Panduan Integrasi Mitra

AWS Security Hub

AWS Security Hub: Panduan Integrasi Mitra

Table of Contents

Ikhtisar integrasi pihak ketiga denganAWS Security Hub

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

Sebagai Partner APN, Anda bisa berintegrasi dengan Security Hub dengan satu atau beberapa cara berikut.

- Kirim temuan ke Security Hub
- Mengkonsumsi temuan dari Security Hub
- Keduanya mengirim temuan dan mengkonsumsi temuan dari Security Hub
- Gunakan Security Hub sebagai pusat penawaran penyedia layanan keamanan terkelola (MSSP)
- Konsultasikan denganAWSpelanggan tentang cara menyebarkan dan menggunakan Security Hub

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

Topik

Mengapa mengintegrasikan denganAWS Security Hub?

AWS Security Hubmemberikan pandangan komprehensif tentang pemberitahuan keamanan prioritas tinggi dan status keamanan di seluruh akun Security Hub. Security Hub memungkinkan mitra seperti Anda untuk mengirim temuan keamanan ke Security Hub untuk memberikan pelanggan Anda wawasan tentang temuan keamanan yang Anda hasilkan.

Integrasi dengan Security Hub dapat menambah nilai dengan cara berikut.

- Memuaskan pelanggan Anda yang telah meminta integrasi Security Hub
- Menyediakan pelanggan Anda dengan pandangan tunggal dari merekaAWSTemuan yang terkait dengan keamanan

- Memungkinkan pelanggan baru untuk menemukan solusi Anda ketika mereka mencari mitra yang memberikan temuan yang terkait dengan jenis peristiwa keamanan tertentu

Sebelum Anda membangun integrasi dengan Security Hub, periksa alasan integrasi Anda. Integrasi lebih mungkin berhasil jika pelanggan Anda menginginkan integrasi 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 keAWS Security Hub

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

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

1. Memetakan temuan keamanan Anda keAWSFormat Pencarian Keamanan (ASFF).
2. Bangun arsitektur integrasi Anda untuk mendorong temuan ke titik akhir Security Hub Regional yang benar. Untuk melakukan ini, Anda menentukan apakah Anda akan mengirim temuan dari Anda sendiriAWSakun atau dari dalam akun pelanggan Anda.
3. Mintalah pelanggan Anda berlangganan produk ke akun mereka. Untuk melakukan ini, mereka bisa menggunakan konsol atau`EnableImportFindingsForProduct`Operasi API. LihatMengelola integrasi produkdi dalamAWS Security HubPanduan Pengguna.

   Anda juga dapat berlangganan produk untuk mereka. Untuk melakukan ini, Anda menggunakan peran lintas-akun untuk mengakses`EnableImportFindingsForProduct`Operasi 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.

- Mengumumkan Integrasi Cloud Kustodian denganAWS Security Hub
- GunakanAWS Fargatedan Prowler untuk mengirim temuan konfigurasi keamanan tentangAWSLayanan ke Security Hub
- Cara mengimporAWS Configevaluasi aturan sebagai temuan di Security Hub

Mempersiapkan untuk menerima temuan dariAWS Security Hub

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

- Minta pelanggan Anda secara otomatis mengirim semua temuan keCloudWatchPeristiwa. Pelanggan dapat membuat spesifikCloudWatchaturan acara untuk mengirim temuan ke target tertentu, seperti SIEM atau ember S3.
- Minta pelanggan Anda memilih temuan tertentu atau kelompok temuan dari dalam konsol Security Hub dan kemudian mengambil tindakan terhadap mereka.

Misalnya, pelanggan Anda dapat mengirimkan temuan ke SIEM, sistem tiket, platform obrolan, atau alur kerja remediasi. Ini akan menjadi bagian dari alur kerja siaga triase bahwa pelanggan melakukan dalam Security Hub.

Ini disebut tindakan kustom. Ketika pengguna mengambil tindakan kustom, aCloudWatchacara dibuat untuk temuan spesifik tersebut. Sebagai mitra, Anda dapat memanfaatkan kemampuan ini dan membangunCloudWatchaturan acara atau target untuk pelanggan untuk digunakan sebagai bagian dari tindakan kustom. Perhatikan bahwa kemampuan ini tidak secara otomatis mengirim semua temuan dari jenis atau kelas tertentu keCloudWatchPeristiwa. Fitur ini adalah bagi pengguna untuk mengambil tindakan pada temuan tertentu.

Posting blog berikut menguraikan solusi yang menggunakan integrasi dengan Security Hub danCloudWatchAcara untuk tindakan kustom.

- Cara MengintegrasikanAWS Security HubTindakan Kustom denganPagerDuty
- Cara Aktifkan Tindakan Kustom diAWS Security Hub
- Cara mengimporAWS Configevaluasi aturan sebagai temuan di Security Hub

Sumber daya tentangAWS Security Hub

Bahan-bahan berikut dapat membantu Anda untuk lebih memahamiAWS Security Hubsolusi dan bagaimanaAWSpelanggan dapat menggunakan layanan ini.

- PengantarAWS Security Hubvideo
- Panduan Pengguna Security Hub
- Referensi API Security Hub
- Webinar

Kami juga mendorong Anda untuk mengaktifkan Security Hub di salah satuAWSaccount dan mendapatkan beberapa pengalaman langsung dengan layanan ini.

Prasyarat mitra

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

- Anda adalahAWSPilih Partner Tingkat atau di atas.
- Anda telah bergabung dengan[AWSJalur Mitra ISV](), dan produk yang Anda gunakan untuk integrasi Security Hub telah menyelesaikan[AWSTinjauan Teknis Dasar (FTR)](). Produk ini kemudian diberikan “Diulas olehAWS“lencana.

Anda juga harus memiliki perjanjian nondisclosure bersama di tempat denganAWS.

Kasus penggunaan integrasi dan izin yang diperlukan

AWS Security HubmemungkinkanAWSpelanggan untuk menerima temuan dari Mitra APN. Produk mitra mungkin berjalan baik di dalam maupun di luar pelangganAWSakun. Konfigurasi izin di akun pelanggan berbeda berdasarkan model yang digunakan oleh produk mitra.

Di Security Hub, pelanggan selalu mengontrol mitra mana yang dapat mengirim 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. Langkah berlangganan diperlukan untuk semua kasus penggunaan yang diuraikan di bawah ini. Untuk detail tentang cara pelanggan mengelola integrasi produk, lihatMengelola Integrasi ProdukdiAWS Security HubPanduan Pengguna.

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

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

Partner host: temuan yang dikirim dari akun mitra

Kasus penggunaan ini mencakup mitra yang meng-host produk sendiriAWSakun. Untuk mengirim temuan keamanan untukAWSpelanggan, mitra memanggil`BatchImportFindings`Operasi API dari akun produk mitra.

Untuk kasus penggunaan ini, akun pelanggan hanya membutuhkan izin yang ditetapkan ketika pelanggan berlangganan produk mitra.

Di akun mitra, kepala sekolah IAM yang memanggil`BatchImportFindings`Operasi API harus memiliki kebijakan IAM yang memungkinkan kepala sekolah untuk menelepon`BatchImportFindings`.

Mengaktifkan produk mitra untuk mengirim temuan kepada pelanggan di Security Hub adalah proses dua langkah:

1. Pelanggan membuat langganan produk mitra di Security Hub.

2. Security Hub menghasilkan kebijakan sumber daya terkelola yang benar dengan konfirmasi pelanggan.

Untuk mengirim temuan keamanan yang terkait dengan akun pelanggan, produk mitra menggunakan kredensialnya sendiri untuk menghubungiBatchImportFindingsOperasi API.

Berikut adalah contoh kebijakan IAM yang memberikan kepala sekolah di akun mitra izin Security Hub yang diperlukan.

```
{
    "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"
        }
    ]
}
```

Partner host: temuan yang dikirim dari akun pelanggan

Kasus penggunaan ini mencakup mitra yang meng-host produk sendiriAWSakun, tetapi menggunakan peran lintas-akun untuk mengakses akun pelanggan. Mereka menyebutBatchImportFindingsOperasi API dari akun pelanggan.

Untuk kasus penggunaan ini, untuk memanggilBatchImportFindingsOperasi API, akun mitra mengasumsikan peran IAM yang dikelola pelanggan dalam akun pelanggan.

Panggilan ini dibuat dari akun pelanggan. Oleh karena itu, kebijakan sumber daya yang dikelola harus memungkinkan ARN produk untuk akun produk mitra untuk digunakan dalam panggilan. Security Hub mengelola kebijakan sumber daya memberikan izin untuk akun produk mitra dan produk mitra ARN. Produk ARN adalah pengenal unik mitra sebagai penyedia. Karena panggilan tidak berasal dari akun produk mitra, pelanggan harus secara eksplisit memberikan izin untuk produk mitra untuk mengirim temuan ke Security Hub.

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 mengasumsikan peran. Pengidentifikasi eksternal menyediakan lapisan keamanan tambahan saat memberikanAWSakses akun ke mitra. Pengenal unik memastikan bahwa mitra menggunakan akun pelanggan yang benar.

Mengaktifkan produk mitra untuk mengirim temuan kepada pelanggan di Security Hub dengan peran lintas-akun terjadi dalam empat langkah:

1. Pelanggan, atau mitra yang menggunakan peran lintas-akun yang bekerja atas nama pelanggan, memulai berlangganan produk di Security Hub.
2. Security Hub menghasilkan kebijakan sumber daya terkelola yang benar dengan konfirmasi pelanggan.
3. Pelanggan mengonfigurasi peran lintas-akun baik secara manual atau menggunakanAWS CloudFormation. Untuk informasi tentang peran lintas akun, lihatMenyediakan akses keAWSakun yang dimiliki oleh pihak ketigadiPanduan Pengguna IAM.
4. Produk ini menyimpan peran pelanggan dan ID eksternal dengan aman.

Selanjutnya, produk mengirimkan temuan ke Security Hub:

1. Produk ini memanggilAWS Security Token Service(AWS STS) untuk mengasumsikan peran pelanggan.
2. Produk ini memanggilBatchImportFindingsOperasi API di Security Hub dengan kredensi sementara peran yang diasumsikan.

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

```
{
    "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"
        }
    ]
```

```
}
```

Parameter`Resource`bagian dari kebijakan mengidentifikasi langganan produk tertentu. Hal ini memastikan bahwa mitra hanya dapat mengirimkan temuan untuk produk mitra yang pelanggan berlangganan.

Pelanggan di-host: temuan yang dikirim dari akun pelanggan

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

Untuk kasus penggunaan ini, produk mitra harus diberikan izin tambahan untuk menghubungi`BatchImportFindings`API. Bagaimana izin ini diberikan berbeda berdasarkan solusi mitra dan bagaimana izin ini 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 kemampuan untuk memanggil`BatchImportFindings`Operasi API. 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 mengirim temuan dari akun pelanggan ke pelanggan di Security Hub:

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

Sekarang produk dapat mengirim temuan ke Security Hub:

1. Produk mitra menggunakanAWSSDK atauAWS CLIuntuk memanggil`BatchImportFindings`Operasi API di Security Hub. 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 untuk berhasil.

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

```
{
    "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 onboarding Anda. Anda harus menyelesaikan langkah-langkah ini sebelum Anda dapat mengirim temuan keamanan keAWS Security Hub.

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

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

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

   Versi awal dari manifes integrasi produk ini tidak harus memiliki rincian lengkap. Tapi setidaknya harus berisi kasus penggunaan dan informasi dataset.

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

   Pemetaan temuan ke ASFF

   Untuk mengirim temuan ke Security Hub, Anda harus memetakan temuan Anda keAWSFormat Pencarian Keamanan (ASFF).

   ASFF memberikan deskripsi konsisten temuan yang dapat dibagi antaraAWSlayanan keamanan, mitra, dan sistem keamanan pelanggan. Hal ini mengurangi upaya integrasi, mendorong bahasa yang sama, dan memberikan cetak biru bagi pelaksana.

ASFF adalah format protokol kawat yang diperlukan untuk digunakan untuk mengirim temuan keAWS Security Hub. Temuan direpresentasikan sebagai dokumen JSON yang mematuhi ASFF JSON Schema dan RFC-7493 The I-JSON Message Format. Untuk rincian tentang skema ASFF, lihatAWSFormat Pencarian Keamanan (ASFF)diAWS Security HubPanduan Pengguna.

Lihat the section called “Pedoman pemetaan ASFF”.

Membangun dan menguji integrasi

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

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

Sepanjang pembangunan integrasi Security Hub,AWSmendorong Anda untuk menjaga kontak APN Partner Anda informasi tentang kemajuan integrasi Anda. Anda juga dapat meminta kontak APN Partner Anda untuk mendapatkan bantuan terkait pertanyaan integrasi.

Lihat the section called “Pedoman penggunaan`BatchImportFindings`API”.

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

   Jika mereka merasa nyaman dengan integrasi, tim Security Hub memberikan persetujuan untuk bergerak maju ke daftar Anda sebagai penyedia.
8. Anda menyediakanAWSdengan manifes akhir untuk ditinjau.
9. Tim Security Hub menciptakan integrasi penyedia di konsol Security Hub. Pelanggan kemudian dapat menemukan dan mengaktifkan integrasi.
10. (Opsional) Anda terlibat dalam upaya pemasaran tambahan untuk mempromosikan integrasi Security Hub Anda. Lihat Go-to-marketaktivitas.

    Minimal, Security Hub merekomendasikan agar Anda menyediakan aset berikut.

    - Video demonstrasi (paling banyak 3 menit) dari integrasi kerja. Video ini digunakan untuk tujuan pemasaran dan diposting keAWS YouTubesaluran.
    - Diagram arsitektur satu-slide untuk ditambahkan ke dek geser panggilan pertama Security Hub.

Go-to-marketaktivitas

Mitra juga dapat terlibat dalam kegiatan pemasaran opsional untuk membantu menjelaskan dan mempromosikan merekaAWS Security Hubintegrasi.

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

Setelah Anda disetujui sebagai mitra Security Hub, solusi Anda dapat ditampilkan diAWS Security HubHalaman mitra.

Untuk tercantum di halaman ini, berikan rincian berikut ke kontak Partner APN Anda. Ini bisa menjadi manajer pengembangan mitra Anda (PDM), arsitek solusi mitra (PSA), atau email ke<securityhub-pms@amazon.com>.

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

Rilis 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 mempublikasikan siaran pers, Anda harus mengirimkannya keAWSuntuk ditinjau oleh pemasaran Mitra APN, kepemimpinan Security Hub, danAWSLayanan Keamanan Eksternal (ESS). Siaran pers dapat mencakup penawaran yang diusulkan untuk VP ESS.

Untuk memulai proses ini, bekerja dengan PDM Anda. Kami memiliki Service Level Agreement (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. Hal ini tidak dapat diposisikan semata-mata 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 item berikut.

Apa yang masuk ke posting blog?

- Posting mitra harus edukasi dan memberikan keahlian mendalam tentang topik yang relevanAWSpelanggan.
- 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 repurpose konten dari sumber seperti posting blog yang ada atau whitepaper.

Apa batasan lain dalam memposting ke blog APN?

- Hanya mitra tingkat lanjut atau Premier yang dapat memposting ke blog APN. Ada pengecualian untuk mitra Pilih yang memiliki Penunjukan Program APN seperti Pengiriman Layanan.
- Setiap mitra terbatas pada tiga posting per tahun. Dengan puluhan ribu Mitra APN,AWSharus adil dalam cakupannya.
- Setiap posting 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 waktu empat sampai enam minggu untuk mengedit.

Mengapa menulis untuk blog APN?

Posting blog APN dapat memberikan manfaat sebagai berikut.

- Kredibilitas— Untuk Mitra APN, memiliki cerita yang diterbitkan olehAWSdapat mempengaruhi pelanggan secara global.
- Visibilitas— Blog APN adalah salah satu blog yang paling banyak dibaca diAWSdengan 1.79 juta tampilan halaman pada tahun 2019, termasuk lalu lintas yang dipengaruhi.
- Bisnis— Posting Partner APN memiliki tombol connect yang dapat menghasilkan prospek melalui program APN Customer Engagements (ACE).

Apa jenis konten 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 bagaimana-untuk. Lebih dari 75% pembaca melihat konten teknis ini.
- Pelanggan menghargai 200 tingkat atau di atas cerita yang menunjukkan bagaimana sesuatu bekerja padaAWSatau bagaimana Mitra APN memecahkan masalah bisnis bagi pelanggan.
- Tulisan yang ditulis oleh para ahli teknis atau ahli materi pelajaran melakukan yang terbaik sejauh ini.

Lembar licin atau lembar pemasaran

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

Jika Anda membuat lembar licin untuk integrasi Anda, kirim salinan ke tim 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 Security Hub. Mereka akan menambahkannya ke halaman mitra Security Hub.

Webinar

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

Tim juga dapat menyediakan ahli subjek Security Hub untuk berpartisipasi dalam webinar Anda.

Video demo

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

manifes integrasi produk

Setiap mitraAWS Security Hub integrasi harus menyelesaikan manifes integrasi produk yang memberikan rincian yang diperlukan untuk integrasi yang diusulkan.

Tim Security Hub menggunakan informasi ini dalam beberapa cara:

- Untuk membuat daftar situs web
- Untuk membuat kartu produk untuk konsol Security Hub
- Untuk menginformasikan tim produk kasus penggunaan Anda.

Untuk mengevaluasi kualitas integrasi yang diusulkan dan informasi yang diberikan, tim Security Hub menggunakanthe 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 halamanAWS Security Hub mitra. Perhatikan bahwa halaman mitra tidak tersedia di Wilayah China (Ningxia).

Daftar Isi

  - Tipe temuan
  - Hotline
  - Temuan detak jantung
- AWS Security Hubinformasi konsol
  - Informasi perusahaan informasi perusahaan
  - Informasi Produk

Kasus penggunaan dan informasi pemasaran

Kasus penggunaan berikut dapat membantu Anda mengonfigurasiAWS Security Hub untuk tujuan yang berbeda.

Menemukan penyedia dan kasus penggunaan konsumen

Diperlukan untuk vendor perangkat lunak independen (ISV).

Untuk menjelaskan kasus penggunaan Anda seputar integrasi AndaAWS Security Hub, 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 mengirim temuan, jenis temuan apa yang akan Anda kirim? Apakah Anda akan mengirim semua temuan atau subset temuan tertentu?
- Jika Anda berencana untuk menerima temuan, apa yang akan Anda lakukan dengan temuan itu? 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 menyarankan agar Anda memperbarui temuan daripada 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 untuk temuan yang telah Anda kirim.

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

Kasus penggunaan Mitra Konsultasi (CP)

Diperlukan jika Anda adalah Mitra Konsultasi Security Hub.

Menyediakan dua kasus penggunaan pelanggan untuk pekerjaan Anda dengan Security Hub. Ini bisa berupa kasus penggunaan pribadi. Tim Security Hub tidak mengiklankannya di mana pun. Mereka harus menggambarkan salah satu atau kedua tindakan berikut.

- Bagaimana Anda membantu pelanggan bootstrap Security Hub? Misalnya, sudahkah Anda membantu pelanggan menggunakan layanan profesional, modul Terraform, atauAWS CloudFormation templat?
- Bagaimana Anda membantu pelanggan mengoperasikan dan memperluas Security Hub? Misalnya, sudahkah Anda memberikan template respons atau remediasi, integrasi kustom yang dibangun, atau menggunakan alat intelijen bisnis untuk menyiapkan dasbor eksekutif?

Set Data

Diperlukan jika Anda mengirim temuan ke Security Hub.

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

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

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

Arsitektur

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

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

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

- AWSLayanan apa, agen sistem operasi, dan sebagainya yang akan Anda gunakan?
- Jika Anda akan mengirim temuan ke Security Hub, apakah Anda akan mengirimkan temuan dariAWS akun pelanggan atau dariAWS akun Anda sendiri?
- Jika Anda akan menerima temuan, bagaimana Anda akan menggunakan integrasi CloudWatch Acara?
- Bagaimana Anda akan mengkonversi temuan ke ASFF?
- Bagaimana Anda akan batch temuan, melacak kondisi temuan, dan menghindari batas throttling?

Konfigurasi

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

Jelaskan bagaimana pelanggan akan mengonfigurasi integrasi Anda dengan Security Hub.

Minimal, Anda harus menggunakanAWS 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.

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

Latensi

Diperlukan jika Anda mengirim temuan ke Security Hub.

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

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.

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

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

Setiap deskripsi tidak boleh lebih dari 700 karakter dengan spasi.

Aset situs web mitra mitra

Diperlukan untuk semua integrasi dengan Security Hub.

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

Jika Anda mengintegrasikan beberapa produk dengan Security Hub, Anda dapat memiliki satu halaman arahan untuk mereka. Security Hub menyarankan agar halaman arahan ini menyertakan tautan ke petunjuk konfigurasi Anda.

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

Logo untuk halaman mitra

Diperlukan untuk semua integrasi Security Hub.

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

- Ukuran: 600 x 300 piksel
- Cropping: ketat tanpa padding
- Latar belakang: transparan
- Format: PNG

Logo untuk konsol Security Hub

Diperlukan untuk semua integrasi.

Berikan URL ke mode cahaya dan logo mode gelap untuk ditampilkan di konsol Security Hub.

Logo harus memenuhi kriteria berikut:

- Format: SVG
- Ukuran: 175 x 40 piksel. Jika lebih besar, gambar harus menggunakan rasio itu.
- Cropping: ketat tidak ada padding
- 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.

Berikan tabel yang mendokumentasikan jenis temuan berformat ASFF yang Anda gunakan dan bagaimana mereka menyelaraskan dengan jenis temuan asli Anda. Untuk detail tentang menemukan jenis di ASFF, lihat Jenis taksonomi untuk ASFF di AWS Security HubUser Guide.

Sebaiknya Anda juga menyertakan informasi ini dalam dokumentasi produk Anda.

Hotline

Diperlukan untuk semua integrasi dengan Security Hub.

Berikan alamat email dan nomor telepon atau nomor pager untuk titik kontak teknis. Security Hub 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.

Temuan detak jantung

Direkomendasikan jika Anda mengirim temuan ke Security Hub.

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

Jika Anda bisa, maka lakukanlah dengan menggunakan jenis temuan`Heartbeat`.

AWS Security Hubinformasi konsol

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

Informasi perusahaan 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 berikut:

Bidang	Diperlukan	Deskripsi
`id`	Ya	Pengenal unik perusahaan. Pengenal perusahaan harus unik di seluruh perusahaan. Ini kemungkinan sama dengan atau mirip dengan`name`. Jenis: String Panjang minimum: 5 karakter Panjang maksimum: 24 karakter Karakter yang diizinkan: huruf kecil, angka, dan tanda hubung

Bidang	Diperlukan	Deskripsi
		Harus dimulai dengan huruf kecil. Harus diakhiri dengan huruf kecil atau angka.
`name`	Ya	Nama perusahaan penyedia yang akan ditampilkan di konsol Security Hub. Jenis: String Panjang maksimum: 16 karakter
`description`	Ya	Deskripsi perusahaan penyedia yang akan ditampilkan pada konsol Security Hub. Jenis: String Panjang maksimum: 200 karakter

Informasi Produk

Bagian ini menyediakan 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 berikut.

Bidang	Diperlukan	Deskripsi
`IntegrationType`	Ya	Menunjukkan apakah produk Anda mengirimk an temuan ke Security Hub, menerima temuan dari Security Hub, atau keduanya mengirim dan menerima temuan. Jika Anda adalah Mitra Konsultasi, biarkan bidang ini kosong. Tipe: Array string: Array string. Nilai yang valid: `SEND_FINDINGS_TO_S ECURITY_HUB` | `RECEIVE_FINDINGS_F ROM_SECURITY_HUB`
`id`	Ya	Pengenal unik produk. Ini harus unik dalam perusahaan. Ia tidak perlu bersifat unik di seluruh perusahaan. Ini kemungkinan sama atau mirip dengan`name`. Jenis: 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 dariAWS Wilayah berikut yang tidak Anda dukung? Dengan kata lain, di Wilayah mana yang seharusnya Security Hub tidak menunjukkan kepada Anda sebagai opsi di halaman mitra kami di konsol Security Hub? Jenis: String

Bidang	Diperlukan	Deskripsi
		Berikan kode Wilayah saja. Sebagai contoh, `us-west-1` . Untuk daftar Wilayah, lihat Titik akhir Regional di Referensi Umum AWS. Kode Wilayah untukAWS GovCloud (US) areus-gov-west-1 (untukAWS GovCloud (AS-Barat)) danus-gov-east-1 (untukAWS GovCloud (AS-timur)). Kode Wilayah untuk Wilayah China adalahcn-north-1 (untuk China (Beijing)) dancn-northwest-1 (untuk Tiongkok (Ningxia)).

Bidang	Diperlukan	Deskripsi
`commercialAccountNumber`	Ya	NomorAWS akun utama untuk produk untukAWS Wilayah. Jika Anda mengirim temuan ke Security Hub, maka akun yang Anda berikan didasarkan pada tempat Anda mengirim temuan tersebut. • DariAWS akun Anda. Dalam hal ini, berikan nomor akun yang Anda gunakan untuk mengirimkan temuan. • DariAWS akun pelanggan. Dalam hal ini, Security Hub menyarankan 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 hal ini tidak memungkinkan, hubungi tim Security Hub. Jika Anda hanya menerima temuan dari Security Hub, nomor akun ini tidak diperlukan. Jenis: String

Bidang	Diperlukan	Deskripsi
`govcloudAccountNumber`	Tidak	NomorAWS akun utama untuk produk untukAWS GovCloud (US) Wilayah (jika produk Anda tersedia diAWS GovCloud (US)). Jika Anda mengirim temuan ke Security Hub, maka akun yang Anda berikan didasarkan pada tempat Anda mengirim temuan tersebut. • DariAWS akun Anda. Dalam hal ini, berikan nomor akun yang Anda gunakan untuk mengirimkan temuan. • DariAWS akun pelanggan. Dalam hal ini, Security Hub menyarankan Anda memberikan nomor akun utama yang Anda gunakan untuk menguji integrasi. Idealnya Anda menggunakan akun yang sama untuk semua produk Anda di semuaAWS GovCloud (US) Wilayah. Jika hal ini tidak memungkinkan, hubungi tim Security Hub. Jika Anda hanya menerima temuan dari Security Hub, nomor akun ini tidak diperlukan. Jenis: String

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

Bidang	Diperlukan	Deskripsi
`description`	Ya	Deskripsi produk penyedia untuk ditampilkan di konsol Security Hub. Jenis: String Panjang maksimum: 200 karakter
`importType`	Ya	Jenis kebijakan sumber daya untuk mitra. Selama proses orientasi mitra, Anda dapat menentukan salah satu dari kebijakan sumber daya berikut, atau Anda dapat menentuka nNEITHER. • DenganBATCH_IMPORT_FINDINGS_FROM_PRODUCT_ACCOUNT , Anda hanya dapat mengirim temuan ke Security Hub dari akun yang tercantum dalam ARN produk Anda. • DenganBATCH_IMPORT_FINDINGS_FROM_CUSTOMER_ACCOUNT , Anda hanya dapat mengirim temuan dari akun pelanggan yang berlangganan Anda. Jenis: 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 Security Hub. Pilih hingga tiga kategori. Pilihan kustom tidak diperbolehkan. Jika menurut Anda kategori Anda hilang, hubungi tim Security Hub. Tipe: 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 keAWS Marketplace tujuan produk Anda. URL ditampilkan di konsol Security Hub. Jenis: String Ini harus berupaAWS Marketplace URL. Jika Anda tidak memilikiAWS Marketplace daftar, biarkan bidang ini kosong.

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

Pedoman dan daftar periksa

Saat Anda menyiapkan bahan yang dibutuhkan untukAWS Security Hubintegrasi, gunakan pedoman ini.

Daftar periksa kesiapan digunakan untuk melakukan tinjauan akhir integrasi sebelum Security Hub membuatnya tersedia untuk pelanggan Security Hub.

Topik

Pedoman untuk logo untuk ditampilkan padaAWS Security Hubkonsol

Agar logo ditampilkan diAWS Security Hubkonsol, ikuti panduan ini.

Mode terang dan gelap

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

Format

Format file SVG

Warna latar belakang

Transparan

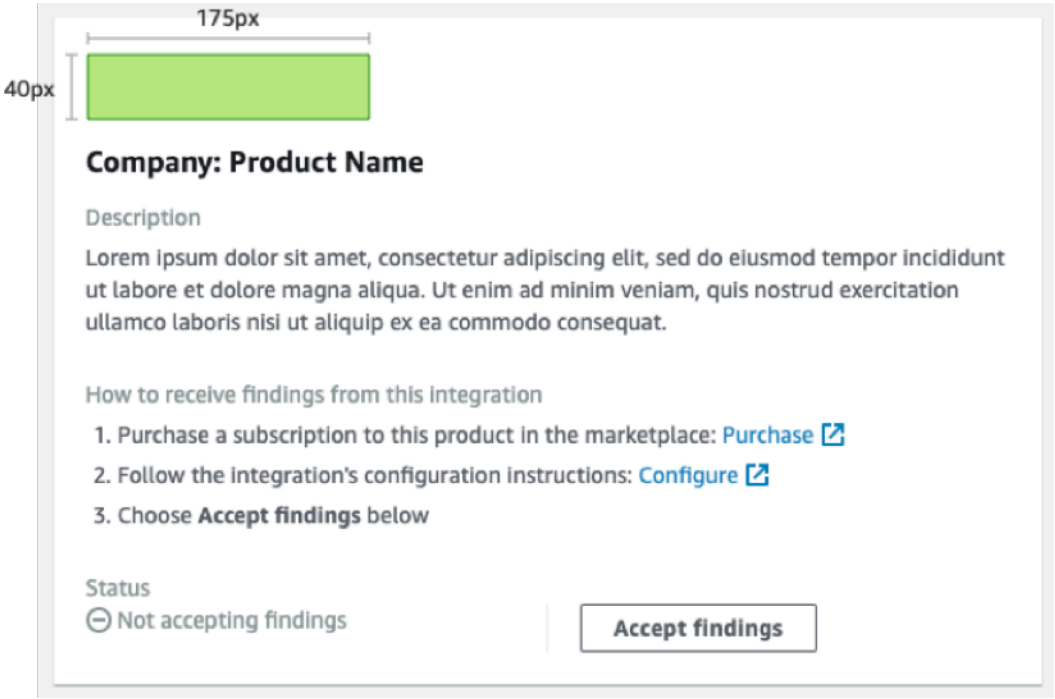
Ukuran

Rasio ideal adalah 175 px lebar dengan tinggi 40 px.

Tinggi minimum adalah 40 px.

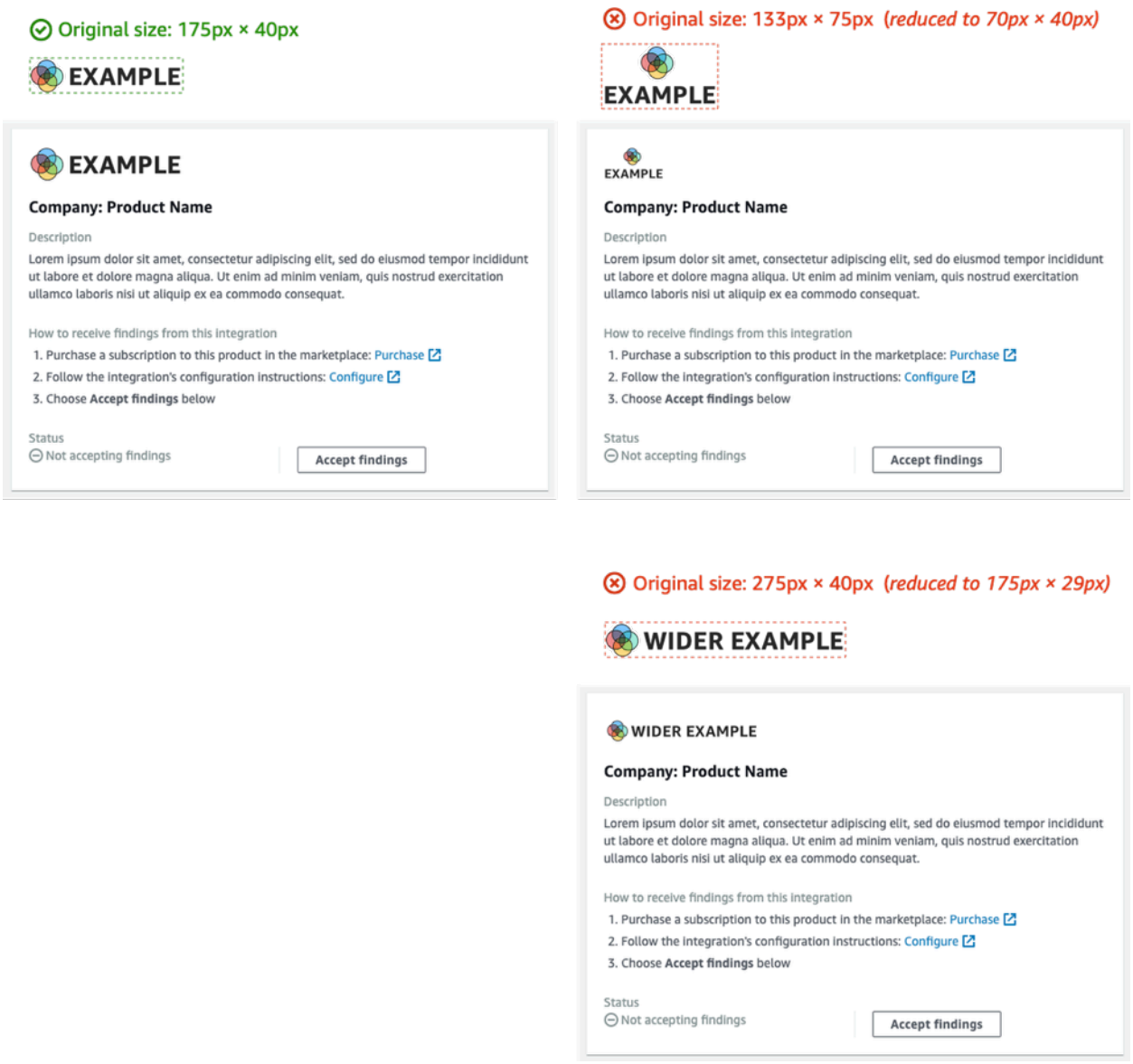
Logo persegi panjang bekerja paling baik.

Gambar berikut menunjukkan bagaimana logo ideal ditampilkan di konsol Security Hub.



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

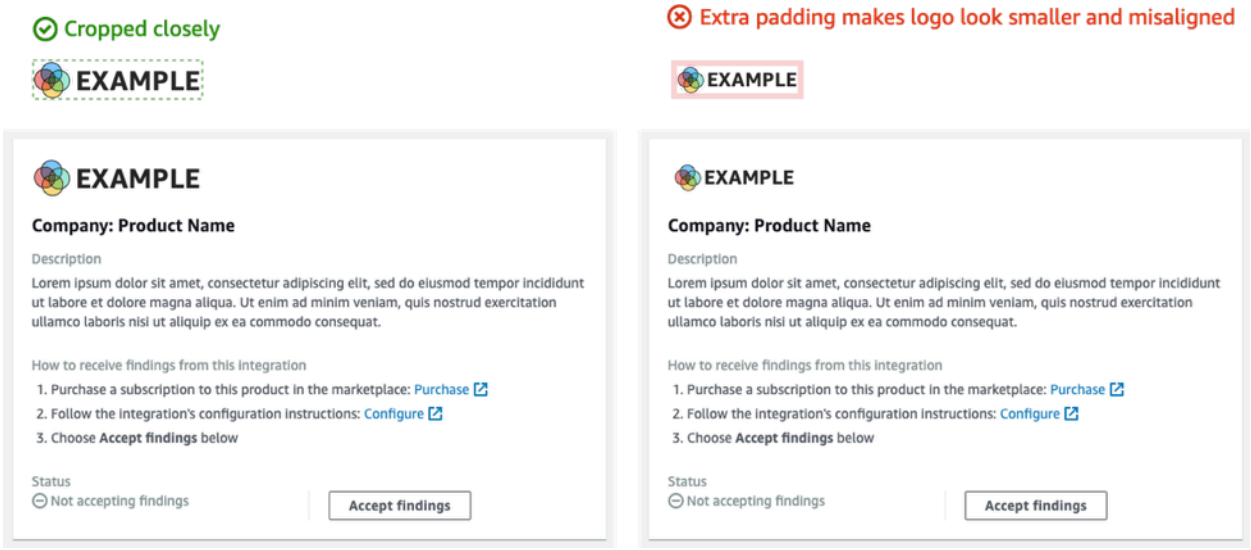
Gambar berikut membandingkan tampilan logo yang menggunakan ukuran ideal untuk logo yang lebih lebar atau lebih tinggi.



Tanam

Potong gambar logo sedekat mungkin. Jangan memberikan bantalan ekstra.

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



Prinsip untuk membuat dan memperbarui temuan

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

Membuat temuan spesifik sehingga pelanggan dapat dengan mudah mengambil tindakan pada mereka.

> Pelanggan ingin mengotomatisasi 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 tipe temuan tunggal.
> - Mereka harus berurusan dengan satu peristiwa keamanan.
>
> Ketika temuan berisi data untuk beberapa peristiwa keamanan, lebih sulit bagi pelanggan untuk mengambil tindakan pada temuan.

Memetakan semua bidang temuan Anda keAWSFormat Pencarian Keamanan (ASFF). Memungkinkan pelanggan untuk mengandalkan Security Hub sebagai sumber kebenaran.

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

Pelanggan ingin semua data hadir dalam versi Security Hub temuan tersebut. Data yang hilang menyebabkan mereka kehilangan kepercayaan di Security Hub sebagai sumber pusat informasi keamanan.

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

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

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

Ketika ada perubahan besar untuk temuan, seperti untuk skor keparahan atau pengenal sumber daya, membuat temuan baru.

Misalnya, untuk membuat temuan untuk pemindaian port individual secara real time tidak dapat ditindaklanjuti. Karena pemindaian port dapat terjadi terus menerus, itu akan menghasilkan sejumlah besar temuan. Hal ini jauh lebih menarik dan tepat untuk hanya memperbarui waktu pemindaian terakhir dan menghitung scan pada satu temuan untuk port scan 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 membuat mereka 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 untuk pemetaan temuan ke dalamAWSFormat Pencarian Keamanan (ASFF)

Gunakan pedoman berikut untuk memetakan temuan Anda ke ASFF. Untuk deskripsi rinci dari setiap bidang ASFF dan objek, lihatAWSFormat Pencarian Keamanan (ASFF)diAWS Security HubPanduan Pengguna.

Mengidentifikasi informasi

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

`ProductArn`adalah ARN yangAWS Security Hubmemberikan kepada Anda.

`Id`adalah nilai yang digunakan Security Hub untuk temuan indeks. Pengenal temuan harus unik, untuk memastikan bahwa temuan lain tidak ditimpa. Untuk memperbarui temuan, kirimkan kembali temuan dengan pengenal yang sama.

`GeneratorId`bisa sama dengan`Id`atau dapat merujuk ke unit logika diskrit, seperti AmazonGuardDutyID detektor,AWS ConfigID 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 rinci 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`FindingProviderFields.Types`.

`Types`harus sesuai denganjenis taksonomi untuk ASFF.

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

Stempel Waktu

Format ASFF mencakup beberapa cap waktu yang berbeda.

`CreatedAt` dan `UpdatedAt`

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

Nilai-nilai harus sesuai dengan format ISO8601 dalam 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. Jika Anda tidak mencatat informasi ini, Anda tidak perlu mengirimkan cap waktu ini.

Nilai-nilai cocok dengan format ISO8601 dalam Python 3.8.

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

Severity

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

`Original`

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

`Label`

Indikator Security Hub yang diperlukan dari tingkat keparahan temuan. Nilai yang diperbolehkan adalah sebagai berikut.

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

Temuan yang sesuai harus selalu memiliki`Label`diatur ke`INFORMATIONAL`. Contoh`INFORMATIONAL`Temuan adalah temuan dari pemeriksaan keamanan yang berlalu dan AWS Firewall Managertemuan yang diperbaiki.

Pelanggan sering menyortir temuan berdasarkan tingkat keparahan mereka untuk memberikan tim operasi keamanan mereka daftar tugas. Bersikap konservatif saat menetapkan keparahan temuan`HIGH`atau`CRITICAL`.

Dokumentasi integrasi Anda harus menyertakan alasan pemetaan Anda.

Remediation

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

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

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

SourceUrl

Hanya menggunakan`SourceUrl`jika Anda dapat memberikan URL yang tertaut dalam ke konsol Anda untuk temuan spesifik tersebut. Jika tidak, hilangkan dari pemetaan.

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

Malware, Network, Process, ThreatIntelIndicators

Jika berlaku, gunakan`Malware`,`Network`,`Process`, atau`ThreatIntelIndicators`. Masing-masing objek ini terpapar di konsol 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 rincian untuk instans EC2 di`Resource.Details.AwsEc2Instance`. Berikan yang relevan`Malware`,`Network`, dan`ThreatIntelIndicator`objek untuk instans EC2.

Malware

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

Setiap entri memiliki bidang berikut.

`Name`

Nama malware. Nilainya adalah string berisi hingga 64 karakter.

`Name`harus dari kecerdasan ancaman diperiksa atau sumber peneliti.

`Path`

Jalur ke malware. Nilainya adalah string hingga 512 karakter.`Path`harus menjadi jalur file sistem Linux atau Windows, kecuali dalam kasus berikut.

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

`State`

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

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

Misalnya, jika`Malware.State`adalah`REMOVED`, maka judul temuan dan deskripsi harus mencerminkan bahwa produk Anda dihapus malware yang terletak di jalan.

Jika`Malware.State`adalah`OBSERVED`, maka judul temuan dan deskripsi harus mencerminkan bahwa produk Anda mengalami malware ini terletak di jalan.

`Type`

Menunjukkan jenis malware. Nilai yang diperbolehkan adalah`ADWARE|BLENDED_THREAT|BOTNET_AGENT|COIN_MINER|EXPLOIT_KIT|KEYLOGGER|MACRO|POT`

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

Network

`Network`adalah satu objek. Anda tidak dapat menambahkan beberapa rincian terkait jaringan. Saat memetakan bidang, gunakan pedoman berikut ini.

Informasi tujuan dan sumber

Tujuan dan sumber mudah untuk memetakan TCP atau VPC Flow Logs atau WAF log. Mereka lebih sulit untuk 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 sumber dalam dokumentasi Anda dan juga menjelaskannya dalam judul temuan dan deskripsi.

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

`Protocol`

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

`Protocol`independen dari sumber dan informasi tujuan. Hanya memberikan itu ketika masuk akal untuk melakukannya.

`Direction`

`Direction`selalu relatif terhadapAWSbatas jaringan.

- `IN`berarti itu memasukiAWS(VPC, layanan).
- `OUT`berarti itu keluarAWSbatas jaringan.

Process

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

`Name`

`Name`harus cocok dengan nama executable. Ia menerima hingga 64 karakter.

`Path`

`Path`adalah path sistem file ke proses executable. Ia menerima hingga 512 karakter.

`Pid`, **`ParentPid`**

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

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

Jika Anda tidak dapat dipercaya mengambil informasi ini, dan itu tidak akurat untuk milidetik, jangan menyediakannya.

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

ThreatIntelIndicators

`ThreatIntelIndicators`menerima array hingga lima objek intelijen ancaman.

Untuk setiap entri,`Type`adalah dalam konteks ancaman spesifik. Nilai yang diperbolehkan adalah`DOMAIN`|`EMAIL_ADDRESS`|`HASH_MD5`|`HASH_SHA1`|`HASH_SHA256`|`HASH_SHA512`|`IPV4_ADDRESS`|`IP`

Berikut ini beberapa contoh cara memetakan indikator intelijen ancaman:

- Anda menemukan proses yang Anda tahu terkait dengan Cobalt Strike. Anda belajar ini dariFireEyeblog.

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

  Membuat dua`ThreatIntelIndicator`benda. Satu objek adalah untuk`DOMAIN`. Yang lainnya adalah untuk`HASH_SHA1`.
- Anda menemukan malware dengan aturan Yara (Loki, Fenrir, Ass3VirusScan,BinaryAlert).

  Membuat dua`ThreatIntelIndicator`benda. Salah satunya adalah untuk malware. Yang lainnya adalah untuk`HASH_SHA1`.

Resources

Untuk`Resources`, gunakan jenis sumber daya yang disediakan dan bidang detail kami bila memungkinkan. Security Hub 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 rincian untuk jenis sumber daya yang dimodelkan, petakan rincian yang tersisa ke`Details.Other`.

Untuk sumber daya yang tidak dimodelkan dalam ASFF, setTypekepadaOther. Untuk informasi rinci, gunakanDetails.Other.

Anda juga dapat menggunakanOtherjenis sumber daya untuk non-AWStemuan.

ProductFields

Hanya menggunakanProductFieldsjika Anda tidak dapat menggunakan bidang curated lain untukResourcesatau objek deskriptif sepertiThreatIntelIndicators,Network, atauMalware.

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

Kepatuhan

Hanya menggunakanCompliancejika temuan Anda terkait dengan kepatuhan.

Penggunaan Security HubComplianceuntuk temuan yang dihasilkannya berdasarkan kontrol.

Firewall Manager menggunakanComplianceuntuk temuannya karena mereka terkait dengan kepatuhan.

Bidang yang dibatasi

Bidang ini ditujukan bagi pelanggan untuk melacak penyelidikan mereka dari temuan.

Jangan memetakan ke bidang atau objek ini.

- Note
- UserDefinedFields
- VerificationState
- Workflow

Untuk bidang ini, petakan ke bidang yang ada diFindingProviderFieldsobjek. Jangan memetakan 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 memberikan temuan terkait jika Anda dapat melacak temuan yang terkait dengan sumber daya yang sama atau jenis pencarian. Untuk mengidentifikasi temuan terkait, Anda harus merujuk ke pengenal temuan temuan yang sudah ada di Security Hub.

Pedoman penggunaan`BatchImportFindings`API

Saat menggunakan`BatchImportFindings`Operasi API untuk mengirim temuan keAWS Security Hub, gunakan panduan berikut.

- Anda harus menelepon`BatchImportFindings`menggunakan akun yang terkait dengan temuan tersebut. Pengenal akun terkait adalah nilai dari`AwsAccountId`atribut untuk temuan.
- Kirim batch terbesar yang Anda bisa. Security Hub 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 keadaan temuan jika ada masalah throttling atau jaringan. Anda juga perlu negara temuan sehingga Anda dapat mengirimkan menemukan update sebagai temuan bergerak masuk dan keluar dari kepatuhan.
- Untuk informasi tentang panjang maksimum string dan keterbatasan lainnya, lihatAWSFormat Pencarian Keamanan (ASFF)diAWS Security HubPanduan Pengguna.

Daftar periksa kesiapan produk

ParameterAWS Security Hubdan tim Mitra APN menggunakan daftar periksa ini untuk memvalidasi bahwa integrasi siap diluncurkan.

Pemetaan ASFF

Pertanyaan-pertanyaan ini terkait dengan pemetaan temuan Anda keAWSFormat Pencarian Keamanan (ASFF).

Apakah semua data temuan mitra dipetakan ke ASFF?

Petakan semua temuan Anda ke ASFF dalam beberapa cara.

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

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

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

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

Memetakan informasi lain yang terkait dengan sumber daya`Resource.Details.Other`hanya ketika tidak ada pertandingan langsung.

Apakah nilai peta mitra untuk**`UserDefinedFields`**?

Jangan gunakan `UserDefinedFields`.

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

Apakah informasi peta mitra ke**`ProductFields`**yang bisa dipetakan ke bidang ASFF lainnya?

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

Apakah mitra mengimpor cap waktu mereka sendiri untuk**`FirstObservedAt`**?

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

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

Semua temuan di Security Hub diindeks pada identifier temuan (`Id`atribut). 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 dihasilkan mereka.

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

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

Jenis temuan taksonomi harus memetakan dengan cermat temuan yang dihasilkan produk.

Ruang nama tingkat pertama yang diuraikan dalamAWSSecurity Finding Format diperlukan.

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

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

Jika produk Anda menangkapNetFlowinformasi, peta ke`Network`Bidang.

Apakah informasi proses pengambilan mitra (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`**bidang, jika mereka memiliki data malware?

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

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

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

Apakah mitra memberikan peringkat kepercayaan untuk temuan? Jika mereka melakukannya, adalah alasan yang diberikan?

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 mengidentifikasiAWSsumber daya, praktek terbaik adalah dengan menggunakan ARN. Jika ARN tidak tersedia, gunakan ID sumber daya kanonik.

Penyiapan dan fungsi integrasi

Pertanyaan-pertanyaan ini terkait dengan pengaturan danday-to-dayfungsi integrasi.

Apakah mitra menyediakaninfrastructure-as-code(IAC) untuk menyebarkan integrasi dengan Security Hub, seperti Terraform,AWS CloudFormation, atauAWS Cloud Development Kit (AWS CDK)?

Untuk integrasi yang akan mengirimkan temuan dari akun pelanggan atau penggunaanCloudWatchAcara untuk mengkonsumsi temuan, beberapa bentuk template IAC diperlukan.

AWS CloudFormationlebih disukai, tapiAWS CDKatau Terraform juga bisa digunakan.

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

Beberapa produk mitra menggunakan toggle 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 disukai.

Apakah mitra hanya mengirimkan temuan nilai?

Anda biasanya hanya harus mengirim temuan yang memiliki nilai keamanan kepada pelanggan Security Hub.

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

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

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

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

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

Saat ini ada tingkat ledakan 30-50 TPS pada`BatchImportFindings`Operasi API. Jika kesalahan 4xx atau 5xx dikembalikan, Anda harus mempertahankan keadaan temuan yang gagal sehingga Anda dapat mencobanya kembali secara totalitas nanti. Anda dapat melakukan ini melalui antrian surat mati atau lainnyaAWSlayanan pesan seperti Amazon SNS atau Amazon SQS.

Apakah mitra mempertahankan keadaan temuan mereka sehingga mereka tahu untuk mengarsipkan temuan yang tidak lagi hadir?

Jika Anda berencana untuk memperbarui temuan dengan Timpa 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 pada temuan.

Apakah mitra menangani retries dengan cara yang tidak berkompromi sebelumnya mengirim temuan sukses?

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

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

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

Parameter`BatchUpdateFindings`operasi hanya boleh digunakan oleh pelanggan.

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

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

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

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

Informasi ini diperlukan dalam manifes.

Jika arsitektur mitra adalah untuk mengirim temuan ke Security Hub dari akun pelanggan, apakah mereka telah menunjukkan hal ini berhasil? Jika arsitektur mitra adalah untuk mengirim temuan ke Security Hub dari akun mereka sendiri, apakah mereka telah menunjukkan hal ini berhasil?

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

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

Apakah pasangan memberikan temuan detak jantung ke Security Hub?

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

Hal ini penting jika Anda mengirim temuan dari akun produk.

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

Selama validasi praproduksi, Anda harus mengirim contoh temuan ke tim produk Security HubAWSakun. 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 hostingGitHubtidak memenuhi persyaratan situs web khusus.

Apakah dokumentasi mitra memberikan petunjuk tentang cara mengatur integrasi Security Hub?

Anda dapat mengatur integrasi menggunakan template 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. Dalam hal ini, Anda harus memberikan alasan mengapa Anda tidak mengirim temuan antivirus.

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

Anda harus memberikan alasan untuk pemetaan temuan asli produk untuk ASFF. Pelanggan ingin tahu di mana untuk 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 negara, memastikan idempotency, dan menimpa temuan denganup-to-dateinformasi.

Apakah dokumentasi mitra menjelaskan menemukan latensi?

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

Informasi ini diperlukan dalam manifes.

Apakah dokumentasi mitra menjelaskan bagaimana tingkat keparahan mereka mencetak peta untuk penilaian tingkat keparahan ASFF?

Memberikan informasi tentang cara Anda memetakan`Severity.Original`kepada`Severity.Label`.

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

Apakah dokumentasi mitra memberikan alasan untuk peringkat kepercayaan diri?

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

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

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

Catatan Daerah yang atau tidak didukung sehingga pelanggan tahu di mana Daerah untuk tidak mencoba integrasi.

Informasi kartu produk

Pertanyaan-pertanyaan ini terkait dengan kartu untuk produk yang ditampilkan padaIntegrasihalaman konsol Security Hub.

Apakah yang disediakanAWSID akun 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 atau lebih sedikit karakter?

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

Apakah link 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 link pembelian (jika disediakan) mengarah keAWS Marketplacedaftar untuk produk?

Jika Anda memberikan link pembelian, itu harus untukAWS Marketplaceentri. Security Hub tidak menerima tautan pembelian yang tidak di-host olehAWS.

Apakah kategori produk dengan benar menggambarkan produk?

Dalam manifes, Anda dapat menyediakan hingga tiga kategori produk. Ini harus sesuai 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 lebih sedikit.

Nama produk harus 24 atau lebih sedikit karakter.

Nama produk dalam kartu produk JSON harus sesuai dengan nama dalam manifes.

Informasi pemasaran

Pertanyaan-pertanyaan ini terkait dengan pemasaran untuk integrasi.

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

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

Tim akan mengedit deskripsi yang lebih panjang.

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

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

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

ParameterPelajari selengkapnyalink tidak boleh mengarah ke situs utama mitra atau informasi dokumentasi.

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

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

Video walkthrough demo atau integrasi bersifat opsional namun disarankan.

Adalah sebuahAWSPosting blog Partner Network dirilis bersama mitra dan manajer pengembangan mitra atau perwakilan pengembangan mitra mereka?

AWSPosting 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 ARN produk pribadi selesai.

Apakah siaran pers yang dipimpin mitra dirilis?

Anda dapat bekerja sama dengan manajer pengembangan mitra atau perwakilan pengembangan mitra Anda untuk mendapatkan penawaran dari VP 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 luarAWSBlog Jaringan Mitra.

Apakah webinar yang dipimpin mitra sedang dirilis?

Anda dapat membuat webinar Anda sendiri untuk menampilkan integrasi.

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

Apakah mitra meminta dukungan media sosial dariAWS?

Setelah rilis Anda, Anda dapat bekerja denganAWSKeamanan pemasaran mengarah untuk menggunakanAWSsaluran media sosial resmi untuk berbagi rincian tentang webinar Anda.

AWS Security HubFAQ Mitra

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

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

     Security Hub adalah pusat keamanan dan kepatuhan untukAWSpelanggan. Hal ini dirancang sebagai pemberhentian pertama di manaAWSprofesional 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 Discovery— Kami mempromosikan mitra dengan integrasi bersertifikat di dalam konsol Security Hub, termasuk tautan ke merekaAWS Marketplacedaftar. Ini adalah cara yang bagus bagi pelanggan untuk menemukan produk keamanan baru.
   - Peluang pemasaran- Vendor dengan integrasi yang disetujui dapat berpartisipasi dalam webinar, menerbitkan siaran pers, membuat lembar licin, dan menunjukkan integrasi mereka untukAWSpelanggan.
2. Apa jenis mitra yang ada?
   - Mitra yang mengirim temuan ke Security Hub
   - Mitra yang menerima temuan dari Security Hub
   - Mitra yang mengirim dan menerima temuan
   - Mitra konsultasi yang membantu pelanggan mengatur, menyesuaikan, dan menggunakan Security Hub di lingkungan mereka
3. Bagaimana cara kerja integrasi mitra dengan Security Hub pada tingkat tinggi?

   Anda mengumpulkan temuan dari dalam akun pelanggan atau dari akun Anda sendiriAWSakun dan mengubah format temuan keAWSFormat Pencarian Keamanan (ASFF). Anda kemudian mendorong temuan tersebut ke titik akhir regional Security Hub yang sesuai.

   Anda juga dapat menggunakanCloudWatchPeristiwa untuk menerima temuan dari Security Hub.
4. Apa langkah-langkah dasar untuk menyelesaikan integrasi dengan Security Hub?

a. Kirimkan informasi manifes mitra Anda.

b. Menerima ARN produk untuk digunakan dengan Security Hub, 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 dan menerima temuan dari Security Hub. Ikuti prinsip yang diuraikan dalamthe section called “Prinsip untuk membuat dan memperbarui temuan”.

e. Buat kerangka kerja penyebaran untuk pelanggan. Misalnya,AWS CloudFormationskrip dapat melayani tujuan ini.

f. Dokumentasikan pengaturan Anda dan berikan instruksi konfigurasi untuk pelanggan.

g. Tentukan wawasan kustom (aturan korelasi) yang dapat digunakan pelanggan dengan produk Anda.

h. Tunjukkan integrasi Anda ke tim Security Hub.

i. Kirim informasi pemasaran untuk persetujuan (bahasa situs web, siaran pers, slide arsitektur, video, lembar licin).

5. Apa proses untuk mengirimkan manifes mitra? dan untukAWSlayanan untuk mengirim temuan ke Security Hub?

   Untuk mengirimkan informasi manifes ke tim Security Hub, gunakan<securityhub-partners@amazon.com>.

   Anda dikeluarkan ARN produk dalam waktu tujuh hari kalender.

6. Jenis temuan apa yang harus saya kirim ke Security Hub?

   Penetapan harga Security Hub sebagian berdasarkan pada jumlah temuan yang dicerna. Karena itu, Anda harus menahan diri dari 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 pendekatan yang berbeda bagi saya untuk mengirim temuan ke Security Hub?

   Ini adalah pendekatan utama:

   - Anda mengirim temuan dari mereka sendiri ditunjukAWSakun menggunakanBatchImportFindingsoperasi.

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

Untuk pedoman keseluruhan tentang penggunaan`BatchImportFindings`, lihatthe section called "Pedoman penggunaan`BatchImportFindings`API".

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

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

   Misalnya, beberapa mitra membuat aplikasi Python yang dapat digunakan sebagaiAWS CloudFormationnaskah. Skrip mengumpulkan temuan mitra dari lingkungan pelanggan, mengubahnya menjadi ASFF, dan mengirimkannya ke titik akhir Regional Security Hub.

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

9. Bagaimana saya mengetahui kapan harus mengirim temuan ke Security Hub?

   Security Hub mendukung otorisasi batch partial untuk`BatchImportFindings`Operasi API, sehingga Anda dapat mengirim semua temuan Anda ke Security Hub untuk semua pelanggan Anda.

   Jika beberapa pelanggan Anda belum berlangganan ke Security Hub, Security Hub tidak menelan temuan tersebut. Ini hanya menelan temuan resmi yang ada di batch.

10. Langkah-langkah apa yang harus saya selesaikan untuk mengirim temuan ke instans Security Hub pelanggan?

    a. Pastikan kebijakan IAM yang benar sudah ada.

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

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

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

e. Pastikan bahwa temuan Anda tidak memiliki data yang cacat sesuai denganAWSFormat Pencarian Keamanan (ASFF). Misalnya, bidang yang diperlukan dihuni, 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`, atur kebijakan IAM untuk pemanggil sebagai berikut:

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

Pastikan untuk memeriksa bahwa tidak ada`Deny`kebijakan untuk penelepon. Setelah Anda mendapatkannya untuk 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 Integrasi halaman. Untuk melakukan ini dari API, mereka menggunakan `EnableImportFindingsForProduct` Operasi API.

Langganan produk menciptakan kebijakan sumber daya yang mengotorisasi temuan dari mitra yang akan diterima atau dikirim oleh pelanggan. Untuk detailnya, lihat Kasus penggunaan dan izin.

Security Hub memiliki jenis kebijakan sumber daya berikut untuk mitra:

- `BATCH_IMPORT_FINDINGS_FROM_PRODUCT_ACCOUNT`
- `BATCH_IMPORT_FINDINGS_FROM_CUSTOMER_ACCOUNT`

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

Dengan `BATCH_IMPORT_FINDINGS_FROM_PRODUCT_ACCOUNT`, Anda hanya dapat mengirim temuan ke Security Hub 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 Anda.

13 Asumsikan pelanggan membuat akun administrator dan menambahkan beberapa akun anggota. Apakah pelanggan harus 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 meletakkan 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 Anda yang dihasilkan Security Hub untuk Anda dan yang Anda gunakan untuk mengirimkan temuan. Anda menerima produk ARN untuk setiap produk yang Anda integrasikan dengan Security Hub. Produk ARN yang benar harus menjadi bagian dari setiap temuan yang Anda kirim ke Security Hub. Temuan tanpa ARN produk dijatuhkan. ARN produk menggunakan format berikut:

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

Berikut ini contohnya:

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

Anda diberi ARN produk untuk setiap Wilayah di mana Security Hub dikerahkan. ID akun, perusahaan, dan nama produk ditentukan oleh pengiriman manifes mitra Anda. Anda tidak pernah mengubah salah satu informasi yang terkait dengan ARN produk Anda, kecuali untuk kode Wilayah. Kode Wilayah harus sesuai dengan Wilayah yang Anda kirimkan temuan.

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

Saat Security Hub diluncurkan di Wilayah baru, secara otomatis menggunakan kode Wilayah standar untuk menghasilkan ARN produk 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?

Temuan harus disediakan dalamAWSFormat Pencarian Keamanan (ASFF). Untuk rincian selengkapnya, lihatAWSFormat Pencarian Keamanan (ASFF)di dalamAWS Security HubPanduan Pengguna.

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

16 Apa titik akhir Regional yang benar untuk digunakan?

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

17 Di mana saya bisa menemukan daftar titik akhir regional?

LihatDaftar titik akhir Security Hub.

18 Dapatkah saya mengirimkan temuan lintas wilayah?

Security Hub belum mendukung pengiriman temuan lintas wilayah untuk penduduk asliAWSlayanan, seperti AmazonGuardDuty, Amazon Macie, dan Amazon Inspector. Jika pelanggan Anda mengizinkannya, Security Hub tidak mencegah Anda mengirimkan temuan dari berbagai Wilayah.

Dalam pengertian ini, Anda dapat menghubungi endpoint Regional dari mana saja, dan informasi sumber daya ASFF tidak harus sesuai dengan Wilayah titik akhir. Namun,`ProductArn`harus sesuai 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 batch sebanyak mungkin temuan sampai batas ini.

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

Lihat the section called “Pedoman penggunaan`BatchImportFindings`API”.

20 Dapatkah saya mengirim update ke temuan yang saya buat?

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

Pelanggan diukur dan ditagih untuk kedua temuan baru dan menemukan pembaruan.

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

Ya, jika pelanggan memberikan Anda akses ke`BatchUpdateFindings`Operasi API, Anda dapat memperbarui bidang tertentu menggunakan operasi itu. Operasi ini dirancang untuk digunakan oleh pelanggan, SIEMS, sistem tiket, dan Orkestrasi Keamanan, Otomasi, dan Response (SOAR) platform.

22 Bagaimana temuan berusia off?

Security Hub menua temuan 90 hari setelah tanggal pembaruan terakhir. Setelah waktu ini, temuan yang sudah tua dibersihkan dari Security HubOpenSearchkluster.

Jika Anda memperbarui temuan dengan ID temuan yang sama, dan telah berusia off, temuan baru dibuat di Security Hub.

Pelanggan dapat menggunakanCloudWatchAcara untuk memindahkan temuan dari Security Hub. Melakukan hal ini memungkinkan semua temuan dikirim ke target pilihan pelanggan.

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

23. Throttles apa yang dilakukan Security Hub?

Throttles Security Hub`GetFindings`Panggilan API, sebagai pendekatan yang disarankan untuk mengakses temuan menggunakanCloudWatchPeristiwa.

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

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

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

25. Bagaimana saya dapat menerima temuan dari Security Hub?

Untuk menerima temuan, gunakan salah satu metode berikut.

- Semua temuan secara otomatis dikirim keCloudWatchPeristiwa. Pelanggan dapat membuat spesifikCloudWatchAturan acara untuk mengirim temuan ke target tertentu, seperti SIEM atau bucket S3. Kemampuan ini menggantikan warisan`GetFindings`Operasi API.
- GunakanCloudWatchAcara untuk tindakan kustom. Security Hub memungkinkan pelanggan untuk memilih temuan tertentu atau kelompok temuan dari dalam konsol dan mengambil tindakan pada mereka. Misalnya, mereka dapat mengirim temuan ke SIEM, sistem tiket, platform obrolan, atau alur kerja remediasi. Ini akan menjadi bagian dari alur kerja siaga triase bahwa pelanggan melakukan dalam Security Hub. Ini disebut tindakan kustom.

  Ketika pengguna memilih tindakan kustom, aCloudWatchacara dibuat untuk temuan tertentu. Anda bisa memanfaatkan kemampuan ini dan membangunCloudWatchPeristiwa aturan dan target untuk pelanggan untuk digunakan sebagai bagian dari tindakan kustom. Perhatikan bahwa kemampuan ini tidak digunakan untuk secara otomatis mengirim semua temuan dari

jenis atau kelas tertentu keCloudWatchPeristiwa. Hal ini bagi pengguna untuk mengambil tindakan pada temuan tertentu.

Anda dapat menggunakan operasi API tindakan kustom, seperti`CreateActionTarget`, untuk secara otomatis membuat tindakan yang tersedia untuk produk Anda (seperti menggunakanAWS CloudFormationtemplat). Anda juga akan menggunakanCloudWatchPeristiwa aturan operasi API untuk membuat sesuaiCloudWatchPeristiwa aturan yang terkait dengan tindakan kustom. MenggunakanAWS CloudFormationtemplate, Anda juga dapat membuatCloudWatchAcara aturan untuk secara otomatis menelan dari Security Hub semua temuan atau semua temuan dengan karakteristik tertentu.

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

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

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

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

Jika MSSP hanya menerima temuan dari Security Hub, mereka harus minimal memilikiAWS CloudFormationtemplate untuk mengatur sesuaiCloudWatchAcara aturan.

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

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

- Siapkan Security Hub dengan izin IAM yang dibutuhkan pelanggan.
- Bantu menghubungkan solusi vendor perangkat lunak independen (ISV) yang sudah terintegrasi ke Security Hub menggunakan petunjuk konfigurasi pada halaman mitra di konsol.
- Membantu pelanggan dengan integrasi produk kustom.
- Membangun wawasan kustom yang relevan dengan kebutuhan pelanggan dan dataset.
- Buat tindakan kustom.
- Membangun playbook remediasi.

- Bangun Quickstarts yang sesuai dengan standar kepatuhan Security Hub. Ini harus divalidasi oleh tim Security Hub.

Studi kasus tidak perlu dibagikan secara publik.

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

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

Jika Anda menerapkan perangkat lunak integrasi ke pelangganAWSlingkungan, Anda harus memanfaatkanAWS CloudFormationtemplate untuk menyederhanakan integrasi. Beberapa mitra telah menciptakan integrasi satu klik, yang sangat dianjurkan.

29 Apa persyaratan dokumentasi saya?

Anda harus menyediakan tautan ke dokumentasi yang menjelaskan proses integrasi dan pengaturan antara produk dan Security Hub Anda, termasuk penggunaan Anda atasAWS CloudFormationtemplat.

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

Pertimbangkan untuk memasukkan informasi potensial lainnya:

- Kasus penggunaan Anda untuk integrasi dengan Security Hub
- Volume rata-rata temuan yang dikirim
- Arsitektur integrasi Anda
- Wilayah yang Anda lakukan dan tidak mendukung
- Latensi antara saat temuan dibuat dan kapan mereka dikirim ke Security Hub
- Apakah Anda memperbarui temuan

30 Apa wawasan kustom?

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

Security Hub memilikiCreateInsightOperasi API. Anda dapat membuat wawasan khusus di dalam akun pelanggan sebagai bagian dariAWS CloudFormationtemplat. Wawasan ini muncul di konsol pelanggan.

31 Dapatkah saya mengirimkan widget dasbor?

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

32 Apa model harga Anda?

LihatInformasi harga Security Hub.

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

Kirim temuan ke akun demo Security Hub menggunakan ARN produk yang Anda berikan, menggunakanus-west-2sebagai Wilayah. Temuan harus menyertakan nomor akun demo diAwsAccountIdbidang ASFF. Untuk mendapatkan nomor akun demo, hubungi tim Security Hub.

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

34 Pesan kesalahan atau kesuksesan apa yang dilakukan**BatchImportFindings**menyediakan?

Security Hub memberikan respons untuk otorisasi dan respons untukBatchImportFindings. Kesuksesan, kegagalan, dan pesan kesalahan yang lebih tajam sedang dalam pengembangan.

35 Penanganan kesalahan apa yang bertanggung jawab atas layanan sumber?

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

36 Apa sajakah resolusi untuk masalah umum?

SesiAuthorizerConfigurationExceptiondisebabkan oleh salah satu cacatAwsAccountIdatauProductArn.

Saat memecahkan masalah, perhatikan hal berikut:

- AwsAccountIdharus 12 digit persis.

- `ProductArn`harus dalam format berikut: arn:securityhub:*<us-west-2 or us-east-1>*:*<accountId>*:produk/*<company-id>*/*<product-id>*

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

`AccessDeniedException`disebabkan ketika temuan dikirim ke atau dari akun yang salah, atau ketika akun tidak memiliki`ProductSubscription`. Pesan galat akan berisi ARN dengan jenis sumber daya`product`atau`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 ARN produk, tetapi cobalah untuk menggunakan akun yang sama sekali berbeda untuk menelepon`BatchImportFindings`. Dalam kasus lain, mereka menciptakan`ProductSubscriptions`untuk akun pelanggan lainnya, atau bahkan untuk akun produk mereka sendiri. Mereka tidak menciptakan`ProductSubscriptions`untuk akun pelanggan bahwa mereka mencoba untuk mengimpor temuan ke dalam.

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

    `<securityhub-partners@amazon.com>`

38. Wilayah mana yang saya kirimkan temuan untuk item yang terkait dengan global AWS layanan? 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 itu terdeteksi.

    Jika pelanggan menjalankan Security Hub di tiga Wilayah, dan masalah IAM yang sama terdeteksi di ketiga Wilayah, kemudian kirim temuan ke ketiga Wilayah.

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

Riwayat dokumen untuk Panduan Integrasi Mitra

Tabel berikut menjelaskan dokumentasi update untuk panduan ini.

Perubahan	Deskripsi	Tanggal
Persyaratan terbaru untuk logo konsol	Memperbarui manifes mitra dan pedoman logo untuk menunjukkan bahwa mitra harus menyediakan mode cahaya dan versi mode gelap logo untuk ditampilkan di konsol Security Hub. Logo harus format SVG.	10 Mei 2021
Memperbarui prasyarat untuk mitra integrasi baru	Security Hub sekarang juga memungkinkan mitra yang telah bergabung denganAWSJalur Mitra ISV, dan siapa yang menggunakan produk integrasi yang telah menyelesaikanAWSTinjauan Teknis Dasar (FTR). Sebelumnya, semua mitra integrasi diharuskanAWSPilih Mitra Tingkat.	29 April 2021
BaruFindingProviderFields objek di ASFF	Memperbarui informasi tentang pemetaan temuan ke ASFF. UntukConfidence ,Criticality ,RelatedFindings ,Severity, danTypes, mitra memetakan nilai-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.	4 Desember 2020
Rilis awal dari panduan ini	IniPanduan Integrasi MitramemberiAWSbermitra dengan informasi tentang cara membangun integrasi denganAWS Security Hub.	23 Juni 2020

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