [CloudFront.4] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi
- [CloudFront.5] CloudFront distribusi seharusnya mengaktifkan logging
- [CloudFront.6] CloudFront distribusi harus mengaktifkan WAF
- [CloudFront.7] CloudFront distribusi harus menggunakan sertifikat SSL/TLS khusus
- [CloudFront.8] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS
- [CloudFront.9] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus
- [CloudFront.10] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal khusus
- [CloudFront.12] CloudFront distribusi seharusnya tidak menunjukkan asal S3 yang tidak ada
- [CloudFront.13] CloudFront distribusi harus menggunakan kontrol akses asal
- [CloudFront.14] CloudFront distribusi harus ditandai
- [CloudTrail.1] CloudTrail harus diaktifkan dan dikonfigurasi dengan setidaknya satu jejak Multi-wilayah yang mencakup acara manajemen baca dan tulis
- [CloudTrail.6] Pastikan bucket S3 yang digunakan untuk menyimpan CloudTrail log tidak dapat diakses publik
- [CloudWatch.15] CloudWatch alarm harus memiliki tindakan tertentu yang dikonfigurasi
- [CloudWatch.16] grup CloudWatch log harus dipertahankan untuk jangka waktu tertentu
- [CloudWatch.17] tindakan CloudWatch alarm harus diaktifkan
- [CodeArtifact.1] CodeArtifact repositori harus diberi tag
- [CodeBuild.1] URL repositori sumber CodeBuild Bitbucket tidak boleh berisi kredensyal sensitif
- [CodeBuild.2] variabel lingkungan CodeBuild proyek tidak boleh berisi kredensil teks yang jelas
- [CodeBuild.3] Log CodeBuild S3 harus dienkripsi
- [CodeBuild.4] lingkungan CodeBuild proyek harus memiliki urasi logging AWS Config
- [DataFirehose.1] Aliran pengiriman Firehose harus dienkripsi saat istirahat

- [Detective.1] Grafik perilaku detektif harus diberi tag
- [DMS.1] Instans replikasi Layanan Migrasi Database tidak boleh bersifat publik
- [DMS.2] Sertifikat DMS harus ditandai
- [DMS.3] Langganan acara DMS harus ditandai
- [DMS.4] Contoh replikasi DMS harus ditandai
- [DMS.5] Grup subnet replikasi DMS harus ditandai
- [DMS.6] Instans replikasi DMS harus mengaktifkan peningkatan versi minor otomatis
- [DMS.7] Tugas replikasi DMS untuk database target seharusnya mengaktifkan logging
- [DMS.8] Tugas replikasi DMS untuk database sumber seharusnya mengaktifkan logging
- [DMS.9] Titik akhir DMS harus menggunakan SSL
- [DMS.10] Titik akhir DMS untuk database Neptunus harus mengaktifkan otorisasi IAM
- [DMS.11] Titik akhir DMS untuk MongoDB harus mengaktifkan mekanisme otentikasi
- [DMS.12] Titik akhir DMS untuk Redis harus mengaktifkan TLS
- [DocumentDB.1] Cluster Amazon DocumentDB harus dienkripsi saat istirahat
- [DocumentDB.2] Cluster Amazon DocumentDB harus memiliki periode retensi cadangan yang memadai
- [DocumentDB.3] Cuplikan cluster manual Amazon DocumentDB seharusnya tidak bersifat publik
- [DocumentDB.4] Cluster Amazon DocumentDB harus mempublikasikan log audit ke Log CloudWatch
- [DocumentDB.5] Cluster Amazon DocumentDB harus mengaktifkan perlindungan penghapusan
- [DynamoDB.3] Cluster DynamoDB Accelerator (DAX) harus dienkripsi saat istirahat
- [DynamoDB.4] Tabel DynamoDB harus ada dalam rencana cadangan
- [DynamoDB.7] Cluster DynamoDB Accelerator harus dienkripsi saat transit
- [EC2.3] Volume Amazon EBS yang terpasang harus dienkripsi saat istirahat
- [EC2.4] Instans EC2 yang dihentikan harus dihapus setelah periode waktu tertentu
- [EC2.6] Pencatatan aliran VPC harus diaktifkan di semua VPC
- [EC2.8] Instans EC2 harus menggunakan Layanan Metadata Instance Versi 2 (IMDSv2)
- [EC2.12] EIP Amazon EC2 yang tidak digunakan harus dihapus
- [EC2.13] Grup keamanan tidak boleh mengizinkan masuknya dari 0.0.0.0/0 atau: :/0 ke port 22
- [EC2.14] Grup keamanan tidak boleh mengizinkan masuknya dari 0.0.0.0/0 atau: :/0 ke port 3389
- [EC2.22] Grup keamanan Amazon EC2 yang tidak digunakan harus dihapus

- [EC2.23] Amazon EC2 Transit Gateways seharusnya tidak secara otomatis menerima permintaan lampiran VPC
- [EC2.24] Jenis instans paravirtual Amazon EC2 tidak boleh digunakan
- [EC2.25] Templat peluncuran Amazon EC2 tidak boleh menetapkan IP publik ke antarmuka jaringan
- [EC2.28] Volume EBS harus dicakup oleh rencana cadangan
- [EC2.51] Titik akhir EC2 Client VPN harus mengaktifkan pencatatan koneksi klien
- [ECR.1] Repositori pribadi ECR harus memiliki pemindaian gambar yang dikonfigurasi
- [ECR.2] Repositori pribadi ECR harus memiliki kekekalan tag yang dikonfigurasi
- [ECR.3] Repositori ECR harus memiliki setidaknya satu kebijakan siklus hidup yang dikonfigurasi
- [ECR.4] Repositori publik ECR harus ditandai
- [ECS.1] Definisi tugas Amazon ECS harus memiliki mode jaringan yang aman dan definisi pengguna.
- [ECS.9] Definisi tugas ECS harus memiliki konfigurasi logging
- [EFS.1] Sistem File Elastis harus dikonfigurasi untuk mengenkripsi data file saat istirahat menggunakan AWS KMS
- [EFS.2] Volume Amazon EFS harus dalam rencana cadangan
- [EFS.3] Titik akses EFS harus menegakkan direktori root
- [EFS.4] Titik akses EFS harus menegakkan identitas pengguna
- [EFS.6] Target pemasangan EFS tidak boleh dikaitkan dengan subnet publik
- [EKS.1] Titik akhir klaster EKS seharusnya tidak dapat diakses publik
- [EKS.2] Kluster EKS harus berjalan pada versi Kubernetes yang didukung
- [EKS.3] Kluster EKS harus menggunakan rahasia Kubernetes terenkripsi
- [ELB.1] Application Load Balancer harus dikonfigurasi untuk mengalihkan semua permintaan HTTP ke HTTPS
- [ELB.3] Pendengar Classic Load Balancer harus dikonfigurasi dengan penghentian HTTPS atau TLS
- [ELB.9] Classic Load Balancer harus mengaktifkan penyeimbangan beban lintas zona
- [ELB.14] Classic Load Balancer harus dikonfigurasi dengan mode mitigasi desync defensif atau paling ketat
- [ELB.16] Application Load Balancers harus dikaitkan dengan ACL web AWS WAF
- [ElastiCache.1] Cluster ElastiCache Redis harus mengaktifkan pencadangan otomatis

- [ElastiCache.2] ElastiCache untuk kluster cache Redis harus mengaktifkan peningkatan versi minor otomatis
- [ElastiCache.3] ElastiCache untuk grup replikasi Redis harus mengaktifkan failover otomatis
- [ElastiCache.4] ElastiCache untuk grup replikasi Redis harus dienkripsi saat istirahat
- [ElastiCache.5] ElastiCache untuk grup replikasi Redis harus dienkripsi saat transit
- [ElastiCache.6] ElastiCache untuk grup replikasi Redis sebelum versi 6.0 harus menggunakan Redis AUTH
- [ElastiCache.7] ElastiCache cluster tidak boleh menggunakan grup subnet default
- [ElasticBeanstalk.1] Lingkungan Elastic Beanstalk seharusnya mengaktifkan pelaporan kesehatan yang ditingkatkan
- [ElasticBeanstalk.2] Pembaruan platform yang dikelola Elastic Beanstalk harus diaktifkan
- [ElasticBeanstalk.3] Elastic Beanstalk harus mengalirkan log ke CloudWatch
- [EMR.1] Node primer cluster EMR Amazon seharusnya tidak memiliki alamat IP publik
- [EventBridge.2] bus EventBridge acara harus diberi tag
- [EventBridge.3] bus acara EventBridge khusus harus memiliki kebijakan berbasis sumber daya terlampir
- [EventBridge.4] titik akhir EventBridge global harus mengaktifkan replikasi acara
- [FSX.1] FSx untuk sistem file OpenZFS harus dikonfigurasi untuk menyalin tag ke cadangan dan volume
- [FSX.2] Sistem file FSx for Lustre harus dikonfigurasi untuk menyalin tag ke cadangan
- [GlobalAccelerator.1] Akselerator Akselerator Global harus diberi tag
- [GuardDuty.1] GuardDuty harus diaktifkan
- [GuardDuty.2] GuardDuty filter harus diberi tag
- [GuardDuty.3] GuardDuty IPset harus ditandai
- [GuardDuty.4] GuardDuty detektor harus ditandai
- [IAM.1] Kebijakan IAM seharusnya tidak mengizinkan hak administratif “*” penuh
- [IAM.2] Pengguna IAM seharusnya tidak memiliki kebijakan IAM yang dilampirkan
- [IAM.3] Kunci akses pengguna IAM harus diputar setiap 90 hari atau kurang
- [IAM.4] Kunci akses pengguna root IAM seharusnya tidak ada
- [IAM.5] MFA harus diaktifkan untuk semua pengguna IAM yang memiliki kata sandi konsol
- [IAM.6] MFA perangkat keras harus diaktifkan untuk pengguna root

- [IAM.8] Kredensyal pengguna IAM yang tidak digunakan harus dihapus
- [IAM.9] MFA harus diaktifkan untuk pengguna root
- [IAM.18] Memastikan peran dukungan telah dibuat untuk mengelola insiden dengan AWS Support
- [IAM.19] MFA harus diaktifkan untuk semua pengguna IAM
- [IAM.21] Kebijakan terkelola pelanggan IAM yang Anda buat seharusnya tidak mengizinkan tindakan wildcard untuk layanan
- [IAM.22] Kredensyal pengguna IAM yang tidak digunakan selama 45 hari harus dihapus
- [IAM.24] Peran IAM harus ditandai
- [IAM.25] Pengguna IAM harus diberi tag
- [IAM.26] Sertifikat SSL/TLS kedaluwarsa yang dikelola di IAM harus dihapus
- [IAM.27] Identitas IAM seharusnya tidak memiliki kebijakan yang dilampirkan AWSCloudShellFullAccess
- [IoT.1] profil AWS IoT Core keamanan harus ditandai
- [IoT.2] tindakan AWS IoT Core mitigasi harus ditandai
- AWS IoT Core Dimensi [IoT.3] harus ditandai
- [Kinesis.1] Aliran kinesis harus dienkripsi saat istirahat
- [KMS.1] Kebijakan yang dikelola pelanggan IAM tidak boleh mengizinkan tindakan dekripsi pada semua kunci KMS
- [KMS.2] Prinsipal IAM tidak boleh memiliki kebijakan inline IAM yang memungkinkan tindakan dekripsi pada semua kunci KMS
- [KMS.4] rotasi AWS KMS tombol harus diaktifkan
- [Lambda.5] Fungsi VPC Lambda harus beroperasi di beberapa Availability Zone
- [Macie.1] Amazon Macie harus diaktifkan
- [Macie.2] Penemuan data sensitif otomatis Macie harus diaktifkan
- [MQ.2] Broker ActiveMQ harus mengalirkan log audit ke CloudWatch
- [MQ.3] Broker Amazon MQ harus mengaktifkan peningkatan versi minor otomatis
- [MSK.1] Cluster MSK harus dienkripsi saat transit di antara node broker
- [MSK.2] Kluster MSK seharusnya telah meningkatkan pemantauan yang dikonfigurasi
- [Neptunus.1] Cluster DB Neptunus harus dienkripsi saat istirahat
- [Neptune.2] Cluster DB Neptunus harus menerbitkan log audit ke Log CloudWatch
- [Neptune.3] Snapshot cluster Neptunus DB seharusnya tidak publik

- [Neptunus.4] Cluster DB Neptunus harus mengaktifkan perlindungan penghapusan
- [Neptunus.5] Cluster DB Neptunus harus mengaktifkan cadangan otomatis
- [Neptune.6] Snapshot cluster Neptunus DB harus dienkripsi saat istirahat
- [Neptunus.7] Cluster DB Neptunus harus mengaktifkan otentikasi basis data IAM
- [Neptunus.8] Cluster DB Neptunus harus dikonfigurasi untuk menyalin tag ke snapshot
- [Neptunus.9] Cluster DB Neptunus harus digunakan di beberapa Availability Zone
- [NetworkFirewall.1] Firewall Firewall Jaringan harus digunakan di beberapa Availability Zone
- [NetworkFirewall.2] Pencatatan Firewall Jaringan harus diaktifkan
- [NetworkFirewall.3] Kebijakan Network Firewall harus memiliki setidaknya satu kelompok aturan yang terkait
- [NetworkFirewall.4] Tindakan stateless default untuk kebijakan Network Firewall harus drop atau forward untuk paket penuh
- [NetworkFirewall.5] Tindakan stateless default untuk kebijakan Network Firewall harus drop atau forward untuk paket yang terfragmentasi
- [NetworkFirewall.6] Grup aturan Stateless Network Firewall tidak boleh kosong
- [NetworkFirewall.7] Firewall Firewall Jaringan harus diberi tag
- [NetworkFirewall.8] Kebijakan firewall Network Firewall harus ditandai
- [NetworkFirewall.9] Firewall Firewall Jaringan harus mengaktifkan perlindungan penghapusan
- [Opensearch.1] OpenSearch domain harus mengaktifkan enkripsi saat istirahat
- [Opensearch.2] OpenSearch domain tidak boleh diakses publik
- [Opensearch.3] OpenSearch domain harus mengenkripsi data yang dikirim antar node
- [Opensearch.4] login kesalahan OpenSearch domain ke Log harus diaktifkan CloudWatch
- [Opensearch.5] OpenSearch domain harus mengaktifkan pencatatan audit
- [Opensearch.6] OpenSearch domain harus memiliki setidaknya tiga node data
- [Opensearch.7] OpenSearch domain harus mengaktifkan kontrol akses berbutir halus
- [Opensearch.8] Koneksi ke OpenSearch domain harus dienkripsi menggunakan kebijakan keamanan TLS terbaru
- [Opensearch.9] domain harus ditandai OpenSearch
- [Opensearch.10] OpenSearch domain harus memiliki pembaruan perangkat lunak terbaru yang diinstal
- [Opensearch.11] OpenSearch domain harus memiliki setidaknya tiga node primer khusus

- [RDS.1] Snapshot RDS harus pribadi
- [RDS.2] Instans RDS DB harus melarang akses publik, sebagaimana ditentukan oleh urasi PubliclyAccessible AWS Config
- [RDS.3] Instans RDS DB harus mengaktifkan enkripsi saat istirahat
- [RDS.5] Instans RDS DB harus dikonfigurasi dengan beberapa Availability Zone
- [RDS.6] Pemantauan yang ditingkatkan harus dikonfigurasi untuk instans RDS DB
- [RDS.8] Instans RDS DB harus mengaktifkan perlindungan penghapusan
- [RDS.11] Instans RDS harus mengaktifkan pencadangan otomatis
- [RDS.14] Cluster Amazon Aurora seharusnya mengaktifkan backtracking
- [RDS.16] Cluster RDS DB harus dikonfigurasi untuk menyalin tag ke snapshot
- [RDS.24] Kluster Database RDS harus menggunakan nama pengguna administrator khusus
- [RDS.26] Instans RDS DB harus dilindungi oleh rencana cadangan
- [RDS.31] Grup keamanan RDS DB harus ditandai
- [RDS.35] Cluster RDS DB harus mengaktifkan peningkatan versi minor otomatis
- [Redshift.9] Cluster Redshift tidak boleh menggunakan nama database default
- [Redshift.12] Langganan pemberitahuan acara Redshift harus ditandai
- [Redshift.15] Grup keamanan Redshift harus mengizinkan masuknya port cluster hanya dari asal yang dibatasi
- [Route53.1] Pemeriksaan kesehatan rute 53 harus ditandai
- [Route53.2] Route 53 zona yang dihosting publik harus mencatat kueri DNS
- [S3.2] Bucket tujuan umum S3 harus memblokir akses baca publik
- [S3.3] Bucket tujuan umum S3 harus memblokir akses tulis publik
- [S3.5] Bucket tujuan umum S3 harus memerlukan permintaan untuk menggunakan SSL
- [S3.6] Kebijakan bucket tujuan umum S3 harus membatasi akses ke yang lain Akun AWS
- [S3.14] Bucket tujuan umum S3 harus mengaktifkan versi
- [SageMaker.1] Instans SageMaker notebook Amazon seharusnya tidak memiliki akses internet langsung
- [SageMaker.2] instance SageMaker notebook harus diluncurkan dalam VPC khusus
- [SageMaker.3] Pengguna seharusnya tidak memiliki akses root ke instance SageMaker notebook
- [SageMaker.4] varian produksi SageMaker titik akhir harus memiliki jumlah instance awal yang lebih besar dari 1

- [SES.1] Daftar kontak SES harus ditandai
- [SES.2] Set konfigurasi SES harus ditandai
- [SecretsManager.1] Rahasia Secrets Manager harus mengaktifkan rotasi otomatis
- [SecretsManager.2] Rahasia Secrets Manager yang dikonfigurasi dengan rotasi otomatis harus berhasil diputar
- [SecretsManager.3] Hapus rahasia Secrets Manager yang tidak digunakan
- [SecretsManager.4] Rahasia Secrets Manager harus diputar dalam jumlah hari tertentu
- [ServiceCatalog.1] Portofolio Service Catalog harus dibagikan hanya dalam suatu organisasi AWS
- [SNS.1] Topik SNS harus dienkripsi saat istirahat menggunakan AWS KMS
- [SNS.3] Topik SNS harus ditandai
- [SQS.1] Antrian Amazon SQS harus dienkripsi saat istirahat
- [SQS.2] Antrian SQS harus ditandai
- [SSM.1] Instans Amazon EC2 harus dikelola oleh AWS Systems Manager
- [StepFunctions.1] Mesin status Step Functions seharusnya mengaktifkan logging
- [Transfer.1] AWS Transfer Family alur kerja harus ditandai
- [Transfer.2] Server Transfer Family tidak boleh menggunakan protokol FTP untuk koneksi titik akhir
- [WAF.1] Pencatatan ACL Web Global AWS WAF Klasik harus diaktifkan
- [WAF.2] Aturan Regional AWS WAF Klasik harus memiliki setidaknya satu syarat
- [WAF.3] Kelompok aturan Regional AWS WAF Klasik harus memiliki setidaknya satu aturan
- [WAF.4] ACL web Regional AWS WAF klasik harus memiliki setidaknya satu aturan atau kelompok aturan
- [WAF.6] Aturan global AWS WAF klasik harus memiliki setidaknya satu syarat
- [WAF.7] Kelompok aturan global AWS WAF klasik harus memiliki setidaknya satu aturan
- [WAF.8] ACL web global AWS WAF klasik harus memiliki setidaknya satu aturan atau kelompok aturan
- [WAF.10] ACL AWS WAF web harus memiliki setidaknya satu aturan atau kelompok aturan
- [WAF.11] pencatatan ACL AWS WAF web harus diaktifkan

Amerika Selatan (Sao Paulo)

Kontrol berikut tidak didukung di Amerika Selatan (São Paulo).

- [CloudFront.1] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi
- [CloudFront.3] CloudFront distribusi harus memerlukan enkripsi dalam perjalanan
- [CloudFront.4] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi
- [CloudFront.5] CloudFront distribusi seharusnya mengaktifkan logging
- [CloudFront.6] CloudFront distribusi harus mengaktifkan WAF
- [CloudFront.7] CloudFront distribusi harus menggunakan sertifikat SSL/TLS khusus
- [CloudFront.8] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS
- [CloudFront.9] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus
- [CloudFront.10] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal khusus
- [CloudFront.12] CloudFront distribusi seharusnya tidak menunjukkan asal S3 yang tidak ada
- [CloudFront.13] CloudFront distribusi harus menggunakan kontrol akses asal
- [CloudFront.14] CloudFront distribusi harus ditandai
- [CodeArtifact.1] CodeArtifact repositori harus diberi tag
- [DataFirehose.1] Aliran pengiriman Firehose harus dienkripsi saat istirahat
- [DMS.10] Titik akhir DMS untuk database Neptunus harus mengaktifkan otorisasi IAM
- [DMS.11] Titik akhir DMS untuk MongoDB harus mengaktifkan mekanisme otentikasi
- [DMS.12] Titik akhir DMS untuk Redis harus mengaktifkan TLS
- [DynamoDB.7] Cluster DynamoDB Accelerator harus dienkripsi saat transit
- [ECR.4] Repositori publik ECR harus ditandai
- [EFS.6] Target pemasangan EFS tidak boleh dikaitkan dengan subnet publik
- [EKS.3] Kluster EKS harus menggunakan rahasia Kubernetes terenkripsi
- [FSX.1] FSx untuk sistem file OpenZFS harus dikonfigurasi untuk menyalin tag ke cadangan dan volume
- [FSX.2] Sistem file FSx for Lustre harus dikonfigurasi untuk menyalin tag ke cadangan
- [GlobalAccelerator.1] Akselerator Akselerator Global harus diberi tag
- [IAM.26] Sertifikat SSL/TLS kedaluwarsa yang dikelola di IAM harus dihapus
- [IoT.1] profil AWS IoT Core keamanan harus ditandai
- [IoT.2] tindakan AWS IoT Core mitigasi harus ditandai
- AWS IoT Core Dimensi [IoT.3] harus ditandai

- [MQ.2] Broker ActiveMQ harus mengalirkan log audit ke CloudWatch
- [MQ.3] Broker Amazon MQ harus mengaktifkan peningkatan versi minor otomatis
- [Opensearch.11] OpenSearch domain harus memiliki setidaknya tiga node primer khusus
- [RDS.7] Cluster RDS harus mengaktifkan perlindungan penghapusan
- [RDS.12] Otentikasi IAM harus dikonfigurasi untuk cluster RDS
- [RDS.14] Cluster Amazon Aurora seharusnya mengaktifkan backtracking
- [RDS.15] Cluster RDS DB harus dikonfigurasi untuk beberapa Availability Zone
- [RDS.16] Cluster RDS DB harus dikonfigurasi untuk menyalin tag ke snapshot
- [RDS.24] Kluster Database RDS harus menggunakan nama pengguna administrator khusus
- [Redshift.15] Grup keamanan Redshift harus mengizinkan masuknya port cluster hanya dari asal yang dibatasi
- [Route53.1] Pemeriksaan kesehatan rute 53 harus ditandai
- [Route53.2] Route 53 zona yang dihosting publik harus mencatat kueri DNS
- [SageMaker.4] varian produksi SageMaker titik akhir harus memiliki jumlah instance awal yang lebih besar dari 1
- [ServiceCatalog.1] Portofolio Service Catalog harus dibagikan hanya dalam suatu organisasi AWS
- [Transfer.2] Server Transfer Family tidak boleh menggunakan protokol FTP untuk koneksi titik akhir
- [WAF.1] Pencatatan ACL Web Global AWS WAF Klasik harus diaktifkan
- [WAF.6] Aturan global AWS WAF klasik harus memiliki setidaknya satu syarat
- [WAF.7] Kelompok aturan global AWS WAF klasik harus memiliki setidaknya satu aturan
- [WAF.8] ACL web global AWS WAF klasik harus memiliki setidaknya satu aturan atau kelompok aturan

AWS GovCloud (AS-Timur)

Kontrol berikut tidak didukung di AWS GovCloud (AS-Timur).

- [ACM.2] Sertifikat RSA yang dikelola oleh ACM harus menggunakan panjang kunci minimal 2.048 bit
- [ACM.3] Sertifikat ACM harus ditandai
- [Akun.1] Informasi kontak keamanan harus disediakan untuk Akun AWS
- [Akun.2] Akun AWS harus menjadi bagian dari organisasi AWS Organizations

- [ApiGateway.2] Tahapan API Gateway REST API harus dikonfigurasi untuk menggunakan sertifikat SSL untuk otentikasi backend
- [ApiGateway.3] Tahapan API Gateway REST API harus mengaktifkan penelusuran AWS X-Ray
- [ApiGateway.4] API Gateway harus dikaitkan dengan ACL Web WAF
- [ApiGateway.8] Rute API Gateway harus menentukan jenis otorisasi
- [ApiGateway.9] Pencatatan akses harus dikonfigurasi untuk Tahapan API Gateway V2
- [AppSync.2] AWS AppSync harus mengaktifkan logging tingkat lapangan
- [AppSync.4] AWS AppSync GraphQL API harus diberi tag
- [AppSync.5] AWS AppSync GraphQL API tidak boleh diautentikasi dengan kunci API
- [Athena.2] Katalog data Athena harus diberi tag
- [Athena.3] Kelompok kerja Athena harus ditandai
- [AutoScaling.2] Grup Auto Scaling Amazon EC2 harus mencakup beberapa Availability Zone
- [AutoScaling.3] Konfigurasi peluncuran grup Auto Scaling harus mengonfigurasi instans EC2 agar memerlukan Layanan Metadata Instans Versi 2 (IMDSv2)
- [AutoScaling.6] Grup Auto Scaling harus menggunakan beberapa jenis instance di beberapa Availability Zone
- [AutoScaling.9] Grup Auto Scaling Amazon EC2 harus menggunakan templat peluncuran Amazon EC2
- [AutoScaling.10] Grup Penskalaan Otomatis EC2 harus diberi tag
- [Autoscaling.5] Instans Amazon EC2 yang diluncurkan menggunakan konfigurasi peluncuran grup Auto Scaling seharusnya tidak memiliki alamat IP Publik
- [Backup.2] poin AWS Backup pemulihan harus ditandai
- [Backup.3] AWS Backup brankas harus ditandai
- [Backup.4] rencana AWS Backup laporan harus ditandai
- [Backup.5] rencana AWS Backup cadangan harus ditandai
- [CloudFormation.2] CloudFormation tumpukan harus ditandai
- [CloudFront.1] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi
- [CloudFront.3] CloudFront distribusi harus memerlukan enkripsi dalam perjalanan
- [CloudFront.4] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi
- [CloudFront.5] CloudFront distribusi seharusnya mengaktifkan logging
- [CloudFront.6] CloudFront distribusi harus mengaktifkan WAF

- [CloudFront.7] CloudFront distribusi harus menggunakan sertifikat SSL/TLS khusus
- [CloudFront.8] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS
- [CloudFront.9] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus
- [CloudFront.10] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal khusus
- [CloudFront.12] CloudFront distribusi seharusnya tidak menunjukkan asal S3 yang tidak ada
- [CloudFront.13] CloudFront distribusi harus menggunakan kontrol akses asal
- [CloudFront.14] CloudFront distribusi harus ditandai
- [CloudTrail.9] CloudTrail jejak harus ditandai
- [CloudWatch.15] CloudWatch alarm harus memiliki tindakan tertentu yang dikonfigurasi
- [CloudWatch.16] grup CloudWatch log harus dipertahankan untuk jangka waktu tertentu
- [CloudWatch.17] tindakan CloudWatch alarm harus diaktifkan
- [CodeArtifact.1] CodeArtifact repositori harus diberi tag
- [CodeBuild.1] URL repositori sumber CodeBuild Bitbucket tidak boleh berisi kredensyal sensitif
- [CodeBuild.2] variabel lingkungan CodeBuild proyek tidak boleh berisi kredensil teks yang jelas
- [CodeBuild.3] Log CodeBuild S3 harus dienkripsi
- [CodeBuild.4] lingkungan CodeBuild proyek harus memiliki urasi logging AWS Config
- [DataFirehose.1] Aliran pengiriman Firehose harus dienkripsi saat istirahat
- [Detective.1] Grafik perilaku detektif harus diberi tag
- [DMS.2] Sertifikat DMS harus ditandai
- [DMS.3] Langganan acara DMS harus ditandai
- [DMS.4] Contoh replikasi DMS harus ditandai
- [DMS.5] Grup subnet replikasi DMS harus ditandai
- [DMS.6] Instans replikasi DMS harus mengaktifkan peningkatan versi minor otomatis
- [DMS.7] Tugas replikasi DMS untuk database target seharusnya mengaktifkan logging
- [DMS.8] Tugas replikasi DMS untuk database sumber seharusnya mengaktifkan logging
- [DMS.9] Titik akhir DMS harus menggunakan SSL
- [DMS.10] Titik akhir DMS untuk database Neptunus harus mengaktifkan otorisasi IAM
- [DMS.11] Titik akhir DMS untuk MongoDB harus mengaktifkan mekanisme otentikasi
- [DMS.12] Titik akhir DMS untuk Redis harus mengaktifkan TLS
- [DocumentDB.1] Cluster Amazon DocumentDB harus dienkripsi saat istirahat

- [DocumentDB.2] Cluster Amazon DocumentDB harus memiliki periode retensi cadangan yang memadai
- [DocumentDB.3] Cuplikan cluster manual Amazon DocumentDB seharusnya tidak bersifat publik
- [DocumentDB.4] Cluster Amazon DocumentDB harus mempublikasikan log audit ke Log CloudWatch
- [DocumentDB.5] Cluster Amazon DocumentDB harus mengaktifkan perlindungan penghapusan
- [DynamoDB.1] Tabel DynamoDB harus secara otomatis menskalakan kapasitas sesuai permintaan
- [DynamoDB.3] Cluster DynamoDB Accelerator (DAX) harus dienkripsi saat istirahat
- [DynamoDB.4] Tabel DynamoDB harus ada dalam rencana cadangan
- [DynamoDB.5] Tabel DynamoDB harus diberi tag
- [DynamoDB.7] Cluster DynamoDB Accelerator harus dienkripsi saat transit
- [EC2.15] Subnet Amazon EC2 seharusnya tidak secara otomatis menetapkan alamat IP publik
- [EC2.16] Daftar Kontrol Akses Jaringan yang Tidak Digunakan harus dihapus
- [EC2.17] Instans Amazon EC2 tidak boleh menggunakan beberapa ENI
- [EC2.21] ACL jaringan seharusnya tidak mengizinkan masuknya dari 0.0.0.0/0 ke port 22 atau port 3389
- [EC2.22] Grup keamanan Amazon EC2 yang tidak digunakan harus dihapus
- [EC2.23] Amazon EC2 Transit Gateways seharusnya tidak secara otomatis menerima permintaan lampiran VPC
- [EC2.24] Jenis instans paravirtual Amazon EC2 tidak boleh digunakan
- [EC2.25] Templat peluncuran Amazon EC2 tidak boleh menetapkan IP publik ke antarmuka jaringan
- [EC2.28] Volume EBS harus dicakup oleh rencana cadangan
- [EC2.33] Lampiran gateway transit EC2 harus ditandai
- [EC2.34] Tabel rute gateway transit EC2 harus ditandai
- [EC2.35] Antarmuka jaringan EC2 harus ditandai
- [EC2.36] Gateway pelanggan EC2 harus ditandai
- [EC2.37] Alamat IP Elastis EC2 harus ditandai
- [EC2.38] Instans EC2 harus ditandai
- [EC2.39] Gerbang internet EC2 harus ditandai
- [EC2.40] Gerbang EC2 NAT harus ditandai

- [EC2.41] ACL jaringan EC2 harus ditandai
- [EC2.42] Tabel rute EC2 harus ditandai
- [EC2.43] Grup keamanan EC2 harus ditandai
- [EC2.44] Subnet EC2 harus ditandai
- [EC2.45] Volume EC2 harus ditandai
- [EC2.46] VPC Amazon harus ditandai
- [EC2.47] Layanan titik akhir Amazon VPC harus ditandai
- [EC2.48] Log aliran VPC Amazon harus ditandai
- [EC2.49] Koneksi peering VPC Amazon harus ditandai
- [EC2.50] Gateway EC2 VPN harus ditandai
- [EC2.52] Gerbang transit EC2 harus ditandai
- [ECR.1] Repositori pribadi ECR harus memiliki pemindaian gambar yang dikonfigurasi
- [ECR.2] Repositori pribadi ECR harus memiliki kekekalan tag yang dikonfigurasi
- [ECR.3] Repositori ECR harus memiliki setidaknya satu kebijakan siklus hidup yang dikonfigurasi
- [ECR.4] Repositori publik ECR harus ditandai
- [ECS.1] Definisi tugas Amazon ECS harus memiliki mode jaringan yang aman dan definisi pengguna.
- [ECS.3] Definisi tugas ECS tidak boleh membagikan namespace proses host
- [ECS.4] Kontainer ECS harus berjalan sebagai non-hak istimewa
- [ECS.5] Wadah ECS harus dibatasi pada akses hanya-baca ke sistem file root
- [ECS.8] Rahasia tidak boleh diteruskan sebagai variabel lingkungan kontainer
- [ECS.9] Definisi tugas ECS harus memiliki konfigurasi logging
- [ECS.10] Layanan ECS Fargate harus berjalan pada versi platform Fargate terbaru
- [ECS.12] Cluster ECS harus menggunakan Wawasan Kontainer
- [ECS.13] Layanan ECS harus ditandai
- [ECS.14] Cluster ECS harus ditandai
- [ECS.15] Definisi tugas ECS harus ditandai
- [EFS.2] Volume Amazon EFS harus dalam rencana cadangan
- [EFS.3] Titik akses EFS harus menegakkan direktori root
- [EFS.4] Titik akses EFS harus menegakkan identitas pengguna
- [EFS.5] Titik akses EFS harus ditandai

- [EFS.6] Target pemasangan EFS tidak boleh dikaitkan dengan subnet publik
- [EKS.1] Titik akhir klaster EKS seharusnya tidak dapat diakses publik
- [EKS.2] Kluster EKS harus berjalan pada versi Kubernetes yang didukung
- [EKS.3] Kluster EKS harus menggunakan rahasia Kubernetes terenkripsi
- [EKS.6] Kluster EKS harus ditandai
- [EKS.7] Konfigurasi penyedia identitas EKS harus ditandai
- [EKS.8] Kluster EKS harus mengaktifkan pencatatan audit
- [ELB.2] Classic Load Balancer dengan pendengar SSL/HTTPS harus menggunakan sertifikat yang disediakan oleh AWS Certificate Manager
- [ELB.8] Classic Load Balancer dengan pendengar SSL harus menggunakan kebijakan keamanan yang telah ditentukan sebelumnya yang memiliki urasi yang kuat AWS Config
- [ELB.10] Classic Load Balancer harus menjangkau beberapa Availability Zone
- [ELB.12] Application Load Balancer harus dikonfigurasi dengan mode mitigasi desync defensif atau paling ketat
- [ELB.13] Penyeimbang Beban Aplikasi, Jaringan, dan Gateway harus mencakup beberapa Availability Zone
- [ELB.14] Classic Load Balancer harus dikonfigurasi dengan mode mitigasi desync defensif atau paling ketat
- [ELB.16] Application Load Balancers harus dikaitkan dengan ACL web AWS WAF
- [ElastiCache.1] Cluster ElastiCache Redis harus mengaktifkan pencadangan otomatis
- [ElastiCache.2] ElastiCache untuk kluster cache Redis harus mengaktifkan peningkatan versi minor otomatis
- [ElastiCache.3] ElastiCache untuk grup replikasi Redis harus mengaktifkan failover otomatis
- [ElastiCache.4] ElastiCache untuk grup replikasi Redis harus dienkripsi saat istirahat
- [ElastiCache.5] ElastiCache untuk grup replikasi Redis harus dienkripsi saat transit
- [ElastiCache.6] ElastiCache untuk grup replikasi Redis sebelum versi 6.0 harus menggunakan Redis AUTH
- [ElastiCache.7] ElastiCache cluster tidak boleh menggunakan grup subnet default
- [ElasticBeanstalk.1] Lingkungan Elastic Beanstalk seharusnya mengaktifkan pelaporan kesehatan yang ditingkatkan
- [ElasticBeanstalk.2] Pembaruan platform yang dikelola Elastic Beanstalk harus diaktifkan
- [ElasticBeanstalk.3] Elastic Beanstalk harus mengalirkan log ke CloudWatch

- [EMR.2] Pengaturan akses publik blok EMR Amazon harus diaktifkan
- [ES.4] Kesalahan domain Elasticsearch yang masuk ke CloudWatch Log harus diaktifkan
- [ES.9] Domain Elasticsearch harus diberi tag
- [EventBridge.2] bus EventBridge acara harus diberi tag
- [EventBridge.3] bus acara EventBridge khusus harus memiliki kebijakan berbasis sumber daya terlampir
- [EventBridge.4] titik akhir EventBridge global harus mengaktifkan replikasi acara
- [FSX.1] FSx untuk sistem file OpenZFS harus dikonfigurasi untuk menyalin tag ke cadangan dan volume
- [FSX.2] Sistem file FSx for Lustre harus dikonfigurasi untuk menyalin tag ke cadangan
- [GlobalAccelerator.1] Akselerator Akselerator Global harus diberi tag
- AWS Glue Pekerjaan [Glue.1] harus ditandai
- [GuardDuty.1] GuardDuty harus diaktifkan
- [GuardDuty.2] GuardDuty filter harus diberi tag
- [GuardDuty.3] GuardDuty IPset harus ditandai
- [GuardDuty.4] GuardDuty detektor harus ditandai
- [IAM.6] MFA perangkat keras harus diaktifkan untuk pengguna root
- [IAM.9] MFA harus diaktifkan untuk pengguna root
- [IAM.21] Kebijakan terkelola pelanggan IAM yang Anda buat seharusnya tidak mengizinkan tindakan wildcard untuk layanan
- [IAM.23] Penganalisis Akses IAM harus ditandai
- [IAM.24] Peran IAM harus ditandai
- [IAM.25] Pengguna IAM harus diberi tag
- [IAM.26] Sertifikat SSL/TLS kedaluwarsa yang dikelola di IAM harus dihapus
- [IAM.28] IAM Access Analyzer penganalisis akses eksternal harus diaktifkan
- [IoT.1] profil AWS IoT Core keamanan harus ditandai
- [IoT.2] tindakan AWS IoT Core mitigasi harus ditandai
- AWS IoT Core Dimensi [IoT.3] harus ditandai
- [IoT.4] AWS IoT Core otorisasi harus diberi tag
- [IoT.5] alias AWS IoT Core peran harus ditandai
- AWS IoT Core Kebijakan [IoT.6] harus ditandai

- [Kinesis.1] Aliran kinesis harus dienkripsi saat istirahat
- [Kinesis.2] Aliran kinesis harus ditandai
- [Lambda.5] Fungsi VPC Lambda harus beroperasi di beberapa Availability Zone
- [Lambda.6] Fungsi Lambda harus ditandai
- [Macie.1] Amazon Macie harus diaktifkan
- [Macie.2] Penemuan data sensitif otomatis Macie harus diaktifkan
- [MQ.2] Broker ActiveMQ harus mengalirkan log audit ke CloudWatch
- [MQ.3] Broker Amazon MQ harus mengaktifkan peningkatan versi minor otomatis
- [MQ.4] Broker Amazon MQ harus diberi tag
- [MQ.5] Broker ActiveMQ harus menggunakan mode penerapan aktif/siaga
- [MQ.6] Broker RabbitMQ harus menggunakan mode penerapan cluster
- [MSK.1] Cluster MSK harus dienkripsi saat transit di antara node broker
- [MSK.2] Kluster MSK seharusnya telah meningkatkan pemantauan yang dikonfigurasi
- [Neptunus.1] Cluster DB Neptunus harus dienkripsi saat istirahat
- [Neptune.2] Cluster DB Neptunus harus menerbitkan log audit ke Log CloudWatch
- [Neptune.3] Snapshot cluster Neptunus DB seharusnya tidak publik
- [Neptunus.4] Cluster DB Neptunus harus mengaktifkan perlindungan penghapusan
- [Neptunus.5] Cluster DB Neptunus harus mengaktifkan cadangan otomatis
- [Neptune.6] Snapshot cluster Neptunus DB harus dienkripsi saat istirahat
- [Neptunus.7] Cluster DB Neptunus harus mengaktifkan otentikasi basis data IAM
- [Neptunus.8] Cluster DB Neptunus harus dikonfigurasi untuk menyalin tag ke snapshot
- [Neptunus.9] Cluster DB Neptunus harus digunakan di beberapa Availability Zone
- [NetworkFirewall.1] Firewall Firewall Jaringan harus digunakan di beberapa Availability Zone
- [NetworkFirewall.2] Pencatatan Firewall Jaringan harus diaktifkan
- [NetworkFirewall.3] Kebijakan Network Firewall harus memiliki setidaknya satu kelompok aturan yang terkait
- [NetworkFirewall.4] Tindakan stateless default untuk kebijakan Network Firewall harus drop atau forward untuk paket penuh
- [NetworkFirewall.5] Tindakan stateless default untuk kebijakan Network Firewall harus drop atau forward untuk paket yang terfragmentasi
- [NetworkFirewall.6] Grup aturan Stateless Network Firewall tidak boleh kosong

- [NetworkFirewall.7] Firewall Firewall Jaringan harus diberi tag
- [NetworkFirewall.8] Kebijakan firewall Network Firewall harus ditandai
- [NetworkFirewall.9] Firewall Firewall Jaringan harus mengaktifkan perlindungan penghapusan
- [Opensearch.1] OpenSearch domain harus mengaktifkan enkripsi saat istirahat
- [Opensearch.2] OpenSearch domain tidak boleh diakses publik
- [Opensearch.3] OpenSearch domain harus mengenkripsi data yang dikirim antar node
- [Opensearch.4] login kesalahan OpenSearch domain ke Log harus diaktifkan CloudWatch
- [Opensearch.5] OpenSearch domain harus mengaktifkan pencatatan audit
- [Opensearch.6] OpenSearch domain harus memiliki setidaknya tiga node data
- [Opensearch.7] OpenSearch domain harus mengaktifkan kontrol akses berbutir halus
- [Opensearch.8] Koneksi ke OpenSearch domain harus dienkripsi menggunakan kebijakan keamanan TLS terbaru
- [Opensearch.9] domain harus ditandai OpenSearch
- [Opensearch.11] OpenSearch domain harus memiliki setidaknya tiga node primer khusus
- [PCA.1] otoritas sertifikat AWS Private CA root harus dinonaktifkan
- [RDS.12] Otentikasi IAM harus dikonfigurasi untuk cluster RDS
- [RDS.13] Peningkatan versi minor otomatis RDS harus diaktifkan
- [RDS.14] Cluster Amazon Aurora seharusnya mengaktifkan backtracking
- [RDS.15] Cluster RDS DB harus dikonfigurasi untuk beberapa Availability Zone
- [RDS.24] Kluster Database RDS harus menggunakan nama pengguna administrator khusus
- [RDS.25] Instans database RDS harus menggunakan nama pengguna administrator khusus
- [RDS.26] Instans RDS DB harus dilindungi oleh rencana cadangan
- [RDS.27] Cluster RDS DB harus dienkripsi saat istirahat
- [RDS.28] Cluster RDS DB harus ditandai
- [RDS.29] Snapshot cluster RDS DB harus ditandai
- [RDS.30] Instans RDS DB harus ditandai
- [RDS.31] Grup keamanan RDS DB harus ditandai
- [RDS.32] Snapshot RDS DB harus ditandai
- [RDS.33] Grup subnet RDS DB harus ditandai
- [RDS.34] Cluster Aurora MySQL DB harus menerbitkan log audit ke Log CloudWatch
- [RDS.35] Cluster RDS DB harus mengaktifkan peningkatan versi minor otomatis

- [Redshift.7] Cluster Redshift harus menggunakan perutean VPC yang ditingkatkan
- [Redshift.8] Cluster Amazon Redshift tidak boleh menggunakan nama pengguna Admin default
- [Redshift.9] Cluster Redshift tidak boleh menggunakan nama database default
- [Redshift.10] Cluster Redshift harus dienkripsi saat istirahat
- [Redshift.11] Cluster Redshift harus ditandai
- [Redshift.12] Langganan pemberitahuan acara Redshift harus ditandai
- [Redshift.13] Snapshot cluster Redshift harus ditandai
- [Redshift.14] Grup subnet cluster Redshift harus ditandai
- [Redshift.15] Grup keamanan Redshift harus mengizinkan masuknya port cluster hanya dari asal yang dibatasi
- [Route53.1] Pemeriksaan kesehatan rute 53 harus ditandai
- [Route53.2] Route 53 zona yang dihosting publik harus mencatat kueri DNS
- [S3.1] Bucket tujuan umum S3 harus mengaktifkan pengaturan akses publik blok
- [S3.8] Bucket tujuan umum S3 harus memblokir akses publik
- [S3.10] Bucket tujuan umum S3 dengan versi diaktifkan harus memiliki konfigurasi Siklus Hidup
- [S3.11] Bucket tujuan umum S3 harus mengaktifkan pemberitahuan acara
- [S3.12] ACL tidak boleh digunakan untuk mengelola akses pengguna ke bucket tujuan umum S3
- [S3.13] Bucket tujuan umum S3 harus memiliki konfigurasi Siklus Hidup
- [S3.14] Bucket tujuan umum S3 harus mengaktifkan versi
- [S3.20] Bucket tujuan umum S3 harus mengaktifkan penghapusan MFA
- [SageMaker.1] Instans SageMaker notebook Amazon seharusnya tidak memiliki akses internet langsung
- [SageMaker.2] instance SageMaker notebook harus diluncurkan dalam VPC khusus
- [SageMaker.3] Pengguna seharusnya tidak memiliki akses root ke instance SageMaker notebook
- [SageMaker.4] varian produksi SageMaker titik akhir harus memiliki jumlah instance awal yang lebih besar dari 1
- [SES.1] Daftar kontak SES harus ditandai
- [SES.2] Set konfigurasi SES harus ditandai
- [SecretsManager.3] Hapus rahasia Secrets Manager yang tidak digunakan
- [SecretsManager.4] Rahasia Secrets Manager harus diputar dalam jumlah hari tertentu
- [SecretsManager.5] Rahasia Secrets Manager harus diberi tag

- [ServiceCatalog.1] Portofolio Service Catalog harus dibagikan hanya dalam suatu organisasi AWS
- [SNS.3] Topik SNS harus ditandai
- [SQS.2] Antrian SQS harus ditandai
- [SSM.4] Dokumen SSM seharusnya tidak bersifat publik
- [StepFunctions.1] Mesin status Step Functions seharusnya mengaktifkan logging
- [StepFunctions.2] Aktivitas Step Functions harus diberi tag
- [Transfer.1] AWS Transfer Family alur kerja harus ditandai
- [Transfer.2] Server Transfer Family tidak boleh menggunakan protokol FTP untuk koneksi titik akhir
- [WAF.1] Pencatatan ACL Web Global AWS WAF Klasik harus diaktifkan
- [WAF.2] Aturan Regional AWS WAF Klasik harus memiliki setidaknya satu syarat
- [WAF.3] Kelompok aturan Regional AWS WAF Klasik harus memiliki setidaknya satu aturan
- [WAF.4] ACL web Regional AWS WAF klasik harus memiliki setidaknya satu aturan atau kelompok aturan
- [WAF.6] Aturan global AWS WAF klasik harus memiliki setidaknya satu syarat
- [WAF.7] Kelompok aturan global AWS WAF klasik harus memiliki setidaknya satu aturan
- [WAF.8] ACL web global AWS WAF klasik harus memiliki setidaknya satu aturan atau kelompok aturan
- [WAF.10] ACL AWS WAF web harus memiliki setidaknya satu aturan atau kelompok aturan
- [WAF.11] pencatatan ACL AWS WAF web harus diaktifkan
- AWS WAF Aturan [WAF.12] harus mengaktifkan metrik CloudWatch

AWS GovCloud (AS-Barat)

Kontrol berikut tidak didukung di AWS GovCloud (AS-Barat).

- [ACM.2] Sertifikat RSA yang dikelola oleh ACM harus menggunakan panjang kunci minimal 2.048 bit
- [ACM.3] Sertifikat ACM harus ditandai
- [Akun.1] Informasi kontak keamanan harus disediakan untuk Akun AWS
- [Akun.2] Akun AWS harus menjadi bagian dari organisasi AWS Organizations
- [ApiGateway.2] Tahapan API Gateway REST API harus dikonfigurasi untuk menggunakan sertifikat SSL untuk otentikasi backend

- [ApiGateway.3] Tahapan API Gateway REST API harus mengaktifkan penelusuran AWS X-Ray
- [ApiGateway.4] API Gateway harus dikaitkan dengan ACL Web WAF
- [ApiGateway.8] Rute API Gateway harus menentukan jenis otorisasi
- [ApiGateway.9] Pencatatan akses harus dikonfigurasi untuk Tahapan API Gateway V2
- [AppSync.2] AWS AppSync harus mengaktifkan logging tingkat lapangan
- [AppSync.4] AWS AppSync GraphQL API harus diberi tag
- [AppSync.5] AWS AppSync GraphQL API tidak boleh diautentikasi dengan kunci API
- [Athena.2] Katalog data Athena harus diberi tag
- [Athena.3] Kelompok kerja Athena harus ditandai
- [AutoScaling.2] Grup Auto Scaling Amazon EC2 harus mencakup beberapa Availability Zone
- [AutoScaling.3] Konfigurasi peluncuran grup Auto Scaling harus mengonfigurasi instans EC2 agar memerlukan Layanan Metadata Instans Versi 2 (IMDSv2)
- [AutoScaling.6] Grup Auto Scaling harus menggunakan beberapa jenis instance di beberapa Availability Zone
- [AutoScaling.9] Grup Auto Scaling Amazon EC2 harus menggunakan templat peluncuran Amazon EC2
- [AutoScaling.10] Grup Penskalaan Otomatis EC2 harus diberi tag
- [Autoscaling.5] Instans Amazon EC2 yang diluncurkan menggunakan konfigurasi peluncuran grup Auto Scaling seharusnya tidak memiliki alamat IP Publik
- [Backup.2] poin AWS Backup pemulihan harus ditandai
- [Backup.3] AWS Backup brankas harus ditandai
- [Backup.4] rencana AWS Backup laporan harus ditandai
- [Backup.5] rencana AWS Backup cadangan harus ditandai
- [CloudFormation.2] CloudFormation tumpukan harus ditandai
- [CloudFront.1] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi
- [CloudFront.3] CloudFront distribusi harus memerlukan enkripsi dalam perjalanan
- [CloudFront.4] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi
- [CloudFront.5] CloudFront distribusi seharusnya mengaktifkan logging
- [CloudFront.6] CloudFront distribusi harus mengaktifkan WAF
- [CloudFront.7] CloudFront distribusi harus menggunakan sertifikat SSL/TLS khusus
- [CloudFront.8] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS

- [CloudFront.9] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus
- [CloudFront.10] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal khusus
- [CloudFront.12] CloudFront distribusi seharusnya tidak menunjukkan asal S3 yang tidak ada
- [CloudFront.13] CloudFront distribusi harus menggunakan kontrol akses asal
- [CloudFront.14] CloudFront distribusi harus ditandai
- [CloudTrail.9] CloudTrail jejak harus ditandai
- [CloudWatch.15] CloudWatch alarm harus memiliki tindakan tertentu yang dikonfigurasi
- [CloudWatch.16] grup CloudWatch log harus dipertahankan untuk jangka waktu tertentu
- [CloudWatch.17] tindakan CloudWatch alarm harus diaktifkan
- [CodeArtifact.1] CodeArtifact repositori harus diberi tag
- [CodeBuild.1] URL repositori sumber CodeBuild Bitbucket tidak boleh berisi kredensyal sensitif
- [CodeBuild.2] variabel lingkungan CodeBuild proyek tidak boleh berisi kredensil teks yang jelas
- [CodeBuild.3] Log CodeBuild S3 harus dienkripsi
- [CodeBuild.4] lingkungan CodeBuild proyek harus memiliki urasi logging AWS Config
- [DataFirehose.1] Aliran pengiriman Firehose harus dienkripsi saat istirahat
- [Detective.1] Grafik perilaku detektif harus diberi tag
- [DMS.2] Sertifikat DMS harus ditandai
- [DMS.3] Langganan acara DMS harus ditandai
- [DMS.4] Contoh replikasi DMS harus ditandai
- [DMS.5] Grup subnet replikasi DMS harus ditandai
- [DMS.6] Instans replikasi DMS harus mengaktifkan peningkatan versi minor otomatis
- [DMS.7] Tugas replikasi DMS untuk database target seharusnya mengaktifkan logging
- [DMS.8] Tugas replikasi DMS untuk database sumber seharusnya mengaktifkan logging
- [DMS.9] Titik akhir DMS harus menggunakan SSL
- [DMS.10] Titik akhir DMS untuk database Neptunus harus mengaktifkan otorisasi IAM
- [DMS.11] Titik akhir DMS untuk MongoDB harus mengaktifkan mekanisme otentikasi
- [DMS.12] Titik akhir DMS untuk Redis harus mengaktifkan TLS
- [DocumentDB.1] Cluster Amazon DocumentDB harus dienkripsi saat istirahat
- [DocumentDB.2] Cluster Amazon DocumentDB harus memiliki periode retensi cadangan yang memadai

- [DocumentDB.3] Cuplikan cluster manual Amazon DocumentDB seharusnya tidak bersifat publik
- [DocumentDB.4] Cluster Amazon DocumentDB harus mempublikasikan log audit ke Log CloudWatch
- [DocumentDB.5] Cluster Amazon DocumentDB harus mengaktifkan perlindungan penghapusan
- [DynamoDB.1] Tabel DynamoDB harus secara otomatis menskalakan kapasitas sesuai permintaan
- [DynamoDB.3] Cluster DynamoDB Accelerator (DAX) harus dienkripsi saat istirahat
- [DynamoDB.4] Tabel DynamoDB harus ada dalam rencana cadangan
- [DynamoDB.5] Tabel DynamoDB harus diberi tag
- [DynamoDB.7] Cluster DynamoDB Accelerator harus dienkripsi saat transit
- [EC2.15] Subnet Amazon EC2 seharusnya tidak secara otomatis menetapkan alamat IP publik
- [EC2.16] Daftar Kontrol Akses Jaringan yang Tidak Digunakan harus dihapus
- [EC2.17] Instans Amazon EC2 tidak boleh menggunakan beberapa ENI
- [EC2.21] ACL jaringan seharusnya tidak mengizinkan masuknya dari 0.0.0.0/0 ke port 22 atau port 3389
- [EC2.22] Grup keamanan Amazon EC2 yang tidak digunakan harus dihapus
- [EC2.23] Amazon EC2 Transit Gateways seharusnya tidak secara otomatis menerima permintaan lampiran VPC
- [EC2.24] Jenis instans paravirtual Amazon EC2 tidak boleh digunakan
- [EC2.25] Templat peluncuran Amazon EC2 tidak boleh menetapkan IP publik ke antarmuka jaringan
- [EC2.28] Volume EBS harus dicakup oleh rencana cadangan
- [EC2.33] Lampiran gateway transit EC2 harus ditandai
- [EC2.34] Tabel rute gateway transit EC2 harus ditandai
- [EC2.35] Antarmuka jaringan EC2 harus ditandai
- [EC2.36] Gateway pelanggan EC2 harus ditandai
- [EC2.37] Alamat IP Elastis EC2 harus ditandai
- [EC2.38] Instans EC2 harus ditandai
- [EC2.39] Gerbang internet EC2 harus ditandai
- [EC2.40] Gerbang EC2 NAT harus ditandai
- [EC2.41] ACL jaringan EC2 harus ditandai
- [EC2.42] Tabel rute EC2 harus ditandai

- [EC2.43] Grup keamanan EC2 harus ditandai
- [EC2.44] Subnet EC2 harus ditandai
- [EC2.45] Volume EC2 harus ditandai
- [EC2.46] VPC Amazon harus ditandai
- [EC2.47] Layanan titik akhir Amazon VPC harus ditandai
- [EC2.48] Log aliran VPC Amazon harus ditandai
- [EC2.49] Koneksi peering VPC Amazon harus ditandai
- [EC2.50] Gateway EC2 VPN harus ditandai
- [EC2.52] Gerbang transit EC2 harus ditandai
- [ECR.1] Repositori pribadi ECR harus memiliki pemindaian gambar yang dikonfigurasi
- [ECR.2] Repositori pribadi ECR harus memiliki kekekalan tag yang dikonfigurasi
- [ECR.3] Repositori ECR harus memiliki setidaknya satu kebijakan siklus hidup yang dikonfigurasi
- [ECR.4] Repositori publik ECR harus ditandai
- [ECS.1] Definisi tugas Amazon ECS harus memiliki mode jaringan yang aman dan definisi pengguna.
- [ECS.3] Definisi tugas ECS tidak boleh membagikan namespace proses host
- [ECS.4] Kontainer ECS harus berjalan sebagai non-hak istimewa
- [ECS.5] Wadah ECS harus dibatasi pada akses hanya-baca ke sistem file root
- [ECS.8] Rahasia tidak boleh diteruskan sebagai variabel lingkungan kontainer
- [ECS.9] Definisi tugas ECS harus memiliki konfigurasi logging
- [ECS.10] Layanan ECS Fargate harus berjalan pada versi platform Fargate terbaru
- [ECS.12] Cluster ECS harus menggunakan Wawasan Kontainer
- [ECS.13] Layanan ECS harus ditandai
- [ECS.14] Cluster ECS harus ditandai
- [ECS.15] Definisi tugas ECS harus ditandai
- [EFS.2] Volume Amazon EFS harus dalam rencana cadangan
- [EFS.3] Titik akses EFS harus menegakkan direktori root
- [EFS.4] Titik akses EFS harus menegakkan identitas pengguna
- [EFS.5] Titik akses EFS harus ditandai
- [EFS.6] Target pemasangan EFS tidak boleh dikaitkan dengan subnet publik
- [EKS.1] Titik akhir klaster EKS seharusnya tidak dapat diakses publik

- [EKS.2] Kluster EKS harus berjalan pada versi Kubernetes yang didukung
- [EKS.3] Kluster EKS harus menggunakan rahasia Kubernetes terenkripsi
- [EKS.6] Kluster EKS harus ditandai
- [EKS.7] Konfigurasi penyedia identitas EKS harus ditandai
- [EKS.8] Kluster EKS harus mengaktifkan pencatatan audit
- [ELB.10] Classic Load Balancer harus menjangkau beberapa Availability Zone
- [ELB.12] Application Load Balancer harus dikonfigurasi dengan mode mitigasi desync defensif atau paling ketat
- [ELB.13] Penyeimbang Beban Aplikasi, Jaringan, dan Gateway harus mencakup beberapa Availability Zone
- [ELB.14] Classic Load Balancer harus dikonfigurasi dengan mode mitigasi desync defensif atau paling ketat
- [ELB.16] Application Load Balancers harus dikaitkan dengan ACL web AWS WAF
- [ElastiCache.1] Cluster ElastiCache Redis harus mengaktifkan pencadangan otomatis
- [ElastiCache.2] ElastiCache untuk kluster cache Redis harus mengaktifkan peningkatan versi minor otomatis
- [ElastiCache.3] ElastiCache untuk grup replikasi Redis harus mengaktifkan failover otomatis
- [ElastiCache.4] ElastiCache untuk grup replikasi Redis harus dienkripsi saat istirahat
- [ElastiCache.5] ElastiCache untuk grup replikasi Redis harus dienkripsi saat transit
- [ElastiCache.6] ElastiCache untuk grup replikasi Redis sebelum versi 6.0 harus menggunakan Redis AUTH
- [ElastiCache.7] ElastiCache cluster tidak boleh menggunakan grup subnet default
- [ElasticBeanstalk.1] Lingkungan Elastic Beanstalk seharusnya mengaktifkan pelaporan kesehatan yang ditingkatkan
- [ElasticBeanstalk.2] Pembaruan platform yang dikelola Elastic Beanstalk harus diaktifkan
- [ElasticBeanstalk.3] Elastic Beanstalk harus mengalirkan log ke CloudWatch
- [EMR.2] Pengaturan akses publik blok EMR Amazon harus diaktifkan
- [ES.4] Kesalahan domain Elasticsearch yang masuk ke CloudWatch Log harus diaktifkan
- [ES.9] Domain Elasticsearch harus diberi tag
- [EventBridge.2] bus EventBridge acara harus diberi tag
- [EventBridge.3] bus acara EventBridge khusus harus memiliki kebijakan berbasis sumber daya terlampir

- [EventBridge.4] titik akhir EventBridge global harus mengaktifkan replikasi acara
- [FSX.1] FSx untuk sistem file OpenZFS harus dikonfigurasi untuk menyalin tag ke cadangan dan volume
- [FSX.2] Sistem file FSx for Lustre harus dikonfigurasi untuk menyalin tag ke cadangan
- [GlobalAccelerator.1] Akselerator Akselerator Global harus diberi tag
- AWS Glue Pekerjaan [Glue.1] harus ditandai
- [GuardDuty.2] GuardDuty filter harus diberi tag
- [GuardDuty.3] GuardDuty IPset harus ditandai
- [GuardDuty.4] GuardDuty detektor harus ditandai
- [IAM.6] MFA perangkat keras harus diaktifkan untuk pengguna root
- [IAM.9] MFA harus diaktifkan untuk pengguna root
- [IAM.21] Kebijakan terkelola pelanggan IAM yang Anda buat seharusnya tidak mengizinkan tindakan wildcard untuk layanan
- [IAM.23] Penganalisis Akses IAM harus ditandai
- [IAM.24] Peran IAM harus ditandai
- [IAM.25] Pengguna IAM harus diberi tag
- [IAM.28] IAM Access Analyzer penganalisis akses eksternal harus diaktifkan
- [IoT.1] profil AWS IoT Core keamanan harus ditandai
- [IoT.2] tindakan AWS IoT Core mitigasi harus ditandai
- AWS IoT Core Dimensi [IoT.3] harus ditandai
- [IoT.4] AWS IoT Core otorisasi harus diberi tag
- [IoT.5] alias AWS IoT Core peran harus ditandai
- AWS IoT Core Kebijakan [IoT.6] harus ditandai
- [Kinesis.1] Aliran kinesis harus dienkripsi saat istirahat
- [Kinesis.2] Aliran kinesis harus ditandai
- [Lambda.5] Fungsi VPC Lambda harus beroperasi di beberapa Availability Zone
- [Lambda.6] Fungsi Lambda harus ditandai
- [Macie.1] Amazon Macie harus diaktifkan
- [Macie.2] Penemuan data sensitif otomatis Macie harus diaktifkan
- [MQ.2] Broker ActiveMQ harus mengalirkan log audit ke CloudWatch
- [MQ.3] Broker Amazon MQ harus mengaktifkan peningkatan versi minor otomatis

- [MQ.4] Broker Amazon MQ harus diberi tag
- [MQ.5] Broker ActiveMQ harus menggunakan mode penerapan aktif/siaga
- [MQ.6] Broker RabbitMQ harus menggunakan mode penerapan cluster
- [MSK.1] Cluster MSK harus dienkripsi saat transit di antara node broker
- [MSK.2] Kluster MSK seharusnya telah meningkatkan pemantauan yang dikonfigurasi
- [Neptunus.1] Cluster DB Neptunus harus dienkripsi saat istirahat
- [Neptune.2] Cluster DB Neptunus harus menerbitkan log audit ke Log CloudWatch
- [Neptune.3] Snapshot cluster Neptunus DB seharusnya tidak publik
- [Neptunus.4] Cluster DB Neptunus harus mengaktifkan perlindungan penghapusan
- [Neptunus.5] Cluster DB Neptunus harus mengaktifkan cadangan otomatis
- [Neptune.6] Snapshot cluster Neptunus DB harus dienkripsi saat istirahat
- [Neptunus.7] Cluster DB Neptunus harus mengaktifkan otentikasi basis data IAM
- [Neptunus.8] Cluster DB Neptunus harus dikonfigurasi untuk menyalin tag ke snapshot
- [Neptunus.9] Cluster DB Neptunus harus digunakan di beberapa Availability Zone
- [NetworkFirewall.1] Firewall Firewall Jaringan harus digunakan di beberapa Availability Zone
- [NetworkFirewall.2] Pencatatan Firewall Jaringan harus diaktifkan
- [NetworkFirewall.3] Kebijakan Network Firewall harus memiliki setidaknya satu kelompok aturan yang terkait
- [NetworkFirewall.4] Tindakan stateless default untuk kebijakan Network Firewall harus drop atau forward untuk paket penuh
- [NetworkFirewall.5] Tindakan stateless default untuk kebijakan Network Firewall harus drop atau forward untuk paket yang terfragmentasi
- [NetworkFirewall.6] Grup aturan Stateless Network Firewall tidak boleh kosong
- [NetworkFirewall.7] Firewall Firewall Jaringan harus diberi tag
- [NetworkFirewall.8] Kebijakan firewall Network Firewall harus ditandai
- [NetworkFirewall.9] Firewall Firewall Jaringan harus mengaktifkan perlindungan penghapusan
- [Opensearch.1] OpenSearch domain harus mengaktifkan enkripsi saat istirahat
- [Opensearch.2] OpenSearch domain tidak boleh diakses publik
- [Opensearch.3] OpenSearch domain harus mengenkripsi data yang dikirim antar node
- [Opensearch.4] login kesalahan OpenSearch domain ke Log harus diaktifkan CloudWatch
- [Opensearch.5] OpenSearch domain harus mengaktifkan pencatatan audit

- [Opensearch.6] OpenSearch domain harus memiliki setidaknya tiga node data
- [Opensearch.7] OpenSearch domain harus mengaktifkan kontrol akses berbutir halus
- [Opensearch.8] Koneksi ke OpenSearch domain harus dienkripsi menggunakan kebijakan keamanan TLS terbaru
- [Opensearch.9] domain harus ditandai OpenSearch
- [Opensearch.11] OpenSearch domain harus memiliki setidaknya tiga node primer khusus
- [PCA.1] otoritas sertifikat AWS Private CA root harus dinonaktifkan
- [RDS.12] Otentikasi IAM harus dikonfigurasi untuk cluster RDS
- [RDS.13] Peningkatan versi minor otomatis RDS harus diaktifkan
- [RDS.14] Cluster Amazon Aurora seharusnya mengaktifkan backtracking
- [RDS.15] Cluster RDS DB harus dikonfigurasi untuk beberapa Availability Zone
- [RDS.24] Kluster Database RDS harus menggunakan nama pengguna administrator khusus
- [RDS.25] Instans database RDS harus menggunakan nama pengguna administrator khusus
- [RDS.26] Instans RDS DB harus dilindungi oleh rencana cadangan
- [RDS.27] Cluster RDS DB harus dienkripsi saat istirahat
- [RDS.28] Cluster RDS DB harus ditandai
- [RDS.29] Snapshot cluster RDS DB harus ditandai
- [RDS.30] Instans RDS DB harus ditandai
- [RDS.31] Grup keamanan RDS DB harus ditandai
- [RDS.32] Snapshot RDS DB harus ditandai
- [RDS.33] Grup subnet RDS DB harus ditandai
- [RDS.34] Cluster Aurora MySQL DB harus menerbitkan log audit ke Log CloudWatch
- [RDS.35] Cluster RDS DB harus mengaktifkan peningkatan versi minor otomatis
- [Redshift.7] Cluster Redshift harus menggunakan perutean VPC yang ditingkatkan
- [Redshift.8] Cluster Amazon Redshift tidak boleh menggunakan nama pengguna Admin default
- [Redshift.9] Cluster Redshift tidak boleh menggunakan nama database default
- [Redshift.10] Cluster Redshift harus dienkripsi saat istirahat
- [Redshift.11] Cluster Redshift harus ditandai
- [Redshift.12] Langganan pemberitahuan acara Redshift harus ditandai
- [Redshift.13] Snapshot cluster Redshift harus ditandai
- [Redshift.14] Grup subnet cluster Redshift harus ditandai

- [Redshift.15] Grup keamanan Redshift harus mengizinkan masuknya port cluster hanya dari asal yang dibatasi
- [Route53.1] Pemeriksaan kesehatan rute 53 harus ditandai
- [Route53.2] Route 53 zona yang dihosting publik harus mencatat kueri DNS
- [S3.1] Bucket tujuan umum S3 harus mengaktifkan pengaturan akses publik blok
- [S3.8] Bucket tujuan umum S3 harus memblokir akses publik
- [S3.10] Bucket tujuan umum S3 dengan versi diaktifkan harus memiliki konfigurasi Siklus Hidup
- [S3.11] Bucket tujuan umum S3 harus mengaktifkan pemberitahuan acara
- [S3.12] ACL tidak boleh digunakan untuk mengelola akses pengguna ke bucket tujuan umum S3
- [S3.13] Bucket tujuan umum S3 harus memiliki konfigurasi Siklus Hidup
- [S3.14] Bucket tujuan umum S3 harus mengaktifkan versi
- [S3.20] Bucket tujuan umum S3 harus mengaktifkan penghapusan MFA
- [SageMaker.2] instance SageMaker notebook harus diluncurkan dalam VPC khusus
- [SageMaker.3] Pengguna seharusnya tidak memiliki akses root ke instance SageMaker notebook
- [SageMaker.4] varian produksi SageMaker titik akhir harus memiliki jumlah instance awal yang lebih besar dari 1
- [SES.1] Daftar kontak SES harus ditandai
- [SES.2] Set konfigurasi SES harus ditandai
- [SecretsManager.3] Hapus rahasia Secrets Manager yang tidak digunakan
- [SecretsManager.4] Rahasia Secrets Manager harus diputar dalam jumlah hari tertentu
- [SecretsManager.5] Rahasia Secrets Manager harus diberi tag
- [ServiceCatalog.1] Portofolio Service Catalog harus dibagikan hanya dalam suatu organisasi AWS
- [SNS.3] Topik SNS harus ditandai
- [SQS.2] Antrian SQS harus ditandai
- [SSM.4] Dokumen SSM seharusnya tidak bersifat publik
- [StepFunctions.1] Mesin status Step Functions seharusnya mengaktifkan logging
- [StepFunctions.2] Aktivitas Step Functions harus diberi tag
- [Transfer.1] AWS Transfer Family alur kerja harus ditandai
- [Transfer.2] Server Transfer Family tidak boleh menggunakan protokol FTP untuk koneksi titik akhir
- [WAF.1] Pencatatan ACL Web Global AWS WAF Klasik harus diaktifkan
- [WAF.2] Aturan Regional AWS WAF Klasik harus memiliki setidaknya satu syarat

- [WAF.3] Kelompok aturan Regional AWS WAF Klasik harus memiliki setidaknya satu aturan
- [WAF.4] ACL web Regional AWS WAF klasik harus memiliki setidaknya satu aturan atau kelompok aturan
- [WAF.6] Aturan global AWS WAF klasik harus memiliki setidaknya satu syarat
- [WAF.7] Kelompok aturan global AWS WAF klasik harus memiliki setidaknya satu aturan
- [WAF.8] ACL web global AWS WAF klasik harus memiliki setidaknya satu aturan atau kelompok aturan
- [WAF.10] ACL AWS WAF web harus memiliki setidaknya satu aturan atau kelompok aturan
- [WAF.11] pencatatan ACL AWS WAF web harus diaktifkan
- AWS WAF Aturan [WAF.12] harus mengaktifkan metrik CloudWatch

Menonaktifkan Security Hub

> **Note**
>
> Jika Anda menggunakan konfigurasi pusat, administrator yang didelegasikan AWS Security Hub dapat membuat kebijakan konfigurasi yang menonaktifkan Security Hub di akun tertentu dan unit organisasi (OU) dan tetap mengaktifkannya di akun lain. Kebijakan konfigurasi berlaku di Wilayah asal Anda dan semua Wilayah yang ditautkan. Untuk informasi selengkapnya, lihat Cara kerja konfigurasi pusat.

Anda dapat menggunakan konsol Security Hub, Security Hub API, atau AWS CLI untuk menonaktifkan Security Hub.

Berikut ini terjadi saat Anda menonaktifkan Security Hub untuk sebuah akun:

- Tidak ada temuan baru yang diproses untuk akun tersebut.
- Setelah 90 hari, temuan dan wawasan Anda yang ada serta setelan konfigurasi Security Hub akan dihapus dan tidak dapat dipulihkan.

  Jika Anda ingin menyimpan temuan yang ada, Anda harus mengekspornya sebelum menonaktifkan Security Hub. Untuk informasi selengkapnya, lihat the section called “Pengaruh tindakan akun pada data Security Hub”.
- Setiap standar dan kontrol yang diaktifkan dinonaktifkan.

Anda tidak dapat menonaktifkan Security Hub dalam kasus berikut:

- Akun Anda adalah akun administrator Security Hub yang ditunjuk untuk suatu organisasi. Jika Anda menggunakan konfigurasi pusat, Anda tidak dapat mengaitkan kebijakan konfigurasi yang menonaktifkan Security Hub dengan akun administrator yang didelegasikan. Asosiasi dapat berhasil untuk akun lain, tetapi Security Hub tidak menerapkan kebijakan tersebut ke akun administrator yang didelegasikan.
- Akun Anda adalah akun administrator Security Hub berdasarkan undangan, dan Anda memiliki akun anggota yang diaktifkan. Sebelum Anda dapat menonaktifkan Security Hub, Anda harus memisahkan semua akun anggota Anda. Lihat the section called “Memutuskan akun anggota”.

Sebelum Anda dapat menonaktifkan Security Hub untuk akun anggota, akun harus dipisahkan dari akun administratornya. Untuk akun organisasi, hanya akun administrator yang dapat memisahkan akun anggota. Untuk informasi selengkapnya, lihat the section called “Memutuskan akun anggota organisasi”. Untuk akun yang diundang secara manual, akun administrator atau akun anggota dapat memisahkan akun anggota. Untuk informasi selengkapnya, lihat the section called “Memutuskan akun anggota” atau the section called “Memutuskan hubungan dari akun administrator Anda”. Pemutusan tidak diperlukan jika Anda menggunakan konfigurasi pusat karena Anda dapat membuat kebijakan yang menonaktifkan Security Hub di akun anggota tertentu.

Saat Anda menonaktifkan Security Hub di akun, itu hanya dinonaktifkan di Wilayah saat ini. Namun, jika Anda menggunakan konfigurasi pusat untuk menonaktifkan Security Hub di akun tertentu, itu dinonaktifkan di Wilayah beranda dan semua Wilayah yang ditautkan.

Pilih metode pilihan Anda, dan ikuti langkah-langkah untuk menonaktifkan Security Hub.

Security Hub console

Untuk menonaktifkan Security Hub

1. Buka konsol AWS Security Hub di https://console.aws.amazon.com/securityhub/.
2. Pada panel navigasi, pilih Pengaturan.
3. Pada halaman Pengaturan, pilih Umum.
4. Di bawah Nonaktifkan AWS Security Hub, pilih Nonaktifkan AWS Security Hub. Kemudian pilih Nonaktifkan AWS Security Hub lagi.

Security Hub API

Untuk menonaktifkan Security Hub

Memanggil `DisableSecurityHub`API.

AWS CLI

Untuk menonaktifkan Security Hub

Jalankan perintah `disable-security-hub`.

Contoh perintah:

```
aws securityhub disable-security-hub
```

Ubah log untuk kontrol Security Hub

Log perubahan berikut melacak perubahan material pada kontrol AWS Security Hub keamanan yang ada, yang dapat mengakibatkan perubahan status keseluruhan kontrol dan status kepatuhan temuannya. Untuk informasi tentang cara Security Hub mengevaluasi status kontrol, lihatStatus kepatuhan dan status kontrol. Perubahan mungkin memakan waktu beberapa hari setelah entri mereka di log ini untuk mempengaruhi semua Wilayah AWS di mana kontrol tersedia.

Log ini melacak perubahan yang terjadi sejak April 2023.

Pilih kontrol untuk melihat detail lebih lanjut tentangnya. Perubahan judul dicatat pada deskripsi rinci masing-masing kontrol selama 90 hari.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
Juni 25, 2024	[Config.1] AWS Config harus diaktifkan dan menggunakan peran terkait layanan untuk perekaman sumber daya	Kontrol ini memeriksa apakah AWS Config diaktifkan, menggunakan peran terkait layanan, dan merekam sumber daya untuk kontrol yang diaktifka n. Security Hub memperbarui judul kontrol untuk mencerminkan apa yang dievaluasi oleh kontrol.
Juni 14, 2024	[RDS.34] Cluster Aurora MySQL DB harus menerbitkan log audit ke Log CloudWatch	Kontrol ini memeriksa apakah kluster DB MySQL Amazon Aurora dikonfigurasi untuk mempublik asikan log audit ke Amazon Logs.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
		CloudWatch Security Hub memperbarui kontrol sehingga tidak menghasilkan temuan untuk cluster Aurora Serverless v1 DB.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
Juni 10, 2024	[Config.1] AWS Config harus diaktifkan dan menggunakan peran terkait layanan untuk perekaman sumber daya	Kontrol ini memeriksa apakah AWS Config diaktifkan dan perekaman AWS Config sumber daya diaktifkan. Sebelumnya, kontrol menghasilkan `PASSED` temuan hanya jika Anda mengonfigurasi rekaman untuk semua sumber daya. Security Hub memperbarui kontrol untuk menghasilkan `PASSED` temuan saat perekaman dihidupkan untuk sumber daya yang diperlukan untuk kontrol yang diaktifkan. Kontrol juga telah diperbarui untuk memeriksa apakah peran AWS Config terkait layanan digunakan, yang memberikan izin untuk merekam sumber daya yang diperlukan.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
8 Mei 2024	[S3.20] Bucket tujuan umum S3 harus mengaktifkan penghapusan MFA	Kontrol ini memeriksa apakah bucket berversi tujuan umum Amazon S3 telah mengaktif kan penghapusan autentikasi multi-fak tor (MFA). Sebelumny a, kontrol menghasil kan `FAILED` temuan untuk bucket yang memiliki konfigura si Siklus Hidup. Namun, penghapus an MFA dengan pembuatan versi tidak dapat diaktifkan pada bucket yang memiliki konfigurasi Siklus Hidup. Security Hub memperbarui kontrol agar tidak menghasil kan temuan untuk bucket yang memiliki konfigurasi Siklus Hidup. Deskripsi kontrol telah diperbaru i untuk mencerminkan perilaku saat ini.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
2 Mei 2024	[EKS.2] Kluster EKS harus berjalan pada versi Kubernetes yang didukung	Security Hub memperbarui versi Kubernetes tertua yang didukung yang dapat dijalankan oleh kluster Amazon EKS untuk menghasilkan temuan yang diteruskan. Versi tertua yang didukung saat ini adalah Kubernetes`1.26`.
April 30, 2024	[CloudTrail.3] Setidaknya satu CloudTrail jejak harus diaktifkan	Judul kontrol yang diubah dari CloudTrail harus diaktifkan ke Setidaknya satu CloudTrail jejak harus diaktifkan. Kontrol ini saat ini menghasilkan `PASSED` temuan jika Akun AWS memiliki setidaknya satu CloudTrail jejak diaktifkan. Judul dan deskripsi telah diubah untuk secara akurat mencerminkan perilaku saat ini.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
April 29, 2024	[AutoScaling.1] Grup Auto Scaling yang terkait dengan penyeimbang beban harus menggunakan pemeriksaan kesehatan ELB	Judul kontrol yang diubah dari grup Auto Scaling yang terkait dengan Classic Load Balancer harus menggunakan pemeriksaan kesehatan penyeimbang beban ke grup Auto Scaling yang terkait dengan penyeimbang beban harus menggunakan pemeriksaan kesehatan ELB. Kontrol ini saat ini mengevaluasi Application, Gateway, Network, dan Classic Load Balancers. Judul dan deskripsi telah diubah untuk secara akurat mencerminkan perilaku saat ini.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
April 19, 2024	[CloudTrail.1] CloudTrail harus diaktifkan dan dikonfigurasi dengan setidaknya satu jejak Multi-wilayah yang mencakup acara manajemen baca dan tulis	Kontrol memeriksa apakah AWS CloudTrail diaktifkan dan dikonfigurasi dengan setidaknya satu jejak Multi-wilayah yang mencakup peristiwa manajemen baca dan tulis. Sebelumnya, kontrol salah menghasilkan `PASSED` temuan ketika akun telah CloudTrail diaktifkan dan dikonfigurasi dengan setidaknya satu jejak Multi-wilayah, bahkan jika tidak ada jejak yang menangkap peristiwa manajemen baca dan tulis. Kontrol sekarang menghasilkan `PASSED` temuan hanya ketika CloudTrail diaktifkan dan dikonfigurasi dengan setidaknya satu jejak Multi-wilayah yang menangkap peristiwa manajemen baca dan tulis.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
April 10, 2024	[Athena.1] Kelompok kerja Athena harus dienkripsi saat istirahat	Security Hub menghentikan kontrol ini dan menghapus nya dari semua standar. Workgroup Athena mengirim log ke bucket Amazon Simple Storage Service (Amazon S3). Amazon S3 sekarang menyediakan enkripsi default dengan kunci terkelola S3 (SS3-S3) pada bucket S3 baru dan yang sudah ada.
April 10, 2024	[AutoScaling.4] Konfigurasi peluncuran grup Auto Scaling seharusnya tidak memiliki batas hop respons metadata yang lebih besar dari 1	Security Hub menghentikan kontrol ini dan menghapus nya dari semua standar. Batas hop respons metadata untuk instans Amazon Elastic Compute Cloud (Amazon EC2) bergantung pada beban kerja.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
April 10, 2024	[CloudFormation.1] CloudFormation tumpukan harus diintegrasikan dengan Simple Notification Service (SNS)	Security Hub menghentikan kontrol ini dan menghapusnya dari semua standar. Mengintegrasikan AWS CloudFormation tumpukan dengan topik Amazon SNS bukan lagi praktik terbaik keamanan. Meskipun menginteg rasikan CloudForm ation tumpukan penting dengan topik SNS dapat bermanfaa t, itu tidak diperluka n untuk semua tumpukan.
April 10, 2024	[CodeBuild.5] lingkungan CodeBuild proyek seharusnya tidak mengaktifkan mode istimewa	Security Hub menghentikan kontrol ini dan menghapus nya dari semua standar. Mengaktifkan mode istimewa dalam CodeBuild proyek tidak menimbulkan risiko tambahan bagi lingkungan pelanggan .

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
April 10, 2024	[IAM.20] Hindari penggunaan pengguna root	Security Hub menghentikan kontrol ini dan menghapus nya dari semua standar. Tujuan dari kontrol ini dicakup oleh kontrol lain,[CloudWatch.1] Filter metrik log dan alarm harus ada untuk penggunaan pengguna “root”.
April 10, 2024	[SNS.2] Pencatatan status pengiriman harus diaktifkan untuk pesan notifikasi yang dikirim ke suatu topik	Security Hub menghentikan kontrol ini dan menghapus nya dari semua standar. Mencatat status pengirima n untuk topik SNS bukan lagi praktik terbaik keamanan. Meskipun mencatat status pengirima n untuk topik SNS penting dapat berguna, itu tidak diperlukan untuk semua topik.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
April 10, 2024	[S3.10] Bucket tujuan umum S3 dengan versi diaktifkan harus memiliki konfigurasi Siklus Hidup	Security Hub menghapus kontrol ini dari Praktik Terbaik Keamanan AWS Dasar dan Standar yang Dikelola Layanan:. AWS Control Tower Tujuan dari kontrol ini dicakup oleh dua kontrol lainnya: [S3.13] Bucket tujuan umum S3 harus memiliki konfigurasi Siklus Hidup dan[S3.14] Bucket tujuan umum S3 harus mengaktif kan versi. Kontrol ini masih merupakan bagian dari NIST SP 800-53 Rev. 5.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
April 10, 2024	[S3.11] Bucket tujuan umum S3 harus mengaktifkan pemberitahuan acara	Security Hub menghapus kontrol ini dari Praktik Terbaik Keamanan AWS Dasar dan Standar yang Dikelola Layanan:. AWS Control Tower Meskipun ada beberapa kasus di mana pemberita huan acara untuk bucket S3 berguna, ini bukan praktik terbaik keamanan universal . Kontrol ini masih merupakan bagian dari NIST SP 800-53 Rev. 5.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
April 10, 2024	[SNS.1] Topik SNS harus dienkripsi saat istirahat menggunakan AWS KMS	Security Hub menghapus kontrol ini dari Praktik Terbaik Keamanan AWS Dasar dan Standar yang Dikelola Layanan:. AWS Control Tower Karena SNS sudah mengenkripsi topik secara default, menggunakan AWS KMS untuk mengenkripsi topik tidak lagi direkomendasikan sebagai praktik terbaik keamanan. Kontrol ini masih merupakan bagian dari NIST SP 800-53 Rev. 5.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
April 8, 2024	[ELB.6] Aplikasi, Gateway, dan Network Load Balancer harus mengaktifkan perlindungan penghapusan	Judul kontrol yang diubah dari perlindungan penghapusan Application Load Balancer harus diaktifkan ke Application, Gateway, dan Network Load Balancer harus mengaktifkan perlindungan penghapusan. Kontrol ini saat ini mengevaluasi Application, Gateway, dan Network Load Balancers. Judul dan deskripsi telah diubah untuk secara akurat mencerminkan perilaku saat ini.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
Maret 22, 2024	[Opensearch.8] Koneksi ke OpenSearch domain harus dienkripsi menggunakan kebijakan keamanan TLS terbaru	Judul kontrol yang diubah dari Koneksi ke OpenSearch domain harus dienkripsi menggunakan TLS 1.2 hingga Koneksi ke OpenSearch domain harus dienkripsi menggunakan kebijakan keamanan TLS terbaru. Sebelumnya, kontrol hanya memeriksa apakah koneksi ke OpenSearch domain menggunakan TLS 1.2. Kontrol sekarang menghasilkan `PASSED` temuan jika OpenSearch domain dienkripsi menggunakan kebijakan keamanan TLS terbaru. Judul kontrol dan deskripsi telah diperbarui untuk mencerminkan perilaku saat ini.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
Maret 22, 2024	[ES.8] Koneksi ke domain Elasticsearch harus dienkripsi menggunakan kebijakan keamanan TLS terbaru	Judul kontrol yang diubah dari Connections ke domain Elasticsearch harus dienkripsi menggunakan TLS 1.2 ke Connections to Elasticsearch domain harus dienkripsi menggunakan kebijakan keamanan TLS terbaru. Sebelumnya, kontrol hanya memeriksa apakah koneksi ke domain Elasticsearch menggunakan TLS 1.2. Kontrol sekarang menghasilkan PASSED temuan jika domain Elasticsearch dienkripsi menggunakan kebijakan keamanan TLS terbaru. Judul kontrol dan deskripsi telah diperbarui untuk mencerminkan perilaku saat ini.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
Maret 12, 2024	[S3.1] Bucket tujuan umum S3 harus mengaktifkan pengaturan akses publik blok	Judul yang diubah dari pengaturan Akses Publik Blok S3 harus diaktifkan ke bucket tujuan umum S3 harus mengaktifkan pengaturan akses publik blok. Security Hub mengubah judul menjadi akun untuk jenis bucket S3 baru.
Maret 12, 2024	[S3.2] Bucket tujuan umum S3 harus memblokir akses baca publik	Judul yang diubah dari bucket S3 harus melarang akses baca publik ke bucket tujuan umum S3 harus memblokir akses baca publik. Security Hub mengubah judul menjadi akun untuk jenis bucket S3 baru.
Maret 12, 2024	[S3.3] Bucket tujuan umum S3 harus memblokir akses tulis publik	Judul yang diubah dari bucket S3 harus melarang akses tulis publik ke bucket tujuan umum S3 harus memblokir akses tulis publik. Security Hub mengubah judul menjadi akun untuk jenis bucket S3 baru.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
Maret 12, 2024	[S3.5] Bucket tujuan umum S3 harus memerlukan permintaan untuk menggunakan SSL	Judul yang diubah dari bucket S3 harus memerluka n permintaan untuk menggunakan Secure Socket Layer ke bucket tujuan umum S3 harus memerluka n permintaan untuk menggunakan SSL. Security Hub mengubah judul menjadi akun untuk jenis bucket S3 baru.
Maret 12, 2024	[S3.6] Kebijakan bucket tujuan umum S3 harus membatasi akses ke yang lain Akun AWS	Judul yang diubah dari izin S3 yang diberikan ke kebijakan bucket lainnya harus dibatasi Akun AWS pada kebijakan bucket tujuan umum S3 yang harus membatasi akses ke yang lain. Akun AWS Security Hub mengubah judul menjadi akun untuk jenis bucket S3 baru.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
Maret 12, 2024	[S3.7] Ember tujuan umum S3 harus menggunakan replikasi lintas wilayah	Judul yang diubah dari bucket S3 harus mengaktifkan replikasi lintas wilayah ke bucket tujuan umum S3 harus menggunakan replikasi lintas wilayah. Security Hub mengubah judul menjadi akun untuk jenis bucket S3 baru.
Maret 12, 2024	[S3.7] Ember tujuan umum S3 harus menggunakan replikasi lintas wilayah	Judul yang diubah dari bucket S3 harus mengaktifkan replikasi lintas wilayah ke bucket tujuan umum S3 harus menggunakan replikasi lintas wilayah. Security Hub mengubah judul menjadi akun untuk jenis bucket S3 baru.
Maret 12, 2024	[S3.8] Bucket tujuan umum S3 harus memblokir akses publik	Judul yang diubah dari pengaturan Akses Publik Blok S3 harus diaktifkan pada bucket tujuan umum tingkat ember ke S3 harus memblokir akses publik. Security Hub mengubah judul menjadi akun untuk jenis bucket S3 baru.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
Maret 12, 2024	[S3.9] Bucket tujuan umum S3 harus mengaktifkan pencatatan akses server	Judul yang diubah dari pencatatan akses server bucket S3 harus diaktifkan ke Pencatatan akses Server harus diaktifkan untuk bucket tujuan umum S3. Security Hub mengubah judul menjadi akun untuk jenis bucket S3 baru.
Maret 12, 2024	[S3.10] Bucket tujuan umum S3 dengan versi diaktifkan harus memiliki konfigurasi Siklus Hidup	Judul yang diubah dari bucket S3 dengan versi diaktifkan harus memiliki kebijakan siklus hidup yang dikonfigurasi ke bucket tujuan umum S3 dengan versi yang diaktifkan harus memiliki konfigurasi Siklus Hidup. Security Hub mengubah judul menjadi akun untuk jenis bucket S3 baru.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
Maret 12, 2024	[S3.11] Bucket tujuan umum S3 harus mengaktifkan pemberitahuan acara	Judul yang diubah dari bucket S3 harus mengaktifkan notifikasi acara ke bucket tujuan umum S3 harus mengaktifkan pemberitahuan acara. Security Hub mengubah judul menjadi akun untuk jenis bucket S3 baru.
Maret 12, 2024	[S3.12] ACL tidak boleh digunakan untuk mengelola akses pengguna ke bucket tujuan umum S3	Judul yang diubah dari daftar kontrol akses S3 (ACL) tidak boleh digunakan untuk mengelola akses pengguna ke bucket ke ACL tidak boleh digunakan untuk mengelola akses pengguna ke bucket tujuan umum S3. Security Hub mengubah judul menjadi akun untuk jenis bucket S3 baru.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
Maret 12, 2024	[S3.13] Bucket tujuan umum S3 harus memiliki konfigurasi Siklus Hidup	Judul yang diubah dari bucket S3 harus memiliki kebijakan siklus hidup yang dikonfigurasi ke bucket tujuan umum S3 harus memiliki konfigurasi Siklus Hidup. Security Hub mengubah judul menjadi akun untuk jenis bucket S3 baru.
Maret 12, 2024	[S3.14] Bucket tujuan umum S3 harus mengaktifkan versi	Judul yang diubah dari bucket S3 harus menggunakan pembuatan versi ke bucket tujuan umum S3 harus mengaktif kan versi. Security Hub mengubah judul menjadi akun untuk jenis bucket S3 baru.
Maret 12, 2024	[S3.15] Bucket tujuan umum S3 harus mengaktifkan Object Lock	Judul yang diubah dari bucket S3 harus dikonfigurasi untuk menggunakan Object Lock ke bucket tujuan umum S3 harus mengaktifkan Object Lock. Security Hub mengubah judul menjadi akun untuk jenis bucket S3 baru.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
Maret 12, 2024	[S3.17] Ember tujuan umum S3 harus dienkripsi saat istirahat AWS KMS keys	Judul yang diubah dari bucket S3 harus dienkripsi saat istirahat dengan AWS KMS keys bucket tujuan umum S3 harus dienkripsi saat istirahat. AWS KMS keys Security Hub mengubah judul menjadi akun untuk jenis bucket S3 baru.
Maret 7, 2024	[Lambda.2] Fungsi Lambda harus menggunakan runtime yang didukung	Lambda.2 memeriksa apakah setelan AWS Lambda fungsi untuk runtime cocok dengan nilai yang diharapkan yang ditetapkan untuk runtime yang didukung dalam setiap bahasa. Security Hub sekarang mendukung `nodejs20.x` dan `ruby3.3` sebagai parameter.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
Februari 22, 2024	[Lambda.2] Fungsi Lambda harus menggunakan runtime yang didukung	Lambda.2 memeriksa apakah setelan AWS Lambda fungsi untuk runtime cocok dengan nilai yang diharapkan yang ditetapkan untuk runtime yang didukung dalam setiap bahasa. Security Hub sekarang mendukung `dotnet8` sebagai parameter.
Februari 5, 2024	[EKS.2] Kluster EKS harus berjalan pada versi Kubernetes yang didukung	Security Hub memperbarui versi Kubernetes tertua yang didukung yang dapat dijalankan oleh kluster Amazon EKS untuk menghasilkan temuan yang diteruskan. Versi tertua yang didukung saat ini adalah Kubernetes`1.25`.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
10 Januari 2024	[CodeBuild.1] URL repositori sumber CodeBuild Bitbucket tidak boleh berisi kredensyal sensitif	Judul yang diubah dari CodeBuild GitHub atau URL repositori sumber Bitbucket harus menggunakan OAuth ke URL repositori sumber CodeBuild Bitbucket tidak boleh berisi kredensya l sensitif. Security Hub menghapus penyebutan OAuth karena metode koneksi lain juga dapat aman. Security Hub menghapus penyebutan GitHub karena tidak mungkin lagi memiliki token akses pribadi atau nama pengguna dan kata sandi di URL repositori GitHub sumber.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
8 Januari 2024	[Lambda.2] Fungsi Lambda harus menggunakan runtime yang didukung	Lambda.2 memeriksa apakah setelan AWS Lambda fungsi untuk runtime cocok dengan nilai yang diharapkan yang ditetapkan untuk runtime yang didukung dalam setiap bahasa. Security Hub tidak lagi mendukung `go1.x` dan `java8` sebagai parameter karena ini adalah runtime yang sudah pensiun.
Desember 29, 2023	[RDS.8] Instans RDS DB harus mengaktifkan perlindungan penghapusan	RDS.8 memeriksa apakah instans Amazon RDS DB yang menggunakan salah satu mesin database yang didukung telah mengaktifkan perlindungan penghapusan. Security Hub sekarang mendukung `custom-oracle-ee`, `oracle-ee-cdb`, dan `oracle-se2-cdb` sebagai mesin database.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
22 Desember 2023	[Lambda.2] Fungsi Lambda harus menggunakan runtime yang didukung	Lambda.2 memeriksa apakah setelan AWS Lambda fungsi untuk runtime cocok dengan nilai yang diharapkan yang ditetapkan untuk runtime yang didukung dalam setiap bahasa. Security Hub sekarang mendukung `java21` dan `python3.12` sebagai parameter. Security Hub tidak lagi mendukung `ruby2.7` sebagai parameter.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
15 Desember 2023	[CloudFront.1] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi	CloudFront.1 memeriksa apakah CloudFront distribusi Amazon memiliki objek root default yang dikonfigurasi. Security Hub menurunkan tingkat keparahan kontrol ini dari CRITICAL ke HIGH karena menambahkan objek root default adalah rekomendasi yang bergantung pada aplikasi pengguna dan persyaratan spesifik.
5 Desember 2023	[EC2.13] Grup keamanan tidak boleh mengizinkan masuknya dari 0.0.0.0/0 atau: :/0 ke port 22	Judul kontrol yang diubah dari Grup keamanan tidak boleh mengizinkan masuknya dari 0.0.0.0/0 ke port 22 ke Grup keamanan tidak boleh mengizinkan masuknya dari 0.0.0.0/0 atau: :/0 ke port 22.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
5 Desember 2023	[EC2.14] Grup keamanan tidak boleh mengizinkan masuknya dari 0.0.0.0/0 atau: :/0 ke port 3389	Judul kontrol yang diubah dari Pastikan tidak ada grup keamanan yang mengizinkan masuknya dari 0.0.0.0/0 ke port 3389 ke Grup keamanan tidak boleh mengizinkan masuknya dari 0.0.0.0/0 atau: :/0 ke port 3389.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
5 Desember 2023	[RDS.9] Instans RDS DB harus menerbitkan log ke Log CloudWatch	Judul kontrol yang diubah dari pencatatan Database harus diaktifkan ke instans RDS DB harus menerbitkan log ke CloudWatch Log. Security Hub mengidentifikasi bahwa kontrol ini hanya memeriksa apakah log dipublikasikan ke Amazon CloudWatch Logs dan tidak memeriksa apakah log RDS diaktifkan. Kontrol menghasilkan `PASSED` temuan jika instans RDS DB dikonfigurasi untuk menerbitkan log ke CloudWatch Log. Judul kontrol telah diperbarui untuk mencerminkan perilaku saat ini.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
17 November 2023	[EC2.19] Grup keamanan tidak boleh mengizinkan akses tidak terbatas ke port dengan risiko tinggi	EC2.19 memeriksa apakah lalu lintas masuk yang tidak dibatasi untuk grup keamanan dapat diakses ke port tertentu yang dianggap berisiko tinggi. Security Hub memperbarui kontrol ini untuk memperhitungkan daftar awalan terkelola saat dipasok sebagai sumber untuk aturan grup keamanan. Kontrol menghasilkan `FAILED` temuan jika daftar awalan berisi string '0.0.0.0/0' atau ': :/0'.
16 November 2023	[CloudWatch.15] CloudWatch alarm harus memiliki tindakan tertentu yang dikonfigurasi	Judul kontrol yang diubah dari CloudWatch alarm harus memiliki tindakan yang dikonfigurasi untuk status ALARM ke CloudWatch alarm harus memiliki tindakan tertentu yang dikonfigurasi.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
16 November 2023	[CloudWatch.16] grup CloudWatch log harus dipertahankan untuk jangka waktu tertentu	Judul kontrol yang diubah dari grup CloudWatch log harus dipertahankan setidaknya selama 1 tahun untuk grup CloudWatch log harus dipertahankan untuk jangka waktu tertentu.
16 November 2023	[Lambda.5] Fungsi VPC Lambda harus beroperasi di beberapa Availability Zone	Judul kontrol yang diubah dari fungsi VPC Lambda harus beroperasi di lebih dari satu Availabil ity Zone ke VPC Lambda fungsi harus beroperasi di beberapa Availability Zone.
16 November 2023	[AppSync.2] AWS AppSync harus mengaktif kan logging tingkat lapangan	Judul kontrol yang diubah dari AWS AppSync seharusny a mengaktifkan pencatatan tingkat permintaan dan tingkat bidang harus mengaktifkan logging tingkat bidang.AWS AppSync

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
16 November 2023	[EMR.1] Node primer cluster EMR Amazon seharusnya tidak memiliki alamat IP publik	Judul kontrol yang diubah dari node master MapReduce cluster Amazon Elastic seharusnya tidak memiliki alamat IP publik ke node primer klaster EMR Amazon seharusnya tidak memiliki alamat IP publik.
16 November 2023	[Opensearch.2] OpenSearch domain tidak boleh diakses publik	Judul kontrol yang diubah dari OpenSearch domain harus dalam VPC OpenSearch ke domain tidak boleh diakses publik.
16 November 2023	[ES.2] Domain Elasticsearch tidak boleh diakses publik	Judul kontrol yang diubah dari domain Elasticsearch harus dalam VPC ke domain Elasticsearch tidak boleh diakses publik.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
31 Oktober 2023	[ES.4] Kesalahan domain Elasticsearch yang masuk ke CloudWatch Log harus diaktifkan	ES.4 memeriksa apakah domain Elasticsearch dikonfigurasi untuk mengirim log kesalahan ke Amazon Logs. CloudWatch Kontrol sebelumnya menghasilkan PASSED temuan untuk domain Elasticsearch yang memiliki log yang dikonfigurasi untuk dikirim ke CloudWatch Log. Security Hub memperbarui kontrol untuk menghasilkan PASSED temuan hanya untuk domain Elasticsearch yang dikonfigurasi untuk mengirim log kesalahan ke Log. CloudWatch Kontrol juga diperbarui untuk mengecualikan versi Elasticsearch yang tidak mendukung log kesalahan dari evaluasi.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
16 Oktober 2023	[EC2.13] Grup keamanan tidak boleh mengizinkan masuknya dari 0.0.0.0/0 atau: :/0 ke port 22	EC2.13 memeriksa apakah grup keamanan mengizinkan akses masuk tidak terbatas ke port 22. Security Hub memperbarui kontrol ini untuk memperhitungkan daftar awalan terkelola saat dipasok sebagai sumber untuk aturan grup keamanan. Kontrol menghasilkan `FAILED` temuan jika daftar awalan berisi string '0.0.0.0/0' atau ': :/0'.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
16 Oktober 2023	[EC2.14] Grup keamanan tidak boleh mengizinkan masuknya dari 0.0.0.0/0 atau: :/0 ke port 3389	EC2.14 memeriksa apakah grup keamanan mengizinkan akses masuk tidak terbatas ke port 3389. Security Hub memperbarui kontrol ini untuk memperhitungkan daftar awalan terkelola saat dipasok sebagai sumber untuk aturan grup keamanan. Kontrol menghasilkan `FAILED` temuan jika daftar awalan berisi string '0.0.0.0/0' atau ': :/0'.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
16 Oktober 2023	[EC2.18] Grup keamanan seharusnya hanya mengizinkan lalu lintas masuk yang tidak terbatas untuk port resmi	EC2.18 memeriksa apakah grup keamanan yang digunakan mengizinkan lalu lintas masuk yang tidak dibatasi. Security Hub memperbarui kontrol ini untuk memperhitungkan daftar awalan terkelola saat dipasok sebagai sumber untuk aturan grup keamanan. Kontrol menghasilkan `FAILED` temuan jika daftar awalan berisi string '0.0.0.0/0' atau ': :/0'.
16 Oktober 2023	[Lambda.2] Fungsi Lambda harus menggunakan runtime yang didukung	Lambda.2 memeriksa apakah setelan AWS Lambda fungsi untuk runtime cocok dengan nilai yang diharapkan yang ditetapkan untuk runtime yang didukung dalam setiap bahasa. Security Hub sekarang mendukung `python3.11` sebagai parameter.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
4 Oktober 2023	[S3.7] Ember tujuan umum S3 harus menggunakan replikasi lintas wilayah	Security Hub menambahk an parameter `ReplicationType` dengan nilai `CROSS-REGION` untuk memastikan bahwa bucket S3 mengaktif kan replikasi lintas wilayah daripada replikasi wilayah yang sama.
27 September 2023	[EKS.2] Kluster EKS harus berjalan pada versi Kubernetes yang didukung	Security Hub memperbarui versi Kubernetes tertua yang didukung yang dapat dijalankan oleh kluster Amazon EKS untuk menghasil kan temuan yang diteruskan. Versi tertua yang didukung saat ini adalah Kubernetes`1.24`.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
20 September 2023	CloudFront.2 — CloudFront distribusi harus mengaktifkan identitas akses asal	Security Hub menghentikan kontrol ini dan menghapus nya dari semua standar. Sebaliknya, gunakan [CloudFront.13] CloudFront distribusi harus menggunakan kontrol akses asal. Kontrol akses asal adalah praktik terbaik keamanan saat ini. Kontrol ini akan dihapus dari dokumentasi dalam 90 hari.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
20 September 2023	[EC2.22] Grup keamanan Amazon EC2 yang tidak digunakan harus dihapus	Security Hub menghapus kontrol ini dari AWS Foundational Security Best Practices (FSBP) dan National Institute of Standards and Technology (NIST) SP 800-53 Rev. 5. Itu masih merupakan bagian dari Standar yang Dikelola Layanan:. AWS Control Tower Kontrol ini menghasilkan temuan yang diteruskan jika grup keamanan dilampirkan ke instans EC2 atau ke elastic network interface. Namun, untuk kasus penggunaan tertentu, kelompok keamanan yang tidak terikat tidak menimbulkan risiko keamanan. Anda dapat menggunakan kontrol EC2 lainnya —seperti EC2.2, EC2.13, EC2.14, EC2.18, dan EC2.19 —untuk memantau grup keamanan Anda.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
20 September 2023	EC2.29 - Instans EC2 harus diluncurkan dalam VPC	Security Hub menghentikan kontrol ini dan menghapus nya dari semua standar. Amazon EC2 telah memigrasikan instans EC2-Class ic ke VPC. Kontrol ini akan dihapus dari dokumentasi dalam 90 hari.
20 September 2023	S3.4 - Bucket S3 harus mengaktifkan enkripsi sisi server	Security Hub menghentikan kontrol ini dan menghapus nya dari semua standar. Amazon S3 sekarang menyediak an enkripsi default dengan kunci terkelola S3 (SS3-S3) pada bucket S3 baru dan yang sudah ada. Pengaturan enkripsi tidak berubah untuk bucket yang ada yang dienkripsi dengan enkripsi sisi server SS3-S3 atau SS3-KMS. Kontrol ini akan dihapus dari dokumentasi dalam 90 hari.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
14 September 2023	[EC2.2] Grup keamanan default VPC tidak boleh mengizinkan lalu lintas masuk atau keluar	Judul kontrol yang diubah dari Grup keamanan default VPC tidak boleh mengizinkan lalu lintas masuk dan keluar ke grup keamanan default VPC tidak boleh mengizinkan lalu lintas masuk atau keluar.
14 September 2023	[IAM.9] MFA harus diaktifkan untuk pengguna root	Judul kontrol yang diubah dari MFA Virtual harus diaktifkan untuk pengguna root ke MFA harus diaktifkan untuk pengguna root.
14 September 2023	[RDS.19] Langganan pemberitahuan acara RDS yang ada harus dikonfigurasi untuk peristiwa klaster penting	Judul kontrol yang diubah dari Langganan pemberitahuan peristiwa RDS harus dikonfigurasi untuk peristiwa klaster penting ke langganan pemberitahuan peristiwa RDS yang ada harus dikonfigurasi untuk peristiwa klaster penting.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
14 September 2023	[RDS.20] Langganan pemberitahuan acara RDS yang ada harus dikonfigurasi untuk peristiwa instance basis data penting	Judul kontrol yang diubah dari Langganan pemberitahuan peristiwa RDS harus dikonfigurasi untuk peristiwa instance database penting ke langganan pemberitahuan peristiwa RDS yang ada harus dikonfigurasi untuk peristiwa instance database penting.
14 September 2023	[WAF.2] Aturan Regional AWS WAF Klasik harus memiliki setidaknya satu syarat	Judul kontrol yang diubah dari Aturan Regional WAF harus memiliki setidaknya satu syarat untuk aturan Regional AWS WAF Klasik harus memiliki setidaknya satu syarat.
14 September 2023	[WAF.3] Kelompok aturan Regional AWS WAF Klasik harus memiliki setidaknya satu aturan	Judul kontrol yang diubah dari grup aturan WAF Regional harus memiliki setidaknya satu aturan untuk grup aturan Regional AWS WAF Klasik harus memiliki setidaknya satu aturan.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
14 September 2023	[WAF.4] ACL web Regional AWS WAF klasik harus memiliki setidaknya satu aturan atau kelompok aturan	Judul kontrol yang diubah dari ACL web regional WAF harus memiliki setidakny a satu aturan atau grup aturan ke ACL web Regional AWS WAF Klasik harus memiliki setidaknya satu aturan atau grup aturan.
14 September 2023	[WAF.6] Aturan global AWS WAF klasik harus memiliki setidaknya satu syarat	Judul kontrol yang diubah dari aturan global WAF harus memiliki setidakny a satu syarat untuk aturan global AWS WAF Klasik harus memiliki setidaknya satu kondisi.
14 September 2023	[WAF.7] Kelompok aturan global AWS WAF klasik harus memiliki setidaknya satu aturan	Judul kontrol yang diubah dari grup aturan global WAF harus memiliki setidaknya satu aturan ke grup aturan global AWS WAF Klasik harus memiliki setidaknya satu aturan.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
14 September 2023	[WAF.8] ACL web global AWS WAF klasik harus memiliki setidaknya satu aturan atau kelompok aturan	Judul kontrol yang diubah dari ACL web global WAF harus memiliki setidakny a satu aturan atau grup aturan ke ACL web global AWS WAF Klasik harus memiliki setidaknya satu aturan atau grup aturan.
14 September 2023	[WAF.10] ACL AWS WAF web harus memiliki setidaknya satu aturan atau kelompok aturan	Judul kontrol yang diubah dari ACL web WAFv2 harus memiliki setidakny a satu aturan atau grup aturan ke ACL AWS WAF web harus memiliki setidaknya satu aturan atau grup aturan.
14 September 2023	[WAF.11] pencatatan ACL AWS WAF web harus diaktifkan	Judul kontrol yang diubah dari AWS WAF v2 web ACL logging harus diaktifka n ke AWS WAF web ACL logging harus diaktifkan.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
Juli 20, 2023	S3.4 - Bucket S3 harus mengaktifkan enkripsi sisi server	S3.4 memeriksa apakah bucket Amazon S3 mengaktifkan enkripsi sisi server atau kebijakan bucket S3 secara eksplisit menolak permintaan tanpa enkripsi sisi server. `PutObject` Security Hub memperbarui kontrol ini untuk menyertakan enkripsi sisi server dual-layer dengan kunci KMS (DSSE-KMS). Kontrol menghasilkan temuan yang dilewatkan ketika bucket S3 dienkripsi dengan SSE-S3, SSE-KMS, atau DSSE-KMS.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
Juli 17, 2023	[S3.17] Ember tujuan umum S3 harus dienkripsi saat istirahat AWS KMS keys	S3.17 memeriksa apakah bucket Amazon S3 dienkripsi dengan file. AWS KMS key Security Hub memperbarui kontrol ini untuk menyertakan enkripsi sisi server dual-layer dengan kunci KMS (DSSE-KMS). Kontrol menghasilkan temuan yang dilewatkan ketika bucket S3 dienkripsi dengan SSE-KMS atau DSSE-KMS.
9 Juni 2023	[EKS.2] Kluster EKS harus berjalan pada versi Kubernetes yang didukung	EKS.2 memeriksa apakah kluster Amazon EKS berjalan pada versi Kubernetes yang didukung. Versi tertua yang didukung sekarang. `1.23`

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
9 Juni 2023	[Lambda.2] Fungsi Lambda harus menggunakan runtime yang didukung	Lambda.2 memeriksa apakah setelan AWS Lambda fungsi untuk runtime cocok dengan nilai yang diharapkan yang ditetapkan untuk runtime yang didukung dalam setiap bahasa. Security Hub sekarang mendukung `ruby3.2` sebagai parameter.
Juni 5, 2023	[ApiGateway.5] Data cache API Gateway REST API harus dienkripsi saat istirahat	ApiGateway.5.memeriksa apakah semua metode di tahapan API Amazon API Gateway REST dienkripsi saat istirahat. Security Hub memperbarui kontrol untuk mengevaluasi enkripsi metode tertentu hanya ketika caching diaktifkan untuk metode itu.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
18 Mei 2023	[Lambda.2] Fungsi Lambda harus menggunakan runtime yang didukung	Lambda.2 memeriksa apakah setelan AWS Lambda fungsi untuk runtime cocok dengan nilai yang diharapkan yang ditetapkan untuk runtime yang didukung dalam setiap bahasa. Security Hub sekarang mendukung `java17` sebagai parameter.
18 Mei 2023	[Lambda.2] Fungsi Lambda harus menggunakan runtime yang didukung	Lambda.2 memeriksa apakah setelan AWS Lambda fungsi untuk runtime cocok dengan nilai yang diharapkan yang ditetapkan untuk runtime yang didukung dalam setiap bahasa. Security Hub tidak lagi mendukung `nodejs12.x` sebagai parameter.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
April 23, 2023	[ECS.10] Layanan ECS Fargate harus berjalan pada versi platform Fargate terbaru	ECS.10 memeriksa apakah layanan Amazon ECS Fargate menjalankan versi platform Fargate terbaru. Pelanggan dapat menyebarkan Amazon ECS melalui ECS secara langsung, atau dengan menggunakan. CodeDeploy Security Hub memperbarui kontrol ini untuk menghasilkan temuan Lulus saat Anda CodeDeploy menggunakan layanan ECS Fargate.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
20 April 2023	[S3.6] Kebijakan bucket tujuan umum S3 harus membatasi akses ke yang lain Akun AWS	S3.6 memeriksa apakah kebijakan bucket Amazon Simple Storage Service (Amazon S3) mencegah prinsipal dari pihak Akun AWS lain melakukan tindakan yang ditolak pada sumber daya di bucket S3. Security Hub memperbar ui kontrol untuk memperhitungkan persyaratan dalam kebijakan bucket.
18 April 2023	[Lambda.2] Fungsi Lambda harus menggunak an runtime yang didukung	Lambda.2 memeriksa apakah setelan AWS Lambda fungsi untuk runtime cocok dengan nilai yang diharapka n yang ditetapkan untuk runtime yang didukung dalam setiap bahasa. Security Hub sekarang mendukung `python3.10` sebagai parameter.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
18 April 2023	[Lambda.2] Fungsi Lambda harus menggunakan runtime yang didukung	Lambda.2 memeriksa apakah setelan AWS Lambda fungsi untuk runtime cocok dengan nilai yang diharapkan yang ditetapkan untuk runtime yang didukung dalam setiap bahasa. Security Hub tidak lagi mendukung `dotnetcore3.1` sebagai parameter.

Tanggal perubahan	Kontrol ID dan judul	Deskripsi perubahan
17 April 2023	[RDS.11] Instans RDS harus mengaktifkan pencadangan otomatis	RDS.11 memeriksa apakah instans Amazon RDS telah mengaktifkan pencadangan otomatis, dengan periode retensi cadangan yang lebih besar dari atau sama dengan tujuh hari. Security Hub memperbarui kontrol ini untuk mengecualikan replika baca dari evaluasi, karena tidak semua mesin mendukung pencadangan otomatis pada replika baca. Selain itu, RDS tidak menyediakan opsi untuk menentukan periode retensi cadangan saat membuat replika baca. Replika baca dibuat dengan periode retensi cadangan secara `0` default.

Riwayat dokumen untuk Panduan Pengguna AWS Security Hub

Tabel berikut menjelaskan pembaruan dokumentasi untuk AWS Security Hub.

> **Note**
>
> Untuk rilis kontrol keamanan, tanggal yang ditentukan adalah tanggal ketika kontrol tersedia di semua akun dan Wilayah. Diperlukan waktu 1-2 minggu untuk kontrol untuk mencapai semua akun dan Wilayah.

Perubahan	Deskripsi	Tanggal
Rilis Tolok Ukur AWS Yayasan CIS v3.0.0	Security Hub merilis Center for Internet Security (CIS) AWS Foundations Benchmark v3.0.0. Rilis ini mencakup kontrol baru berikut, serta pemetaan ke beberapa kontrol yang ada. • the section called “[EC2.53] Grup keamanan EC2 tidak boleh mengizinkan masuknya dari 0.0.0.0/0 ke port administrasi server jarak jauh” • the section called “[EC2.54] Grup keamanan EC2 tidak boleh mengizinkan masuknya dari: :/0 ke port administrasi server jarak jauh”	13 Mei 2024

- the section called “[IAM.26] Sertifikat SSL/TLS kedaluwarsa yang dikelola di IAM harus dihapus”
- the section called “[IAM.27] Identitas IAM seharusnya tidak memiliki kebijakan yang dilampirkan AWSCloudShellFullAccess ”
- the section called “[IAM.28] IAM Access Analyzer penganalisis akses eksternal harus diaktifkan”
- the section called “[S3.22] Bucket tujuan umum S3 harus mencatat peristiwa penulisan tingkat objek”
- the section called “[S3.23] Bucket tujuan umum S3 harus mencatat peristiwa pembacaan tingkat objek”

Kontrol keamanan baru	Kontrol Security Hub baru berikut ini tersedia: • the section called “[DataFirehose.1] Aliran pengiriman Firehose harus dienkripsi saat istirahat” • the section called “[DMS.10] Titik akhir DMS untuk database Neptunus harus mengaktifkan otorisasi IAM” • the section called “[DMS.11] Titik akhir DMS untuk MongoDB harus mengaktifkan mekanisme otentikasi” • the section called “[DMS.12] Titik akhir DMS untuk Redis harus mengaktifkan TLS” • the section called “[DynamoDB.7] Cluster DynamoDB Accelerator harus dienkripsi saat transit” • the section called “[EFS.6] Target pemasangan EFS tidak boleh dikaitkan dengan subnet publik” • the section called “[EKS.3] Kluster EKS harus menggunakan rahasia Kubernetes terenkripsi” • the section called “[FSX.2] Sistem file FSx for Lustre harus dikonfigurasi untuk menyalin tag ke cadangan”	3 Mei 2024

- the section called “[MQ.2] Broker ActiveMQ harus mengalirkan log audit ke CloudWatch”
- the section called “[MQ.3] Broker Amazon MQ harus mengaktifkan peningkatan versi minor otomatis”
- the section called “[Opensearch.11] OpenSearch domain harus memiliki setidaknya tiga node primer khusus”
- the section called “[Redshift.15] Grup keamanan Redshift harus mengizinkan masuknya port cluster hanya dari asal yang dibatasi”
- the section called “[SageMaker.4] varian produksi SageMaker titik akhir harus memiliki jumlah instance awal yang lebih besar dari 1”
- the section called “[Service Catalog.1] Portofolio Service Catalog harus dibagikan hanya dalam suatu organisasi AWS”
- the section called “[Transfer.2] Server Transfer Family tidak boleh menggunakan protokol FTP untuk koneksi titik akhir”

AWS Standar Penandaan Sumber Daya	Standar Penandaan AWS Sumber Daya dari Security Hub sekarang tersedia secara umum, bersama dengan kontrol baru yang berlaku untuk standar.	April 30, 2024
Memperbarui ke kebijakan terkelola yang ada	Security Hub memperbarui kebijakan AWS terkelola yang diberi nama `AmazonSecurityHubFullAccess` untuk mendapatkan detail harga Layanan AWS dan produk.	April 24, 2024
Konfigurasi parameter kontrol dalam konteks	Jika Anda menggunakan konfigurasi pusat, Anda sekarang dapat mengonfigurasi parameter kontrol dalam konteks, dari halaman detail kontrol pada konsol Security Hub.	Maret 29, 2024
Memperbarui ke kebijakan terkelola yang ada	Security Hub memperbarui kebijakan AWS terkelola bernama `AWSSecurityHubReadOnlyAccess` dengan menambahkan `Sid` bidang.	Februari 22, 2024
Kontrol keamanan baru	Kontrol [Macie.2] Penemuan data sensitif otomatis Macie harus diaktifkan sekarang tersedia. Untuk batasan Regional pada kontrol ini, lihat Ketersediaan kontrol menurut Wilayah.	Februari 19, 2024

Security Hub tersedia di Kanada Barat (Calgary)	Security Hub sekarang tersedia di Canada West (Calgary). Semua fitur Security Hub sekarang tersedia di Wilayah ini, dengan pengecualian kontrol keamanan tertentu. Untuk informasi selengkapnya, lihat Ketersediaan kontrol menurut Wilayah.	20 Desember 2023

Kontrol keamanan baru	Kontrol Security Hub baru berikut ini tersedia: • the section called “[Backup.1] titik AWS Backup pemulihan harus dienkripsi saat istirahat” • the section called “[DynamoDB.6] Tabel DynamoDB harus mengaktifkan perlindungan penghapusan” • the section called “[EC2.51] Titik akhir EC2 Client VPN harus mengaktifkan pencatatan koneksi klien” • the section called “[EKS.8] Kluster EKS harus mengaktifkan pencatatan audit” • the section called “[EMR.2] Pengaturan akses publik blok EMR Amazon harus diaktifkan” • the section called “[FSX.1] FSx untuk sistem file OpenZFS harus dikonfigurasi untuk menyalin tag ke cadangan dan volume” • the section called “[Macie.1] Amazon Macie harus diaktifkan” • the section called “[MSK.2] Kluster MSK seharusnya telah meningkatkan	14 Desember 2023

pemantauan yang dikonfigurasi”

- the section called “[Neptunus.9] Cluster DB Neptunus harus digunakan di beberapa Availability Zone”
- the section called “[Network Firewall.1] Firewall Firewall Jaringan harus digunakan di beberapa Availability Zone”
- the section called “[Network Firewall.2] Pencatatan Firewall Jaringan harus diaktifkan”
- the section called “[Opensearch.10] OpenSearch domain harus memiliki pembaruan perangkat lunak terbaru yang diinstal”
- the section called “[PCA.1] otoritas sertifikat AWS Private CA root harus dinonaktifkan”
- the section called “[S3.19] Titik akses S3 harus mengaktifkan pengaturan akses publik blok”
- the section called “[S3.20] Bucket tujuan umum S3 harus mengaktifkan penghapusan MFA”

Menemukan pengayaan	Security Hub menambahkan bidang pencarian baru `AwsAccountName`, `ApplicationArn`, dan `ApplicationName` ke AWS Security Finding Format (ASFF).	27 November 2023
Penyempurnaan dasbor Ringkasan	Sekarang Anda dapat mengakses lebih banyak widget dasbor di halaman Ringkasan konsol Security Hub, menyimpan set filter dasbor untuk fokus dengan cepat pada masalah keamanan tertentu, dan menyesuaikan tata letak dasbor.	27 November 2023
Konfigurasi pusat	Konfigurasi pusat sekarang tersedia. Dengan konfigurasi pusat, administrator yang didelegasikan Security Hub dapat mengonfigurasi Security Hub, standar, dan kontrol di beberapa akun organisasi, unit organisasi (OU), dan Wilayah.	27 November 2023
Pembaruan kebijakan terkelola	Security Hub menambahkan izin baru ke kebijakan `AWSSecurityHubServiceRolePolicy` terkelola yang memungkinkan Security Hub membaca dan memperbarui properti kontrol keamanan yang dapat disesuaikan.	26 November 2023

Parameter kontrol khusus	Sekarang Anda dapat menyesuaikan nilai parameter untuk kontrol Security Hub tertentu. Ini dapat membuat temuan untuk kontrol spesifik lebih relevan dengan persyaratan bisnis dan harapan keamanan Anda.	26 November 2023
Pembaruan kebijakan terkelola	Security Hub memperbarui `AWSSecurityHubFullAccess` dan `AWSSecurityHubOrganizationsAccess` mengelola kebijakan yang memungkinkan Anda untuk menggunakan, masing-masing, fitur Security Hub dan integrasi dengan AWS Organizations.	16 November 2023

Kontrol keamanan yang ada ditambahkan ke Standar yang Dikelola Layanan: AWS Control Tower	Kontrol Security Hub berikut telah ditambahkan ke Service-Managed Standard:. AWS Control Tower • ACM.2 • AppSync.5 • CloudTrail.6 • DMS.9 • DokumenDB.3 • DynamoDB.3 • EC2.23 • EKS.1 • ElastiCache.3 • ElastiCache.4 • ElastiCache.5 • ElastiCache.6 • EventBridge.3 • KMS.4 • Lambda.3 • MQ.5 • MQ.6 • MSK.1 • RDS.12 • RDS.15 • S3.17	14 November 2023

Pembaruan kebijakan terkelola	Security Hub menambahkan izin penandaan baru ke kebijakan `AWSSecurityHubServiceRolePolicy` terkelola yang memungkinkan Security Hub membaca tag sumber daya yang terkait dengan temuan.	7 November 2023

Kontrol keamanan baru	Kontrol Security Hub baru berikut ini tersedia: • the section called “[AppSync .5] AWS AppSync GraphQL API tidak boleh diautentikasi dengan kunci API” • the section called “[DMS.6] Instans replikasi DMS harus mengaktifkan peningkatan versi minor otomatis” • the section called “[DMS.7] Tugas replikasi DMS untuk database target seharusnya mengaktifkan logging” • the section called “[DMS.8] Tugas replikasi DMS untuk database sumber seharusny a mengaktifkan logging” • the section called “[DMS.9] Titik akhir DMS harus menggunakan SSL” • the section called “[DocumentDB.3] Cuplikan cluster manual Amazon DocumentDB seharusnya tidak bersifat publik” • the section called “[DocumentDB.4] Cluster Amazon DocumentDB harus mempublikasikan log audit ke Log CloudWatch ” • the section called “[DocumentDB.5] Cluster Amazon DocumentDB harus	10 Oktober 2023

mengaktifkan perlindungan penghapusan”

- the section called “[ECS.9] Definisi tugas ECS harus memiliki konfigurasi logging”
- the section called “[EventBridge.3] bus acara EventBridge khusus harus memiliki kebijakan berbasis sumber daya terlampir”
- the section called “[EventBridge.4] titik akhir EventBridge global harus mengaktifkan replikasi acara”
- the section called “[MSK.1] Cluster MSK harus dienkripsi saat transit di antara node broker”
- the section called “[MQ.5] Broker ActiveMQ harus menggunakan mode penerapan aktif/siaga”
- the section called “[MQ.6] Broker RabbitMQ harus menggunakan mode penerapan cluster”
- the section called “[Network Firewall.9] Firewall Firewall Jaringan harus mengaktifkan perlindungan penghapusan”
- the section called “[RDS.34] Cluster Aurora MySQL DB harus menerbitkan log audit ke Log CloudWatch ”

	• the section called “[RDS.35] Cluster RDS DB harus mengaktifkan peningkatan versi minor otomatis” • the section called “[Route53 .2] Route 53 zona yang dihosting publik harus mencatat kueri DNS” • the section called “AWS WAF Aturan [WAF.12] harus mengaktifkan metrik CloudWatch ”	
Pembaruan kebijakan terkelola	Security Hub menambahk an tindakan Organizat ions baru ke kebijakan `AWSSecurityHubServ iceRolePolicy` terkelola yang memungkinkan Security Hub mengambil informasi akun dan unit organisasi (OU). Kami juga menambahk an tindakan Security Hub baru yang memungkinkan Security Hub membaca dan memperbarui konfigurasi layanan, termasuk standar dan kontrol.	27 September 2023

Kontrol keamanan yang ada ditambahkan ke Standar yang Dikelola Layanan: AWS Control Tower	Kontrol Security Hub berikut telah ditambahkan ke Service-Managed Standard:. AWS Control Tower • the section called “[Athena. 1] Kelompok kerja Athena harus dienkripsi saat istirahat” • the section called “[DocumentDB.1] Cluster Amazon DocumentDB harus dienkripsi saat istirahat” • the section called “[DocumentDB.2] Cluster Amazon DocumentDB harus memiliki periode retensi cadangan yang memadai” • the section called “[Neptunus.1] Cluster DB Neptunus harus dienkripsi saat istirahat” • the section called “[Neptune .2] Cluster DB Neptunus harus menerbitkan log audit ke Log CloudWatch ” • the section called “[Neptune .3] Snapshot cluster Neptunus DB seharusnya tidak publik” • the section called “[Neptunus.4] Cluster DB Neptunus harus mengaktifkan perlindungan penghapusan”	26 September 2023

- the section called “[Neptunus.5] Cluster DB Neptunus harus mengaktifkan cadangan otomatis”
- the section called “[Neptune.6] Snapshot cluster Neptunus DB harus dienkripsi saat istirahat”
- the section called “[Neptunus.7] Cluster DB Neptunus harus mengaktifkan otentikasi basis data IAM”
- the section called “[Neptunus.8] Cluster DB Neptunus harus dikonfigurasi untuk menyalin tag ke snapshot”
- the section called “[RDS.27] Cluster RDS DB harus dienkripsi saat istirahat”

Tampilan kontrol konsolidasi dan temuan kontrol terkonsolidasi tersedia di AWS GovCloud (US)	Tampilan kontrol konsolidasi dan temuan kontrol terkonsolidasi sekarang tersedia di. AWS GovCloud (US) Region Halaman Kontrol konsol Security Hub menampilkan semua kontrol Anda di seluruh standar. Setiap kontrol memiliki ID kontrol yang sama di seluruh standar. Ketika Anda mengaktifkan temuan kontrol konsolidasi, Anda menerima satu temuan per pemeriksaan keamanan bahkan ketika kontrol berlaku untuk beberapa standar yang diaktifkan.	September 6, 2023
Tampilan kontrol konsolidasi dan temuan kontrol konsolidasi tersedia di Wilayah China	Pandangan kontrol konsolidasi dan temuan kontrol konsolidasi sekarang tersedia di Wilayah China. Halaman Kontrol konsol Security Hub menampilkan semua kontrol Anda di seluruh standar. Setiap kontrol memiliki ID kontrol yang sama di seluruh standar. Ketika Anda mengaktifkan temuan kontrol konsolidasi, Anda menerima satu temuan per pemeriksaan keamanan bahkan ketika kontrol berlaku untuk beberapa standar yang diaktifkan.	28 Agustus 2023

Security Hub tersedia di Wilayah Israel (Tel Aviv)	Security Hub sekarang tersedia di Israel (Tel Aviv). Semua fitur Security Hub sekarang tersedia di Wilayah ini, dengan pengecualian kontrol keamanan tertentu. Untuk informasi selengkap nya, lihat Ketersediaan kontrol menurut Wilayah.	8 Agustus 2023

Kontrol keamanan baru	Kontrol Security Hub baru berikut ini tersedia: • the section called “[Athena.1] Kelompok kerja Athena harus dienkripsi saat istirahat” • the section called “[DocumentDB.1] Cluster Amazon DocumentDB harus dienkripsi saat istirahat” • the section called “[DocumentDB.2] Cluster Amazon DocumentDB harus memiliki periode retensi cadangan yang memadai” • the section called “[Neptunus.1] Cluster DB Neptunus harus dienkripsi saat istirahat” • the section called “[Neptune.2] Cluster DB Neptunus harus menerbitkan log audit ke Log CloudWatch ” • the section called “[Neptune.3] Snapshot cluster Neptunus DB seharusnya tidak publik” • the section called “[Neptunus.4] Cluster DB Neptunus harus mengaktifkan perlindungan penghapusan” • the section called “[Neptunus.5] Cluster DB Neptunus	28 Juli 2023

	harus mengaktifkan cadangan otomatis” • the section called “[Neptune .6] Snapshot cluster Neptunus DB harus dienkripsi saat istirahat” • the section called “[Neptunus.7] Cluster DB Neptunus harus mengaktifkan otentikasi basis data IAM” • the section called “[Neptunus.8] Cluster DB Neptunus harus dikonfigurasi untuk menyalin tag ke snapshot” • the section called “[RDS.27] Cluster RDS DB harus dienkripsi saat istirahat”	
Operator baru untuk kriteria aturan otomatisasi	Anda sekarang dapat menggunakan operator perbandingan CONTAINS dan NOT_CONTAINS untuk peta aturan otomatisasi dan kriteria string.	25 Juli 2023
Aturan otomatisasi	Security Hub sekarang menawarkan aturan otomatisasi yang secara otomatis memperbarui temuan berdasarkan kriteria yang Anda tentukan.	13 Juni 2023
Integrasi pihak ketiga yang baru	Snykadalah integrasi pihak ketiga baru yang mengirimkan temuan ke Security Hub.	12 Juni 2023

Kontrol keamanan yang ada ditambahkan ke Standar yang Dikelola Layanan: AWS Control Tower	Kontrol Security Hub berikut telah ditambahkan ke Service-Managed Standard:. AWS Control Tower • the section called “[Akun.1] Informasi kontak keamanan harus disediakan untuk Akun AWS” • the section called “[ApiGateway.8] Rute API Gateway harus menentukan jenis otorisasi” • the section called “[ApiGateway.9] Pencatatan akses harus dikonfigurasi untuk Tahapan API Gateway V2” • the section called “[CodeBuild.3] Log CodeBuild S3 harus dienkripsi” • the section called “[EC2.25] Templat peluncuran Amazon EC2 tidak boleh menetapkan IP publik ke antarmuka jaringan” • the section called “[ELB.1] Application Load Balancer harus dikonfigurasi untuk mengalihkan semua permintaan HTTP ke HTTPS” • the section called “[Redshift.10] Cluster Redshift harus dienkripsi saat istirahat”	12 Juni 2023

- the section called “[SageMaker.2] instance SageMaker notebook harus diluncurkan dalam VPC khusus”
- the section called “[SageMaker.3] Pengguna seharusnya tidak memiliki akses root ke instance SageMaker notebook”
- the section called “[WAF.10] ACL AWS WAF web harus memiliki setidaknya satu aturan atau kelompok aturan”

Kontrol keamanan baru	Kontrol Security Hub baru berikut ini tersedia: • the section called “[ACM.2] Sertifikat RSA yang dikelola oleh ACM harus menggunakan panjang kunci minimal 2.048 bit” • the section called “[AppSync.2] AWS AppSync harus mengaktifkan logging tingkat lapangan” • the section called “[CloudFront.13] CloudFront distribusi harus menggunakan kontrol akses asal” • the section called “[Elastic Beanstalk.3] Elastic Beanstalk harus mengalirkan log ke CloudWatch” • the section called “[S3.17] Ember tujuan umum S3 harus dienkripsi saat istirahat AWS KMS keys” • the section called “[StepFunctions.1] Mesin status Step Functions seharusnya mengaktifkan logging”	6 Juni 2023

Security Hub tersedia di Asia Pasifik (Melbourne)	Security Hub sekarang tersedia di Asia Pasifik (Melbourne). Semua fitur Security Hub sekarang tersedia di Wilayah ini, dengan pengecualian kontrol keamanan tertentu. Untuk informasi selengkapnya, lihat Ketersediaan kontrol menurut Wilayah.	25 Mei 2023
Menemukan sejarah	Security Hub sekarang dapat melacak riwayat temuan selama 90 hari terakhir.	4 Mei 2023
Kontrol keamanan baru	Kontrol Security Hub baru berikut ini tersedia: • the section called “[EKS.1] Titik akhir klaster EKS seharusnya tidak dapat diakses publik” • the section called “[ELB.16] Application Load Balancers harus dikaitkan dengan ACL web AWS WAF” • the section called “[Redshift.10] Cluster Redshift harus dienkripsi saat istirahat” • the section called “[S3.15] Bucket tujuan umum S3 harus mengaktifkan Object Lock”	29 Maret 2023

Dukungan yang diperluas untuk temuan kontrol terkonsolidasi	Respon Keamanan Otomatis pada AWS v2.0.0 sekarang mendukung temuan kontrol terkonsolidasi.	24 Maret 2023
Security Hub tersedia dalam versi baru Wilayah AWS	Security Hub sekarang tersedia di Asia Pasifik (Hyderabad), Eropa (Spanyol), dan Eropa (Zurich). Ada batasan di mana kontrol tersedia di Wilayah ini.	21 Maret 2023
Memperbarui ke kebijakan terkelola	Security Hub telah memperbarui izin yang ada dalam kebijakan `AWSSecurityHubServiceRolePolicy` terkelola.	Maret 17, 2023

Kontrol keamanan baru untuk standar NIST 800-53	Security Hub telah menambahkan kontrol keamanan berikut, yang berlaku untuk standar NIST 800-53: • the section called “[Akun.2] Akun AWS harus menjadi bagian dari organisasi AWS Organizations” • the section called “[CloudWatch.15] CloudWatch alarm harus memiliki tindakan tertentu yang dikonfigurasi” • the section called “[CloudWatch.16] grup CloudWatch log harus dipertahankan untuk jangka waktu tertentu” • the section called “[CloudWatch.17] tindakan CloudWatch alarm harus diaktifkan” • the section called “[DynamoDB.4] Tabel DynamoDB harus ada dalam rencana cadangan” • the section called “[EC2.28] Volume EBS harus dicakup oleh rencana cadangan” • EC2.29 - Instans EC2 harus diluncurkan dalam VPC (pensiun) • the section called “[RDS.26] Instans RDS DB harus dilindungi oleh rencana cadangan”	3 Maret 2023

	• the section called “[S3.14] Bucket tujuan umum S3 harus mengaktifkan versi” • the section called “[WAF.11] pencatatan ACL AWS WAF web harus diaktifkan”	
Institut Nasional Standar dan Teknologi (NIST) 800-53 Wahyu 5	Security Hub sekarang mendukung standar NIST 800-53 Rev. 5 dengan lebih dari 200 kontrol keamanan yang berlaku.	28 Februari 2023
Kontrol konsolidasi melihat dan mengendalikan temuan	Dengan rilis tampilan kontrol konsolidasi, halaman Kontrol konsol Security Hub menampilkan semua kontrol Anda di seluruh standar. Setiap kontrol memiliki ID kontrol yang sama di seluruh standar. Ketika Anda mengaktifkan temuan kontrol konsolidasi, Anda menerima satu temuan per pemeriksaan keamanan bahkan ketika kontrol berlaku untuk beberapa standar yang diaktifkan.	23 Februari 2023

Kontrol keamanan baru	Kontrol Security Hub baru berikut tersedia. Beberapa kontrol memiliki keterbatasan Regional. • the section called “[ElastiCache.1] Cluster ElastiCache Redis harus mengaktifkan pencadangan otomatis” • the section called “[ElastiCache.2] ElastiCache untuk kluster cache Redis harus mengaktifkan peningkatan versi minor otomatis” • the section called “[ElastiCache.3] ElastiCache untuk grup replikasi Redis harus mengaktifkan failover otomatis” • the section called “[ElastiCache.4] ElastiCache untuk grup replikasi Redis harus dienkripsi saat istirahat” • the section called “[ElastiCache.5] ElastiCache untuk grup replikasi Redis harus dienkripsi saat transit” • the section called “[ElastiCache.6] ElastiCache untuk grup replikasi Redis sebelum versi 6.0 harus menggunakan Redis AUTH” • the section called “[ElastiCache.7] ElastiCache cluster	16 Februari 2023

	tidak boleh menggunakan grup subnet default”	
Bidang ASFF baru	Security Hub telah ditambahkan ProductFields. ArchivalReasons:0/Deskripsi dan. ProductFields ArchivalReasons0/ ReasonCode ke AWS Security Finding Format (ASFF).	Februari 8, 2023
Bidang ASFF baru	Security Hub telah menambahkan Kepatuhan. AssociatedStandards dan Kepatuhan. SecurityControlId ke AWS Security Finding Format (ASFF).	31 Januari 2023
Detail kerentanan sekarang tersedia	Anda sekarang dapat melihat detail kerentanan di konsol Security Hub untuk mengetahui temuan yang dikirim Amazon Inspector ke Security Hub.	Januari 14, 2023
Security Hub tersedia di Timur Tengah (UEA)	Security Hub sekarang tersedia di Timur Tengah (UEA). Beberapa kontrol memiliki batas Regional.	Januari 12, 2023
Menambahkan integrasi pihak ketiga dengan MetricStream	Security Hub sekarang mendukung integrasi pihak ketiga dengan MetricStream di semua Wilayah kecuali China dan AWS GovCloud (US).	11 Januari 2023

Peningkatan batas akun organisasi	Security Hub sekarang mendukung hingga 11.000 akun anggota untuk setiap akun administrator Security Hub per Wilayah.	Desember 27, 2022
ElasticBeanstalk.3 digulung kembali	Security Hub memutar kembali kontrol [ElasticBeanstalk. 3] Elastic Beanstalk harus mengalirkan CloudWatch log dari standar FSBP di semua Wilayah.	21 Desember 2022
Security Hub menambahkan kontrol keamanan baru	Kontrol Security Hub baru tersedia untuk pelanggan yang telah mengaktifkan standar FSBP. Beberapa kontrol memiliki keterbatasan Regional.	Desember 15, 2022
Panduan tentang fitur yang akan datang	Security Hub berencana untuk merilis dua fitur baru: tampilan kontrol terkonsol idasi dan temuan kontrol terkonsolidasi. Fitur yang akan datang ini dapat memengaru hi alur kerja yang ada yang bergantung pada bidang dan nilai pencarian kontrol.	Desember 9, 2022
Integrasi Amazon Security Lake sekarang tersedia	Security Lake sekarang terintegrasi dengan Security Hub dengan menerima temuan Security Hub.	29 November 2022

Dukungan untuk Standar yang Dikelola Layanan: AWS Control Tower	Security Hub mendukung standar keamanan baru yang disebut Service-Managed Standard:. AWS Control Tower AWS Control Tower mengelola standar ini.	28 November 2022
CIS AWS Foundations Benchmark v1.4.0 sekarang tersedia di Wilayah China	Security Hub sekarang mendukung CIS AWS Foundations Benchmark v1.4.0 di Wilayah China.	18 November 2022
Integrasi Cloud Manajemen Layanan Jira sekarang tersedia	Jira Service Management Cloud sekarang menerima temuan Security Hub di semua Wilayah yang tersedia, kecuali Wilayah China.	17 November 2022
AWS IoT Device Defender integrasi sekarang tersedia	AWS IoT Device Defender sekarang mengirimkan temuan ke Security Hub di semua Wilayah yang tersedia.	17 November 2022
Support untuk CIS AWS Foundations Benchmark v1.4.0	Security Hub sekarang menyediakan kontrol keamanan yang mendukung CIS AWS Foundations Benchmark v1.4.0. Standar ini tersedia di semua Wilayah yang tersedia, kecuali Wilayah China.	9 November 2022

Dukungan untuk pengumuman Security Hub di AWS GovCloud (US)	Anda sekarang dapat berlangganan pengumuman Security Hub dengan Amazon Simple Notification Service (Amazon SNS) di (AS-Timur) dan AWS GovCloud AWS GovCloud (AS-Barat) untuk menerima pemberitahuan tentang Security Hub.	3 Oktober 2022
AWS Security Hub menambahkan kontrol keamanan baru	Kontrol Security Hub yang baru AutoScaling.9 tersedia untuk pelanggan yang telah mengaktifkan standar FSBP. Kontrol mungkin memiliki batasan Regional.	September 1, 2022
Berlangganan pengumuman Security Hub	Anda sekarang dapat berlangganan pengumuman Security Hub dengan Amazon Simple Notification Service (Amazon SNS) untuk menerima pemberitahuan tentang Security Hub.	Agustus 29, 2022
Perluasan wilayah untuk agregasi lintas wilayah	Agregasi Lintas Wilayah sekarang tersedia untuk temuan, menemukan pembaruan, dan wawasan di seluruh wilayah. AWS GovCloud (US)	Agustus 2, 2022

Integrasi produk pihak ketiga yang baru	Fortinet - FortiCNP adalah integrasi pihak ketiga yang menerima temuan Security Hub, dan jFrog adalah integrasi pihak ketiga yang mengirimkan temuan ke Security Hub.	26 Juli 2022
EC2.27 sudah pensiun	Security Hub telah menghentikan EC2.27 - Menjalankan Instans EC2 tidak boleh menggunakan pasangan kunci, kontrol sebelumnya dalam standar Praktik Terbaik Keamanan AWS Dasar (FSBP).	20 Juli 2022
Lambda.2 tidak lagi mendukung python3.6	Security Hub tidak lagi mendukung python3.6 sebagai parameter untuk Lambda.2 - Fungsi Lambda harus menggunakan runtime yang didukung, kontrol dalam standar Foundational Security Best Practices (FSBP). AWS	19 Juli 2022
AWS Security Hub menambahkan kontrol keamanan baru	Kontrol Security Hub baru tersedia untuk pelanggan yang telah mengaktifkan standar FSBP. Beberapa kontrol memiliki keterbatasan Regional.	Juni 22, 2022
AWS Security Hub mendukung Wilayah baru	Security Hub sekarang tersedia di Asia Pasifik (Jakarta). Beberapa kontrol tidak tersedia di Wilayah ini.	7 Juni 2022

Peningkatan integrasi antara AWS Security Hub dan AWS Config	Pengguna Security Hub dapat melihat hasil evaluasi AWS Config aturan sebagai temuan di Security Hub.	6 Juni 2022
Menambahkan kemampuan untuk memilih keluar dari standar yang diaktifkan secara otomatis	Untuk pengguna yang telah terintegrasi AWS Organizations, fitur ini memungkinkan Anda untuk masuk ke akun administrator Security Hub dan memilih akun anggota baru di luar standar yang diaktifkan secara otomatis.	April 25, 2022
Agregasi lintas wilayah yang diperluas	Menambahkan agregasi lintas wilayah untuk mengontrol status dan skor keamanan.	20 April 2022
CompanyName dan ProductName sekarang atribut tingkat atas	Menambahkan atribut tingkat atas baru untuk menetapkan nama perusahaan dan produk yang terkait dengan integrasi kustom	1 April 2022
Menambahkan kontrol baru ke standar Praktik Terbaik Keamanan AWS Dasar	Menambahkan 5 kontrol baru ke standar Praktik Terbaik Keamanan AWS Dasar.	31 Maret 2022
Menambahkan rincian sumber daya baru keberatan dengan ASFF	Menambahkan jenis `AwsRdsDbSecurityGroup` sumber daya ke ASFF.	Maret 25, 2022

Menambahkan rincian sumber daya tambahan di ASFF	Menambahkan detail tambahan ke`AwsAutoScalingScalingGroup` ,`AwsElbLoadBalancer` ,`AwsRedshiftCluster` , dan`AwsCodeBuildProject` .	Maret 25, 2022
Menambahkan kontrol baru ke standar Praktik Terbaik Keamanan AWS Dasar	Menambahkan 15 kontrol baru ke standar Praktik Terbaik Keamanan AWS Dasar.	16 Maret 2022
Menambahkan kontrol baru ke standar Praktik Terbaik Keamanan AWS Dasar dan Standar Keamanan Data Industri Kartu Pembayaran (PCI DSS)	Menambahkan kontrol baru untuk Amazon OpenSearch Service, Amazon RDS, Amazon EC2, Elastic Load Balancing CloudFront , dan standar Praktik AWS Terbaik Keamanan Dasar. Juga menambahkan dua kontrol baru untuk OpenSearch Layanan ke PCI DSS.	Februari 15, 2022
Menambahkan bidang baru ke ASFF	Ditambahkan bidang baru: Contoh.	26 Januari 2022
Integrasi ditambahkan dengan AWS Health	AWS Health menggunakan pesan service-to-service acara untuk mengirim temuan ke Security Hub.	Januari 19, 2022

Integrasi ditambahkan dengan AWS Trusted Advisor	Trusted Advisor mengirimkan hasil pemeriksaannya ke Security Hub sebagai temuan Security Hub. Security Hub mengirimkan hasil pemeriksaan Praktik Terbaik Keamanan AWS Dasar ke Trusted Advisor.	18 Januari 2022
Diperbarui objek rincian sumber daya di ASFF	Ditambahkan `MixedInstancesPolicy` dan `AvailabilityZones` ke `AwsAutoScalingAutoScalingGroup`. Menambahkan `MetadataOptions` ke `AwsAutoScalingLaunchConfiguration`. Menambahkan `BucketVersioningConfiguration` ke `AwsS3Bucket`.	Desember 20, 2021
Diperbarui output untuk dokumentasi ASFF	Deskripsi atribut ASFF sebelumnya dalam satu topik. Setiap objek tingkat atas dan setiap objek detail sumber daya sekarang dalam topiknya sendiri. Topik sintaks ASFF berisi tautan ke topik tersebut.	Desember 20, 2021

Menambahkan objek detail sumber daya baru ke ASFF untuk AWS Network Firewall	Untuk AWS Network Firewall, menambahkan objek detail sumber daya berikut:`AwsNetworkFirewallFirewall` ,`AwsNetworkFireFirewallPolicy` , dan`AwsNetworkFirewallRuleGroup` .	Desember 20, 2021
Ditambahkan dukungan untuk versi baru Amazon Inspector	Security Hub terintegrasi dengan versi baru Amazon Inspector serta dengan Amazon Inspector Classic. Amazon Inspector mengirimkan temuan ke Security Hub.	29 November 2021
Mengubah tingkat keparahan EC2.19	Tingkat keparahan EC2.19 (Grup keamanan tidak boleh mengizinkan akses tidak terbatas ke port dengan risiko tinggi) diubah dari Tinggi ke Kritis.	17 November 2021
Integrasi baru dengan Sonrai Dig	Security Hub sekarang menawarkan integrasi denganSonrai Dig. Sonrai Digmemantau lingkungan cloud untuk mengidentifikasi risiko keamanan. Sonrai Digmengirimkan temuan ke Security Hub.	12 November 2021

Pemeriksaan yang diperbarui untuk kontrol CIS 2.1 dan CloudTrail .1	Selain memeriksa bahwa setidaknya satu CloudTrail jejak Multi-wilayah sudah ada, CIS 2.1 dan CloudTrail .1 sekarang juga memeriksa apakah `ExcludeManagementEventSources` parameternya kosong di setidaknya satu jalur Multi-wilayah. CloudTrail	November 9, 2021
Menambahkan dukungan untuk titik akhir VPC	Security Hub sekarang terintegrasi dengan AWS PrivateLink dan mendukung titik akhir VPC.	3 November 2021
Menambahkan kontrol ke standar Praktik Terbaik Keamanan AWS Dasar	Menambahkan kontrol baru untuk Elastic Load Balancing (ELB.2 dan ELB.8) dan (SSM.4). AWS Systems Manager	2 November 2021
Menambahkan port ke cek untuk kontrol EC2.19	EC2.19 sekarang juga memeriksa bahwa grup keamanan tidak mengizinkan akses masuk tanpa batas ke port berikut: 3000 (kerangka kerja pengembangan web Go, Node.js, dan Ruby), 5000 (kerangka kerja pengembangan web Python), 8088 (port HTTP lama), dan 8888 (port HTTP alternatif)	27 Oktober 2021

Menambahkan integrasi dengan Logz.io Cloud SIEM	Logz.io adalah penyedia Cloud SIEM yang menyediakan korelasi lanjutan data log dan peristiwa untuk membantu tim keamanan mendeteksi, menganalisis, dan merespons ancaman keamanan secara real time. Logz.io menerima temuan dari Security Hub.	25 Oktober 2021
Menambahkan dukungan untuk agregasi temuan lintas wilayah	Agregasi Lintas Wilayah memungkinkan Anda untuk melihat semua temuan Anda tanpa harus mengubah Wilayah. Akun administrator memilih Wilayah agregasi dan Wilayah yang ditautkan. Temuan untuk akun administrator dan akun anggotanya dikumpulkan dari Wilayah yang ditautkan ke Wilayah agregasi.	20 Oktober 2021
Diperbarui objek rincian sumber daya di ASFF	Menambahkan detail sertifikat penampil ke`AwsCloudFrontDistribution`. Menambahkan detail tambahan ke`AwsCodeBuildProject`. Menambahkan atribut penyeimbang beban ke`AwsElbV2LoadBalancer`. Menambahkan pengenal akun pemilik bucket S3 ke. `AwsS3Bucket`	Oktober 8, 2021

Menambahkan objek detail sumber daya baru ke ASFF	Menambahkan objek rincian sumber daya baru berikut ke ASFF:`AwsEc2VpcEndpointService`, `AwsEcrRepository`, `AwsEksCluster`, `AwsOpenSearchServiceDomain`, `AwsWafRateBasedRule`, `AwsWafRegionalRateBasedRule`, `AwsXrayEncryptionConfig`	Oktober 8, 2021
Menghapus runtime usang dari kontrol Lambda.2	Dalam standar Praktik Terbaik Keamanan AWS Dasar, menghapus `dotnetcore2.1` runtime dari fungsi Lambda [Lambda.2] harus menggunakan runtime yang didukung.	Oktober 6, 2021
Nama baru untuk integrasi Check Point	Integrasi dengan Check Point Dome9 Arc sekarang Check Point CloudGuard Posture Management. Integrasi ARN tidak berubah.	1 Oktober 2021
Menghapus integrasi dengan Alcide	Integrasi dengan Alcide Kaudit dihentikan.	30 September 2021
Mengubah tingkat keparahan EC2.19	Tingkat keparahan [EC2.19] Grup keamanan tidak boleh mengizinkan akses tidak terbatas ke port dengan risiko tinggi diubah dari Medium ke High.	30 September 2021

AWS Organizations Integrasi dengan sekarang didukung di Wilayah China	Integrasi Security Hub dengan Organizations sekarang didukung di China (Beijing) dan China (Ningxia).	September 20, 2021
AWS Config Aturan baru untuk kontrol S3.1 dan PCI.S3.6	Baik S3.1 dan PCI.S3.6 memverifikasi bahwa pengaturan Akses Publik Blok Amazon S3 diaktifkan. AWS Config Aturan untuk kontrol ini diubah dari `s3-account-level-public-access-blocks` menjadi`s3-account-level-public-access-blocks-periodic` .	14 September 2021
Menghapus runtime usang dari kontrol Lambda.2	Dalam standar Praktik Terbaik Keamanan AWS Dasar, menghapus `nodejs10.x` dan `ruby2.5` runtime dari fungsi Lambda [Lambda.2] harus menggunakan runtime yang didukung.	13 September 2021
Mengubah tingkat keparahan kontrol CIS 2.2	Dalam standar CIS AWS Foundations Benchmark , tingkat keparahan untuk 2.2. — Pastikan validasi file CloudTrail log diaktifkan diubah dari Rendah ke Sedang.	13 September 2021

Memperbarui ECS.1, Lambda.2, dan SSM.1 dalam standar Praktik Terbaik Keamanan Dasar AWS	Dalam standar Praktik Terbaik Keamanan AWS Dasar, ECS.1 sekarang memiliki `SkipInactiveTaskDefinitions` parameter yang disetel ke. `true` Ini memastikan bahwa kontrol hanya memeriksa definisi tugas aktif. Untuk Lambda.2, menambahkan Python 3.9 ke daftar runtime. SSM.1 sekarang memeriksa instance berhenti dan berjalan.	7 September 2021
Kontrol PCI.lambda.2 sekarang mengecualikan sumber daya Lambda @Edge	Dalam standar Standar Keamanan Data Industri Kartu Pembayaran (PCI DSS), kontrol PCI.lambda.2 sekarang mengecualikan sumber daya Lambda @Edge.	7 September 2021
Menambahkan integrasi dengan HackerOne Vulnerability Intelligence	Security Hub sekarang menawarkan integrasi denganHackerOne Vulnerability Intelligence. Integrasi mengirimkan temuan ke Security Hub.	7 September 2021

Diperbarui objek rincian sumber daya di ASFF	Untuk `AwsKmsKey` , ditambahkan `KeyRotationStatus` . Untuk `AwsS3Bucket` , ditambahkan `AccessControlList` , `BucketLoggingConfiguration` , `BucketNotificationConfiguration` , dan `BucketWebsiteConfiguration` .	2 September 2021
Menambahkan objek detail sumber daya baru ke ASFF	Menambahkan objek rincian sumber daya baru berikut ke ASFF: `AwsAutoScalingLaunchConfiguration` , `AwsEc2VpnConnection` , dan `AwsEcrContainerImage` .	2 September 2021
Menambahkan detail ke `Vulnerabilities` objek di ASFF	Di `Cvss` , ditambahkan `Adjustments` dan `Source` . Di `VulnerablePackages` , menambahkan jalur file dan manajer paket.	2 September 2021
Systems Manager Explorer dan OpsCenter integrasi sekarang didukung di Wilayah China	Integrasi Security Hub dengan SSM Explorer dan sekarang OpsCenter didukung di China (Beijing) dan China (Ningxia).	31 Agustus 2021

Menghentikan kontrol Lambda.4	Security Hub menghentikan kontrol [Lambda.4] Fungsi Lambda harus memiliki antrian huruf mati yang dikonfigu rasi. Ketika kontrol dihentika n, kontrol tidak lagi ditampilk an di konsol, dan Security Hub tidak melakukan pemeriksaan terhadapnya.	31 Agustus 2021
Pensiun kontrol PCI.EC2.3	Security Hub menghentikan kontrol [PCI.EC2.3] Grup keamanan EC2 yang tidak digunakan harus dihapus. Ketika kontrol dihentikan, kontrol tidak lagi ditampilkan di konsol, dan Security Hub tidak melakukan pemeriksaan terhadapnya.	Agustus 27, 2021
Ubah cara Security Hub mengirimkan temuan ke tindakan kustom	Saat Anda mengirim temuan ke tindakan kustom, Security Hub sekarang mengirimkan setiap temuan dalam Security Hub Findings - Custom Actionacara terpisah.	Agustus 20, 2021
Menambahkan kode alasan status kepatuhan baru untuk runtime Lambda kustom	Menambahkan kode alasan status `LAMBDA_CU STOM_RUNTIME_DETAI LS_NOT_AVAILABLE` kepatuhan baru. Kode alasan ini menunjukkan bahwa Security Hub tidak dapat melakukan pemeriksaan terhadap runtime Lambda kustom.	Agustus 20, 2021

AWS Firewall Manager integrasi sekarang didukung di Wilayah China	Integrasi Security Hub dengan Firewall Manager sekarang didukung di China (Beijing) dan China (Ningxia).	19 Agustus 2021
Integrasi baru dengan Caveonix Cloud dan Forcepoint Cloud Security Gateway	Security Hub sekarang menawarkan integrasi dengan Caveonix Cloud danForcepoint Cloud Security Gateway. Kedua integrasi mengirimkan temuan ke Security Hub.	Agustus 10, 2021
Ditambahkan baru`CompanyName` ,`ProductName` , dan `Region` atribut ke ASFF	Ditambahkan `CompanyName` `ProductName` ,, dan `Region` bidang ke tingkat atas ASFF. Bidang ini diisi secara otomatis dan, kecuali untuk integrasi produk khusus, tidak dapat diperbarui menggunakan `BatchImportFindings` atau. `BatchUpdateFindings` Di konsol, menemukan filter menggunakan bidang baru ini. Di API, `ProductName` filter `CompanyName` dan menggunakan atribut yang ada di bawah`ProductFields` .	23 Juli 2021

Ditambahkan dan diperbarui rincian sumber daya objek di ASFF	Menambahkan jenis `AwsRdsEventSubscription` sumber daya baru dan detail sumber daya. Menambahkan detail sumber daya untuk jenis `AwsEcsService` sumber daya. Ditambahkan atribut ke objek rincian `AwsElasticsearchDomain` sumber daya.	23 Juli 2021
Menambahkan kontrol ke standar Praktik Terbaik Keamanan AWS Dasar	Menambahkan kontrol baru untuk Amazon API Gateway (ApiGateway.5), Amazon EC2 (EC2.19), Amazon ECS (ECS.2), Elastic Load Balancing (ELB.7), Amazon Service (ES.5 hingga ES.8), Amazon RDS (RDS.16 melalui RDS.23), OpenSearch Amazon Redshift (Redshift.4), dan Amazon SQS (SQS.1).	20 Juli 2021
Memindahkan izin dalam kebijakan terkelola peran terkait layanan	Memindahkan `config:PutEvaluations` izin dalam kebijakan terkelola`AWSSecurityHubServiceRolePolicy` , sehingga diterapkan ke semua sumber daya.	14 Juli 2021

Menambahkan kontrol ke standar Praktik Terbaik Keamanan AWS Dasar	Menambahkan kontrol baru untuk Amazon API Gateway (ApiGateway.4), Amazon CloudFront (.5 dan CloudFron t .6), CloudFront Amazon EC2 (EC2.17 dan EC2.18), Amazon ECS (ECS.1), Amazon Service AWS Identity and Access Management (ES.4), (IAM.21), Amazon RDS (RDS.15 OpenSearch), dan Amazon S3 (S3.8).	8 Juli 2021
Menambahkan kode alasan status kepatuhan baru untuk temuan kontrol	`INTERNAL_SERVICE_E RROR` menunjukkan bahwa kesalahan yang tidak diketahui terjadi. `SNS_TOPIC_CROSS_AC COUNT` menunjukkan bahwa topik SNS dimiliki oleh akun yang berbeda. `SNS_TOPIC _INVALID` menunjukkan bahwa topik SNS terkait tidak valid.	6 Juli 2021
Menambahkan integrasi dengan AWS Chatbot	Menambahkan integrasi dengan AWS Chatbot. Security Hub mengirimkan temuan ke AWS Chatbot.	30 Juni 2021
Menambahkan izin baru ke kebijakan terkelola peran terkait layanan	Menambahkan izin baru ke kebijakan terkelola `AWSSecurityHubServ iceRolePolicy` untuk memungkinkan peran terkait layanan memberikan hasil evaluasi. AWS Config	29 Juni 2021

Objek detail sumber daya baru dan diperbarui di ASFF	Menambahkan objek detail sumber daya baru untuk cluster ECS dan definisi tugas ECS. Diperbarui objek instans EC2 untuk daftar antarmuka jaringan terkait. Menambahkan ID sertifikat klien untuk tahap API Gateway V2. Menambahk an konfigurasi siklus hidup untuk bucket S3.	24 Juni 2021
Memperbarui perhitungan status kontrol agregat dan skor keamanan standar	Security Hub sekarang menghitung status kontrol keseluruhan dan skor keamanan standar setiap 24 jam. Untuk akun administrator, skor sekarang mencerminkan apakah setiap kontrol diaktifka n atau dinonaktifkan untuk setiap akun.	23 Juni 2021
Informasi terbaru tentang penanganan Security Hub atas akun yang ditangguhkan	Menambahkan informasi tentang cara Security Hub menangani akun yang ditangguhkan AWS.	23 Juni 2021
Menambahkan tab untuk menampilkan kontrol yang diaktifkan dan dinonaktifkan untuk akun administrator individu	Untuk akun administrator, tab utama pada halaman detail standar berisi informasi agregat di seluruh akun. Tab baru Diaktifkan untuk akun ini dan Dinonaktifkan untuk akun ini mencantumkan akun yang diaktifkan atau dinonakti fkan untuk akun administrator individu.	23 Juni 2021

Ditambahkan `java8.al2` ke parameter untuk `Lambda.2`	Dalam standar Praktik Terbaik Keamanan AWS Dasar, ditambahkan `java8.al2` ke runtime yang didukung untuk kontrol. `Lambda.2`	8 Juni 2021
Integrasi baru dengan MicroFocus ArcSight dan NETSCOUT Cyber Investigator	Menambahkan integrasi dengan MicroFocus ArcSight dan NETSCOUT Cyber Investigator. MicroFocus ArcSight menerima temuan dari Security Hub. NETSCOUT Cyber Investigator mengirimkan temuan ke Security Hub.	7 Juni 2021
Menambahkan rincian untuk `AWSSecurityHubServiceRolePolicy`	Memperbarui bagian kebijakan terkelola untuk menambahkan detail kebijakan terkelola yang ada`AWSSecurityHubServiceRolePolicy` , yang digunakan oleh peran terkait layanan Security Hub.	4 Juni 2021
Integrasi baru dengan Manajemen Layanan Jira	Konektor Manajemen AWS Layanan untuk Jira mengirimkan temuan ke Jira dan menggunakannya untuk membuat masalah Jira. Ketika masalah Jira diperbarui, temuan terkait di Security Hub juga diperbarui.	26 Mei 2021

Memperbarui daftar kontrol yang didukung untuk Wilayah Asia Pasifik (Osaka)	Memperbarui standar CIS AWS Foundations dan Payment Card Industry Data Security Standard (PCI DSS) untuk menunjukkan kontrol yang tidak didukung di Asia Pasifik (Osaka).	21 Mei 2021
Integrasi baru dengan Sysdig Secure untuk cloud	Menambahkan integrasi dengan Sysdig Secure untuk cloud. Integrasi mengirimkan temuan ke Security Hub.	14 Mei 2021
Menambahkan kontrol ke standar Praktik Terbaik Keamanan AWS Dasar	Menambahkan kontrol baru untuk Amazon API Gateway (ApiGateway.2 dan ApiGatewa y.3), (.4 dan CloudTrail .5) CloudTrail, Amazon EC2 (EC2.15 AWS CloudTrai l dan EC2.16), (.1 dan .2), (Lambda.4), Amazon RDS (RDS.12 - AWS Elastic Beanstalk RDS.14), Amazon ElasticBeanstalk Redshift (Redshift.7) ElasticBeanstalk, (.3 dan .4 AWS Lambda), dan (WAF.1). AWS Secrets Manager SecretsManager SecretsManager AWS WAF	10 Mei 2021
Pembaruan untuk GuardDuty dan kontrol Amazon RDS	Mengubah tingkat keparahan `GuardDuty.1` dan `PCI.GuardDuty.1` dari Sedang ke Tinggi. Menambahkan `databaseE ngines` parameter ke`RDS.8`.	4 Mei 2021

Menambahkan rincian sumber daya baru ke ASFF	Di`Resources.Details` , menambahkan objek detail sumber daya baru untuk ACL jaringan Amazon EC2, subnet Amazon EC2, dan lingkungan. AWS Elastic Beanstalk	3 Mei 2021
Menambahkan bidang konsol untuk memberikan nilai filter untuk EventBridge aturan Amazon	Pola filter baru yang telah ditentukan untuk EventBrid ge aturan Security Hub menyediakan bidang konsol yang dapat Anda gunakan untuk menentukan nilai filter.	30 April 2021
Menambahkan integrasi dengan AWS Systems Manager Explorer dan OpsCenter	Security Hub sekarang mendukung integrasi dengan Systems Manager Explorer dan OpsCenter. Integrasi ini menerima temuan dari Security Hub dan memperbar ui temuan tersebut di Security Hub.	26 April 2021
Tipe baru untuk integrasi produk	Jenis integrasi baru,`UPDATE_FINDINGS_IN _SECURITY_HUB` , menunjukkan bahwa integrasi produk memperbarui temuan yang diterimanya dari Security Hub.	22 April 2021
Mengubah “akun master” menjadi “akun administrator”	Istilah "akun utama" diubah menjadi "akun administrator." Istilah ini juga diubah di konsol Security Hub dan API.	22 April 2021

Diperbarui ApiGateway.1 untuk mengganti HTTP dengan Websocket	Memperbarui judul, deskripsi , dan remediasi untuk ApiGateway.1. Kontrol sekarang memeriksa logging eksekusi API Websocket alih-alih untuk logging eksekusi HTTP API.	9 April 2021
GuardDuty Integrasi Amazon sekarang didukung di Beijing dan Ningxia	Integrasi Security Hub dengan GuardDuty sekarang didukung di Wilayah China (Beijing) dan China (Ningxia).	5 April 2021
Ditambahkan `nodejs14.x` ke runtime yang didukung untuk kontrol Lambda.2	Kontrol Lambda.2 dalam standar Praktik Terbaik Keamanan Dasar sekarang mendukung runtime. `nodejs14.x`	30 Maret 2021
Security Hub diluncurkan di Asia Pasifik (Osaka)	Security Hub sekarang tersedia di Wilayah Asia Pasifik (Osaka).	29 Maret 2021
Menambahkan bidang penyedia pencarian untuk menemukan detail	Pada panel rincian temuan, bagian Finding Provider Fields yang baru berisi nilai penyedia temuan untuk kepercayaan diri, kekritisan, temuan terkait, tingkat keparahan, dan jenis.	24 Maret 2021
Menambahkan opsi untuk menerima temuan sensitif dari Amazon Macie	Integrasi dengan Macie sekarang dapat dikonfigu rasi untuk mengirim temuan sensitif ke Security Hub.	23 Maret 2021

Transisi ke manajemen AWS Organizations akun	Untuk pelanggan yang memiliki akun administrator dengan akun anggota, menambahkan informasi baru tentang cara mengubah dari mengelola akun dengan undangan menjadi mengelola akun menggunakan Organizations.	22 Maret 2021
Objek baru di ASFF untuk informasi tentang konfigurasi Blok Akses Publik Amazon S3	Di `Resources` , objek tipe dan detail `AwsS3AccountPublicAccessBlock` sumber daya baru memberikan informasi tentang konfigurasi Blok Akses Publik Amazon S3 untuk akun. Dalam objek detail `AwsS3Bucket` sumber daya, `PublicAccessBlockConfiguration` objek menyediakan konfigurasi Blok Akses Publik untuk bucket S3.	18 Maret 2021

Objek baru di ASFF untuk memungkinkan penyedia pencarian memperbarui bidang tertentu	`FindingProviderFields` Objek baru di ASFF digunakan `BatchImportFindings` untuk memberikan nilai untuk`Confidence` ,,`Criticality` , `RelatedFindings` `Severity`, dan`Types`. Bidang asli hanya boleh diperbarui menggunakan`BatchUpdateFindings` .	18 Maret 2021
`DataClassification` Objek baru untuk sumber daya di ASFF	`Resources.DataClassification` Objek baru di ASFF digunakan untuk memberikan informasi tentang data sensitif yang terdeteksi pada sumber daya.	18 Maret 2021
`CONFIG_RETURNS_NOT_APPLICABLE` Nilai tambah pada kode status kepatuhan yang tersedia	Untuk status `NOT_AVAILABLE` kepatuhan, hapus kode alasan `RESOURCE_NO_LONGER_EXISTS` dan tambahkan kode alasan`CONFIG_RETURNS_NOT_APPLICABLE` .	16 Maret 2021

Kebijakan terkelola baru untuk integrasi dengan AWS Organizations	Kebijakan terkelola baru`AWSSecurityHubOrganizationsAccess` , menyediakan izin Organizations yang diperlukan oleh akun manajemen organisasi dan akun administrator Security Hub yang didelegasikan.	15 Maret 2021
Kebijakan terkelola dan informasi peran terkait layanan dipindahkan ke bagian Keamanan	Informasi tentang kebijakan yang dikelola direvisi dan diperluas. Baik informasi kebijakan terkelola maupun informasi tentang peran terkait layanan telah dipindahkan ke bagian Keamanan.	15 Maret 2021
Integrasi baru dengan SecureCloud DB	Menambahkan SecureCloud DB ke daftar integrasi pihak ketiga. SecureCloudDB adalah alat keamanan database asli cloud yang menyediakan visibilitas komprehensif postur dan aktivitas keamanan internal dan eksternal. SecureCloudDB mengirimkan temuan ke Security Hub.	4 Maret 2021
Tingkat keparahan yang direvisi untuk kontrol CIS 1.1 dan CIS 3.1 - CIS 3.14	Tingkat keparahan kontrol CIS 1.1 dan CIS 3.1 - CIS 3.14 diubah menjadi Rendah.	3 Maret 2021
Menghapus kontrol RDS.11	Menghapus kontrol RDS.11 dari standar Praktik Terbaik Keamanan Dasar.	3 Maret 2021

Integrasi yang diperbarui untuk Turbot	Integrasi Turbot diperbarui untuk mengirim dan menerima temuan.	26 Februari 2021
Menambahkan kontrol ke standar Praktik Terbaik Keamanan Dasar	Menambahkan kontrol baru untuk Amazon API Gateway (ApiGateway.1), Amazon EC2 (EC2.9 dan EC2.10), Amazon Elastic File System (EFS.2), Amazon Service (ES.2 dan ES.3), Elastic Load Balancing OpenSearch (ELB.6), dan () (KMS.3). AWS Key Management Service AWS KMS	11 Februari 2021
Menambahkan `ProductArn` filter opsional ke `DescribeProducts` API	Operasi `DescribeProducts` API sekarang menyertakan `ProductArn` parameter opsional. `ProductArn` Parameter ini digunakan untuk mengidentifikasi integrasi produk tertentu untuk mengembalikan detail untuk.	3 Februari 2021
Integrasi baru dengan Antivirus untuk Amazon S3 dari Cloud Storage Security	Integrasi dengan Antivirus untuk Amazon S3 mengirimkan hasil pemindaian virus ke Security Hub sebagai temuan.	27 Januari 2021

Memperbarui proses perhitungan skor keamanan untuk akun administrator	Untuk akun administrator, Security Hub menggunakan proses terpisah untuk menghitung skor keamanan. Proses baru memastikan bahwa skor mencakup kontrol yang diaktifkan untuk akun anggota tetapi dinonaktifkan untuk akun administrator.	21 Januari 2021
Bidang dan objek baru di ASFF	Menambahkan `Action` objek baru untuk melacak tindakan yang terjadi terhadap sumber daya. Menambahkan bidang ke `AwsEc2NetworkInterface` objek untuk melacak nama DNS dan alamat IP. Menambahkan `AwsSsmPatchCompliance` objek baru ke detail sumber daya.	21 Januari 2021
Menambahkan kontrol ke standar Praktik Terbaik Keamanan Dasar	Menambahkan kontrol baru untuk Amazon CloudFront (CloudFront.1 hingga CloudFront .4), Amazon DynamoDB (DynamoDB.1 melalui DynamoDB.3), Elastic Load Balancing (ELB.3 hingga ELB.5), Amazon RDS (RDS.9 hingga RDS.11), Amazon Redshift (Redshift.1 melalui Redshift.3 dan Redshift.6), dan Amazon SNS (SNS.1).	15 Januari 2021

Status alur kerja diatur ulang berdasarkan status catatan atau status kepatuhan	Security Hub secara otomatis mengatur ulang status alur kerja dari `NOTIFIED` atau `RESOLVED` ke `NEW` jika temuan yang diarsipkan dibuat aktif, atau jika status kepatuhan temuan berubah dari `PASSED` salah satu`FAILED`,, `WARNING` atau. `NOT_AVAILABLE` Perubahan ini menunjukkan bahwa penyelidikan tambahan diperlukan.	7 Januari 2021
Menambahkan `ProductFields` informasi untuk temuan berbasis kontrol	Untuk temuan yang dihasilkan dari kontrol, tambahkan informasi tentang konten `ProductFields` objek dalam AWS Security Finding Format (ASFF).	29 Desember 2020
Pembaruan untuk wawasan terkelola	Mengubah judul wawasan 5. Menambahkan wawasan baru, 32, yang memeriksa pengguna IAM dengan aktivitas mencurigakan.	22 Desember 2020
Pembaruan untuk kontrol IAM.7 dan Lambda.1	Dalam standar Praktik Terbaik Keamanan AWS Dasar, memperbarui parameter untuk IAM.7. Memperbarui judul dan deskripsi Lambda.1.	22 Desember 2020

Integrasi yang diperluas dengan ServiceNow ITSM	Integrasi ServiceNow ITSM memungkinkan pengguna untuk secara otomatis membuat insiden atau masalah ketika temuan Security Hub diterima. Pembaruan untuk insiden atau masalah ini menghasilkan pembaruan temuan di Security Hub.	11 Desember 2020
Integrasi baru dengan AWS Audit Manager	Security Hub sekarang menawarkan integrasi dengan AWS Audit Manager. Integrasi ini memungkinkan Audit Manager menerima temuan berbasis kontrol dari Security Hub.	8 Desember 2020
Integrasi baru dengan Aqua Security Kube-Bench	Security Hub menambahk an integrasi dengan Aqua Security Kube-Bench. Integrasi mengirimkan temuan ke Security Hub.	24 November 2020
Cloud Custodian sekarang tersedia di Wilayah China	Integrasi dengan Cloud Custodian sekarang tersedia di Wilayah China (Beijing) dan China (Ningxia).	24 November 2020

BatchImportFindings sekarang dapat digunakan untuk memperbarui bidang tambahan	Sebelumnya, Anda tidak dapat menggunakan BatchImportFindings untuk memperbarui Confidence, Criticality, RelatedFindings, Severity, dan Types bidang. Sekarang, jika bidang ini belum diperbarui oleh BatchUpdateFindings, mereka dapat diperbarui oleh BatchImportFindings. Setelah diperbarui oleh BatchUpdateFindings, mereka tidak dapat diperbarui oleh BatchImportFindings.	24 November 2020
Security Hub kini terintegrasi dengan AWS Organizations	Pelanggan sekarang dapat mengelola akun anggota menggunakan konfigurasi akun Organizations mereka. Akun manajemen organisasi menunjuk akun administrator Security Hub, yang menentukan akun organisasi mana yang akan diaktifkan di Security Hub. Proses undangan manual masih dapat digunakan untuk akun yang bukan bagian dari organisasi.	23 November 2020
Menghapus format daftar temuan terpisah untuk kontrol volume tinggi	Daftar temuan untuk kontrol tidak lagi menggunakan format halaman Temuan ketika ada sejumlah besar temuan.	19 November 2020

Integrasi pihak ketiga yang baru dan diperbarui	Security Hub sekarang mendukung integrasi dengan cloudtamer.io, 3CoreSec, Prowler, dan Kubernete s Security. StackRox IBM QRadar tidak lagi mengirimkan temuan. Itu hanya menerima temuan.	30 Oktober 2020
Ditambahkan pilihan untuk men-download daftar temuan dari halaman rincian kontrol.	Pada halaman detail kontrol, opsi Unduh baru memungkin kan Anda mengunduh daftar temuan ke file.csv. Daftar yang diunduh menghorma ti filter apa pun yang ada dalam daftar. Jika Anda memilih temuan spesifik, maka daftar yang diunduh hanya mencakup temuan tersebut.	26 Oktober 2020
Ditambahkan pilihan untuk men-download daftar kontrol dari halaman rincian standar.	Pada halaman detail standar, opsi Unduh baru memungkin kan Anda mengunduh daftar kontrol ke file.csv. Daftar yang diunduh menghorma ti filter apa pun yang ada dalam daftar. Jika Anda memilih kontrol tertentu, maka daftar yang diunduh hanya menyertakan kontrol itu.	26 Oktober 2020

Integrasi mitra baru dan diperbarui	Security Hub sekarang terintegrasi dengan ThreatModeler. Memperbarui integrasi mitra berikut untuk mencerminkan nama produk baru mereka. Twistlock Enterprise Edition sekarang Palo Alto Networks - Prisma Cloud Compute. Juga dari Palo Alto Networks, Demisto sekarang Cortex XSOAR dan Redlock sekarang Prisma Cloud Enterprise.	23 Oktober 2020
Security Hub diluncurkan di China (Beijing) dan China (Ningxia)	Security Hub sekarang tersedia di Wilayah China (Beijing) dan China (Ningxia).	21 Oktober 2020
Format yang direvisi untuk atribut ASFF dan integrasi pihak ketiga	Daftar atribut ASFF dan integrasi mitra sekarang menggunakan format berbasis daftar, bukan tabel. Sintaks ASFF, atribut, dan tipe taksonomi sekarang dalam topik terpisah.	15 Oktober 2020
Halaman detail standar yang didesain ulang	Halaman detail standar untuk standar yang diaktifkan sekarang menampilkan daftar kontrol tab. Tab memfilter daftar kontrol berdasarkan status kontrol.	7 Oktober 2020
CloudWatch Acara yang diganti dengan EventBridge	Mengganti referensi ke CloudWatch Acara Amazon dengan Amazon EventBridge.	1 Oktober 2020

Integrasi baru dengan Blue Hexagon for AWS, Alcide KaUdit, dan Palo Alto Networks VM-series.	Security Hub sekarang terintegrasi dengan Blue Hexagon for AWS, Alcide Kaudit, dan Palo Alto Networks VM-series. Blue Hexagon for AWS dan Kaudit mengirimkan temuan ke Security Hub. Seri VM menerima temuan dari Security Hub.	30 September 2020
Objek detail sumber daya baru dan diperbarui di ASFF	Ditambahkan `Resources .Details` objek baru untuk `AwsApiGat ewayRestApi` `AwsApiGat ewayStage` ,,`AwsApiGat ewayV2Api` ,`AwsApiGat ewayV2Stage` ,`AwsCertif icateManagerCertif icate` ,`AwsElbLoa dBalancer` ,`AwsIamGro up` , dan`AwsRedshi ftCluster` . Menambahk an detail ke`AwsCloudF rontDistribution` , `AwsIamRole` dan `AwsIamAccessKey` objek.	30 September 2020
`ResourceRole` Atribut baru untuk sumber daya di ASFF untuk melacak apakah sumber daya adalah aktor atau target.	`ResourceRole` Atribut untuk sumber daya menunjukkan apakah sumber daya adalah target dari aktivitas pencarian atau pelaku aktivitas pencarian . Nilai yang valid adalah `ACTOR` dan `TARGET`.	30 September 2020

Menambahkan AWS Systems Manager Patch Manager ke integrasi AWS layanan yang tersedia	AWS Systems Manager Patch Manager sekarang terintegrasi dengan Security Hub. Patch Manager mengirimkan temuan ke Security Hub ketika instance dalam armada pelanggan tidak sesuai dengan standar kepatuhan patch mereka.	22 September 2020
Menambahkan kontrol baru ke standar Praktik Terbaik Keamanan AWS Dasar	Menambahkan kontrol baru untuk layanan berikut: Amazon EC2 (EC2.7 dan EC2.8), Amazon EMR (EMR.1), IAM (IAM.8), Amazon RDS (RDS.4 hingga RDS.8), Amazon S3 (S3.6), dan (.1 dan .2). AWS Secrets Manager SecretsManager SecretsManager	15 September 2020
Kunci konteks baru untuk kebijakan IAM untuk mengontrol akses ke bidang `BatchUpdateFindings`	Kebijakan IAM sekarang dapat dikonfigurasi untuk membatasi akses ke bidang dan nilai bidang saat menggunakan. `BatchUpdateFindings`	10 September 2020
Akses yang diperluas ke `BatchUpdateFindings` akun anggota	Secara default, akun anggota sekarang memiliki akses yang `BatchUpdateFindings` sama dengan akun administrator.	10 September 2020

Kontrol baru untuk AWS KMS Standar Praktik Terbaik Keamanan Dasar	Menambahkan dua kontrol baru (KMS.1 dan KMS.2) ke Standar Praktik Terbaik Keamanan Dasar. Kontrol baru memeriksa apakah kebijakan IAM membatasi akses ke tindakan AWS KMS dekripsi.	9 September 2020
Menghapus temuan tingkat akun untuk kontrol	Security Hub tidak lagi menghasilkan temuan tingkat akun untuk kontrol. Hanya temuan tingkat sumber daya yang dihasilkan.	1 September 2020
PatchSummaryObjek baru di ASFF	Menambahkan `PatchSummary` objek ke ASFF. `PatchSummary` Objek memberikan informasi tentang kepatuhan tambalan sumber daya relatif terhadap standar kepatuhan yang dipilih.	1 September 2020
Halaman detail kontrol yang didesain ulang	Halaman detail untuk kontrol didesain ulang. Daftar pencarian kontrol menyediakan tab untuk memungkinkan Anda memfilter daftar dengan cepat berdasarkan status kepatuhan. Anda juga dapat dengan cepat melihat temuan yang ditekan. Setiap entri menyediakan akses ke detail tambahan tentang sumber daya penemuan, AWS Config aturan, dan catatan pencarian.	28 Agustus 2020

Opsi filter baru untuk temuan	Untuk menemukan filter, Anda dapat menggunakan filter is not untuk menemukan temuan yang nilai bidangnya tidak sama dengan nilai filter. Anda dapat menggunak an tidak dimulai dengan untuk menemukan temuan yang nilai bidangnya tidak dimulai dengan nilai filter yang ditentukan.	28 Agustus 2020
Objek detail sumber daya baru di ASFF	Menambahkan `Resources .Details` objek baru untuk jenis sumber daya berikut: `AwsDynamo DbTable AwsEc2Eip ,AwsIamPol icy ,AwsIamUse r ,AwsRdsDbC luster ,AwsRdsDbC lusterSna pshot ,AwsRdsDbS napshot , AwsSecret sManagerSecret`	18 Agustus 2020
Integrasi baru dengan RSA Archer	Security Hub sekarang terintegrasi dengan RSA Archer. RSA Archer menerima temuan dari Security Hub.	18 Agustus 2020
Bidang Deskripsi Baru untuk AwsKmsKey	Menambahkan `Descripti on` bidang ke `AwsKmsKey` objek di bawah`Resources .Details` .	18 Agustus 2020

Menambahkan bidang ke AwsRdsDbInstance	Menambahkan beberapa atribut ke `AwsRdsDbInstance` objek di bawah`Resources.Details`.	18 Agustus 2020
Memperbarui cara Security Hub menentukan status keseluruhan kontrol	Untuk kontrol yang tidak memiliki temuan, statusnya adalah No data, bukan Unknown. Status kontrol mencakup temuan tingkat akun dan tingkat sumber daya. Status kontrol tidak menggunakan status alur kerja temuan, kecuali untuk mengabaikan temuan yang ditekan.	13 Agustus 2020
Memperbarui cara Security Hub menghitung skor keamanan untuk standar	Saat menghitung skor keamanan untuk standar, Security Hub sekarang mengabaikan kontrol dengan status No Data. Skor keamanan adalah proporsi kontrol yang diteruskan ke kontrol yang diaktifkan, tidak termasuk kontrol tanpa data.	13 Agustus 2020
Opsi baru untuk mengaktifkan kontrol baru secara otomatis dalam standar yang diaktifkan	Menambahkan opsi Pengaturan untuk secara otomatis mengaktifkan kontrol baru dalam standar yang diaktifkan. Anda juga dapat menggunakan operasi `UpdateSecurityHubConfiguration` API untuk mengonfigurasi opsi ini.	31 Juli 2020

Kontrol baru untuk standar Standar Keamanan Data Industri Kartu Pembayaran (PCI DSS)	Menambahkan kontrol baru ke standar PCI DSS. Pengidentifikasi kontrol baru adalah PCI.DMS.1, PCI.EC2.5, PCI.EC2.6, PCI.ELBV2.1, PCI. GuardDuty.1, PCI.IAM.7, PCI.IAM.8, PCI.S3.5, PCI.S3.6, PCI. SageMaker.1, PCI.SSM.2, dan PCI.SSM.3.	29 Juli 2020
Kontrol baru dan diperbarui untuk standar Praktik Terbaik Keamanan Dasar	Menambahkan kontrol baru ke standar Praktik Terbaik Keamanan Dasar. Pengidentifikasi kontrol baru adalah .1, AutoScaling DMS.1, EC2.4, EC2.6, S3.5, dan SSM.3. Memperbarui judul ACM.1 dan mengubah nilai `daysToExpiration` parameter menjadi 30.	29 Juli 2020
`Vulnerabilities` Objek baru di ASFF	Menambahkan `Vulnerabilities` objek, yang memberikan informasi tentang kerentanan yang terkait dengan temuan.	1 Juli 2020
`Resource.Details` Objek baru di ASFF untuk grup Auto Scaling, volume EC2, dan VPC EC2	Menambahkan`AwsAutoScalingAutoScalingGroup` ,`AWSEc2Volume` , dan `AwsEc2Vpc` objek ke`Resource.Details` .	1 Juli 2020
`NetworkPath` Objek baru di ASFF	Ditambahkan `NetworkPath` objek, yang memberikan informasi tentang jalur jaringan yang terkait dengan temuan.	1 Juli 2020

Secara otomatis menyelesaikan temuan kapan `Compliance.Status` `PASSED`	Untuk temuan dari kontrol, jika `Compliance.Status` ada`PASSED`, maka Security Hub secara otomatis disetel `Workflow.Status` ke`RESOLVED`.	24 Juni 2020
AWS Command Line Interface contoh	Ditambahkan AWS CLI sintaks dan contoh untuk beberapa tugas Security Hub. Termasuk mengaktifkan Security Hub, mengelola wawasan, mengelola standar dan kontrol, mengelola integrasi produk, dan menonaktifkan Security Hub.	24 Juni 2020
`Severity.Original` Atribut baru di ASFF	Menambahkan `Severity.Original` atribut, yang merupakan tingkat keparahan asli dari penyedia temuan. Ini menggantikan atribut usang`Severity.Product` .	20 Mei 2020
`Compliance.StatusReasons` Objek baru di ASFF untuk detail tentang status kontrol	Ditambahkan `Compliance.StatusReasons` objek, yang menyediakan konteks tambahan untuk status kontrol saat ini.	20 Mei 2020

Standar Praktik Terbaik Keamanan AWS Dasar Baru	Menambahkan standar Praktik Terbaik Keamanan AWS Dasar yang baru, yang merupakan serangkaian kontrol yang mendeteksi kapan akun dan sumber daya yang Anda gunakan menyimpang dari praktik terbaik keamanan.	22 April 2020
Opsi konsol baru untuk memperbarui status alur kerja untuk temuan	Menambahkan informasi untuk menggunakan konsol Security Hub atau API untuk menyetel status alur kerja untuk temuan.	16 April 2020
`BatchUpdateFindings` API baru untuk pembaruan pelanggan terhadap temuan	Menambahkan informasi tentang penggunaan `BatchUpdateFindings` untuk memperbarui informasi yang terkait dengan proses investigasi temuan. `BatchUpdateFindings` menggantikan `UpdateFindings`, yang sudah usang.	16 April 2020

Pembaruan untuk AWS Security Finding Format (ASFF)	Menambahkan beberapa jenis sumber daya baru. Menambahkan `Label` atribut baru ke `Severity` objek. `Label`dimaksudkan untuk menggantikan `Normalized` bidang. Menambahkan `Workflow` objek baru untuk melacak proses investigasi terhadap sebuah temuan. `Workflow`berisi `Status` atribut, yang menggantikan `Workflowstate` atribut yang ada.	12 Maret 2020
Pembaruan ke halaman Integrasi	Diperbarui untuk mencerminkan perubahan pada halaman Integrasi. Untuk setiap integrasi, halaman sekarang menunjukkan kategori integrasi dan apakah setiap integrasi mengirimkan temuan ke atau menerima temuan dari Security Hub. Ini juga menyediakan langkah-langkah spesifik yang diperlukan untuk mengaktifkan setiap integrasi.	26 Februari 2020
Integrasi produk pihak ketiga yang baru	Menambahkan integrasi produk baru berikut: Cloud Custodian, FireEye Helix, Forcepoint CASB, Forcepoint DLP, Forcepoint NGFW, Rackspace Cloud Native Security, dan Vectra.ai Cognito Detect.	Februari 21, 2020

Standar keamanan baru untuk Standar Keamanan Data Industri Kartu Pembayaran (PCI DSS)	Menambahkan standar keamanan Security Hub untuk Payment Card Industry Data Security Standard (PCI DSS). Ketika standar ini diaktifkan, Security Hub melakukan pemeriksaan otomatis terhadap kontrol yang terkait dengan persyaratan PCI DSS.	13 Februari 2020
Pembaruan untuk AWS Security Finding Format (ASFF)	Menambahkan bidang untuk persyaratan terkait untuk kontrol standar. Menambahkan jenis sumber daya baru dan detail sumber daya baru. ASFF juga sekarang memungkinkan Anda menyediakan hingga 32 sumber daya.	5 Februari 2020
Opsi baru untuk menonaktifkan kontrol standar keamanan individu	Menambahkan informasi tentang cara mengontrol apakah setiap kontrol standar keamanan individu diaktifkan.	15 Januari 2020
Pembaruan Terminologi dan Konsep	Memperbarui beberapa deskripsi dan menambahkan istilah baru ke Terminologi dan Konsep.	September 21, 2019
AWS Rilis ketersediaan umum Security Hub	Pembaruan konten untuk mencerminkan peningkatan yang dilakukan pada Security Hub selama periode pratinjau.	25 Juni 2019

Menambahkan langkah-langkah remediasi untuk pemeriksaan CIS AWS Foundations	Menambahkan langkah-langkah remediasi ke Standar Keamanan yang Didukung di AWS Security Hub.	April 15, 2019
Pratinjau rilis AWS Security Hub	Menerbitkan versi rilis pratinjau Panduan Pengguna AWS Security Hub.	November 18, 2018

Terjemahan disediakan oleh mesin penerjemah. Jika konten terjemahan yang diberikan bertentangan dengan versi bahasa Inggris aslinya, utamakan versi bahasa Inggris.