Panduan Integrasi Mitra

AWS Security Hub CSPM

AWS Security Hub CSPM: Panduan Integrasi Mitra

Table of Contents

Ikhtisar integrasi pihak ketiga dengan AWS Security Hub CSPM

Panduan ini ditujukan untuk AWS Mitra Jaringan Mitra (APN) yang ingin membuat integrasi denganAWS Security Hub CSPM.

Sebagai Mitra APN, Anda dapat berintegrasi dengan Security Hub CSPM dalam satu atau beberapa cara berikut.

- Kirim temuan ke Security Hub CSPM
- Mengkonsumsi temuan dari Security Hub CSPM
- Keduanya mengirimkan temuan ke dan mengkonsumsi temuan dari Security Hub CSPM
- Gunakan Security Hub CSPM sebagai pusat penawaran Managed Security Service Provider (MSSP)
- Konsultasikan dengan AWS pelanggan tentang cara menyebarkan dan menggunakan Security Hub CSPM

Panduan orientasi ini terutama berfokus pada mitra yang mengirimkan temuan ke Security Hub CSPM.

Topik

Mengapa berintegrasi denganAWS Security Hub CSPM?

AWS Security Hub CSPMmemberikan pandangan komprehensif tentang peringatan keamanan prioritas tinggi dan status keamanan di seluruh akun CSPM Security Hub. Security Hub CSPM memungkinkan mitra seperti Anda untuk mengirim temuan keamanan ke Security Hub CSPM untuk memberi pelanggan Anda wawasan tentang temuan keamanan yang Anda hasilkan.

Integrasi dengan Security Hub CSPM dapat menambah nilai dengan cara berikut.

- Memuaskan pelanggan Anda yang telah meminta integrasi CSPM Security Hub
- Memberikan pelanggan Anda satu pandangan tentang temuan terkait AWS keamanan mereka
- Memungkinkan pelanggan baru menemukan solusi Anda ketika mereka mencari mitra yang memberikan temuan terkait dengan jenis peristiwa keamanan tertentu

Sebelum Anda membangun integrasi dengan Security Hub CSPM, periksa alasan integrasi Anda. Integrasi lebih mungkin berhasil jika pelanggan Anda menginginkan integrasi CSPM Security Hub dengan produk Anda. Anda dapat membangun integrasi murni untuk alasan pemasaran atau untuk mendapatkan pelanggan baru. Namun, jika Anda membangun integrasi tanpa masukan pelanggan saat ini dan tidak mempertimbangkan kebutuhan pelanggan Anda, integrasi mungkin tidak menghasilkan hasil yang diharapkan.

Bersiap untuk mengirim temuan ke AWS Security Hub CSPM

Sebagai Mitra APN, Anda tidak dapat mengirim informasi ke Security Hub CSPM untuk pelanggan Anda sampai tim CSPM Security Hub memungkinkan Anda sebagai penyedia pencarian. Agar diaktifkan sebagai penyedia pencarian, Anda harus menyelesaikan langkah-langkah orientasi berikut. Melakukannya memastikan pengalaman positif Security Hub CSPM untuk Anda dan pelanggan Anda.

Saat Anda menyelesaikan langkah-langkah orientasi, pastikan untuk mengikuti pedoman dithe section called “Prinsip untuk membuat dan memperbarui temuan”,the section called “Pedoman pemetaan ASFF”, danthe section called “Pedoman untuk menggunakan `BatchImportFindings` API”.

1. Petakan temuan keamanan Anda ke AWS Security Finding Format (ASFF).
2. Bangun arsitektur integrasi Anda untuk mendorong temuan ke titik akhir CSPM Regional Security Hub yang benar. Untuk melakukan ini, Anda menentukan apakah Anda akan mengirim temuan dari AWS akun Anda sendiri atau dari dalam akun pelanggan Anda.
3. Mintalah pelanggan Anda berlangganan produk ke akun mereka. Untuk melakukan ini, mereka dapat menggunakan konsol atau operasi `EnableImportFindingsForProduct`API. Lihat Mengelola integrasi produk di Panduan AWS Security Hub Pengguna.

   Anda juga dapat berlangganan produk untuk mereka. Untuk melakukan ini, Anda menggunakan peran lintas akun untuk mengakses operasi `EnableImportFindingsForProduct`API atas nama pelanggan.

Langkah ini menetapkan kebijakan sumber daya yang diperlukan untuk menerima temuan dari produk tersebut untuk akun tersebut.

Posting blog berikut membahas beberapa integrasi mitra yang ada dengan Security Hub CSPM.

- Mengumumkan Integrasi Cloud Custodian dengan AWS Security Hub CSPM
- Gunakan AWS Fargate dan Prowler untuk mengirim temuan konfigurasi keamanan tentang AWS layanan ke Security Hub CSPM
- Cara mengimpor evaluasi AWS Config aturan sebagai temuan di Security Hub CSPM

Mempersiapkan untuk menerima temuan dari AWS Security Hub CSPM

Untuk menerima temuan dariAWS Security Hub CSPM, gunakan salah satu opsi berikut:

- Mintalah pelanggan Anda secara otomatis mengirim semua temuan ke CloudWatch Acara. Pelanggan dapat membuat aturan CloudWatch acara khusus untuk mengirim temuan ke target tertentu, seperti ember SIEM atau S3.
- Mintalah pelanggan Anda memilih temuan atau kelompok temuan tertentu dari dalam konsol CSPM Security Hub dan kemudian mengambil tindakan terhadapnya.

Misalnya, pelanggan Anda dapat mengirim temuan ke SIEM, sistem tiket, platform obrolan, atau alur kerja remediasi. Ini akan menjadi bagian dari alur kerja triase peringatan yang dilakukan pelanggan dalam Security Hub CSPM.

Ini disebut tindakan khusus. Ketika pengguna mengambil tindakan kustom, sebuah CloudWatch peristiwa dibuat untuk temuan spesifik tersebut. Sebagai mitra, Anda dapat memanfaatkan kemampuan ini dan membangun aturan atau target CloudWatch acara untuk digunakan pelanggan sebagai bagian dari tindakan khusus. Perhatikan bahwa kemampuan ini tidak secara otomatis mengirim semua temuan dari jenis atau kelas tertentu ke CloudWatch Acara. Fitur ini bagi pengguna untuk mengambil tindakan atas temuan tertentu.

Posting blog berikut menguraikan solusi yang menggunakan integrasi dengan Security Hub CSPM dan CloudWatch Events untuk tindakan kustom.

- Cara Mengintegrasikan Tindakan AWS Security Hub CSPM Kustom dengan PagerDuty

- Cara Mengaktifkan Tindakan Kustom di AWS Security Hub CSPM
- Cara mengimpor evaluasi AWS Config aturan sebagai temuan di Security Hub CSPM

Sumber daya untuk belajar tentang AWS Security Hub CSPM

Materi berikut dapat membantu Anda untuk lebih memahami AWS Security Hub CSPM solusi dan bagaimana AWS pelanggan dapat menggunakan layanan ini.

- Pengantar AWS Security Hub CSPM video
- Panduan Pengguna Security Hub
- Referensi API Security Hub
- Webinar orientasi

Kami juga mendorong Anda untuk mengaktifkan Security Hub CSPM di salah satu AWS akun Anda dan mendapatkan pengalaman langsung dengan layanan ini.

Prasyarat mitra

Sebelum Anda dapat memulai integrasi denganAWS Security Hub CSPM, Anda harus memenuhi salah satu kriteria berikut:

- Anda adalah AWS Select Tier Partner atau lebih tinggi.
- Anda telah bergabung dengan Jalur Mitra AWS ISV, dan produk yang Anda gunakan untuk integrasi CSPM Security Hub telah menyelesaikan AWSFoundational Technical Review (FTR). Produk tersebut kemudian diberikan lencana “Ditinjau olehAWS”.

Anda juga harus memiliki perjanjian kerahasiaan timbal balik di tempat dengan. AWS

Kasus penggunaan integrasi dan izin yang diperlukan

AWS Security Hub CSPM memungkinkan AWS pelanggan untuk menerima temuan dari APN Partners. Produk mitra dapat berjalan baik di dalam atau di luar AWS akun pelanggan. Konfigurasi izin di akun pelanggan berbeda berdasarkan model yang digunakan produk mitra.

Di Security Hub CSPM, pelanggan selalu mengontrol mitra mana yang dapat mengirimkan temuan ke akun pelanggan. Pelanggan dapat mencabut izin dari mitra kapan saja.

Untuk memungkinkan mitra mengirimkan temuan keamanan ke akun mereka, pelanggan terlebih dahulu berlangganan produk mitra di Security Hub CSPM. Langkah berlangganan diperlukan untuk semua kasus penggunaan yang diuraikan di bawah ini. Untuk detail tentang cara pelanggan mengelola integrasi produk, lihat Mengelola integrasi produk di AWS Security Hub Panduan Pengguna.

Setelah pelanggan berlangganan produk mitra, Security Hub CSPM secara otomatis membuat kebijakan sumber daya terkelola. Kebijakan ini memberikan izin kepada produk mitra untuk menggunakan operasi `BatchImportFindings`API untuk mengirimkan temuan ke Security Hub CSPM untuk akun pelanggan.

Berikut adalah kasus umum untuk produk mitra yang terintegrasi dengan Security Hub CSPM. Informasi tersebut mencakup izin tambahan yang diperlukan untuk setiap kasus penggunaan.

Mitra yang dihosting: temuan dikirim dari akun mitra

Kasus penggunaan ini mencakup mitra yang meng-host produk di AWS akun mereka sendiri. Untuk mengirim temuan keamanan bagi AWS pelanggan, mitra memanggil operasi `BatchImportFindings`API dari akun produk mitra.

Untuk kasus penggunaan ini, akun pelanggan hanya memerlukan izin yang ditetapkan saat pelanggan berlangganan produk mitra.

Di akun mitra, prinsipal IAM yang memanggil operasi `BatchImportFindings`API harus memiliki kebijakan IAM yang memungkinkan prinsipal untuk memanggil. `BatchImportFindings`

Memungkinkan produk mitra untuk mengirimkan temuan ke pelanggan di Security Hub CSPM adalah proses dua langkah:

1. Pelanggan membuat langganan ke produk mitra di Security Hub CSPM.
2. Security Hub CSPM menghasilkan kebijakan sumber daya terkelola yang benar dengan konfirmasi pelanggan.

Untuk mengirimkan temuan keamanan yang terkait dengan akun pelanggan, produk mitra menggunakan kredensialnya sendiri untuk memanggil operasi `BatchImportFindings`API.

Berikut adalah contoh kebijakan IAM yang memberikan izin CSPM Security Hub kepada prinsipal di akun mitra.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "securityhub:BatchImportFindings",
            "Resource": "arn:aws:securityhub:us-west-1:*:product-subscription/
company-name/product-name"
        }
    ]
}
```

Mitra yang dihosting: temuan dikirim dari akun pelanggan

Kasus penggunaan ini mencakup mitra yang meng-host produk di AWS akun mereka sendiri, tetapi menggunakan peran lintas akun untuk mengakses akun pelanggan. Mereka memanggil operasi `BatchImportFindings`API dari akun pelanggan.

Untuk kasus penggunaan ini, untuk memanggil operasi `BatchImportFindings`API, akun mitra mengasumsikan peran IAM yang dikelola pelanggan dalam akun pelanggan.

Panggilan ini dilakukan dari akun pelanggan. Oleh karena itu, kebijakan sumber daya terkelola harus memungkinkan ARN produk untuk akun produk mitra untuk digunakan dalam panggilan. Kebijakan sumber daya terkelola CSPM Security Hub memberikan izin untuk akun produk mitra dan ARN produk mitra. Produk ARN adalah pengenal unik mitra sebagai penyedia. Karena panggilan tidak

berasal dari akun produk mitra, pelanggan harus secara eksplisit memberikan izin kepada produk mitra untuk mengirimkan temuan ke Security Hub CSPM.

Praktik terbaik untuk peran lintas akun antara akun mitra dan pelanggan adalah dengan menggunakan pengenal eksternal yang disediakan mitra. Pengenal eksternal ini merupakan bagian dari definisi kebijakan lintas akun di akun pelanggan. Mitra harus memberikan pengenal ketika mengambil peran. Pengenal eksternal menyediakan lapisan keamanan tambahan saat memberikan akses AWS akun ke mitra. Pengidentifikasi unik memastikan bahwa mitra menggunakan akun pelanggan yang benar.

Memungkinkan produk mitra untuk mengirimkan temuan ke pelanggan di Security Hub CSPM dengan peran lintas akun terjadi dalam empat langkah:

1. Pelanggan, atau mitra yang menggunakan peran lintas akun yang bekerja atas nama pelanggan, memulai langganan produk di Security Hub CSPM.
2. Security Hub CSPM menghasilkan kebijakan sumber daya terkelola yang benar dengan konfirmasi pelanggan.
3. Pelanggan mengonfigurasi peran lintas akun baik secara manual atau menggunakan. CloudFormation Untuk informasi tentang peran lintas akun, lihat Menyediakan akses ke AWS akun yang dimiliki oleh pihak ketiga dalam Panduan Pengguna IAM.
4. Produk menyimpan peran pelanggan dan ID eksternal dengan aman.

Selanjutnya, produk mengirimkan temuan ke Security Hub CSPM:

1. Produk memanggil AWS Security Token Service (AWS STS) untuk mengambil peran pelanggan.
2. Produk memanggil operasi `BatchImportFindings`API pada Security Hub CSPM dengan kredenal sementara peran yang diasumsikan.

Berikut adalah contoh kebijakan IAM yang memberikan izin CSPM Security Hub yang diperlukan untuk peran lintas akun mitra.

JSON

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

```
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "securityhub:BatchImportFindings",
            "Resource": "arn:aws:securityhub:us-west-1:111122223333:product-
subscription/company-name/product-name"
        }
    ]
}
```

`Resource`Bagian kebijakan mengidentifikasi langganan produk tertentu. Ini memastikan bahwa mitra hanya dapat mengirimkan temuan untuk produk mitra yang pelanggan berlangganan.

Pelanggan di-host: temuan dikirim dari akun pelanggan

Kasus penggunaan ini mencakup mitra yang memiliki produk yang digunakan di AWS akun pelanggan. `BatchImportFindings`API dipanggil dari solusi yang berjalan di akun pelanggan.

Untuk kasus penggunaan ini, produk mitra harus diberikan izin tambahan untuk memanggil `BatchImportFindings`API. Bagaimana izin ini diberikan berbeda berdasarkan solusi mitra dan bagaimana hal itu dikonfigurasi di akun pelanggan.

Contoh dari pendekatan ini adalah produk mitra yang berjalan pada instans EC2 di akun pelanggan. Instans EC2 ini harus memiliki peran instans EC2 yang melekat padanya yang memberikan instance itu kemampuan untuk memanggil operasi API. `BatchImportFindings` Hal ini memungkinkan instans EC2 untuk mengirim temuan keamanan ke akun pelanggan.

Kasus penggunaan ini secara fungsional setara dengan skenario di mana pelanggan memuat temuan ke akun mereka untuk produk yang mereka miliki.

Pelanggan memungkinkan produk mitra untuk mengirimkan temuan dari akun pelanggan ke pelanggan di Security Hub CSPM:

1. Pelanggan menyebarkan produk mitra ke AWS akun mereka secara manual menggunakan CloudFormation, atau alat penyebaran lainnya.
2. Pelanggan mendefinisikan kebijakan IAM yang diperlukan untuk produk mitra untuk digunakan ketika mengirimkan temuan ke Security Hub CSPM.
3. Pelanggan melampirkan kebijakan ke komponen yang diperlukan dari produk mitra, seperti instans EC2, wadah, atau fungsi Lambda.

Sekarang produk dapat mengirimkan temuan ke Security Hub CSPM:

1. Produk mitra menggunakan AWS SDK atau AWS CLI untuk memanggil operasi `BatchImportFindings`API di Security Hub CSPM. Itu membuat panggilan dari komponen di akun pelanggan di mana kebijakan dilampirkan.
2. Selama panggilan API, kredensi sementara yang diperlukan dihasilkan untuk memungkinkan `BatchImportFindings`panggilan berhasil.

Berikut adalah contoh kebijakan IAM yang memberikan izin CSPM Security Hub yang diperlukan untuk produk mitra di akun pelanggan.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "securityhub:BatchImportFindings",
            "Resource": "arn:aws:securityhub:us-west-2:111122223333:product-
subscription/company-name/product-name"
        }
    ]
}
```

Proses orientasi mitra

Sebagai mitra, Anda dapat mengharapkan untuk menyelesaikan beberapa langkah tingkat tinggi sebagai bagian dari proses orientasi Anda. Anda harus menyelesaikan langkah-langkah ini sebelum Anda dapat mengirim temuan keamanan keAWS Security Hub CSPM.

1. Anda memulai keterlibatan dengan tim Mitra APN atau tim CSPM Security Hub dan menyatakan minat untuk menjadi mitra dengan Security Hub CSPM. Anda mengidentifikasi alamat email yang akan ditambahkan ke saluran komunikasi CSPM Security Hub.
2. AWSmemberi Anda materi orientasi mitra CSPM Security Hub.
3. Anda diundang ke saluran Slack mitra Security Hub CSPM, di mana Anda dapat mengajukan pertanyaan terkait integrasi Anda.
4. Anda menyediakan draft manifes integrasi produk kepada kontak APN Partner untuk ditinjau.

   Manifes integrasi produk berisi informasi yang digunakan untuk membuat produk mitra Amazon Resource Name (ARN) untuk integrasi dengan. AWS Security Hub CSPM

   Ini memberi tim CSPM Security Hub informasi yang muncul di halaman penyedia mitra di konsol CSPM Security Hub. Ini juga digunakan untuk mengusulkan wawasan terkelola baru yang terkait dengan integrasi untuk ditambahkan ke perpustakaan wawasan CSPM Security Hub.

   Versi awal manifes integrasi produk ini tidak harus memiliki detail lengkap. Tetapi setidaknya harus berisi kasus penggunaan dan informasi kumpulan data.

   Untuk detail tentang manifes dan informasi yang diperlukan, lihatManifes integrasi produk.
5. Tim CSPM Security Hub memberi Anda ARN produk untuk produk Anda. Anda menggunakan ARN untuk mengirim temuan ke Security Hub CSPM.
6. Anda membangun integrasi untuk mengirim temuan ke atau menerima temuan dari Security Hub CSPM.

   Memetakan temuan ke ASFF

   Untuk mengirim temuan ke Security Hub CSPM, Anda harus memetakan temuan Anda ke AWS Security Finding Format (ASFF).

   ASFF memberikan deskripsi yang konsisten tentang temuan yang dapat dibagikan di antara layanan AWS keamanan, mitra, dan sistem keamanan pelanggan. Ini mengurangi upaya integrasi, mendorong bahasa umum, dan menyediakan cetak biru bagi pelaksana.

ASFF adalah format protokol kawat yang diperlukan untuk digunakan untuk mengirim temuan keAWS Security Hub CSPM. Temuan direpresentasikan sebagai dokumen JSON yang mematuhi Skema JSON ASFF dan RFC-7493 Format Pesan I-JSON. Untuk detail tentang skema ASFF, lihat AWSSecurity Finding Format (ASFF) di Panduan Pengguna. AWS Security Hub

Lihat the section called “Pedoman pemetaan ASFF”.

Membangun dan menguji integrasi

Anda dapat menyelesaikan semua pengujian untuk integrasi Anda menggunakan AWS akun yang Anda miliki. Melakukan hal itu memberi Anda visibilitas penuh tentang bagaimana temuan muncul di Security Hub CSPM. Ini juga membantu Anda memahami pengalaman pelanggan dengan temuan keamanan Anda.

Anda menggunakan operasi `BatchImportFindings`API untuk mengirim temuan baru dan terbaru ke Security Hub CSPM.

Selama membangun integrasi CSPM Security Hub, AWS mendorong Anda untuk terus menginformasikan kontak Mitra APN Anda tentang kemajuan integrasi Anda. Anda juga dapat meminta kontak Mitra APN Anda untuk bantuan terkait pertanyaan integrasi.

Lihat the section called “Pedoman untuk menggunakan `BatchImportFindings` API”.

7. Anda mendemonstrasikan integrasi ke tim produk CSPM Security Hub. Integrasi ini harus ditunjukkan menggunakan akun yang dimiliki tim CSPM Security Hub.

   Jika mereka merasa nyaman dengan integrasi, tim CSPM Security Hub memberikan persetujuan untuk bergerak maju untuk mendaftarkan Anda sebagai penyedia.

8. Anda memberikan AWS manifes akhir untuk ditinjau.
9. Tim CSPM Security Hub membuat integrasi penyedia di konsol CSPM Security Hub. Pelanggan kemudian dapat menemukan dan mengaktifkan integrasi.
10. (Opsional) Anda terlibat dalam upaya pemasaran tambahan untuk mempromosikan integrasi CSPM Security Hub Anda. Lihat Go-to-market kegiatan.

    Minimal, Security Hub CSPM merekomendasikan agar Anda menyediakan aset berikut.

    - Video demonstrasi (paling lama 3 menit) dari integrasi kerja. Video ini digunakan untuk tujuan pemasaran dan diposting ke AWS YouTube saluran.

- Diagram arsitektur satu-slide untuk ditambahkan ke dek slide panggilan pertama Security Hub CSPM.

Go-to-market kegiatan

Mitra juga dapat terlibat dalam kegiatan pemasaran opsional untuk membantu menjelaskan dan mempromosikan AWS Security Hub CSPM integrasi mereka.

Jika Anda ingin membuat konten pemasaran Anda sendiri yang terkait dengan Security Hub CSPM, sebelum Anda merilis konten, kirim draf ke manajer Partner APN Anda untuk ditinjau dan disetujui. Ini memastikan bahwa semua orang selaras dengan pesan.

AWSMitra Jaringan Mitra (APN) dapat menggunakan APN Partner Marketing Central dan program Market Development Funds (MDF) untuk membuat kampanye dan mendapatkan dukungan pendanaan. Untuk detail tentang program ini, hubungi manajer mitra Anda.

Entri di halaman mitra CSPM Security Hub

Setelah Anda disetujui sebagai mitra CSPM Security Hub, solusi Anda dapat ditampilkan di halaman AWS Security Hub CSPMmitra.

Untuk dicantumkan di halaman ini, berikan rincian berikut ke kontak Mitra APN Anda.
`<Ini bisa berupa manajer pengembangan mitra Anda (PDM), arsitek solusi mitra (PS`

- Penjelasan singkat tentang solusi Anda, integrasinya dengan Security Hub CSPM, dan nilai yang diberikan integrasi dengan Security Hub CSPM kepada pelanggan. Deskripsi ini terbatas pada 700 karakter termasuk spasi.
- URL ke halaman yang menjelaskan solusi Anda. Situs ini harus spesifik untuk AWS integrasi Anda dan lebih khusus lagi integrasi CSPM Security Hub Anda. Ini harus fokus pada pengalaman pelanggan dan nilai yang diterima pelanggan ketika mereka menggunakan integrasi.
- Salinan resolusi tinggi logo Anda yang berukuran 600 x 300 piksel. Untuk detail tentang persyaratan untuk logo ini, lihatthe section called “Logo untuk halaman mitra”.

Siaran pers

Sebagai mitra yang disetujui, Anda dapat secara opsional mempublikasikan siaran pers di situs web dan saluran hubungan masyarakat Anda. Siaran pers harus disetujui olehAWS.

Sebelum Anda mempublikasikan siaran pers, Anda harus mengirimkannya AWS untuk ditinjau oleh APN Partner Marketing, Security Hub CSPM leadership, dan AWS External Security Services (ESS). Siaran pers dapat mencakup kutipan yang diusulkan untuk VP ESS.

Untuk memulai proses ini, bekerja dengan PDM Anda. Kami memiliki Perjanjian Tingkat Layanan (SLA) 10 hari kerja untuk meninjau siaran pers.

AWSBlog Jaringan Mitra (APN)

Kami juga dapat membantu Anda memposting entri blog yang Anda penulis ke blog APN. Entri blog harus fokus pada cerita pelanggan dan kasus penggunaan. Itu tidak dapat diposisikan hanya di sekitar menjadi mitra peluncuran integrasi.

Jika Anda tertarik, hubungi PDM atau PSA Anda untuk memulai prosesnya. Blog APN dapat memakan waktu 8 minggu atau lebih untuk persetujuan akhir dan penerbitan.

Hal-hal penting yang perlu diketahui tentang blog APN

Saat Anda membuat posting blog, ingatlah hal-hal berikut.

Apa yang masuk ke posting blog?

- Posting mitra harus mendidik dan memberikan keahlian mendalam tentang topik yang relevan dengan AWS pelanggan.
- Panjang ideal tidak lebih dari 1.500 kata. Pembaca menghargai konten pendidikan yang mendalam yang mengajarkan mereka apa yang mungkin terjadiAWS.
- Konten harus asli ke blog APN. Jangan menggunakan kembali konten dari sumber seperti posting blog atau whitepaper yang ada.

Apa batasan lain untuk memposting ke blog APN?

- Hanya mitra tingkat Advanced atau Premier yang dapat memposting ke blog APN. Ada pengecualian untuk mitra Terpilih yang memiliki Penunjukan Program APN seperti Pengiriman Layanan.
- Setiap mitra dibatasi hingga tiga posting per tahun. Dengan puluhan ribu APN Partner, AWS harus adil dalam cakupannya.

Setiap pos harus memiliki sponsor teknis yang dapat memvalidasi solusi atau kasus penggunaan.

Berapa lama waktu yang dibutuhkan untuk mengedit posting blog sebelum diposting?

Setelah Anda mengirimkan draf penuh pertama dari posting blog, dibutuhkan empat hingga enam minggu untuk mengedit.

Mengapa menulis untuk blog APN?

Posting blog APN dapat memberikan manfaat berikut.

- Kredibilitas — Bagi Mitra APN, memiliki cerita yang diterbitkan oleh AWS dapat memengaruhi pelanggan secara global.
- Visibilitas — Blog APN adalah salah satu blog yang paling banyak dibaca AWS dengan 1,79 juta tampilan halaman pada tahun 2019, termasuk lalu lintas yang dipengaruhi.
- Bisnis — Postingan APN Partner memiliki tombol sambung yang dapat menghasilkan prospek melalui program APN Customer Engagements (ACE).

Jenis konten apa yang paling cocok?

Jenis konten berikut paling cocok untuk posting blog APN.

- Konten teknis adalah jenis cerita yang paling populer. Ini termasuk lampu sorot solusi dan informasi cara. Lebih dari 75% pembaca melihat konten teknis ini.
- Pelanggan menghargai cerita 200 tingkat atau di atas yang menunjukkan cara kerja sesuatu AWS atau bagaimana Mitra APN memecahkan masalah bisnis bagi pelanggan.
- Tulisan yang ditulis oleh pakar teknis atau ahli materi pelajaran berkinerja terbaik sejauh ini.

Lembar licin atau lembar pemasaran

Slick sheet adalah dokumen satu halaman yang menguraikan produk Anda, arsitektur integrasinya, dan kasus penggunaan pelanggan bersama.

Jika Anda membuat lembar apik untuk integrasi Anda, kirim salinannya ke tim CSPM Security Hub. Mereka akan menambahkannya ke halaman mitra.

Whitepaper atau ebook

Jika Anda membuat whitepaper atau ebook yang menguraikan produk Anda, arsitektur integrasinya, dan kasus penggunaan pelanggan bersama, kirim salinannya ke tim CSPM Security Hub. Mereka akan menambahkannya ke halaman mitra CSPM Security Hub.

Webinar

Jika Anda melakukan webinar tentang integrasi Anda, kirim rekaman webinar ke tim CSPM Security Hub. Tim akan menautkannya dari halaman mitra.

Tim juga dapat menyediakan ahli materi pelajaran CSPM Security Hub untuk berpartisipasi dalam webinar Anda.

Video Demo

Untuk tujuan pemasaran, Anda dapat menghasilkan video demo integrasi kerja. Posting video tersebut di akun platform video Anda, dan tim CSPM Security Hub akan menautkannya dari halaman mitra.

Manifes integrasi produk

Setiap mitra AWS Security Hub CSPM integrasi harus menyelesaikan manifes integrasi produk yang memberikan rincian yang diperlukan untuk integrasi yang diusulkan.

Tim CSPM Security Hub menggunakan informasi ini dalam beberapa cara:

- Untuk membuat daftar situs web Anda
- Untuk membuat kartu produk untuk konsol CSPM Security Hub
- Untuk memberi tahu tim produk tentang kasus penggunaan Anda.

Untuk mengevaluasi kualitas integrasi yang diusulkan dan informasi yang diberikan, tim CSPM Security Hub menggunakan. the section called “Daftar periksa kesiapan produk” Daftar periksa ini menentukan apakah integrasi Anda siap diluncurkan.

Semua informasi teknis yang Anda berikan juga harus tercermin dalam dokumentasi Anda.

Anda dapat mengunduh versi PDF dari manifes integrasi produk dari bagian Sumber daya di halaman AWS Security Hub CSPM mitra. Perhatikan bahwa halaman mitra tidak tersedia di Wilayah Tiongkok (Beijing) dan Tiongkok (Ningxia).

Daftar Isi

  - Tipe temuan
  - Hotline
  - Penemuan detak jantung
- AWS Security Hub CSPM informasi konsol
  - Informasi perusahaan
  - Informasi Produk

Kasus penggunaan dan informasi pemasaran

Kasus penggunaan berikut dapat membantu Anda mengonfigurasi AWS Security Hub CSPM untuk tujuan yang berbeda.

Menemukan penyedia dan kasus penggunaan konsumen

Diperlukan untuk vendor perangkat lunak independen (ISV).

Untuk menjelaskan kasus penggunaan Anda seputar integrasi Anda dengan AWS Security Hub CSPM, jawab pertanyaan-pertanyaan berikut. Jika Anda tidak berencana untuk mengirim atau menerima temuan, perhatikan bahwa di bagian ini dan kemudian lengkapi bagian berikutnya.

Informasi berikut harus tercermin dalam dokumentasi Anda.

- Apakah Anda akan mengirim temuan, menerima temuan, atau keduanya?
- Jika Anda berencana untuk mengirim temuan, jenis temuan apa yang akan Anda kirimkan? Apakah Anda akan mengirimkan semua temuan atau bagian tertentu dari temuan?
- Jika Anda berencana untuk menerima temuan, apa yang akan Anda lakukan dengan temuan tersebut? Jenis temuan apa yang akan Anda terima? Misalnya, apakah Anda akan menerima semua temuan, temuan dari jenis tertentu, atau hanya temuan spesifik yang dipilih pelanggan?
- Apakah Anda berencana untuk memperbarui temuan? Jika demikian, bidang mana yang akan Anda perbarui? Security Hub CSPM merekomendasikan agar Anda memperbarui temuan alih-alih selalu membuat yang baru. Memperbarui temuan yang ada membantu mengurangi kebisingan temuan bagi pelanggan.

  Untuk memperbarui temuan, Anda mengirim temuan dengan ID temuan yang ditetapkan ke temuan yang sudah Anda kirim.

Untuk mendapatkan umpan balik awal tentang kasus penggunaan dan kumpulan data Anda, hubungi tim APN Partner atau Security Hub CSPM.

Kasus penggunaan Mitra Konsultasi (CP)

Diperlukan jika Anda adalah Security Hub CSPM Consulting Partner.

Berikan dua kasus penggunaan pelanggan untuk pekerjaan Anda dengan Security Hub CSPM. Ini bisa menjadi kasus penggunaan pribadi. Tim CSPM Security Hub tidak mengiklankan mereka di mana pun. Mereka harus menggambarkan salah satu atau kedua tindakan berikut.

- Bagaimana Anda membantu pelanggan bootstrap Security Hub CSPM? Misalnya, sudahkah Anda membantu pelanggan menggunakan layanan profesional, modul Terraform, atau templat? CloudFormation
- Bagaimana Anda membantu pelanggan mengoperasionalkan dan memperluas CSPM Security Hub? Misalnya, sudahkah Anda menyediakan template respons atau remediasi, membangun integrasi khusus, atau menggunakan alat intelijen bisnis untuk menyiapkan dasbor eksekutif?

Set data

Diperlukan jika Anda mengirim temuan ke Security Hub CSPM.

Untuk temuan yang akan Anda kirimkan ke Security Hub CSPM, berikan informasi berikut.

- Temuan dalam format asli mereka, seperti JSON atau XML.
- Contoh bagaimana Anda akan mengonversi temuan ke AWS Security Finding Format (ASFF)

Beri tahu tim CSPM Security Hub jika Anda memerlukan pembaruan apa pun pada ASFF untuk mendukung integrasi Anda.

Arsitektur

Diperlukan jika Anda mengirim temuan ke atau menerima temuan dari Security Hub CSPM.

Jelaskan bagaimana Anda akan berintegrasi dengan Security Hub CSPM. Informasi ini juga harus tercermin dalam dokumentasi Anda.

Anda harus menyediakan diagram arsitektur. Saat menyiapkan diagram arsitektur Anda, pertimbangkan hal berikut:

- AWS Layanan apa, agen sistem operasi, dan sebagainya yang akan Anda gunakan?
- Jika Anda akan mengirimkan temuan ke Security Hub CSPM, apakah Anda akan mengirimkan temuan dari AWS akun pelanggan atau dari akun Anda sendiri? AWS
- Jika Anda akan menerima temuan, bagaimana Anda akan menggunakan integrasi CloudWatch Acara?
- Bagaimana Anda akan mengubah temuan menjadi ASFF?
- Bagaimana Anda akan mengumpulkan temuan, melacak status temuan, dan menghindari batas pelambatan?

Konfigurasi

Diperlukan jika Anda mengirim temuan ke atau menerima temuan dari Security Hub CSPM.

Jelaskan bagaimana pelanggan akan mengonfigurasi integrasi Anda dengan Security Hub.

Minimal, Anda harus menggunakan CloudFormation templat atau infrastruktur serupa seperti templat kode. Beberapa mitra telah menyediakan antarmuka pengguna untuk mendukung integrasi satu klik.

Konfigurasi harus memakan waktu tidak lebih dari 15 menit. Dokumentasi produk Anda juga harus memberikan panduan konfigurasi untuk integrasi Anda.

Temuan rata-rata per hari per pelanggan

Diperlukan jika Anda mengirim temuan ke Security Hub CSPM.

Berapa banyak pembaruan pencarian per bulan (rata-rata dan maksimum) yang Anda harapkan untuk dikirim ke Security Hub CSPM di seluruh basis pelanggan Anda? Perkiraan urutan besarnya dapat diterima.

Latensi

Diperlukan jika Anda mengirim temuan ke Security Hub CSPM.

Seberapa cepat Anda akan mengumpulkan dan mengirim temuan ke Security Hub CSPM? Dengan kata lain, apa latensi dari saat temuan dibuat di produk Anda hingga saat dikirim ke Security Hub CSPM?

Informasi ini harus tercermin dalam dokumentasi produk Anda untuk integrasi Anda. Ini adalah pertanyaan umum dari pelanggan.

Deskripsi perusahaan dan produk

Diperlukan untuk semua integrasi dengan Security Hub CSPM.

Jelaskan secara singkat perusahaan dan produk Anda, dengan penekanan khusus pada sifat integrasi CSPM Security Hub Anda. Kami menggunakan ini di halaman mitra CSPM Security Hub kami.

Jika Anda mengintegrasikan beberapa produk dengan Security Hub CSPM, Anda dapat memberikan deskripsi terpisah untuk setiap produk, tetapi kami akan menggabungkannya menjadi satu entri di halaman mitra.

Setiap deskripsi dapat tidak lebih dari 700 karakter dengan spasi.

Aset situs web mitra

Diperlukan untuk semua integrasi dengan Security Hub CSPM.

Minimal, Anda harus memberikan URL yang akan digunakan untuk hyperlink Pelajari Lebih Lanjut di halaman mitra CSPM Security Hub. Ini harus menjadi halaman arahan pemasaran yang menjelaskan integrasi antara produk Anda dan Security Hub CSPM.

Jika Anda mengintegrasikan beberapa produk dengan Security Hub CSPM, Anda dapat memiliki satu halaman arahan untuk mereka. Security Hub CSPM merekomendasikan agar halaman landing ini menyertakan tautan ke instruksi konfigurasi Anda.

Anda juga dapat memberikan tautan ke sumber daya lain seperti blog, webinar, video demo, atau whitepaper. Security Hub CSPM juga akan menautkan ke orang-orang dari halaman mitra mereka.

Logo untuk halaman mitra

Diperlukan untuk semua integrasi CSPM Security Hub.

Berikan URL ke logo untuk ditampilkan di halaman mitra CSPM Security Hub. Logo harus memenuhi kriteria berikut:

- Ukuran: 600 x 300 piksel
- Memangkas: kencang tanpa bantalan
- Latar Belakang: transparan
- Format: PNG

Logo untuk konsol CSPM Security Hub

Diperlukan untuk semua integrasi.

Berikan URLs logo mode terang dan mode gelap untuk ditampilkan di konsol CSPM Security Hub.

Logo harus memenuhi kriteria berikut:

- Format: SVG
- Ukuran: 175 x 40 piksel. Jika lebih besar, gambar harus menggunakan rasio itu.
- Memangkas: kencang tanpa bantalan
- Latar Belakang: transparan

Untuk panduan rinci untuk logo kecil, lihatthe section called “Pedoman untuk logo konsol”.

Tipe temuan

Diperlukan jika Anda mengirim temuan ke Security Hub CSPM.

Berikan tabel yang mendokumentasikan tipe temuan berformat ASFF yang Anda gunakan dan bagaimana mereka menyelaraskannya dengan tipe temuan asli Anda. Untuk detail tentang menemukan jenis di ASFF, lihat Jenis taksonomi untuk ASFF di Panduan Pengguna.AWS Security Hub

Kami menyarankan Anda juga menyertakan informasi ini dalam dokumentasi produk Anda.

Hotline

Diperlukan untuk semua integrasi dengan Security Hub CSPM.

Berikan alamat email dan nomor telepon atau nomor pager untuk titik kontak teknis. Security Hub CSPM akan berkomunikasi dengan kontak ini mengenai masalah teknis apa pun, seperti ketika integrasi tidak lagi berfungsi.

Juga berikan titik kontak 24/7 untuk masalah teknis tingkat keparahan tinggi.

Penemuan detak jantung

Direkomendasikan jika Anda mengirimkan temuan ke Security Hub CSPM.

Dapatkah Anda mengirim Security Hub CSPM sebuah “detak jantung” temuan setiap lima menit yang menunjukkan bahwa integrasi Anda dengan Security Hub CSPM berfungsi?

Jika Anda bisa, maka lakukan dengan menggunakan tipe temuan`Heartbeat`.

AWS Security Hub CSPM informasi konsol

Berikan teks JSON kepada AWS Security Hub CSPM tim yang berisi informasi berikut. Security Hub CSPM menggunakan informasi ini untuk membuat ARN produk Anda, menampilkan daftar penyedia di konsol, dan menyertakan wawasan terkelola yang Anda usulkan di pustaka wawasan CSPM Security Hub.

Informasi perusahaan

Informasi perusahaan memberikan informasi tentang perusahaan Anda. Inilah contohnya:

```
{
    "id": "example",
    "name": "Example Corp",
    "description": "Example Corp is a network security company that monitors your
 network for vulnerabilities.",
}
```

Informasi perusahaan berisi bidang-bidang berikut:

Bidang	Diperlukan	Deskripsi
`id`	Ya	Pengidentifikasi unik perusahaan. Pengident ifikasi perusahaan harus unik di seluruh perusahaan. Ini mungkin sama dengan atau mirip dengan`name`. Tipe: String Panjang minimum: 5 karakter Panjang maksimum: 24 karakter

Bidang	Diperlukan	Deskripsi
		Karakter yang diizinkan: huruf kecil, angka, dan tanda hubung Harus dimulai dengan huruf kecil. Harus diakhiri dengan huruf kecil atau angka.
`name`	Ya	Nama perusahaan penyedia akan ditampilkan di konsol CSPM Security Hub. Tipe: String Panjang maksimum: 16 karakter
`description`	Ya	Deskripsi perusahaan penyedia akan ditampilkan di konsol CSPM Security Hub. Tipe: String Panjang maksimum: 200 karakter

Informasi Produk

Bagian ini memberikan informasi tentang produk Anda. Inilah contohnya:

```
{
    "IntegrationTypes": ["SEND_FINDINGS_TO_SECURITY_HUB"],
    "id": "example-corp-network-defender",
    "regionsNotSupported": "us-west-1",
    "commercialAccountNumber": "111122223333",
    "govcloudAccountNumber": "444455556666",
    "chinaAccountNumber": "777788889999",
    "name": "Example Corp Product",
    "description": "Example Corp Product is a managed threat detection service.",
    "importType": "BATCH_IMPORT_FINDINGS_FROM_CUSTOMER_ACCOUNT",
    "category": "Intrusion Detection Systems (IDS)",
    "marketplaceUrl": "marketplace_url",
    "configurationUrl": "configuration_url"
}
```

Informasi produk berisi bidang-bidang berikut.

Bidang	Diperlukan	Deskripsi
`IntegrationType`	Ya	Menunjukkan apakah produk Anda mengirimk an temuan ke Security Hub CSPM, menerima temuan dari Security Hub CSPM, atau keduanya mengirim dan menerima temuan. Jika Anda adalah Mitra Konsultasi, biarkan bidang ini kosong. Jenis: Array string Nilai yang valid: `SEND_FINDINGS_TO_S ECURITY_HUB` | `RECEIVE_FINDINGS_F ROM_SECURITY_HUB`
`id`	Ya	Pengidentifikasi unik produk. Ini harus unik dalam sebuah perusahaan. Mereka tidak perlu unik di seluruh perusahaan. Ini mungkin sama atau mirip dengan`name`. Tipe: String Panjang minimum: 5 karakter Panjang maksimum: 24 karakter Karakter yang diizinkan: huruf kecil, angka, dan tanda hubung Harus dimulai dengan huruf kecil. Harus diakhiri dengan huruf kecil atau angka.
`regionsNotSupported`	Ya	Manakah dari AWS Wilayah berikut yang tidak Anda dukung? Dengan kata lain, di Wilayah mana Security Hub CSPM tidak menampilkan Anda sebagai opsi di halaman mitra kami di konsol CSPM Security Hub?

Bidang	Diperlukan	Deskripsi
		Tipe: String Berikan kode Region saja. Misalnya, `us-west-1` . Untuk daftar Wilayah, lihat Titik akhir Regional di. Referensi Umum AWS Kode Wilayah untuk AWS GovCloud (US) adalah `us-gov-west-1` (untuk AWS GovCloud (AS-Barat)) dan `us-gov-east-1` (untuk AWS GovCloud (AS-Timur)). Kode Wilayah untuk Wilayah Tiongkok `cn-north-1` adalah (untuk Tiongkok (Beijing)) `cn-northwest-1` dan (untuk Tiongkok (Ningxia)).

Bidang	Diperlukan	Deskripsi
`commercialAccountNumber`	Ya	Nomor AWS rekening utama untuk produk untuk AWS Daerah. Jika Anda mengirim temuan ke Security Hub CSPM, maka akun yang Anda berikan didasarkan pada dari mana Anda mengirim temuan tersebut. • Dari AWS akun Anda. Dalam hal ini, berikan nomor rekening yang Anda gunakan untuk mengirimkan temuan. • Dari AWS akun pelanggan. Dalam hal ini, Security Hub CSPM merekomendasikan agar Anda memberikan nomor akun utama yang Anda gunakan untuk menguji integrasi. Idealnya Anda akan menggunakan akun yang sama untuk semua produk Anda di semua Wilayah. Jika ini tidak memungkinkan, hubungi tim CSPM Security Hub. Jika Anda hanya menerima temuan dari Security Hub CSPM, nomor akun ini tidak diperlukan. Tipe: String

Bidang	Diperlukan	Deskripsi
`govcloudAccountNumber`	Tidak	Nomor AWS akun utama untuk produk untuk AWS GovCloud (US) Wilayah (jika produk Anda tersedia di AWS GovCloud (US)). Jika Anda mengirim temuan ke Security Hub CSPM, maka akun yang Anda berikan didasarkan pada dari mana Anda mengirim temuan tersebut. • Dari AWS akun Anda. Dalam hal ini, berikan nomor rekening yang Anda gunakan untuk mengirimkan temuan. • Dari AWS akun pelanggan. Dalam hal ini, Security Hub CSPM merekomendasikan agar Anda memberikan nomor akun utama yang Anda gunakan untuk menguji integrasi. Idealnya Anda menggunakan akun yang sama untuk semua produk Anda di semua AWS GovCloud (US) Wilayah. Jika ini tidak memungkinkan, hubungi tim CSPM Security Hub. Jika Anda hanya menerima temuan dari Security Hub CSPM, nomor akun ini tidak diperlukan. Tipe: String

Bidang	Diperlukan	Deskripsi
`chinaAccountNumber`	Tidak	Nomor AWS akun utama untuk produk untuk wilayah Tiongkok (jika produk Anda tersedia di wilayah Tiongkok). Jika Anda mengirim temuan ke Security Hub CSPM, maka akun yang Anda berikan didasarkan pada dari mana Anda mengirim temuan tersebut. • Dari AWS akun Anda. Dalam hal ini, berikan nomor rekening yang Anda gunakan untuk mengirimkan temuan. • Dari AWS akun pelanggan. Dalam hal ini, Security Hub CSPM merekomendasikan agar Anda memberikan nomor akun utama yang Anda gunakan untuk menguji integrasi produk. Idealnya Anda menggunakan akun yang sama untuk semua produk Anda di semua wilayah Tiongkok. Jika ini tidak memungkinkan, hubungi tim CSPM Security Hub. Jika Anda hanya menerima temuan dari Security Hub CSPM, ini bisa berupa akun apa pun yang Anda miliki di wilayah Tiongkok. Tipe: String
`name`	Ya	Nama produk penyedia untuk ditampilkan di konsol CSPM Security Hub. Tipe: String Panjang maksimum: 24 karakter

Bidang	Diperlukan	Deskripsi
`description`	Ya	Deskripsi produk penyedia untuk ditampilkan di konsol CSPM Security Hub. Tipe: String Panjang maksimum: 200 karakter
`importType`	Ya	Jenis kebijakan sumber daya untuk mitra. Selama proses orientasi mitra, Anda dapat menentukan salah satu kebijakan sumber daya berikut, atau Anda dapat menentukan`NEITHER`. • Dengan`BATCH_IMPORT_FINDINGS_FROM_PRODUCT_ACCOUNT`, Anda hanya dapat mengirim temuan ke Security Hub dari akun yang tercantum di ARN produk Anda. • Dengan`BATCH_IMPORT_FINDINGS_FROM_CUSTOMER_ACCOUNT`, Anda hanya dapat mengirim temuan dari akun pelanggan yang berlangganan kepada Anda. Tipe: String Nilai yang valid: `BATCH_IMPORT_FINDINGS_FROM_PRODUCT_ACCOUNT` | `BATCH_IMPORT_FINDINGS_FROM_CUSTOMER_ACCOUNT` | `NEITHER`

Bidang	Diperlukan	Deskripsi
`category`	Ya	Kategori yang menentukan produk Anda. Pilihan Anda ditampilkan di konsol CSPM Security Hub. Pilih hingga tiga kategori. Pilihan kustom tidak diperbolehkan. Jika Anda merasa kategori Anda hilang, hubungi tim CSPM Security Hub. Jenis: Array Kategori yang tersedia: • `API Firewall` • `Asset Management` • `AV Scanning and Sandboxing` • `Backup and Disaster Recovery` • `Breach and Attack Simulation` • `Bug Bounty Platform` • `Certificate Management` • `Cloud Access Security Broker` • `Cloud Security Posture Managemen t` • `Configuration and Patch Management` • `Configuration Management Database (CMDB)` • `Consulting Partner` • `Container Security` • `Cyber Range` • `Data Access Management` • `Data Classification`

Bidang	Diperlukan	Deskripsi
		• Data Loss Prevention • Data Masking and Tokenization • Database Activity Monitoring • DDoS Protection • Deception • Device Control • Dynamic Application Security Testing • Data Encryption • Email Gateway • Encrypted Search • Endpoint Detection and Response (EDR) • Endpoint Forensics • Forensics Toolkit • Fraud Detection • Governance, Risk, and Compliance (GRC) • Host-based Intrusion Detection (HIDs) • Human Resources Information System • Interactive Application Security Testing (IAST) • Instant Messaging • IoT Security • IT Security Training • IT Ticketing and Incident Management

Bidang	Diperlukan	Deskripsi
		• `Managed Security Service Provider (MSSP)` • `Micro-Segmentation` • `Multi-Cloud Management` • `Multi-Factor Authentication` • `Network Access Control (NAC)` • `Network Firewall` • `Network Forensics` • `Network Intrusion Detection Systems (IDS)` • `Network Intrusion Prevention Systems (IPS)` • `Phishing Simulation and Training` • `Privacy Operations` • `Privileged Access Management` • `Rogue Device Detection` • `Runtime Application Self-Protection (RASP)` • `Secure Web Gateway`
`marketplaceUrl`	Tidak	URL ke AWS Marketplace tujuan produk Anda. URL ditampilkan di konsol CSPM Security Hub. Tipe: String Ini harus berupa AWS Marketplace URL. Jika Anda tidak memiliki AWS Marketplace daftar, biarkan bidang ini kosong.

Bidang	Diperlukan	Deskripsi
`configurationUrl`	Ya	URL ke dokumentasi produk Anda tentang integrasi dengan Security Hub CSPM. Konten ini di-host di situs web Anda atau di halaman web yang Anda kelola, seperti GitHub halaman. Tipe: String Dokumentasi Anda harus menyertakan informasi berikut. • Instruksi konfigurasi • Tautan ke CloudFormation templat (jika perlu) • Informasi tentang kasus penggunaan Anda untuk integrasi • Latensi • Pemetaan ASFF • Jenis temuan termasuk • Arsitektur

Pedoman dan daftar periksa

Saat Anda menyiapkan materi yang diperlukan untuk AWS Security Hub CSPM integrasi Anda, gunakan pedoman ini.

Checklist kesiapan digunakan untuk melakukan tinjauan akhir integrasi sebelum Security Hub CSPM membuatnya tersedia untuk pelanggan CSPM Security Hub.

Topik

Pedoman untuk logo untuk ditampilkan di AWS Security Hub CSPM konsol

Agar logo ditampilkan di AWS Security Hub CSPM konsol, ikuti panduan ini.

Mode terang dan gelap

Anda harus menyediakan mode terang dan versi mode gelap dari logo.

Format

Format file SVG

Warna latar belakang

Transparan

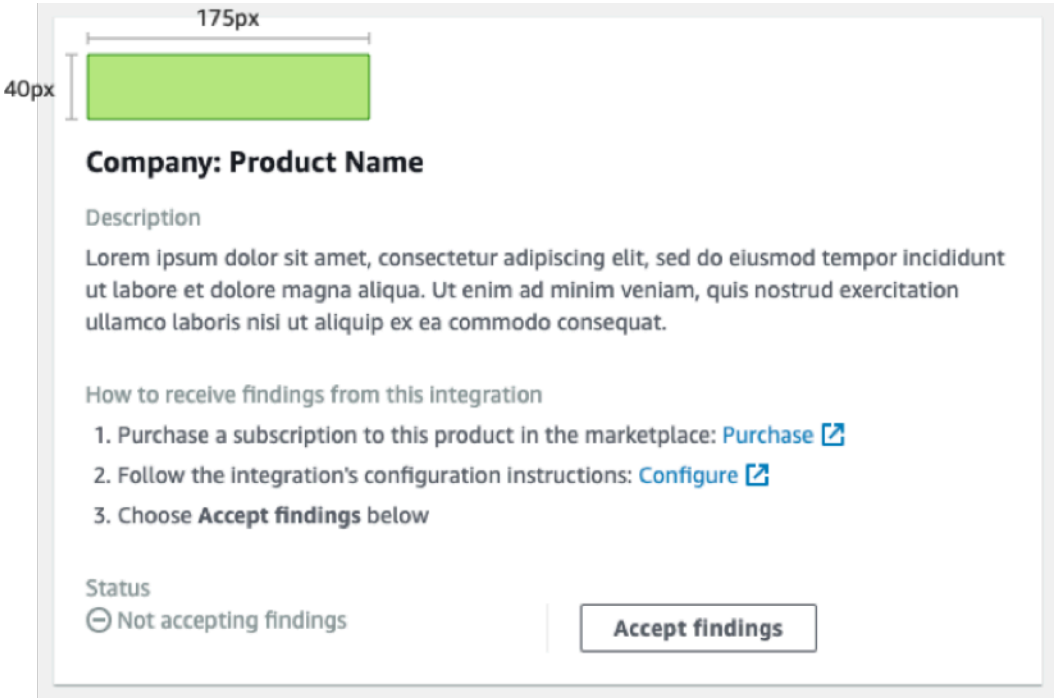
Size

Rasio ideal adalah 175 px lebar dengan tinggi 40 px.

Tinggi minimum adalah 40 px.

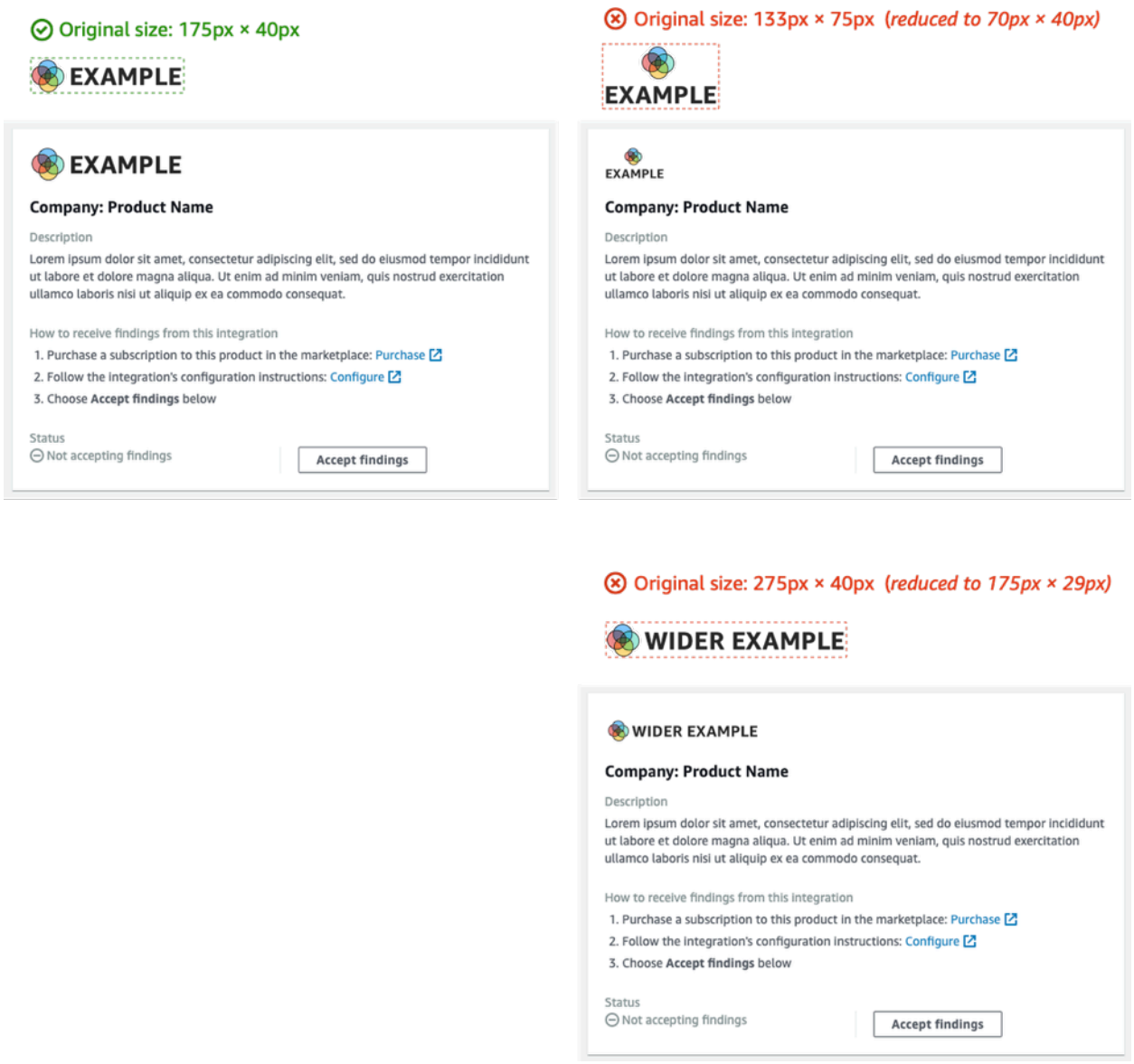
Logo persegi panjang bekerja paling baik.

Gambar berikut menunjukkan bagaimana logo ideal ditampilkan pada konsol CSPM Security Hub.



Jika logo Anda tidak cocok dengan dimensi ini, Security Hub mengurangi ukuran hingga tinggi maksimum 40 px dan lebar maksimum 175 px. Ini memengaruhi bagaimana logo ditampilkan di konsol CSPM Security Hub.

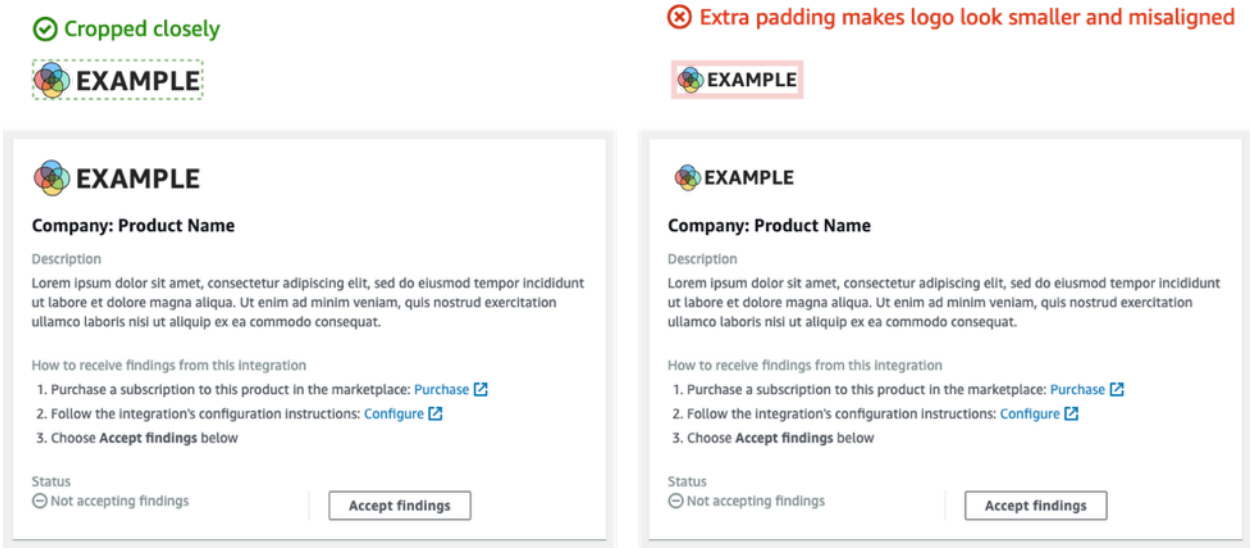
Gambar berikut membandingkan tampilan logo yang menggunakan ukuran ideal dengan logo yang lebih lebar atau lebih tinggi.



Memangkas

Pangkas gambar logo sedekat mungkin. Jangan berikan padding tambahan.

Gambar berikut menunjukkan perbedaan antara logo yang dipotong rapat dan logo yang memiliki padding ekstra.



Prinsip untuk membuat dan memperbarui temuan

Saat Anda merencanakan bagaimana Anda akan membuat dan memperbarui temuan AWS Security Hub CSPM, ingatlah prinsip-prinsip berikut.

Buatlah temuan spesifik sehingga pelanggan dapat dengan mudah mengambil tindakan terhadapnya.

Pelanggan ingin mengotomatiskan tindakan respons dan remediasi dan mengkorelasikan temuan dengan temuan lain. Untuk mendukung hal ini, temuan harus memiliki karakteristik sebagai berikut:

- Mereka umumnya harus berurusan dengan sumber daya tunggal atau primer.
- Mereka harus memiliki jenis temuan tunggal.
- Mereka harus berurusan dengan satu peristiwa keamanan.

Ketika sebuah temuan berisi data untuk beberapa peristiwa keamanan, lebih sulit bagi pelanggan untuk mengambil tindakan atas temuan tersebut.

Petakan semua bidang temuan Anda ke AWS Security Finding Format (ASFF). Memungkinkan pelanggan untuk mengandalkan Security Hub CSPM sebagai sumber kebenaran.

Pelanggan berharap bahwa setiap bidang yang ada dalam format pencarian asli Anda juga diwakili dalam Security Hub CSPM ASFF.

Pelanggan ingin semua data hadir dalam versi CSPM Security Hub. Data yang hilang menyebabkan mereka kehilangan kepercayaan pada Security Hub CSPM sebagai sumber utama informasi keamanan.

Minimalkan redundansi dalam temuan. Jangan membanjiri pelanggan dengan menemukan volume.

Security Hub CSPM bukanlah alat manajemen log umum. Anda harus mengirimkan temuan ke Security Hub CSPM yang sangat dapat ditindaklanjuti, dan bahwa pelanggan dapat langsung merespons, memulihkan, atau berkorelasi dengan temuan lain.

Ketika hanya ada perubahan kecil pada temuan, perbarui temuan alih-alih membuat temuan baru.

Ketika ada perubahan besar pada temuan, seperti skor keparahan atau pengidentifikasi sumber daya, buat temuan baru.

Misalnya, untuk membuat temuan untuk pemindaian port individu secara real time sangat tidak dapat ditindaklanjuti. Karena pemindaian port dapat terjadi terus menerus, itu akan menghasilkan sejumlah besar temuan. Jauh lebih menarik dan tepat untuk hanya memperbarui waktu pemindaian terakhir dan menghitung pemindaian pada satu temuan untuk pemindaian port pada port MongoDB dari node TOR.

Memungkinkan pelanggan untuk menyesuaikan temuan mereka untuk membuat mereka lebih bermakna.

Pelanggan ingin dapat menyesuaikan bidang temuan tertentu untuk membuatnya lebih relevan dengan lingkungan atau persyaratan mereka.

Misalnya, pelanggan ingin dapat menambahkan catatan, tag, dan menyesuaikan skor keparahan berdasarkan jenis akun atau jenis sumber daya yang terkait dengan temuan tersebut.

Pedoman pemetaan temuan ke dalam AWS Security Finding Format (ASFF)

Gunakan panduan berikut untuk memetakan temuan Anda ke ASFF. Untuk deskripsi rinci dari setiap bidang dan objek ASFF, lihat AWS Security Finding Format (ASFF) di Panduan Pengguna.AWS Security Hub

Mengidentifikasi informasi

`SchemaVersion` selalu `2018-10-08`.

`ProductArn`adalah ARN yang AWS Security Hub CSPM memberikan kepada Anda.

`Id`adalah nilai yang digunakan Security Hub CSPM untuk mengindeks temuan. Pengidentifikasi temuan harus unik, untuk memastikan bahwa temuan lain tidak ditimpa. Untuk memperbarui temuan, kirim ulang temuan dengan pengenal yang sama.

`GeneratorId`dapat sama dengan `Id` atau dapat merujuk ke unit logika diskrit, seperti ID GuardDuty detektor Amazon, ID AWS Config perekam, atau ID Penganalisis Akses IAM.

Title dan Description

`Title`harus berisi beberapa informasi tentang sumber daya yang terpengaruh. `Title`terbatas pada 256 karakter, termasuk spasi.

Tambahkan informasi terperinci yang lebih panjang ke`Description`. `Description`terbatas pada 1024 karakter, termasuk spasi. Anda dapat mempertimbangkan untuk menambahkan pemotongan ke deskripsi. Inilah contohnya:

```
"Title": "Instance i-12345678901 is vulnerable to CVE-2019-1234",
"Description": "Instance i-12345678901 is vulnerable to CVE-2019-1234. This
 vulnerability affects version 1.0.1 of widget-1 and earlier, and can lead to buffer
 overflow when someone sends a ping.",
```

Tipe temuan

Anda memberikan informasi jenis temuan Anda di`FindingProviderFields.Types`.

`Types`harus cocok dengan jenis taksonomi untuk ASFF.

Jika diperlukan, Anda dapat menentukan pengklasifikasi kustom (namespace ketiga).

Stempel waktu

Format ASFF mencakup beberapa stempel waktu yang berbeda.

`CreatedAt` dan `UpdatedAt`

Anda harus mengirimkan `CreatedAt` dan `UpdatedAt` setiap kali Anda menelepon `BatchImportFindings`untuk setiap temuan.

Nilai harus sesuai dengan ISO8601 format di Python 3.8.

```
datetime.datetime.utcnow().replace(tzinfo=datetime.timezone.utc).isoformat()
```

`FirstObservedAt` dan `LastObservedAt`

`FirstObservedAt`dan `LastObservedAt` harus cocok ketika sistem Anda mengamati temuan tersebut. Jika Anda tidak mencatat informasi ini, Anda tidak perlu mengirimkan stempel waktu ini.

Nilai-nilai cocok dengan ISO8601 format di Python 3.8.

```
datetime.datetime.utcnow().replace(tzinfo=datetime.timezone.utc).isoformat()
```

Severity

Anda memberikan informasi tingkat keparahan dalam `FindingProviderFields.Severity` objek, yang berisi bidang berikut.

`Original`

Nilai keparahan dari sistem Anda. `Original`dapat berupa string apa saja, untuk mengakomodasi sistem yang Anda gunakan.

`Label`

Indikator CSPM Security Hub yang diperlukan untuk tingkat keparahan temuan. Nilai yang diizinkan adalah sebagai berikut.

- `INFORMATIONAL`Tidak ada masalah yang ditemukan.
- `LOW`— Masalah ini tidak memerlukan tindakan sendiri.
- `MEDIUM`Masalah ini harus diatasi tetapi tidak mendesak.
- `HIGH`Masalah ini harus diatasi sebagai prioritas.
- `CRITICAL`— Masalah ini harus segera diperbaiki untuk mencegah kerusakan lebih lanjut.

Temuan yang sesuai harus selalu `Label` ditetapkan. `INFORMATIONAL` Contoh `INFORMATIONAL` temuan adalah temuan dari pemeriksaan keamanan yang lulus dan AWS Firewall Manager temuan yang diperbaiki.

Pelanggan sering mengurutkan temuan berdasarkan tingkat keparahannya untuk memberi tim operasi keamanan mereka daftar tugas. Bersikaplah konservatif saat mengatur tingkat keparahan temuan ke `HIGH` atau`CRITICAL`.

Dokumentasi integrasi Anda harus menyertakan alasan pemetaan Anda.

Remediation

`Remediation`memiliki dua elemen. Elemen-elemen ini digabungkan pada konsol CSPM Security Hub.

`Remediation.Recommendation.Text`muncul di bagian Remediasi dari detail temuan. Hal ini hyperlink ke nilai. `Remediation.Recommendation.Url`

Saat ini, hanya temuan dari standar CSPM Security Hub, IAM Access Analyzer, dan Firewall Manager yang menampilkan hyperlink ke dokumentasi tentang cara memulihkan temuan.

SourceUrl

Gunakan hanya `SourceUrl` jika Anda dapat memberikan URL yang ditautkan dalam ke konsol Anda untuk temuan spesifik tersebut. Jika tidak, hilangkan dari pemetaan.

Security Hub CSPM tidak mendukung hyperlink dari bidang ini, tetapi terpapar di konsol CSPM Security Hub.

Malware, Network, Process, ThreatIntelIndicators

Jika berlaku, gunakan`Malware`,`Network`,`Process`, atau`ThreatIntelIndicators`. Masing-masing objek ini diekspos di konsol CSPM Security Hub. Gunakan benda-benda ini dalam konteks temuan yang Anda kirim.

Misalnya, jika Anda mendeteksi malware yang membuat koneksi keluar ke node perintah dan kontrol yang diketahui, berikan detail untuk instans EC2 di. `Resource.Details.AwsEc2Instance` Berikan `ThreatIntelIndicator` objek yang relevan`Malware`,`Network`, dan untuk instans EC2 itu.

Malware

`Malware`adalah daftar yang menerima hingga lima array informasi malware. Buat entri malware yang relevan dengan sumber daya dan temuan.

Setiap entri memiliki bidang berikut.

`Name`

Nama malware. Nilainya adalah string hingga 64 karakter.

`Name`harus dari intelijen ancaman yang diperiksa atau sumber peneliti.

`Path`

Jalan menuju malware. Nilainya adalah string hingga 512 karakter. `Path`harus berupa jalur file sistem Linux atau Windows, kecuali dalam kasus berikut.

- Jika Anda memindai objek dalam bucket S3 atau berbagi EFS terhadap aturan YARA, maka `Path` adalah jalur objek S3://atau HTTPS.
- Jika Anda memindai file dalam repositori Git, maka `Path` adalah URL Git atau jalur klon.

`State`

Status malware. Nilai yang diizinkan adalah `OBSERVED` | `REMOVAL_FAILED` |`REMOVED`.

Dalam judul dan deskripsi temuan, pastikan Anda memberikan konteks untuk apa yang terjadi dengan malware.

Misalnya, jika `Malware.State` ya`REMOVED`, maka judul dan deskripsi temuan harus mencerminkan bahwa produk Anda menghapus malware yang terletak di jalur.

Jika `Malware.State` ya`OBSERVED`, maka judul dan deskripsi temuan harus mencerminkan bahwa produk Anda menemukan malware ini yang terletak di jalur.

`Type`

Menunjukkan jenis malware. Nilai yang diizinkan adalah `ADWARE` | `BLENDED_THREAT` | `BOTNET_AGENT` | `COIN_MINER` | `EXPLOIT_KIT` `KEYLOGGER` | `MACRO` | `POTENTIALLY_UNWANTED` | `SPYWARE` | `RANSOMWARE` | `REMOTE_ACCESS` | `ROOTKIT` | `TROJAN` | `VIRUS` |`WORM`.

Jika Anda membutuhkan nilai tambahan`Type`, hubungi tim CSPM Security Hub.

Network

`Network`adalah objek tunggal. Anda tidak dapat menambahkan beberapa detail terkait jaringan. Saat memetakan bidang, gunakan pedoman berikut.

Informasi tujuan dan sumber

Tujuan dan sumbernya mudah untuk memetakan TCP atau VPC Flow Logs atau log WAF. Mereka lebih sulit digunakan ketika Anda menggambarkan informasi jaringan untuk menemukan tentang serangan.

Biasanya, sumbernya adalah tempat serangan itu berasal, tetapi bisa memiliki sumber lain seperti yang tercantum di bawah ini. Anda harus menjelaskan sumbernya dalam dokumentasi Anda dan juga menjelaskannya dalam judul dan deskripsi temuan.

- Untuk serangan DDoS pada instans EC2, sumbernya adalah penyerang, meskipun serangan DDoS nyata dapat menggunakan jutaan host. Tujuannya adalah alamat IPv4 publik dari instans EC2. `Direction`ada di.
- Untuk malware yang diamati berkomunikasi dari instans EC2 ke node perintah dan kontrol yang diketahui, sumbernya adalah alamat IPV4 dari instans EC2. Tujuannya adalah simpul perintah dan kontrol. `Direction`adalah`OUT`. Anda juga akan menyediakan `Malware` dan`ThreatIntelIndicators`.

`Protocol`

`Protocol`selalu memetakan ke nama terdaftar Internet Assigned Numbers Authority (IANA), kecuali jika Anda dapat memberikan protokol tertentu. Anda harus selalu menggunakan ini dan memberikan informasi port.

`Protocol`independen dari sumber dan informasi tujuan. Sediakan hanya ketika masuk akal untuk melakukannya.

`Direction`

`Direction`selalu relatif terhadap batas-batas AWS jaringan.

- `IN`berarti itu masuk AWS (VPC, layanan).
- `OUT`berarti keluar dari batas-batas AWS jaringan.

Process

`Process`adalah objek tunggal. Anda tidak dapat menambahkan beberapa detail terkait proses. Saat memetakan bidang, gunakan pedoman berikut.

`Name`

`Name`harus cocok dengan nama yang dapat dieksekusi. Ini menerima hingga 64 karakter.

`Path`

`Path`adalah jalur sistem file ke proses yang dapat dieksekusi. Ia menerima hingga 512 karakter.

`Pid`, **`ParentPid`**

`Pid`dan `ParentPid` harus cocok dengan pengidentifikasi proses Linux (PID) atau ID peristiwa Windows. Untuk membedakan, gunakan EC2 Amazon Machine Images (AMI) untuk memberikan informasi. Pelanggan mungkin dapat membedakan antara Windows dan Linux.

Stempel waktu (**`LaunchedAt`**dan) **`TerminatedAt`**

Jika Anda tidak dapat mengambil informasi ini dengan andal, dan itu tidak akurat hingga milidetik, jangan berikan.

Jika pelanggan mengandalkan stempel waktu untuk penyelidikan forensik, maka tidak memiliki stempel waktu lebih baik daripada memiliki stempel waktu yang salah.

ThreatIntelIndicators

`ThreatIntelIndicators`menerima array hingga lima objek intelijen ancaman.

Untuk setiap entri, `Type` adalah dalam konteks ancaman spesifik. Nilai yang diizinkan adalah `DOMAIN` `EMAIL_ADDRESS` | `HASH_MD5` | `HASH_SHA1` | `HASH_SHA256` | `HASH_SHA512` | `IPV4_ADDRESS` `IPV6_ADDRESS` | `MUTEX` | `PROCESS` |`URL`.

Berikut adalah beberapa contoh cara memetakan indikator intelijen ancaman:

- Anda menemukan proses yang Anda tahu terkait dengan Cobalt Strike. Anda belajar ini dari FireEye blog.

  Atur `Type` ke `PROCESS`. Juga buat `Process` objek untuk proses tersebut.
- Filter email Anda menemukan seseorang mengirim paket hash terkenal dari domain berbahaya yang dikenal.

  Buat dua `ThreatIntelIndicator` objek. Satu objek adalah untuk`DOMAIN`. Yang lainnya adalah untuk`HASH_SHA1`.
- Anda menemukan malware dengan aturan Yara (Loki, Fenrir, Awss3,). VirusScan BinaryAlert

  Buat dua `ThreatIntelIndicator` objek. Salah satunya untuk malware. Yang lainnya adalah untuk`HASH_SHA1`.

Resources

UntukResources, gunakan jenis sumber daya dan bidang detail yang kami sediakan bila memungkinkan. Security Hub CSPM terus menambahkan sumber daya baru ke ASFF. Untuk menerima log bulanan perubahan ASFF, hubungi <securityhub-partners@amazon.com>.

Jika Anda tidak dapat memasukkan informasi di bidang detail untuk jenis sumber daya yang dimodelkan, petakan detail yang tersisa. Details.Other

Untuk sumber daya yang tidak dimodelkan dalam ASFF, atur Type ke. Other Untuk informasi rinci, gunakanDetails.Other.

Anda juga dapat menggunakan jenis Other sumber daya untuk AWS non-temuan.

ProductFields

Hanya gunakan ProductFields jika Anda tidak dapat menggunakan bidang kurasi lain untuk Resources atau objek deskriptif sepertiThreatIntelIndicators,Network, atau. Malware

Jika Anda menggunakannyaProductFields, Anda harus memberikan alasan yang ketat untuk keputusan ini.

Kepatuhan

Gunakan hanya Compliance jika temuan Anda terkait dengan kepatuhan.

Security Hub menggunakan CSPM Compliance untuk temuan yang dihasilkannya berdasarkan kontrol.

Firewall Manager menggunakan Compliance temuannya karena mereka terkait dengan kepatuhan.

Bidang yang dibatasi

Bidang ini ditujukan bagi pelanggan untuk melacak penyelidikan mereka terhadap suatu temuan.

Jangan memetakan ke bidang atau objek ini.

- Note
- UserDefinedFields

- `VerificationState`
- `Workflow`

Untuk bidang ini, petakan ke bidang yang ada di `FindingProviderFields` objek. Jangan memetakan ke bidang tingkat atas.

- `Confidence`— Hanya sertakan skor kepercayaan (0-99) jika layanan Anda memiliki fungsi yang sama, atau jika Anda berdiri 100% dengan temuan Anda.
- `Criticality`— Skor kekritisan (0-99) dimaksudkan untuk mengungkapkan pentingnya sumber daya yang terkait dengan temuan tersebut.
- `RelatedFindings`— Hanya berikan temuan terkait jika Anda dapat melacak temuan yang terkait dengan sumber daya atau jenis temuan yang sama. Untuk mengidentifikasi temuan terkait, Anda harus merujuk ke pengidentifikasi temuan dari temuan yang sudah ada di Security Hub CSPM.

Pedoman untuk menggunakan **`BatchImportFindings`** API

Saat menggunakan operasi `BatchImportFindings`API untuk mengirim temuan AWS Security Hub CSPM, gunakan pedoman berikut.

- Anda harus menelepon `BatchImportFindings`menggunakan akun yang terkait dengan temuan. Pengidentifikasi akun terkait adalah nilai `AwsAccountId` atribut untuk temuan tersebut.
- Kirim batch terbesar yang Anda bisa. Security Hub CSPM 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.
- Anda harus menerapkan mekanisme untuk mempertahankan status temuan jika ada masalah pelambatan atau jaringan. Anda juga memerlukan status temuan sehingga Anda dapat mengirimkan pembaruan temuan saat temuan bergerak masuk dan keluar dari kepatuhan.
- Untuk informasi tentang panjang maksimum string dan batasan lainnya, lihat AWS Security Finding Format (ASFF) di Panduan Pengguna.AWS Security Hub

Daftar periksa kesiapan produk

Tim Mitra APN AWS Security Hub CSPM dan APN menggunakan daftar periksa ini untuk memvalidasi bahwa integrasi siap diluncurkan.

Pemetaan ASFF

Pertanyaan-pertanyaan ini terkait dengan pemetaan temuan Anda ke AWS Security Finding Format (ASFF).

Apakah semua data temuan mitra dipetakan ke ASFF?

Petakan semua temuan Anda ke ASFF dengan cara tertentu.

Gunakan bidang yang dikuratori seperti tipe sumber daya yang dimodelkan,, `NetworkMalware`, atau. `ThreatIntelIndicators`

Memetakan apa pun ke dalam `Resource.Details.Other` atau yang `ProductFields` sesuai.

Apakah mitra menggunakan **`Resource.Details`** bidang, seperti**`AwsEc2instance`**,**`AwsS3Bucket`**, dan**`Container`**? Apakah mitra menggunakan **`Resource.Details.Other`** untuk menentukan detail sumber daya yang tidak dimodelkan dalam ASFF?

Jika memungkinkan, gunakan bidang yang disediakan untuk sumber daya yang dikurasi seperti instans EC2, bucket S3, dan grup keamanan dalam temuan Anda.

Petakan informasi lain yang terkait dengan sumber daya `Resource.Details.Other` hanya jika tidak ada kecocokan langsung.

Apakah mitra memetakan nilai ke**`UserDefinedFields`**?

Jangan gunakan `UserDefinedFields`.

Pertimbangkan untuk menggunakan bidang lain yang dikuratori, seperti `Resource.Details.Other` atau`ProductFields`.

Apakah mitra memetakan informasi ke dalamnya **`ProductFields`** dapat dipetakan ke bidang ASFF lainnya?

Hanya digunakan `ProductFields` untuk informasi spesifik produk seperti informasi versi, temuan tingkat keparahan spesifik produk, atau informasi lain yang tidak dapat dipetakan ke dalam bidang yang dikuratori atau. `Resources.Details.Other`

Apakah mitra mengimpor stempel waktu mereka sendiri? **`FirstObservedAt`**

`FirstObservedAt`Stempel waktu dimaksudkan untuk mencatat waktu ketika temuan diamati dalam produk. Petakan bidang ini jika memungkinkan.

Apakah mitra memberikan nilai unik yang dihasilkan untuk setiap pengidentifikasi temuan, kecuali untuk temuan yang ingin mereka perbarui?

Semua temuan di Security Hub CSPM diindeks pada identifier temuan (atribut). `Id` Nilai ini harus selalu unik untuk memastikan bahwa temuan tidak diperbarui secara tidak sengaja.

Anda juga harus mempertahankan status pengenal temuan untuk tujuan memperbarui temuan.

Apakah mitra memberikan nilai yang memetakan temuan ke ID generator?

`GeneratorID`seharusnya tidak memiliki nilai yang sama dengan ID temuan.

`GeneratorID`harus dapat secara logis menghubungkan temuan dengan apa yang menghasilkannya.

Ini bisa menjadi subkomponen dalam suatu produk (Produk A - Kerentanan vs Produk A - EDR) atau yang serupa.

Apakah mitra menggunakan ruang nama tipe temuan yang diperlukan dengan cara yang relevan dengan produk mereka? Apakah mitra menggunakan kategori atau pengklasifikasi tipe temuan yang direkomendasikan dalam tipe temuan mereka?

Taksonomi tipe temuan harus dipetakan secara dekat dengan temuan yang dihasilkan produk.

Ruang nama tingkat pertama yang diuraikan dalam Format Pencarian AWS Keamanan diperlukan.

Anda dapat menggunakan nilai kustom untuk ruang nama tingkat kedua dan ketiga (Kategori atau Pengklasifikasi).

Apakah mitra menangkap informasi aliran jaringan di **`Network`** bidang, jika mereka memiliki data jaringan?

Jika produk Anda menangkap NetFlow informasi, petakan ke `Network` bidang.

Apakah mitra menangkap informasi proses (PID) di **`Process`** bidang, jika mereka memiliki data proses?

Jika produk Anda menangkap informasi proses, petakan ke `Process` bidang.

Apakah mitra menangkap informasi malware di **`Malware`** lapangan, jika mereka memiliki data malware?

Jika produk Anda menangkap informasi malware, petakan ke `Malware` bidang.

Apakah mitra menangkap informasi intelijen ancaman di **`ThreatIntelIndicators`** lapangan, jika mereka memiliki data intelijen ancaman?

Jika produk Anda menangkap informasi intelijen ancaman, petakan ke `ThreatIntelIndicators` lapangan.

Apakah pasangan memberikan peringkat kepercayaan untuk temuan? Jika mereka melakukannya, apakah alasan disediakan?

Setiap kali Anda menggunakan bidang ini, berikan alasan dalam dokumentasi dan manifes Anda.

Apakah mitra menggunakan ID kanonik atau ARN untuk ID sumber daya dalam temuan?

Saat mengidentifikasi AWS sumber daya, praktik terbaik adalah menggunakan ARN. Jika ARN tidak tersedia, gunakan ID sumber daya kanonik.

Pengaturan dan fungsi integrasi

Pertanyaan-pertanyaan ini terkait dengan pengaturan dan day-to-day fungsi integrasi.

Apakah mitra menyediakan templat infrastructure-as-code (IAc) untuk menerapkan integrasi dengan Security Hub CSPM, seperti Terraform,, atau? CloudFormation AWS Cloud Development Kit (AWS CDK)

Untuk integrasi yang akan mengirimkan temuan dari akun pelanggan atau menggunakan CloudWatch Events untuk mengkonsumsi temuan, diperlukan beberapa bentuk template IAc.

CloudFormation lebih disukai, tetapi AWS CDK atau Terraform juga dapat digunakan.

Apakah produk mitra memiliki pengaturan satu klik di konsol mereka untuk integrasi mereka dengan Security Hub CSPM?

Beberapa produk mitra menggunakan sakelar atau mekanisme serupa dalam produk mereka untuk mengaktifkan integrasi. Ini mungkin memerlukan penyediaan sumber daya dan izin secara otomatis. Jika Anda mengirim temuan dari akun produk, pengaturan satu klik adalah metode yang lebih disukai.

Apakah pasangan hanya mengirimkan temuan nilai?

Anda umumnya hanya harus mengirimkan temuan yang memiliki nilai keamanan kepada pelanggan CSPM Security Hub.

Security Hub CSPM bukanlah alat manajemen log umum. Anda tidak boleh mengirim setiap log yang mungkin ke Security Hub CSPM.

Apakah mitra memberikan perkiraan berapa banyak temuan yang akan mereka kirim per hari per pelanggan dan pada frekuensi berapa (rata-rata dan ledakan)?

Jumlah temuan unik digunakan untuk menghitung beban pada Security Hub CSPM. Temuan unik didefinisikan sebagai temuan dengan pemetaan ASFF yang berbeda dari temuan lain.

Misalnya, jika satu temuan hanya dihuni `ThreatIntelIndicators` dan yang lain hanya berpenduduk`Resources.Details.AWSEc2Instance`, itu adalah dua temuan unik.

Apakah pasangan memiliki cara yang anggun untuk menangani kesalahan 4xx dan 5xx sehingga tidak dibatasi dan semua temuan dapat dikirim di lain waktu?

Saat ini ada burst rate 30—50 TPS pada operasi API. `BatchImportFindings` Jika kesalahan 4xx atau 5xx dikembalikan, Anda harus mempertahankan status temuan yang gagal tersebut sehingga Anda dapat mencobanya kembali secara totalitas nanti. Anda dapat melakukan ini melalui antrian surat mati atau layanan AWS pesan lain seperti Amazon SNS atau Amazon SQS.

Apakah pasangan mempertahankan keadaan temuan mereka sehingga mereka tahu untuk mengarsipkan temuan yang tidak lagi ada?

Jika Anda berencana untuk memperbarui temuan dengan menimpa ID temuan asli, Anda harus memiliki mekanisme untuk mempertahankan status sehingga informasi yang benar diperbarui untuk temuan yang benar.

Jika Anda memberikan temuan, jangan gunakan `BatchUpdateFindings`operasi untuk memperbarui temuan. Operasi ini hanya boleh digunakan oleh pelanggan. Anda hanya menggunakan `BatchUpdateFindings`ketika Anda menyelidiki dan mengambil tindakan atas temuan.

Apakah mitra menangani percobaan ulang dengan cara yang tidak membahayakan temuan sukses yang dikirim sebelumnya?

Anda harus memiliki mekanisme untuk mempertahankan temuan asli IDs dalam kasus kesalahan sehingga Anda tidak menduplikasi atau menimpa temuan yang berhasil dalam kesalahan.

Apakah mitra memperbarui temuan dengan memanggil **`BatchImportFindings`** operasi dengan ID temuan temuan yang ada?

Untuk memperbarui temuan, Anda harus menimpa temuan yang ada dengan mengirimkan ID temuan yang sama.

`BatchUpdateFindings`Operasi hanya boleh digunakan oleh pelanggan.

Apakah mitra memperbarui temuan menggunakan **`BatchUpdateFindings`** API?

Jika Anda mengambil tindakan atas temuan, Anda dapat menggunakan `BatchUpdateFindings`operasi untuk memperbarui bidang tertentu.

Apakah mitra memberikan informasi tentang jumlah latensi antara saat temuan dibuat dan kapan dikirim dari produk mereka ke Security Hub CSPM?

Anda harus meminimalkan latensi untuk memastikan bahwa pelanggan melihat temuan sesegera mungkin di Security Hub CSPM.

Informasi ini diperlukan dalam manifes.

Jika arsitektur mitra adalah mengirim temuan ke Security Hub CSPM dari akun pelanggan, apakah mereka berhasil mendemonstrasikannya? Jika arsitektur mitra adalah untuk mengirim temuan ke Security Hub CSPM dari akun mereka sendiri, apakah mereka berhasil mendemonstrasikannya?

Selama pengujian, temuan harus berhasil dikirim dari akun yang Anda miliki yang berbeda dari akun yang disediakan untuk produk ARN.

Mengirim temuan dari akun pemilik ARN produk dapat melewati pengecualian kesalahan tertentu dari operasi API.

Apakah mitra memberikan temuan detak jantung ke Security Hub CSPM?

Untuk menunjukkan bahwa integrasi Anda berfungsi dengan benar, Anda harus mengirim temuan detak jantung. Temuan detak jantung dikirim setiap lima menit dan menggunakan jenis `Heartbeat` temuan.

Ini penting jika Anda mengirim temuan dari akun produk.

Apakah mitra berintegrasi dengan akun tim produk CSPM Security Hub selama pengujian?

Selama validasi praproduksi, Anda harus mengirim contoh pencarian ke akun tim produk CSPM Security Hub. AWS Contoh-contoh ini menunjukkan bahwa temuan dikirim dan dipetakan dengan benar.

Dokumentasi

Pertanyaan-pertanyaan ini terkait dengan dokumentasi integrasi yang Anda berikan.

Apakah mitra meng-host dokumentasi mereka di situs web khusus?

Dokumentasi harus di-host di situs web Anda sebagai halaman web statis, wiki, Baca Dokumen, atau format khusus lainnya.

Dokumentasi hosting di GitHub tidak memenuhi persyaratan situs web khusus.

Apakah dokumentasi mitra memberikan instruksi tentang cara mengatur integrasi CSPM Security Hub?

Anda dapat mengatur integrasi menggunakan templat IAC atau integrasi “satu-klik” berbasis konsol.

Apakah dokumentasi mitra memberikan deskripsi kasus penggunaannya?

Kasus penggunaan yang Anda berikan dalam manifes juga harus dijelaskan dalam dokumentasi

Apakah dokumentasi mitra memberikan alasan untuk temuan yang mereka kirim?

Anda harus memberikan alasan untuk jenis temuan yang Anda kirim.

Misalnya, produk Anda mungkin menghasilkan temuan untuk kerentanan, malware, dan antivirus, tetapi Anda hanya mengirim temuan kerentanan dan malware ke Security Hub CSPM. Dalam hal ini, Anda harus memberikan alasan mengapa Anda tidak mengirim temuan antivirus.

Apakah dokumentasi mitra memberikan alasan bagaimana mitra memetakan temuan mereka ke ASFF?

Anda harus memberikan alasan untuk pemetaan temuan asli produk ke ASFF. Pelanggan ingin tahu di mana mencari informasi produk tertentu.

Apakah dokumentasi mitra memberikan panduan tentang bagaimana mitra memperbarui temuan, jika mereka memperbarui temuan?

Berikan informasi kepada pelanggan tentang bagaimana Anda mempertahankan status, memastikan idempotensi, dan menimpa temuan dengan informasi. up-to-date

Apakah dokumentasi mitra menjelaskan menemukan latensi?

Minimalkan latensi untuk memastikan bahwa pelanggan melihat temuan sesegera mungkin di Security Hub CSPM.

Informasi ini diperlukan dalam manifes.

Apakah dokumentasi mitra menjelaskan bagaimana penilaian tingkat keparahan mereka memetakan skor keparahan ASFF?

Berikan informasi tentang cara Anda `Severity.Original` memetakan`Severity.Label`.

Misalnya, jika nilai keparahan Anda adalah nilai huruf (A, B, C), Anda harus memberikan informasi tentang bagaimana Anda memetakan nilai huruf ke label keparahan.

Apakah dokumentasi mitra memberikan alasan untuk peringkat kepercayaan?

Jika Anda memberikan skor kepercayaan diri, skor ini harus diberi peringkat.

Jika Anda menggunakan skor kepercayaan yang diisi secara statis atau pemetaan yang berasal dari kecerdasan buatan atau pembelajaran mesin, Anda harus memberikan konteks tambahan.

Apakah dokumentasi mitra mencatat Wilayah mana yang didukung dan tidak didukung oleh mitra?

Perhatikan Wilayah yang didukung atau tidak sehingga pelanggan tahu di Wilayah mana yang tidak mencoba integrasi.

Informasi kartu produk

Pertanyaan-pertanyaan ini terkait dengan kartu untuk produk yang ditampilkan di halaman Integrasi konsol CSPM Security Hub.

Apakah ID AWS akun yang diberikan valid dan berisi 12 digit?

Pengidentifikasi akun memiliki panjang 12 digit. Jika ID akun berisi kurang dari 12 digit, maka ARN produk tidak akan valid.

Apakah deskripsi produk mengandung 200 karakter atau lebih sedikit?

Deskripsi produk yang disediakan di JSON dalam manifes tidak boleh lebih dari 200 karakter termasuk spasi.

Apakah tautan konfigurasi mengarah ke dokumentasi untuk integrasi?

Tautan konfigurasi harus mengarah ke dokumentasi online Anda. Seharusnya tidak mengarah ke situs web utama Anda atau ke halaman pemasaran.

Apakah tautan pembelian (jika disediakan) mengarah ke AWS Marketplace daftar produk?

Jika Anda memberikan tautan pembelian, itu harus untuk AWS Marketplace entri. Security Hub CSPM tidak menerima tautan pembelian yang tidak di-host oleh. AWS

Apakah kategori produk menggambarkan produk dengan benar?

Dalam manifes, Anda dapat menyediakan hingga tiga kategori produk. Ini harus cocok dengan JSON dan tidak dapat disesuaikan. Anda tidak dapat menyediakan lebih dari tiga kategori produk.

Apakah nama perusahaan dan produk valid dan benar?

Nama perusahaan harus 16 karakter atau kurang.

Nama produk harus 24 karakter atau kurang.

Nama produk di kartu produk JSON harus cocok dengan nama dalam manifes.

Informasi pemasaran

Pertanyaan-pertanyaan ini terkait dengan pemasaran untuk integrasi.

Apakah deskripsi produk untuk halaman mitra CSPM Security Hub dalam 700 karakter, termasuk spasi?

Halaman mitra CSPM Security Hub hanya menerima hingga 700 karakter, termasuk spasi.

Tim akan mengedit deskripsi yang lebih panjang.

Apakah logo halaman mitra CSPM Security Hub tidak lebih besar dari 600 x 300 px?

Berikan URL yang dapat diakses publik dengan logo perusahaan dalam PNG atau JPG yang tidak lebih besar dari 600 x 300 piksel.

Apakah hyperlink Pelajari lebih lanjut di halaman mitra CSPM Security Hub mengarah ke halaman web khusus mitra tentang integrasi?

Tautan Pelajari lebih lanjut tidak boleh mengarah ke situs web utama mitra atau ke informasi dokumentasi.

Tautan ini harus selalu menuju ke halaman web khusus dengan informasi pemasaran tentang integrasi.

Apakah mitra menyediakan demo atau video instruksional tentang cara menggunakan integrasi mereka?

Video panduan demo atau integrasi adalah opsional tetapi disarankan.

Apakah posting blog Jaringan AWS Mitra dirilis dengan mitra dan manajer pengembangan mitra mereka atau perwakilan pengembangan mitra?

AWS Posting blog Jaringan Mitra harus dikoordinasikan sebelumnya dengan manajer pengembangan mitra atau perwakilan pengembangan mitra.

Ini terpisah dari posting blog apa pun yang Anda buat sendiri.

Biarkan selama 4-6 minggu lead time. Upaya ini harus dimulai setelah pengujian dengan produk pribadi ARN selesai.

Apakah siaran pers yang dipimpin mitra sedang dirilis?

Anda dapat bekerja dengan manajer pengembangan mitra atau perwakilan pengembangan mitra Anda untuk mendapatkan penawaran dari Wakil Presiden Layanan Keamanan Eksternal. Anda dapat menggunakan kutipan ini dalam siaran pers Anda.

Apakah posting blog yang dipimpin mitra sedang dirilis?

Anda dapat membuat posting blog Anda sendiri untuk menampilkan integrasi di luar blog Jaringan AWS Mitra.

Apakah webinar yang dipimpin mitra sedang dirilis?

Anda dapat membuat webinar Anda sendiri untuk menampilkan integrasi.

Jika Anda memerlukan bantuan dari tim CSPM Security Hub, bekerjalah dengan tim produk setelah Anda menyelesaikan pengujian dengan ARN produk pribadi.

Apakah mitra meminta dukungan media sosial dari AWS?

Setelah rilis, Anda dapat bekerja dengan prospek pemasaran AWS Keamanan untuk menggunakan saluran media sosial AWS resmi untuk berbagi detail tentang webinar Anda.

AWS Security Hub CSPMFAQ mitra

Berikut ini adalah pertanyaan umum tentang pengaturan dan pemeliharaan integrasi denganAWS Security Hub CSPM.

1. Apa manfaat integrasi CSPM Security Hub?
   - Kepuasan pelanggan — Alasan nomor satu untuk berintegrasi dengan Security Hub CSPM adalah karena Anda memiliki permintaan pelanggan untuk melakukannya.

     Security Hub CSPM adalah pusat keamanan dan kepatuhan bagi AWS pelanggan. Ini dirancang sebagai pemberhentian pertama di mana para profesional AWS keamanan dan kepatuhan pergi setiap hari untuk memahami keadaan keamanan dan kepatuhan mereka.

     Dengarkan pelanggan Anda. Mereka akan memberi tahu Anda jika mereka ingin melihat temuan Anda di Security Hub.
   - Peluang penemuan — Kami mempromosikan mitra dengan integrasi bersertifikat di dalam konsol CSPM Security Hub, termasuk tautan ke daftar mereka. AWS Marketplace Ini adalah cara yang bagus bagi pelanggan untuk menemukan produk keamanan baru.
   - Peluang pemasaran — Vendor dengan integrasi yang disetujui dapat berpartisipasi dalam webinar, mengeluarkan siaran pers, membuat lembar apik, dan menunjukkan integrasi mereka kepada pelanggan. AWS
2. Jenis mitra apa yang ada?
   - Mitra yang mengirimkan temuan ke Security Hub CSPM
   - Mitra yang menerima temuan dari Security Hub CSPM
   - Mitra yang mengirim dan menerima temuan
   - Mitra konsultasi yang membantu pelanggan mengatur, menyesuaikan, dan menggunakan CSPM Security Hub di lingkungan mereka
3. Bagaimana integrasi mitra dengan Security Hub CSPM bekerja pada tingkat tinggi?

   Anda mengumpulkan temuan dari dalam akun pelanggan atau dari AWS akun Anda sendiri dan mengubah format temuan ke AWS Security Finding Format (ASFF). Anda kemudian mendorong temuan tersebut ke titik akhir regional CSPM Security Hub yang sesuai.

   Anda juga dapat menggunakan CloudWatch Acara untuk menerima temuan dari Security Hub CSPM.

4. Apa langkah-langkah dasar untuk menyelesaikan integrasi dengan Security Hub CSPM?
   a. Kirimkan informasi manifes pasangan Anda.
   b. Terima produk ARNs untuk digunakan dengan Security Hub CSPM, jika Anda akan mengirimkan temuan ke Security Hub.
   c. Petakan temuan Anda ke ASFF. Lihat the section called “Pedoman pemetaan ASFF”.
   d. Tentukan arsitektur Anda untuk mengirim temuan ke dan menerima temuan dari Security Hub CSPM. Ikuti prinsip yang diuraikan dalam. the section called “Prinsip untuk membuat dan memperbarui temuan”
   e. Buat kerangka kerja penerapan untuk pelanggan. Misalnya, CloudFormation skrip dapat melayani tujuan ini.
   f. Dokumentasikan pengaturan Anda dan berikan instruksi konfigurasi untuk pelanggan.
   g. Tentukan setiap wawasan khusus (aturan korelasi) yang dapat digunakan pelanggan dengan produk Anda.
   h. Tunjukkan integrasi Anda ke tim CSPM Security Hub.
   i. Kirim informasi pemasaran untuk persetujuan (bahasa situs web, siaran pers, slide arsitektur, video, lembar apik).
5. Bagaimana proses untuk mengirimkan manifes mitra? Dan untuk AWS layanan untuk mengirimkan temuan ke Security Hub CSPM?

   ```
   <Untuk mengirimkan informasi manifes ke tim CSPM Security Hub, gunakan securit
   ```

   Anda mengeluarkan produk ARNs dalam waktu tujuh hari kalender.
6. Jenis temuan apa yang harus saya kirim ke Security Hub CSPM?

   Harga CSPM Security Hub sebagian didasarkan pada jumlah temuan yang dicerna. Karena itu, Anda harus menahan diri untuk tidak mengirimkan temuan yang tidak memberikan nilai kepada pelanggan.

   Misalnya, beberapa vendor manajemen kerentanan hanya mengirim temuan dengan skor Common Vulnerability Scoring System (CVSS) 3 atau di atas dari kemungkinan 10.
7. Apa saja pendekatan berbeda bagi saya untuk mengirim temuan ke Security Hub CSPM?

   Ini adalah pendekatan utama:

   - Anda mengirim temuan dari AWS akun mereka sendiri yang ditunjuk menggunakan `BatchImportFindings`operasi

- Anda mengirim temuan dari dalam akun pelanggan menggunakan `BatchImportFindings`operasi. Anda dapat menggunakan pendekatan peran asumsi, tetapi pendekatan ini tidak diperlukan.

Untuk panduan keseluruhan tentang penggunaan `BatchImportFindings`, lihatthe section called "Pedoman untuk menggunakan `BatchImportFindings` API".

8. Bagaimana cara mengumpulkan temuan saya dan mendorongnya ke titik akhir Regional Security Hub CSPM?

   Mitra telah menggunakan pendekatan yang berbeda untuk ini, karena sangat tergantung pada arsitektur solusi Anda.

   Misalnya, beberapa mitra membangun aplikasi Python yang dapat digunakan sebagai skrip. CloudFormation Skrip mengumpulkan temuan mitra dari lingkungan pelanggan, mengubahnya menjadi ASFF, dan mengirimkannya ke titik akhir Regional Security Hub CSPM.

   Mitra lain membangun wizard lengkap yang memberi pelanggan pengalaman sekali klik untuk mendorong temuan ke Security Hub CSPM.

9. Bagaimana saya tahu kapan harus mulai mengirimkan temuan ke Security Hub CSPM?

   Security Hub CSPM mendukung otorisasi batch sebagian untuk operasi `BatchImportFindings`API, sehingga Anda dapat mengirim semua temuan Anda ke Security Hub CSPM untuk semua pelanggan Anda.

   Jika beberapa pelanggan Anda belum berlangganan Security Hub CSPM, Security Hub CSPM tidak menyerap temuan tersebut. Itu hanya menelan temuan resmi yang ada dalam batch.

10. Langkah apa yang harus saya selesaikan untuk mengirimkan temuan ke instans CSPM Security Hub pelanggan?

    a. Pastikan kebijakan IAM yang benar berlaku.

    b. Aktifkan langganan produk (kebijakan sumber daya) untuk akun. Gunakan operasi `EnableImportFindingsForProduct`API atau halaman Integrasi. Pelanggan dapat melakukan ini, atau Anda dapat menggunakan peran lintas akun untuk bertindak atas nama pelanggan.

    c. Pastikan bahwa temuan tersebut adalah ARN publik produk Anda. `ProductArn`

    d. Pastikan bahwa temuan tersebut adalah ID akun pelanggan. `AwsAccountId`

    e. Pastikan bahwa temuan Anda tidak memiliki data yang salah sesuai dengan AWS Security Finding Format (ASFF). Misalnya, bidang wajib diisi, dan tidak ada nilai yang tidak valid.

f. Kirim temuan dalam batch ke titik akhir Regional yang benar.

11 Izin IAM apa yang harus ada bagi saya untuk mengirim temuan?

Kebijakan IAM harus dikonfigurasi untuk pengguna IAM atau peran yang memanggil `BatchImportFindings`atau panggilan API lainnya.

Tes termudah adalah melakukan ini dari akun admin. Anda dapat membatasi ini untuk `action: 'securityhub:BatchImportFindings'` dan`resource: <productArn and/or productSubscriptionArn>`.

Sumber daya di akun yang sama dapat dikonfigurasi dengan kebijakan IAM tanpa memerlukan kebijakan sumber daya.

Untuk mengesampingkan masalah kebijakan IAM dari pemanggil `BatchImportFindings`, tetapkan kebijakan IAM untuk pemanggil sebagai berikut:

```
{
    Action: 'securityhub:*',
    Effect: 'Allow',
    Resource: '*'
}
```

Pastikan untuk memeriksa bahwa tidak ada `Deny` kebijakan untuk penelepon. Setelah Anda membuatnya bekerja dengan itu, Anda dapat membatasi kebijakan sebagai berikut:

```
{
    Action: 'securityhub:BatchImportFindings',
    Effect: 'Allow',
    Resource: 'arn:aws:securityhub:<region>:<account>:product/mycompany/myproduct'
},
{
    Action: 'securityhub:BatchImportFindings',
    Effect: 'Allow',
    Resource: 'arn:aws:securityhub:<region>:*:product-subscription/mycompany/
myproduct'
}
```

12 Apa itu langganan produk?

Untuk menerima temuan dari produk mitra tertentu, pelanggan (atau mitra dengan peran lintas akun yang bekerja atas nama pelanggan) harus membuat langganan produk. Untuk melakukan

ini dari konsol, mereka menggunakan halaman Integrasi. Untuk melakukan ini dari API, mereka menggunakan operasi `EnableImportFindingsForProduct`API.

Langganan produk membuat kebijakan sumber daya yang mengizinkan temuan dari mitra untuk diterima atau dikirim oleh pelanggan. Lihat perinciannya di Kasus penggunaan dan izin.

Security Hub CSPM memiliki jenis kebijakan sumber daya berikut untuk mitra:

- `BATCH_IMPORT_FINDINGS_FROM_PRODUCT_ACCOUNT`
- `BATCH_IMPORT_FINDINGS_FROM_CUSTOMER_ACCOUNT`

Selama proses orientasi mitra, Anda dapat meminta salah satu atau kedua jenis kebijakan.

Dengan`BATCH_IMPORT_FINDINGS_FROM_PRODUCT_ACCOUNT`, Anda hanya dapat mengirimkan temuan ke Security Hub CSPM dari akun yang tercantum dalam ARN produk Anda.

Dengan`BATCH_IMPORT_FINDINGS_FROM_CUSTOMER_ACCOUNT`, Anda hanya dapat mengirim temuan dari akun pelanggan yang berlangganan kepada Anda.

13 Asumsikan pelanggan membuat akun administrator dan menambahkan beberapa akun anggota. Apakah pelanggan perlu berlangganan setiap akun anggota kepada saya? Atau apakah pelanggan hanya berlangganan dari akun administrator, dan saya kemudian dapat mengirim temuan terhadap sumber daya di semua akun anggota?

Pertanyaan ini menanyakan apakah izin dibuat untuk semua akun anggota berdasarkan pendaftaran akun administrator.

Pelanggan harus menempatkan langganan produk di tempat untuk setiap akun. Mereka dapat melakukan ini secara terprogram melalui API.

14 Apa produk ARN saya?

ARN produk Anda adalah pengenal unik yang dihasilkan oleh Security Hub CSPM untuk Anda dan yang Anda gunakan untuk mengirimkan temuan. Anda menerima produk ARN untuk setiap produk yang Anda integrasikan dengan Security Hub CSPM. Produk ARN yang benar harus menjadi bagian dari setiap temuan yang Anda kirim ke Security Hub CSPM. Temuan tanpa produk ARN dijatuhkan. Produk ARN menggunakan format berikut:

`arn:aws:securityhub:`*`[region code]`*`:`*`[account ID]`*`:product/`*`[company name]`*`/`*`[product name]`*

Inilah contohnya:

```
arn:aws:securityhub:us-west-2:222222222222:product/generico/secure-pro
```

Anda diberikan produk ARN untuk setiap Wilayah di mana Security Hub CSPM digunakan. ID akun, perusahaan, dan nama produk ditentukan oleh kiriman manifes mitra Anda. Anda tidak pernah mengubah informasi apa pun yang terkait dengan ARN produk Anda, kecuali kode Wilayah. Kode Region harus sesuai dengan Wilayah tempat Anda mengirimkan temuannya.

Kesalahan umum adalah mengubah ID akun agar sesuai dengan akun tempat Anda bekerja saat ini. ID akun tidak berubah. Anda mengirimkan ID akun “rumah” sebagai bagian dari pengiriman manifes. ID akun ini dikunci ke ARN produk Anda.

Ketika Security Hub CSPM diluncurkan di Wilayah baru, secara otomatis menggunakan kode Wilayah standar untuk menghasilkan produk ARNs Anda untuk Wilayah tersebut.

Setiap akun juga secara otomatis disediakan dengan ARN produk pribadi. Anda dapat menggunakan ARN ini untuk menguji temuan impor dalam akun pengembangan Anda sendiri sebelum Anda menerima ARN produk publik resmi Anda.

15 Format apa yang harus digunakan untuk mengirim temuan ke Security Hub CSPM?

Temuan harus disediakan dalam AWS Security Finding Format (ASFF). Untuk detailnya, lihat AWSSecurity Finding Format (ASFF) di Panduan AWS Security Hub Pengguna.

Harapannya adalah bahwa semua informasi dalam temuan asli Anda sepenuhnya tercermin dalam ASFF. Bidang kustom seperti `ProductFields` dan `Resource.Details.Other` memungkinkan Anda untuk memetakan data yang tidak cocok dengan rapi ke dalam bidang yang telah ditentukan.

16 Apa titik akhir Regional yang benar untuk digunakan?

Anda harus mengirimkan temuan ke titik akhir Regional Security Hub CSPM yang terkait dengan akun pelanggan.

17 Di mana saya dapat menemukan daftar titik akhir regional?

Lihat daftar titik akhir CSPM Security Hub.

18 Dapatkah saya mengirimkan temuan lintas wilayah?

Security Hub CSPM belum mendukung pengajuan temuan lintas wilayah untuk AWS layanan asli, seperti Amazon, Amazon GuardDuty Macie, dan Amazon Inspector. Jika pelanggan Anda mengizinkannya, Security Hub CSPM tidak mencegah Anda mengirimkan temuan dari Wilayah yang berbeda.

Dalam hal ini, Anda dapat memanggil titik akhir Regional dari mana saja, dan informasi sumber daya ASFF tidak harus cocok dengan Wilayah titik akhir. Namun, `ProductArn` harus cocok dengan Wilayah titik akhir.

19 Apa aturan dan pedoman untuk mengirim batch temuan?

Anda dapat mengumpulkan hingga 100 temuan atau 240 KB dalam satu panggilan `BatchImportFindings`. Antrian dan kumpulkan temuan sebanyak mungkin hingga batas ini.

Anda dapat mengumpulkan serangkaian temuan dari akun yang berbeda. Namun, jika salah satu akun dalam batch tidak berlangganan Security Hub CSPM, seluruh batch gagal. Ini adalah batasan model otorisasi dasar API Gateway.

Lihat the section called “Pedoman untuk menggunakan `BatchImportFindings` API”.

20 Dapatkah saya mengirim pembaruan untuk temuan yang saya buat?

Ya, jika Anda mengirimkan temuan dengan ARN produk yang sama dan ID temuan yang sama, itu menimpa data sebelumnya untuk temuan itu. Perhatikan bahwa semua data ditimpa, jadi Anda harus mengirimkan temuan lengkap.

Pelanggan diukur dan ditagih untuk temuan baru dan menemukan pembaruan.

21 Dapatkah saya mengirim pembaruan pada temuan yang dibuat orang lain?

Ya, jika pelanggan memberi Anda akses ke operasi `BatchUpdateFindings`API, Anda dapat memperbarui bidang tertentu menggunakan operasi tersebut. Operasi ini dirancang untuk digunakan oleh pelanggan, sistem tiket SIEMs, dan platform Security Orchestration, Automation, and Response (SOAR).

22 Bagaimana temuan menua?

Security Hub CSPM menua temuan 90 hari setelah tanggal pembaruan terakhir. Setelah waktu ini, temuan yang sudah tua dihapus dari cluster CSPM Security Hub. OpenSearch

Jika Anda memperbarui temuan dengan ID temuan yang sama, dan sudah tua, temuan baru akan dibuat di Security Hub CSPM.

Pelanggan dapat menggunakan CloudWatch Acara untuk memindahkan temuan dari Security Hub CSPM. Melakukan hal itu memungkinkan semua temuan dikirim ke target pilihan pelanggan.

Secara umum, Security Hub CSPM merekomendasikan agar Anda membuat temuan baru setiap 90 hari dan tidak memperbarui temuan selamanya.

23. Throttle apa yang dipasang Security Hub CSPM?

    Security Hub CSPM membatasi panggilan `GetFindings` API, karena pendekatan yang disarankan untuk mengakses temuan menggunakan Events. CloudWatch

    Security Hub CSPM tidak menerapkan pembatasan lain pada layanan internal, mitra, atau pelanggan di luar yang diberlakukan oleh pemanggilan API Gateway dan Lambda.

24. Apa ketepatan waktu atau latensi SLAs atau harapan untuk temuan yang dikirim ke Security Hub CSPM dari layanan sumber?

    Tujuannya adalah untuk mendekati waktu nyata mungkin untuk temuan awal dan pembaruan temuan. Anda harus mengirim temuan ke Security Hub CSPM dalam waktu lima menit setelah dibuat.

25. Bagaimana saya bisa menerima temuan dari Security Hub CSPM?

    Untuk menerima temuan, gunakan salah satu metode berikut.

    - Semua temuan secara otomatis dikirim ke CloudWatch Acara. Pelanggan dapat membuat aturan CloudWatch Acara tertentu untuk mengirim temuan ke target tertentu, seperti ember SIEM atau S3. Kemampuan ini menggantikan operasi `GetFindings` API lama.
    - Gunakan CloudWatch Acara untuk tindakan kustom. Security Hub CSPM memungkinkan pelanggan untuk memilih temuan atau kelompok temuan tertentu dari dalam konsol dan mengambil tindakan terhadapnya. Misalnya, mereka dapat mengirim temuan ke SIEM, sistem tiket, platform obrolan, atau alur kerja remediasi. Ini akan menjadi bagian dari alur kerja triase peringatan yang dilakukan pelanggan dalam Security Hub CSPM. Ini disebut tindakan khusus.

      Saat pengguna memilih tindakan kustom, CloudWatch peristiwa dibuat untuk temuan spesifik tersebut. Anda dapat memanfaatkan kemampuan ini dan membangun aturan dan target CloudWatch Acara untuk digunakan pelanggan sebagai bagian dari tindakan khusus. Perhatikan bahwa kemampuan ini tidak digunakan untuk secara otomatis mengirim semua temuan dari jenis atau kelas tertentu ke CloudWatch Acara. Adalah bagi pengguna untuk mengambil tindakan atas temuan tertentu.

      Anda dapat menggunakan operasi API tindakan kustom, seperti`CreateActionTarget`, untuk secara otomatis membuat tindakan yang tersedia untuk produk Anda (seperti menggunakan CloudFormation templat). Anda juga akan menggunakan operasi API aturan CloudWatch Acara

untuk membuat aturan CloudWatch Peristiwa terkait yang terkait dengan tindakan kustom. Menggunakan CloudFormation template, Anda juga dapat membuat aturan CloudWatch Acara untuk secara otomatis menyerap dari Security Hub CSPM semua temuan atau semua temuan dengan karakteristik tertentu.

26 Apa persyaratan penyedia layanan keamanan terkelola (MSSP) untuk menjadi mitra CSPM Security Hub?

Anda harus menunjukkan bagaimana Security Hub CSPM digunakan sebagai bagian dari pengiriman layanan Anda kepada pelanggan.

Anda harus memiliki dokumentasi pengguna yang menjelaskan penggunaan Security Hub CSPM.

Jika MSSP adalah penyedia temuan, mereka harus menunjukkan pengiriman temuan ke Security Hub CSPM.

Jika MSSP hanya menerima temuan dari Security Hub CSPM, mereka harus setidaknya memiliki CloudFormation template untuk mengatur aturan Acara yang sesuai. CloudWatch

27 Apa persyaratan bagi Mitra Konsultasi APN non-MSSP untuk menjadi mitra CSPM Security Hub?

Jika Anda adalah APN Consulting Partner, Anda dapat menjadi mitra CSPM Security Hub. Anda harus menyerahkan dua studi kasus pribadi tentang bagaimana Anda membantu pelanggan tertentu melakukan hal berikut.

- Siapkan Security Hub CSPM dengan izin IAM yang dibutuhkan pelanggan.
- Membantu menghubungkan solusi vendor perangkat lunak independen (ISV) yang sudah terintegrasi ke Security Hub CSPM menggunakan instruksi konfigurasi pada halaman mitra di konsol.
- Bantu pelanggan dengan integrasi produk khusus.
- Bangun wawasan khusus yang relevan dengan kebutuhan dan kumpulan data pelanggan.
- Membangun tindakan kustom.
- Bangun buku pedoman remediasi.
- Bangun Quickstarts yang selaras dengan standar kepatuhan CSPM Security Hub. Ini harus divalidasi oleh tim CSPM Security Hub.

Studi kasus tidak perlu dibagikan secara publik.

28 Apa persyaratan seputar bagaimana saya menerapkan integrasi saya dengan Security Hub CSPM dengan pelanggan saya?

Arsitektur integrasi antara Security Hub CSPM dan produk mitra bervariasi dari mitra ke mitra dalam hal bagaimana solusi mitra tersebut dioperasikan. Anda harus memastikan bahwa proses penyiapan untuk integrasi tidak lebih dari 15 menit.

Jika Anda menerapkan perangkat lunak integrasi ke AWS lingkungan pelanggan, Anda harus memanfaatkan CloudFormation template untuk menyederhanakan integrasi. Beberapa mitra telah menciptakan integrasi satu klik, yang sangat dianjurkan.

29 Apa persyaratan dokumentasi saya?

Anda harus memberikan tautan ke dokumentasi yang menjelaskan proses integrasi dan penyiapan antara produk Anda dan CSPM Security Hub, termasuk penggunaan CloudFormation templat Anda.

Dokumentasi itu juga harus mencakup informasi tentang penggunaan ASFF Anda. Secara khusus, ini harus mencantumkan jenis temuan ASFF yang Anda gunakan untuk temuan Anda yang berbeda. Jika Anda memiliki definisi wawasan default, kami sarankan Anda juga memasukkannya di sini.

Pertimbangkan untuk memasukkan informasi potensial lainnya:

- Kasus penggunaan Anda untuk integrasi dengan Security Hub CSPM
- Rata-rata volume temuan yang dikirim
- Arsitektur integrasi Anda
- Daerah yang Anda lakukan dan tidak mendukung
- Latensi antara saat temuan dibuat dan saat dikirim ke Security Hub
- Apakah Anda memperbarui temuan

30 Apa itu wawasan khusus?

Anda didorong untuk mendefinisikan wawasan khusus untuk temuan Anda. Wawasan adalah aturan korelasi ringan yang membantu pelanggan memprioritaskan temuan dan sumber daya mana yang paling membutuhkan perhatian dan tindakan.

Security Hub CSPM memiliki operasi `CreateInsight` API. Anda dapat membuat wawasan khusus di dalam akun pelanggan sebagai bagian dari CloudFormation template Anda. Wawasan ini muncul di konsol pelanggan.

31 Bisakah saya mengirimkan widget dasbor?

Tidak, tidak saat ini. Anda hanya dapat membuat wawasan terkelola.

32 Apa model harga Anda?

Lihat informasi harga CSPM Security Hub.

33 Bagaimana cara mengirimkan temuan ke akun demo CSPM Security Hub sebagai bagian dari proses persetujuan akhir untuk integrasi saya?

Kirim temuan ke akun demo CSPM Security Hub menggunakan ARN produk yang Anda berikan, gunakan `us-west-2` sebagai Wilayah. Temuan harus mencakup nomor akun demo di `AwsAccountId` bidang ASFF. Untuk mendapatkan nomor akun demo, hubungi tim CSPM Security Hub.

Jangan mengirimkan data sensitif atau informasi identitas pribadi kepada kami. Data ini digunakan untuk demo publik. Ketika Anda mengirimkan data ini kepada kami, Anda memberi wewenang kepada kami untuk menggunakannya dalam demo.

34 Kesalahan atau pesan sukses apa yang **`BatchImportFindings`** diberikan?

Security Hub CSPM memberikan respons untuk otorisasi dan respons untuk. `BatchImportFindings` Pesan sukses, kegagalan, dan kesalahan yang lebih tajam sedang dalam pengembangan.

35 Penanganan kesalahan apa yang menjadi tanggung jawab layanan sumber?

Layanan sumber bertanggung jawab atas semua penanganan kesalahan. Mereka harus menangani pesan kesalahan, percobaan ulang, pelambatan, dan mengkhawatirkan. Mereka juga harus menangani umpan balik atau pesan kesalahan yang dikirim melalui mekanisme umpan balik CSPM Security Hub.

36 Apa sajakah resolusi untuk masalah umum?

An `AuthorizerConfigurationException` disebabkan oleh cacat `AwsAccountId` atau`ProductArn`.

Saat memecahkan masalah, perhatikan hal berikut:

- `AwsAccountId`harus 12 digit persis.
- `ProductArn`harus dalam format berikut: arn:aws:securityhub: ::product//*<us-west-2 or us-east-1><accountId><company-id><product-id>*

ID akun tidak berubah dari yang disertakan oleh tim CSPM Security Hub dalam produk ARNs yang mereka berikan kepada Anda.

`AccessDeniedException`disebabkan ketika temuan dikirim ke atau dari akun yang salah, atau ketika akun tidak memiliki`ProductSubscription`. Pesan kesalahan akan berisi ARN dengan jenis sumber daya atau. `product` `product-subscription` Kesalahan ini hanya terjadi selama panggilan lintas akun. Jika Anda menelepon `BatchImportFindings`dengan akun Anda sendiri untuk akun yang sama di `AwsAccountId` dan`ProductArn`, operasi menggunakan kebijakan IAM dan tidak ada hubungannya dengan`ProductSubscriptions`.

Pastikan akun pelanggan dan akun produk yang Anda gunakan adalah akun terdaftar yang sebenarnya. Beberapa mitra telah menggunakan nomor akun untuk produk dari produk ARN, tetapi cobalah untuk menggunakan akun yang sama sekali berbeda untuk menelepon. `BatchImportFindings` Dalam kasus lain, mereka membuat `ProductSubscriptions` untuk akun pelanggan lain, atau bahkan untuk akun produk mereka sendiri. Mereka tidak membuat `ProductSubscriptions` akun pelanggan yang mereka coba impor temuannya.

37 Di mana saya mengirim pertanyaan, komentar, dan bug?

`<securityhub-partners@amazon.com>`

38 Ke Wilayah mana saya mengirimkan temuan untuk item yang terkait dengan AWS layanan global? Misalnya, di mana saya mengirim temuan terkait IAM?

Kirim temuan ke Wilayah yang sama di mana temuan itu terdeteksi. Untuk layanan seperti IAM, solusi Anda kemungkinan akan menemukan masalah IAM yang sama di beberapa Wilayah. Dalam hal ini, temuan dikirim ke setiap Wilayah di mana masalah terdeteksi.

Jika pelanggan menjalankan Security Hub CSPM di tiga Wilayah, dan masalah IAM yang sama terdeteksi di ketiga Region, maka kirimkan temuan tersebut ke ketiga Region.

Saat masalah teratasi, kirim pembaruan ke temuan ke semua Wilayah tempat Anda mengirim temuan asli.

Riwayat dokumen untuk Panduan Integrasi Mitra

Tabel berikut menjelaskan pembaruan dokumentasi untuk panduan ini.

Perubahan	Deskripsi	Tanggal
Persyaratan yang diperbarui untuk logo konsol	Memperbarui manifes mitra dan pedoman logo untuk menunjukkan bahwa mitra harus menyediakan mode terang dan versi mode gelap logo untuk ditampilkan di konsol CSPM Security Hub. Logo harus format SVG.	10 Mei 2021
Memperbarui prasyarat untuk mitra integrasi baru	Security Hub CSPM sekarang juga memungkinkan mitra yang telah bergabung dengan jalur Mitra AWS ISV, dan yang menggunakan produk integrasi yang telah menyelesaikan AWS Foundational Technical Review (FTR). Sebelumnya, semua mitra integrasi diharuskan menjadi AWS Select Tier Partners.	29 April 2021
`FindingProviderFields` Objek baru di ASFF	Memperbarui informasi tentang temuan pemetaan ke ASFF. Untuk`Confidence`, `Criticality`, `RelatedFindings`, `Severity`, dan`Types`, mitra memetakan nilai mereka ke bidang	18 Maret 2021

	di`FindingProviderFields` .	
Prinsip baru untuk membuat dan memperbarui temuan	Menambahkan seperangkat pedoman baru untuk membuat temuan baru dan memperbarui temuan yang ada di Security Hub CSPM.	4 Desember 2020
Rilis awal panduan ini	Panduan Integrasi Mitra ini memberi AWS mitra informasi tentang cara membangun integrasi denganAWS Security Hub CSPM.	23 Juni 2020

Terjemahan disediakan oleh mesin penerjemah. Jika konten terjemahan yang diberikan bertentangan dengan versi bahasa Inggris aslinya, utamakan versi bahasa Inggris.