Guia de integração do parceiro

AWS Security Hub

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS Security Hub: Guia de integração do parceiro

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

As marcas comerciais e imagens comerciais da Amazon não podem ser usadas no contexto de nenhum produto ou serviço que não seja da Amazon, nem de qualquer maneira que possa gerar confusão entre os clientes ou que deprecie ou desprestigie a Amazon. Todas as outras marcas comerciais que não pertencem à Amazon pertencem a seus respectivos proprietários, que podem ou não ser afiliados, patrocinados pela Amazon ou ter conexão com ela.

Table of Contents

Visão geral da integração de terceiros com AWS Security Hub 1
Por que fazer a integração? 1
Como se preparar para enviar descobertas 2
Preparar-se para receber descobertas 3
Recursos de informações do Security Hub 4
Pré-requisitos do parceiro 5
Casos de uso e permissões 6
Hospedado pelo parceiro: descobertas enviadas da conta do parceiro 6
Hospedado pelo parceiro: descobertas enviadas da conta do parceiro 7
Hospedado pelo cliente: descobertas enviadas da conta do cliente 9
Processo de integração de parceiro 11
Go-to-market atividades 14
Entrada na página de parceiros do Security Hub 14
Comunicados à imprensa 14
AWS Blog da Partner Network (APN) 15
Coisas importantes que você deve saber sobre o blog da APN 15
Por que escrever para o blog da APN? 16
Que tipo de conteúdo é mais adequado? 16
Planilha simples ou planilha de marketing 16
Whitepaper ou e-book 17
Webinário 17
Vídeo de demonstração 17
Manifesto de integração 18
Caso de uso e informações de marketing 19
Caso de uso de provedores e consumidores de descobertas 19
Caso de uso de parceiro de consultoria (CP) 20
Conjuntos de dados 20
Arquitetura 20
Configuração 21
Média de descobertas por dia por cliente 21
Latência 21
Descrição da empresa e do produto 22
Ativos do site do parceiro 22
Logotipo para página de parceiros 22

Logotipos para o console do Security Hub ... 23
Tipos de descoberta ... 23
Linha direta ... 23
Descoberta sobre pulsação ... 23
Informações do console do Security Hub ... 24
Informações da empresa ... 24
Informações do produto ... 25
Diretrizes e listas de verificação ... 36
Diretrizes para o logotipo do console ... 36
Princípios para criar e atualizar descobertas ... 39
Diretrizes para mapeamento do ASFF ... 40
Informações de identificação ... 40
Title and Description ... 41
Tipos de descoberta ... 41
Timestamps ... 41
Severity ... 42
Remediation ... 43
SourceUrl ... 43
Malware, Network, Process, ThreatIntelIndicators ... 43
Resources ... 47
ProductFields ... 47
Compliance ... 47
Campos restritos ... 47
Diretrizes para o uso da API `BatchImportFindings` ... 48
Lista de verificação de preparação do produto ... 48
Mapeamento do ASFF ... 49
Configuração e função de integração ... 51
Documentação ... 53
Informações sobre o cartão do produto ... 55
Informações de marketing ... 56
Perguntas frequentes sobre parceiros ... 58
Histórico de documentos ... 71
... lxxiii

Visão geral da integração de terceiros com AWS Security Hub

Este guia é destinado aos AWS parceiros da Partner Network (APN) que gostariam de criar uma integração com o. AWS Security Hub

Como parceiro da APN, você pode se integrar com o Security Hub de uma ou mais das seguintes maneiras:

- Enviar descobertas para o Security Hub
- Consumir as descobertas do Security Hub
- Ambos enviam e consomem descobertas do Security Hub
- Usar o Security Hub como o centro da oferta de um provedor de serviços de segurança gerenciados (MSSP)
- Consulte os AWS clientes sobre como implantar e usar o Security Hub

Este guia de integração se concentra principalmente em parceiros que enviam descobertas para o Security Hub.

Tópicos

- Por que integrar com AWS Security Hub?
- Preparando-se para enviar descobertas para AWS Security Hub
- Preparando-se para receber as descobertas de AWS Security Hub
- Recursos para aprender sobre AWS Security Hub

Por que integrar com AWS Security Hub?

AWS Security Hub fornece uma visão abrangente dos alertas de segurança de alta prioridade e do status de segurança em todas as contas do Security Hub. O Security Hub permite que parceiros como você enviem descobertas de segurança ao Security Hub para fornecer aos seus clientes informações sobre as descobertas de segurança que você gera.

Uma integração com o Security Hub pode agregar valor das formas a seguir.

- Satisfaz seus clientes que solicitaram uma integração com o Security Hub

- Oferece aos seus clientes uma visão única de suas descobertas relacionadas AWS à segurança
- Permite que novos clientes descubram sua solução quando procuram parceiros que forneçam descobertas relacionadas a tipos específicos de eventos de segurança

Antes de criar uma integração com o Security Hub, examine os motivos da integração. É mais provável que uma integração seja bem-sucedida se seus clientes quiserem uma integração do Security Hub com seu produto. Você pode criar uma integração apenas por motivos de marketing ou para adquirir novos clientes. No entanto, se você criar a integração sem nenhuma contribuição atual do cliente e não considerar as necessidades de seus clientes, a integração pode não produzir os resultados esperados.

Preparando-se para enviar descobertas para AWS Security Hub

Como parceiro do APN, você não pode enviar informações de seus clientes ao Security Hub até que a equipe do Security Hub o habilite como provedor de descoberta. Para ser habilitado como provedor de descoberta, é necessário concluir as etapas de integração a seguir. Isso garante uma experiência positiva no Security Hub para você e seus clientes.

Ao concluir as etapas de integração, siga as diretrizes em the section called “Princípios para criar e atualizar descobertas”, the section called “Diretrizes para mapeamento do ASFF” e the section called “Diretrizes para o uso da API `BatchImportFindings`”.

1. Mapeie suas descobertas de segurança para o AWS Security Finding Format (ASFF).
2. Crie sua arquitetura de integração para enviar as descobertas para o endpoint regional correto do Security Hub. Para fazer isso, você define se enviará descobertas de sua própria AWS conta ou de dentro das contas de seus clientes.
3. Faça com que seus clientes assinem o produto em suas contas. Para fazer isso, eles podem usar o console ou a operação de API `EnableImportFindingsForProduct`. Consulte Managing product integrations no Guia do usuário do AWS Security Hub .

   Você também pode assinar o produto para eles. Para fazer isso, você usa uma função entre contas para acessar a operação de API `EnableImportFindingsForProduct` em nome do cliente.

   Essa etapa estabelece as políticas de recursos necessárias para aceitar as descobertas desse produto para essa conta.

As publicações de blog a seguir discutem algumas das integrações de parceiros existentes com o Security Hub.

- Anunciando a integração do Cloud Custodian com AWS Security Hub
- Use AWS Fargate e Prowler para enviar descobertas de configuração de segurança sobre AWS serviços ao Security Hub
- Como importar avaliações de regras do AWS Config como descobertas no Security Hub

Preparando-se para receber as descobertas de AWS Security Hub

Para receber descobertas de AWS Security Hub, use uma das seguintes opções:

- Faça com que seus clientes enviem automaticamente todas as descobertas para CloudWatch Eventos. Um cliente pode criar regras de CloudWatch eventos específicas para enviar descobertas para alvos específicos, como um SIEM ou um bucket S3.
- Faça com que seus clientes selecionem descobertas específicas ou grupos de descobertas no console do Security Hub e, em seguida, tomem medidas sobre elas.

Por exemplo, seus clientes podem enviar descobertas para um SIEM, um sistema de emissão de tíquetes, uma plataforma de bate-papo ou um fluxo de trabalho de correção. Isso faria parte de um fluxo de trabalho de triagem de alertas que um cliente executa no Security Hub.

Essas ações são chamadas de ações personalizadas. Quando um usuário realiza uma ação personalizada, um CloudWatch evento é criado para essas descobertas específicas. Como parceiro, você pode aproveitar esse recurso e criar regras ou metas de CloudWatch eventos para um cliente usar como parte de uma ação personalizada. Observe que esse recurso não envia automaticamente todas as descobertas de um determinado tipo ou classe para CloudWatch Eventos. Este recurso permite que o usuário tome medidas em relação a descobertas específicas.

As postagens de blog a seguir descrevem soluções que usam a integração com o Security Hub and CloudWatch Events para ações personalizadas.

- Como integrar ações AWS Security Hub personalizadas com PagerDuty
- Como habilitar ações personalizadas em AWS Security Hub
- Como importar avaliações de regras do AWS Config como descobertas no Security Hub

Recursos para aprender sobre AWS Security Hub

Os materiais a seguir podem ajudar você a entender melhor a AWS Security Hub solução e como AWS os clientes podem usar o serviço.

- Vídeo Introduction to AWS Security Hub
- Guia do usuário do Security Hub
- Referência da API do Security Hub
- Webinar de integração

Também recomendamos que você habilite o Security Hub em uma de suas AWS contas e tenha alguma experiência prática com o serviço.

Pré-requisitos do parceiro

Antes de começar uma integração com AWS Security Hub, você deve atender a um dos seguintes critérios:

- Você é um AWS Select Tier Partner ou superior.
- Você ingressou no AWS percurso de parceiro ISV e o produto que você usa para a integração do Security Hub concluiu uma Revisão técnica básica (FTR) da AWS. Em seguida, o produto recebe o selo “Avaliado por AWS”.

Você também deve ter um acordo mútuo de confidencialidade em vigor com AWS.

Casos de uso de integração e permissões necessárias

AWS Security Hub permite que AWS os clientes recebam descobertas dos parceiros da APN. Os produtos do parceiro podem ser executados dentro ou fora da AWS conta do cliente. A configuração de permissão na conta do cliente difere com base no modelo que o produto parceiro usa.

No Security Hub, o cliente sempre controla quais parceiros podem enviar descobertas para a conta do cliente. Os clientes podem revogar as permissões de um parceiro a qualquer momento.

Para permitir que um parceiro envie descobertas de segurança para sua conta, o cliente primeiro assina o produto parceiro no Security Hub. A etapa de assinatura é necessária para todos os casos de uso descritos abaixo. Para obter detalhes sobre como os clientes gerenciam integrações de produtos, consulte Managing product integrations no Guia do usuário do AWS Security Hub .

Depois que um cliente assina um produto parceiro, o Security Hub cria automaticamente uma política de recursos gerenciados. A política concede ao produto parceiro permissão para usar a operação de API `BatchImportFindings` para enviar descobertas ao Security Hub para a conta do cliente.

Aqui estão os casos comuns de produtos de parceiros que se integram ao Security Hub. As informações incluem as permissões adicionais necessárias para cada caso de uso.

Hospedado pelo parceiro: descobertas enviadas da conta do parceiro

Esse caso de uso abrange parceiros que hospedam um produto em sua própria AWS conta. Para enviar descobertas de segurança para um AWS cliente, o parceiro chama a operação da `BatchImportFindings`API a partir da conta do produto parceiro.

Para esse caso de uso, a conta do cliente só precisa das permissões estabelecidas quando o cliente assina o produto do parceiro.

Na conta do parceiro, a entidade principal do IAM que chama a operação de API `BatchImportFindings` deve ter uma política do IAM que permita que a entidade principal chame `BatchImportFindings`.

Permitir que um produto parceiro envie descobertas ao cliente no Security Hub é um processo de duas etapas:

1. O cliente cria uma assinatura para um produto parceiro no Security Hub.
2. O Security Hub gera a política correta de recursos gerenciados com a confirmação do cliente.

Para enviar descobertas de segurança relacionadas à conta do cliente, o produto parceiro usa suas próprias credenciais para chamar a operação de API `BatchImportFindings`.

Veja a seguir o exemplo de uma política do IAM que concede à entidade principal da conta do parceiro as permissões do Security Hub necessárias.

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

Hospedado pelo parceiro: descobertas enviadas da conta do parceiro

Esse caso de uso abrange parceiros que hospedam um produto em sua própria AWS conta, mas usam uma função entre contas para acessar a conta do cliente. Eles chamam a operação de API `BatchImportFindings` por meio da conta do cliente.

Para esse caso de uso, para chamar a operação de API `BatchImportFindings`, a conta do parceiro assume um perfil do IAM gerenciado pelo cliente na conta do cliente.

Essa chamada é feita a partir da conta do cliente. Portanto, a política de recursos gerenciados deve permitir que o ARN do produto da conta do produto parceiro seja usado na chamada. A política de recursos gerenciados do Security Hub concede permissão para a conta do produto parceiro e o ARN do produto parceiro. O ARN do produto é o identificador exclusivo do parceiro como fornecedor. Como a chamada não vem da conta do produto parceiro, o cliente deve conceder permissão explícita para que o produto parceiro envie as descobertas ao Security Hub.

A prática recomendada para funções entre contas de parceiros e clientes é usar um identificador externo fornecido pelo parceiro. Esse identificador externo faz parte da definição da política entre contas na conta do cliente. O parceiro deve fornecer o identificador ao assumir a função. Um identificador externo fornece uma camada adicional de segurança ao conceder acesso à AWS conta a um parceiro. O identificador exclusivo garante que o parceiro use a conta correta do cliente.

Permitir que um produto parceiro envie descobertas ao cliente no Security Hub com uma função entre contas acontece em quatro etapas:

1. O cliente, ou parceiro que usa funções entre contas e trabalha em nome do cliente, inicia a assinatura de um produto no Security Hub.
2. O Security Hub gera a política correta de recursos gerenciados com a confirmação do cliente.
3. O cliente configura a função entre contas manualmente ou usando. AWS CloudFormation Para obter informações sobre funções entre contas, consulte Como fornecer acesso a AWS contas pertencentes a terceiros no Guia do usuário do IAM.
4. O produto armazena com segurança a função do cliente e o ID externo.

Em seguida, o produto envia as descobertas para o Security Hub:

1. O produto chama o AWS Security Token Service (AWS STS) para assumir a função de cliente.
2. O produto chama a operação de API `BatchImportFindings` no Security Hub com as credenciais temporárias da função assumida.

Veja a seguir o exemplo de uma política do IAM que concede as permissões do Security Hub necessárias à função entre contas do parceiro.

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

A seção `Resource` da política identifica a assinatura específica do produto. Isso garante que o parceiro só possa enviar descobertas para o produto parceiro no qual o cliente está inscrito.

Hospedado pelo cliente: descobertas enviadas da conta do cliente

Esse caso de uso abrange parceiros que têm um produto implantado na conta da AWS do cliente. A API `BatchImportFindings` é chamada por meio da solução que é executada na conta do cliente.

Para esse caso de uso, o produto parceiro deve receber permissões adicionais para chamar a API `BatchImportFindings`. A forma como essa permissão é concedida varia de acordo com a solução do parceiro e como ela é configurada na conta do cliente.

Um exemplo dessa abordagem é um produto parceiro executado em uma EC2 instância na conta do cliente. Essa EC2 instância deve ter uma função de EC2 instância associada a ela que conceda à instância a capacidade de chamar a operação da `BatchImportFindings`API. Isso permite que a EC2 instância envie descobertas de segurança para a conta do cliente.

Esse caso de uso é funcionalmente equivalente a um cenário em que um cliente carrega as descobertas de um produto que ele possui em sua conta.

O cliente permite que o produto parceiro envie descobertas da conta do cliente para o cliente no Security Hub:

1. O cliente implanta o produto do parceiro em sua AWS conta manualmente usando AWS CloudFormation ou outra ferramenta de implantação.
2. O cliente define a política do IAM necessária para o produto do parceiro usar ao enviar as descobertas para o Security Hub.
3. O cliente associa a política aos componentes necessários do produto do parceiro, como uma EC2 instância, um contêiner ou uma função Lambda.

Agora o produto pode enviar descobertas para o Security Hub:

1. O produto parceiro usa o AWS SDK ou AWS CLI para chamar a operação da `BatchImportFindings`API no Security Hub. Ele faz a chamada usando o componente na conta do cliente ao qual a política está anexada.
2. Durante a chamada da API, as credenciais temporárias necessárias são geradas para permitir que a chamada de `BatchImportFindings` seja bem-sucedida.

Aqui está um exemplo de uma política do IAM que concede as permissões necessárias do Security Hub ao produto parceiro na conta do cliente.

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

Processo de integração de parceiro

Como parceiro, você pode esperar concluir várias etapas de alto nível como parte do seu processo de integração. Você deve concluir essas etapas antes de enviar as descobertas de segurança para AWS Security Hub o.

1. Você inicia um compromisso com a equipe de parceiros do APN ou com a equipe do Security Hub e expressa interesse em se tornar um parceiro do Security Hub. Você identifica os endereços de e-mail a serem adicionados aos canais de comunicação do Security Hub.
2. AWS fornece os materiais de integração do parceiro do Security Hub.
3. Você está convidado para o canal Slack, parceiro do Security Hub, onde pode fazer perguntas relacionadas à sua integração.
4. Você fornece aos contatos dos parceiros da APN um rascunho do manifesto de integração do produto para análise.

   O manifesto de integração do produto contém informações que são usadas para criar o Amazon Resource Name (ARN) do produto parceiro para a integração com. AWS Security Hub

   Ele fornece à equipe do Security Hub as informações que aparecem na página do provedor parceiro no console do Security Hub. Ele também é usado para propor novos insights gerenciados relacionados à integração a serem adicionados à biblioteca de insights do Security Hub.

   Essa versão inicial do manifesto de integração do produto não precisa ter os detalhes completos. Mas ele deve conter pelo menos o caso de uso e as informações do conjunto de dados.

   Para obter detalhes sobre o manifesto e as informações necessárias, consulte Manifesto de integração.
5. A equipe do Security Hub fornece um ARN de produto para seu produto. Você usa o ARN para enviar descobertas para o Security Hub.
6. Você cria sua integração para enviar ou receber descobertas do Security Hub.

   Como mapear descobertas para o ASFF

   Para enviar descobertas ao Security Hub, você deve mapear suas descobertas para o AWS Security Finding Format (ASFF).

   O ASFF fornece uma descrição consistente das descobertas que podem ser compartilhadas entre serviços da AWS de segurança, parceiros e sistemas de segurança do cliente. Isso reduz

os esforços de integração, incentiva uma linguagem comum e fornece um esquema para os implementadores.

ASFF é o formato de protocolo eletrônico necessário para enviar descobertas para o AWS Security Hub. As descobertas são representadas como documentos JSON que aderem ao esquema JSON ASFF e ao RFC-7493, o formato de mensagem I-JSON. Para mais detalhes sobre os esquemas do ASFF, consulte AWS Security Finding Format (ASFF) no Guia do usuário do AWS Security Hub .

Consulte the section called “Diretrizes para mapeamento do ASFF”.

Como criar e testar a integração

Você pode concluir todos os testes de sua integração usando uma AWS conta que você possui. Isso dá a você visibilidade total de como as descobertas aparecem no Security Hub. Também ajuda você a entender a experiência do cliente com suas descobertas de segurança.

Você usa a operação de API `BatchImportFindings` para enviar descobertas novas e atualizadas para o Security Hub.

Durante a criação de uma integração do Security Hub, AWS incentiva você a manter seus contatos de parceiros da APN informados sobre o progresso da integração. Você também pode pedir ajuda aos contatos do seu parceiro da APN com questões de integração.

Consulte the section called “Diretrizes para o uso da API `BatchImportFindings`”.

7. Quanto tempo leva para receber as descobertas do Security Hub? Essa integração deve ser demonstrada usando uma conta de propriedade da equipe do Security Hub.

   Se eles se sentirem confortáveis com a integração, a equipe do Security Hub aprova a possibilidade de listá-lo como provedor.

8. Você AWS fornece um manifesto final para análise.
9. A equipe do Security Hub cria a integração do provedor no console do Security Hub. Os clientes podem então descobrir e habilitar a integração.
10. (Opcional) Você se envolve em iniciativas adicionais de marketing para promover sua integração com o Security Hub. Consulte Go-to-market atividades.

    No mínimo, o Security Hub recomenda que você forneça os ativos a seguir.

    - Um vídeo de demonstração (3 minutos no máximo) da integração funcional. O vídeo é usado para fins de marketing e é postado no AWS YouTube canal.

- Um diagrama de arquitetura em um único slide para adicionar ao conjunto de slides de primeira chamada do Security Hub.

Go-to-market atividades

Os parceiros também podem participar de atividades de marketing opcionais para ajudar a explicar e promover sua integração do AWS Security Hub .

Se você quiser criar seu próprio conteúdo de marketing relacionado ao Security Hub, antes de lançar o conteúdo, envie um rascunho para seu gerente de parceiros da APN para análise e aprovação. Isso garante que todos estejam alinhados com as mensagens.

AWS Os parceiros da Rede de Parceiros (APN) podem usar a Central de Marketing de Parceiros da APN e o programa Market Development Funds (MDF) para criar campanhas e obter apoio financeiro. Para obter detalhes sobre esses programas, entre em contato com seu gerente de parceiros.

Entrada na página de parceiros do Security Hub

Depois que você for aprovado como parceiro do Security Hub, sua solução poderá ser exibida na página dos parceiros do AWS Security Hub.

Para ser listado nesta página, forneça os detalhes a seguir aos seus contatos de parceiros da APN. Pode ser seu gerente de desenvolvimento de parceiros (PDM), arquiteto de soluções de parceiros (PSA) ou um e-mail para `<securityhub-pms@amazon.com>`.

- Uma breve descrição de sua solução, sua integração com o Security Hub e o valor que a integração com o Security Hub oferece aos clientes. Essa descrição está limitada a 700 caracteres, incluindo espaços.
- O URL de uma página que descreve sua solução. Esse site deve ser específico para sua integração da AWS e, mais especificamente, para sua integração com o Security Hub. Ele deve se concentrar na experiência do cliente e no valor que os clientes recebem quando usam a integração.
- Uma cópia em alta resolução do seu logotipo com 600 x 300 pixels. Para obter detalhes sobre os requisitos para este logotipo, consulte the section called “Logotipo para página de parceiros”.

Comunicados à imprensa

Como parceiro aprovado, você pode, opcionalmente, publicar um comunicado à imprensa em seu site e canais de relações públicas. O comunicado à imprensa deve ser aprovado por AWS.

Antes de publicar o comunicado à imprensa, você deve enviá-lo AWS para análise pelo marketing de parceiros da APN, pela liderança do Security Hub e pelos Serviços de Segurança AWS Externos (ESS). O comunicado de imprensa pode incluir uma proposta de cotação para o vice-presidente dos ESS.

Para iniciar esse processo, trabalhe com seu PDM. Temos um acordo de serviço (SLA) de dez dias úteis para analisar os comunicados à imprensa.

AWS Blog da Partner Network (APN)

Também podemos ajudar você a publicar uma entrada de blog de sua autoria no blog da APN. A entrada do blog deve se concentrar na história do cliente e no caso de uso. Ele não pode ser posicionado apenas como um parceiro de lançamento de integração.

Se você estiver interessado, entre em contato com seu PDM ou PSA para iniciar o processo. Os blogs da APN podem levar oito semanas ou mais para serem aprovados e publicados.

Coisas importantes que você deve saber sobre o blog da APN

Quando uma publicação do blog é criada, lembre-se do seguinte:

O que entra em uma publicação no blog?

- As publicações dos parceiros devem ser instrutivas e fornecer conhecimento aprofundado sobre um tópico relevante para os clientes da AWS .
- O tamanho ideal é no máximo 1.500 palavras. Os leitores valorizam um conteúdo educacional profundo que lhes ensine o que é possível fazer AWS.
- O conteúdo deve ser original para o blog da APN. Não reutilize conteúdo de fontes como publicações de blog ou whitepapers existentes.

Quais são os outros limites de publicação no blog da APN?

- Somente parceiros de nível avançado ou premier podem publicar no blog da APN. Há exceções para parceiros selecionados que têm uma designação de programa da APN, como o Entrega de Serviços.
- Cada parceiro está limitado a três cargos por ano. Com dezenas de milhares de parceiros da APN, a AWS deve ser justa em sua cobertura.

Cada publicação deve ter um patrocinador técnico que possa validar a solução ou o caso de uso.

Quanto tempo leva para editar uma publicação de blog antes de ela ser publicada?

Depois de enviar o primeiro rascunho completo da publicação do blog, a edição leva de quatro a seis semanas.

Por que escrever para o blog da APN?

Uma publicação de blog da APN pode fornecer os benefícios a seguir.

- Credibilidade — Para os parceiros da APN, ter uma história publicada pela AWS pode influenciar clientes em todo o mundo.
- Visibilidade — O blog da APN é um dos blogs mais lidos, AWS com 1,79 milhão de visualizações de página em 2019, incluindo tráfego influenciado.
- Negócios: as publicações dos parceiros da APN têm botões de conexão que podem gerar leads por meio do programa Interações com Clientes da APN (ACE).

Que tipo de conteúdo é mais adequado?

Os tipos de conteúdo a seguir são mais adequados para uma publicação no blog da APN.

- O conteúdo técnico é o tipo de história mais popular. Isso inclui destaques da solução e informações práticas. Mais de 75% dos leitores veem esse conteúdo técnico.
- Os clientes valorizam histórias de 200 níveis ou mais que demonstram como algo funciona na AWS ou como um parceiro da APN resolveu um problema comercial para os clientes.
- Publicações escritas por especialistas técnicos ou especialistas no assunto têm, de longe, o melhor desempenho.

Planilha simples ou planilha de marketing

Uma planilha simples é um documento de uma página que descreve seu produto, sua arquitetura de integração e casos de uso conjuntos de clientes.

Se você criar uma planilha simples para sua integração, envie uma cópia para a equipe do Security Hub, que a adicionará à página do parceiro.

Whitepaper ou e-book

Se você criar um whitepaper ou e-book descrevendo seu produto, sua arquitetura de integração e casos de uso conjuntos de clientes, envie uma cópia para a equipe do Security Hub, que o adicionará à página de parceiros do Security Hub.

Webinário

Se você realizar um webinar sobre sua integração, envie uma gravação do webinar para a equipe do Security Hub. A equipe criará um link para ele a partir da página do parceiro.

A equipe também pode fornecer um especialista no assunto do Security Hub para participar do seu webinar.

Vídeo de demonstração

Para fins de marketing, você pode produzir um vídeo de demonstração da integração funcional. Publique esse vídeo na sua conta da plataforma de vídeo. A equipe do Security Hub criará um link para ele na página do parceiro.

Manifesto de integração

Cada parceiro de AWS Security Hub integração deve preencher um manifesto de integração do produto que forneça os detalhes necessários para a integração proposta.

A equipe do Security Hub usa essas informações de várias maneiras:

- Para criar a listagem do seu site
- Para criar o cartão do produto para o console do Security Hub
- Para informar a equipe de produto sobre seu caso de uso

Para avaliar a qualidade da integração proposta e das informações fornecidas, a equipe do Security Hub usa a the section called “Lista de verificação de preparação do produto”. Essa lista de verificação determina se sua integração está pronta para ser lançada.

Todas as informações técnicas que você fornece também devem estar refletidas em sua documentação.

Você pode baixar uma versão em PDF do manifesto de integração do produto na seção Recursos da página de AWS Security Hub parceiros. Observe que a página de parceiros não está disponível nas regiões China (Pequim) e China (Ningxia).

Conteúdo

- Caso de uso e informações de marketing
  - Caso de uso de provedores e consumidores de descobertas
  - Caso de uso de parceiro de consultoria (CP)
  - Conjuntos de dados
  - Arquitetura
  - Configuração
  - Média de descobertas por dia por cliente
  - Latência
  - Descrição da empresa e do produto
  - Ativos do site do parceiro
  - Logotipo para página de parceiros
  - Logotipos para o console do Security Hub

- Tipos de descoberta
  - Linha direta
  - Descoberta sobre pulsação
- AWS Security Hub informações do console
  - Informações da empresa
  - Informações do produto

Caso de uso e informações de marketing

Os casos de uso a seguir podem ajudá-lo a configurar AWS Security Hub para diferentes propósitos.

Caso de uso de provedores e consumidores de descobertas

Obrigatório para provedores de software independentes (ISV).

Para descrever seu caso de uso relacionado à sua integração com AWS Security Hub, responda às perguntas a seguir. Se você não planeja enviar ou receber descobertas, observe isso nesta seção e conclua a próxima seção.

As informações a seguir devem ser refletidas em sua documentação.

- Você enviará descobertas, receberá descobertas ou ambas?
- Se você planeja enviar descobertas, que tipos de descobertas você enviará? Você enviará todas as descobertas ou um subconjunto específico das descobertas?
- Se você planeja receber descobertas, o que você fará com essas descobertas? Que tipos de descobertas você receberá? Por exemplo, você receberá todas as descobertas, descobertas de um determinado tipo ou somente descobertas específicas que um cliente selecionar?
- Você planeja atualizar as descobertas? Em caso afirmativo, quais campos você atualizará? O Security Hub recomenda que você atualize as descobertas em vez de sempre criar novas. A atualização das descobertas existentes ajuda a diminuir o ruído de descoberta para os clientes.

  Para atualizar uma descoberta, você envia uma descoberta com um ID de descoberta atribuído a uma descoberta que você já enviou.

Para obter feedback antecipado sobre seu caso de uso e conjuntos de dados, entre em contato com o parceiro da APN ou com a equipe do Security Hub.

Caso de uso de parceiro de consultoria (CP)

Obrigatório se você for um parceiro de consultoria do Security Hub.

Forneça dois casos de uso de clientes para seu trabalho com o Security Hub. Esses podem ser casos de uso privado. A equipe do Security Hub não os anuncia em nenhum lugar. Eles devem descrever uma das ações a seguir ou ambas.

- Como você ajuda os clientes a inicializar o Security Hub? Por exemplo, você ajudou clientes a usar serviços profissionais, um módulo do Terraform ou um AWS CloudFormation modelo?
- Como você ajuda os clientes a operacionalizar e ampliar o Security Hub? Por exemplo, você forneceu modelos de resposta ou correção, criou integrações personalizadas ou usou ferramentas de business intelligence para configurar um painel executivo?

Conjuntos de dados

Obrigatório se você enviar descobertas para o Security Hub.

Para as descobertas que você enviará ao Security Hub, forneça as informações a seguir.

- As descobertas em seu formato nativo, como JSON ou XML
- Um exemplo de como você converterá as descobertas para o AWS Security Finding Format (ASFF)

Informe à equipe do Security Hub se você precisar de alguma atualização no ASFF para apoiar sua integração.

Arquitetura

Obrigatório se você enviar descobertas para o Security Hub.

Descreva como você se integrará ao Security Hub. Essas informações também devem ser refletidas em sua documentação.

Você deve fornecer diagramas de arquitetura. Ao preparar seus diagramas de arquitetura, considere o seguinte:

- Quais AWS serviços, agentes do sistema operacional e assim por diante você usará?

- Se você enviar descobertas para o Security Hub, enviará descobertas da AWS conta do cliente ou da sua própria AWS conta?
- Se você receber descobertas, como usará a integração de CloudWatch eventos?
- Como você converterá as descobertas em ASFF?
- Como você agrupará as descobertas, rastreará o estado da descoberta e evitará limites de controle de utilização?

Configuração

Obrigatório se você enviar descobertas para o Security Hub.

Descrever como um cliente configurará sua integração com o Security Hub.

No mínimo, você deve usar AWS CloudFormation modelos ou uma infraestrutura similar, como modelos de código. Alguns parceiros forneceram uma interface de usuário para oferecer suporte à integração com um clique.

A configuração não deve levar mais de 15 minutos. A documentação do produto também deve fornecer orientação de configuração para sua integração.

Média de descobertas por dia por cliente

Obrigatório se você enviar descobertas para o Security Hub.

Quantas atualizações de descobertas por mês (média e máxima) você espera enviar para o Security Hub em toda a sua base de clientes? As estimativas de ordens de magnitude são aceitáveis.

Latência

Obrigatório se você enviar descobertas para o Security Hub.

Com que rapidez você agrupa e envia descobertas para o Security Hub? Em outras palavras, qual é a latência desde o momento em que a descoberta é criada em seu produto até o momento em que ela é enviada ao Security Hub?

Essas informações também devem ser refletidas em sua documentação. É uma pergunta comum dos clientes.

Descrição da empresa e do produto

Necessário para todas as integrações com o Security Hub.

Descreva resumidamente sua empresa e seu produto, com ênfase específica na natureza da integração com o Security Hub. Usamos isso em nossa página de parceiros do Security Hub.

Se você estiver integrando vários produtos com o Security Hub, poderá fornecer uma descrição separada para cada produto, mas os combinaremos em uma única entrada na página do parceiro.

Cada descrição não pode ter mais de 700 caracteres com espaços.

Ativos do site do parceiro

Necessário para todas as integrações com o Security Hub.

No mínimo, você deve fornecer um URL para usar no hiperlink Saiba mais na página de parceiros do Security Hub. Deve ser uma página inicial de marketing que descreva a integração entre seu produto e o Security Hub.

Se você integrar vários produtos ao Security Hub, poderá ter uma única página de destino para eles. O Security Hub recomenda que essa página inicial inclua um link para suas instruções de configuração.

Você também pode fornecer links para outros recursos, como blogs, webinars, vídeos de demonstração ou whitepapers. O Security Hub também terá links para aqueles da página de seus parceiros.

Logotipo para página de parceiros

Necessário para todas as integrações do Security Hub.

Forneça um URL para um logotipo a ser exibido na página de parceiros do Security Hub. O logotipo deve atender aos seguintes critérios:

- Tamanho: 600 x 300 pixels
- Recorte: justo, sem preenchimento
- Plano de fundo: transparente
- Formato: PNG

Logotipos para o console do Security Hub

Necessário para todas as integrações.

URLs Forneça os logotipos do modo claro e do modo escuro para serem exibidos no console do Security Hub.

Os logotipos devem atender aos seguintes critérios:

- Formato: SVG
- Tamanho: 175 x 40 pixels. Se for maior, a imagem deve usar essa proporção.
- Recorte: justo, sem preenchimento
- Plano de fundo: transparente

Para obter diretrizes detalhadas para o logotipo pequeno, consulte the section called “Diretrizes para o logotipo do console”.

Tipos de descoberta

Obrigatório se você enviar descobertas para o Security Hub.

Forneça uma tabela que documente os tipos de descoberta formatados em ASFF que você usa e como eles se alinham aos seus tipos de descoberta nativos. Para obter detalhes sobre como tipos de descoberta no ASFF, consulte Types taxonomy for ASFF no Guia do usuário do AWS Security Hub .

Recomendamos também incluir essas informações na documentação do produto.

Linha direta

Necessário para todas as integrações com o Security Hub.

Forneça um endereço de e-mail e número de telefone ou número de pager para um ponto de contato técnico. O Security Hub se comunicará com esse contato sobre quaisquer problemas técnicos, como quando uma integração não funcionar mais.

Também forneça um ponto de contato 24 horas por dia, 7 dias por semana, para problemas técnicos de alta gravidade.

Descoberta sobre pulsação

Recomendado se você enviar descobertas para o Security Hub.

Você pode enviar ao Security Hub uma descoberta “pulsante” a cada cinco minutos que indique que sua integração com o Security Hub está funcionando?

Se você puder, faça isso usando o tipo de descoberta `Heartbeat`.

AWS Security Hub informações do console

Forneça um texto JSON para a AWS Security Hub equipe que contém as informações a seguir. O Security Hub usa essas informações para criar o ARN do seu produto, exibir a lista de provedores no console e incluir seus insights gerenciados propostos na biblioteca de insights do Security Hub.

Informações da empresa

As informações da empresa fornecem informações sobre sua empresa. Veja um exemplo abaixo:

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

As informações da empresa contêm os seguintes campos:

Campo	Obrigatório	Descrição
`id`	Sim	O identificador exclusivo da empresa. O identificador da empresa deve ser exclusivo entre as empresas. Provavelmente é o mesmo ou semelhante a `name`. Tipo: string Tamanho mínimo: 5 caracteres Tamanho máximo: 24 caracteres Caracteres permitidos: letras minúsculas, números e hifens

Campo	Obrigatório	Descrição
		Devem começar com uma letra minúscula. Deve terminar com um número ou uma letra minúscula.
`name`	Sim	O nome da empresa do provedor a ser exibido no console do Security Hub. Tipo: string Tamanho máximo: 16 caracteres
`description`	Sim	O nome da empresa do provedor a ser exibido no console do Security Hub. Tipo: string Tamanho máximo: 200 caracteres

Informações do produto

Esta seção dispõe de informações sobre esse produto. Veja um exemplo abaixo:

```
{
    "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"
}
```

As informações do produto contêm os campos a seguir.

Campo	Obrigatório	Descrição
`IntegrationType`	Sim	Indica se seu produto envia descobertas para o Security Hub, recebe descobertas do Security Hub ou se ambos envia e recebe descobertas. Se você for um parceiro de consultoria, deixe esse campo em branco. Tipo: matriz de strings Valores válidos: `SEND_FINDINGS_TO_SECURITY_HUB` | `RECEIVE_FINDINGS_FROM_SECURITY_HUB`
`id`	Sim	O identificador exclusivo do produto. Ele deve ser exclusivo dentro de uma empresa. Ele não precisa ser exclusivo em todas as empresas. Provavelmente é o mesmo ou semelhante a `name`. Tipo: string Tamanho mínimo: 5 caracteres Tamanho máximo: 24 caracteres Caracteres permitidos: letras minúsculas, números e hifens Devem começar com uma letra minúscula. Deve terminar com um número ou uma letra minúscula.
`regionsNotSupported`	Sim	Quais das seguintes AWS regiões você não suporta? Em outras palavras, em quais regiões o Security Hub não deve mostrar você como uma opção na página de nossos parceiros no console do Security Hub?

Campo	Obrigatório	Descrição
		Tipo: string Forneça somente o código da região. Por exemplo, `us-west-1` . Para obter uma lista de regiões, consulte Regional endpoints, na Referência geral da AWS. Os códigos de região para o AWS GovCloud (US) são `us-gov-west-1` (para AWS GovCloud (Oeste dos EUA)) e `us-gov-east-1` (para AWS GovCloud (Leste dos EUA)). Os códigos de região para regiões da China são `cn-north-1` [para China (Pequim)] e `cn-northwest-1` [para China (Ningxia)].

Campo	Obrigatório	Descrição
`commercialAccountNumber`	Sim	O número AWS da conta principal do produto para as AWS regiões. Se você enviar descobertas para o Security Hub, a conta fornecida será baseada no local de onde você envia as descobertas. • Da sua AWS conta. Nesse caso, forneça o número da conta que você usa para enviar as descobertas. • Da AWS conta do cliente. Nesse caso, o Security Hub recomenda que você forneça o número da conta principal que você usa para testar a integração. O ideal é que você use a mesma conta para todos os seus produtos em todas as regiões. Se isso não for possível, entre em contato com a equipe do Security Hub. Se você receber apenas descobertas do Security Hub, esse número de conta não será necessário. Tipo: string

Campo	Obrigatório	Descrição
`govcloudAccountNumber`	Não	O número da AWS conta principal do produto para AWS GovCloud (US) regiões (se seu produto estiver disponível em AWS GovCloud (US)). Se você enviar descobertas para o Security Hub, a conta fornecida será baseada no local de onde você envia as descobertas. • Da sua AWS conta. Nesse caso, forneça o número da conta que você usa para enviar as descobertas. • Da AWS conta do cliente. Nesse caso, o Security Hub recomenda que você forneça o número da conta principal que você usa para testar a integração. O ideal é que você use a mesma conta para todos os seus produtos em todas as regiões AWS GovCloud (US) . Se isso não for possível, entre em contato com a equipe do Security Hub. Se você receber apenas descobertas do Security Hub, esse número de conta não será necessário. Tipo: string

Campo	Obrigatório	Descrição
`chinaAccountNumber`	Não	O número da AWS conta principal do produto para as regiões da China (se seu produto estiver disponível nas regiões da China). Se você enviar descobertas para o Security Hub, a conta fornecida será baseada no local de onde você envia as descobertas. • Da sua AWS conta. Nesse caso, forneça o número da conta que você usa para enviar as descobertas. • Da AWS conta do cliente. Nesse caso, o Security Hub recomenda que você forneça o número da conta principal que você usa para testar a integração do produto. O ideal é que você use a mesma conta para todos os seus produtos em todas as regiões. Se isso não for possível, entre em contato com a equipe do Security Hub. Se você receber apenas descobertas do Security Hub, isso pode ser qualquer conta que você possua em uma região da China. Tipo: string
`name`	Sim	O nome da empresa do provedor a ser exibido no console do Security Hub. Tipo: string Tamanho máximo: 24 caracteres

Campo	Obrigatório	Descrição
`description`	Sim	O nome da empresa do provedor a ser exibido no console do Security Hub. Tipo: string Tamanho máximo: 200 caracteres
`importType`	Sim	O tipo de política de recursos para o parceiro. Durante o processo de integração de parceiro, você pode especificar `NEITHER` ou especificar uma das políticas de recursos a seguir. • Com `BATCH_IMPORT_FINDINGS_FROM_PRODUCT_ACCOUNT`, você só pode enviar descobertas para o Security Hub por meio da conta listada no ARN do seu produto. • Com `BATCH_IMPORT_FINDINGS_FROM_CUSTOMER_ACCOUNT`, você só pode enviar descobertas da conta do cliente que se inscreveu com você. Tipo: string Valores válidos: `BATCH_IMPORT_FINDINGS_FROM_PRODUCT_ACCOUNT` | `BATCH_IMPORT_FINDINGS_FROM_CUSTOMER_ACCOUNT` | `NEITHER`

Campo	Obrigatório	Descrição
`category`	Sim	As categorias que definem seu produto. Suas seleções são exibidas no console do Security Hub. Escolha até três categorias. Seleções personalizadas não são permitidas. Se você acha que sua categoria está ausente, entre em contato com a equipe do Security Hub. Tipo: matriz Categorias disponíveis: • `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`

Campo	Obrigatório	Descrição
		• Data Classification • 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

Campo	Obrigatório	Descrição
		• `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`	Não	O URL para o AWS Marketplace destino do seu produto. O URL é exibido no console do Security Hub. Tipo: string Isso deve ser um AWS Marketplace URL. Se você não tiver um AWS Marketplace anúncio, deixe esse campo em branco.

Campo	Obrigatório	Descrição
`configurationUrl`	Sim	O URL da documentação do seu produto sobre a integração com o Security Hub. Esse conteúdo é hospedado em seu site ou em uma página da Web que você gerencia, como uma GitHub página. Tipo: string Sua documentação deve incluir as seguintes informações: • Instruções de configuração • Links para AWS CloudFormation modelos (se necessário) • Informações sobre seu caso de uso para a integração • Latência • Mapeamento do ASFF • Tipos de descobertas incluídas • Arquitetura

Diretrizes e listas de verificação

Ao preparar os materiais necessários para sua AWS Security Hub integração, use essas diretrizes.

A lista de verificação de prontidão é usada para realizar uma revisão final da integração antes que o Security Hub a disponibilize aos clientes do Security Hub.

Tópicos

- Diretrizes para o logotipo a ser exibido no console do AWS Security Hub
- Princípios para criar e atualizar descobertas
- Diretrizes para mapear descobertas no AWS Security Finding Format (ASFF)
- Diretrizes para o uso da API BatchImportFindings
- Lista de verificação de preparação do produto

Diretrizes para o logotipo a ser exibido no console do AWS Security Hub

Para que o logotipo seja exibido no AWS Security Hub console, siga estas diretrizes.

Modos claro e escuro

Você deve fornecer uma versão do logotipo no modo claro e no modo escuro.

Formato

Formato do arquivo SVG

Cor de fundo

Transparente

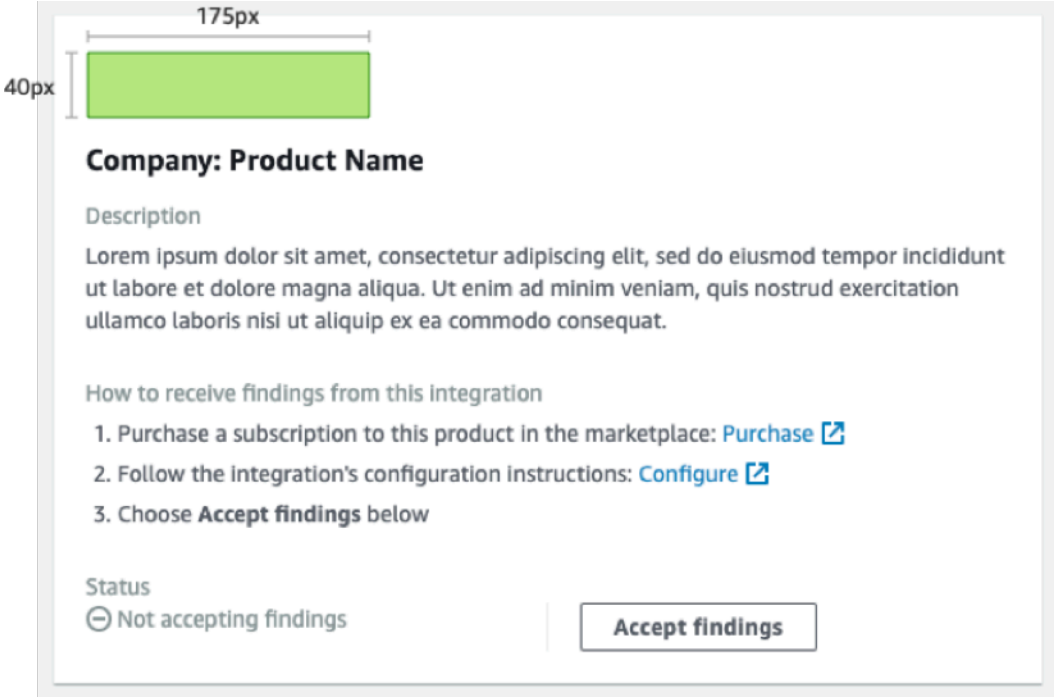
Tamanho

A proporção ideal é 175 px de largura por 40 px de altura.

A altura mínima é de 40 px.

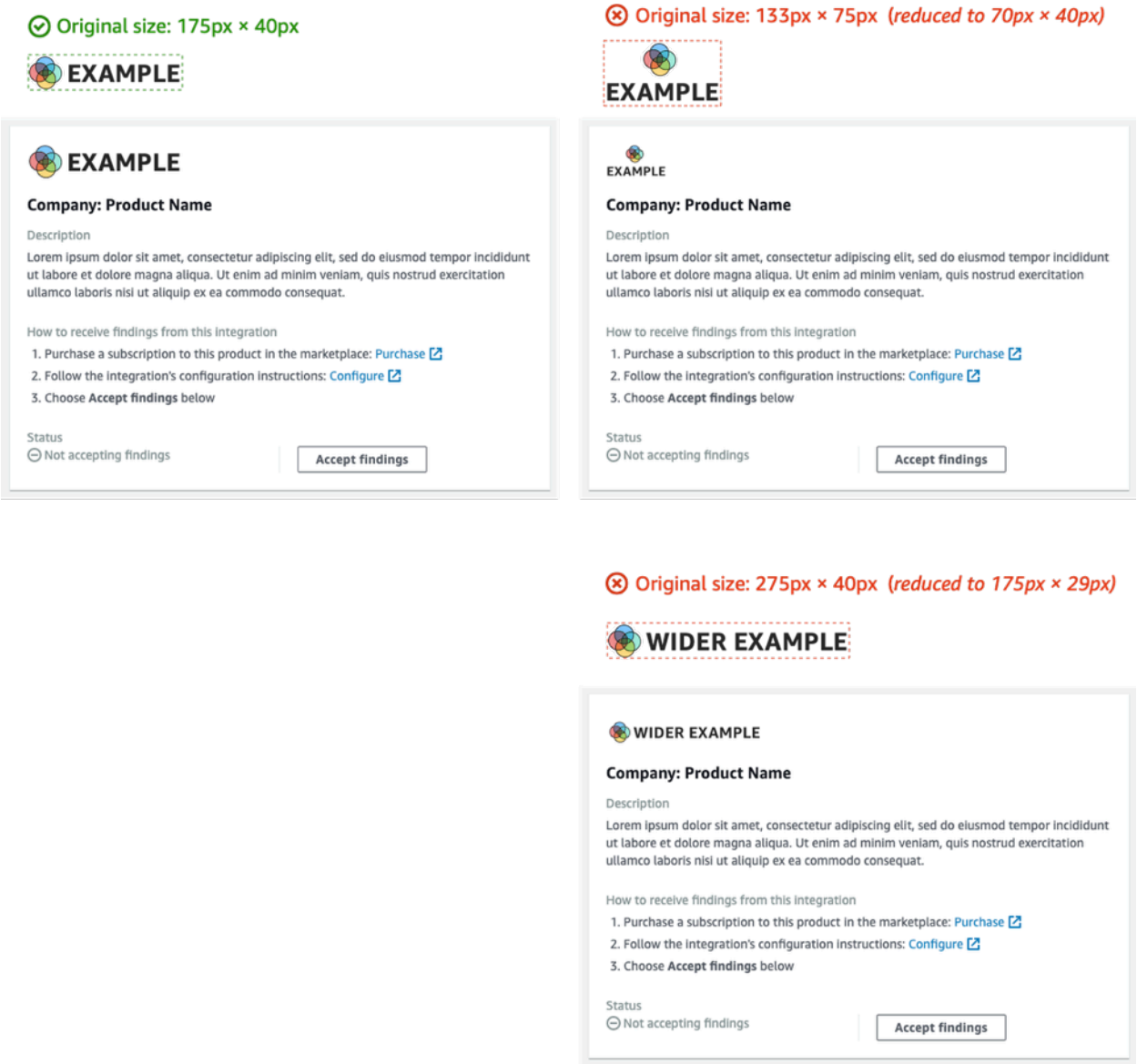
Logotipos retangulares funcionam melhor.

A imagem a seguir mostra como um logotipo ideal é exibido no console do Security Hub.



Se seu logotipo não corresponder a essas dimensões, o Security Hub reduzirá o tamanho para uma altura máxima de 40 px e uma largura máxima de 175 px. Isso afeta a forma como o logotipo é exibido no console do Security Hub.

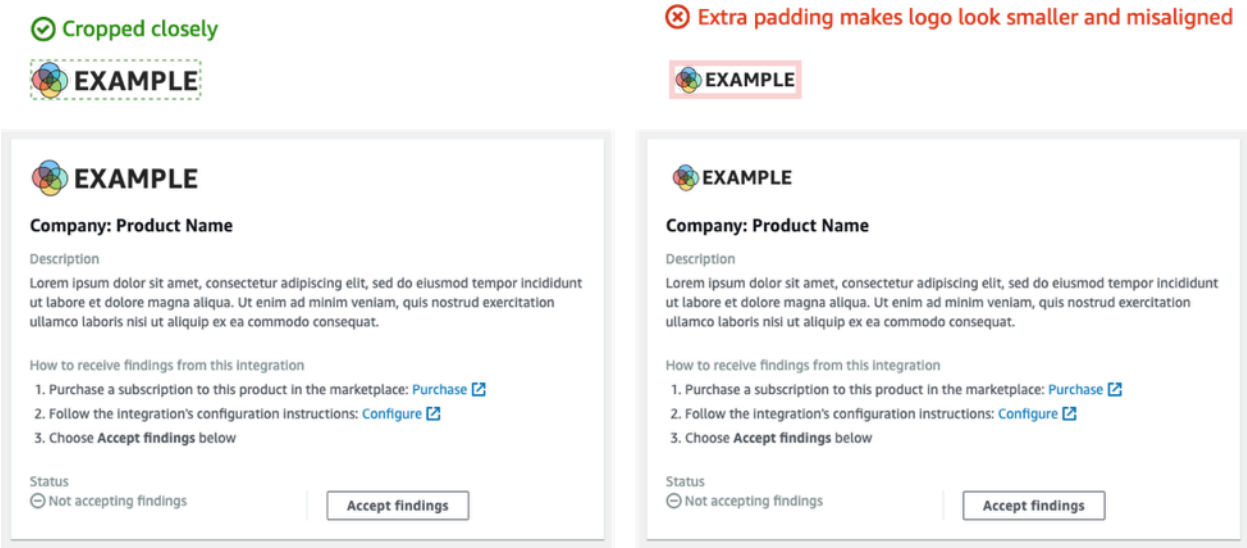
A imagem a seguir compara a exibição de um logotipo que usava o tamanho ideal com logotipos mais largos ou mais altos.



Recorte

Recorte a imagem do logotipo o mais próximo possível. Não forneça preenchimento extra.

A imagem a seguir mostra a diferença entre um logotipo bem recortado e um logotipo com preenchimento extra.



Princípios para criar e atualizar descobertas

Ao planejar como você criará e atualizará as descobertas em AWS Security Hub, lembre-se dos seguintes princípios.

Faça descobertas específicas para que os clientes possam utilizá-las facilmente.

Os clientes querem automatizar as ações de resposta e correção e correlacionar as descobertas com outras descobertas. Para que isso seja possível, as descobertas devem ter as seguintes características:

- Geralmente devem lidar com um recurso único ou primário.
- Devem ter um único tipo de descoberta.
- Devem lidar com um único evento de segurança.

Quando uma descoberta contém dados de vários eventos de segurança, é mais difícil para os clientes tomarem medidas em relação à descoberta.

Mapeie todos os seus campos de descoberta para o Formato de Descoberta de AWS Segurança (ASFF). Permita que os clientes recorram ao Security Hub como fonte confiável.

Os clientes esperam que cada campo que esteja em seu formato de descoberta nativo também seja representado no ASFF no Security Hub.

Os clientes querem que todos os dados estejam presentes na versão da descoberta do Security Hub. A falta de dados faz com que eles percam a confiança no Security Hub como fonte central de informações de segurança.

Minimize a redundância nas descobertas. Não sobrecarregue os clientes com volumes de descobertas.

O Security Hub não é uma ferramenta geral de gerenciamento de logs. Você deve enviar descobertas para o Security Hub que sejam altamente acionáveis e às quais os clientes possam responder e corrigir ou correlacionar diretamente com outras descobertas.

Quando houver apenas uma pequena alteração na descoberta, atualize a descoberta em vez de criar outra.

Quando houver uma grande alteração na descoberta, como na pontuação de gravidade ou no identificador do recurso, crie outra descoberta.

Por exemplo, criar descobertas para verificações de portas individuais em tempo real não é altamente prático. Como a verificação de portas pode ocorrer continuamente, ela produziria um grande volume de descobertas. É muito mais convincente e preciso simplesmente atualizar o horário da última verificação e a contagem de verificações em uma única descoberta para uma verificação de porta em uma porta MongoDB a partir de um nó TOR.

Permita que os clientes personalizem suas descobertas para torná-las mais significativas.

Os clientes querem poder ajustar determinados campos de descoberta para torná-los mais relevantes ao ambiente ou aos requisitos.

Por exemplo, os clientes querem poder adicionar notas, etiquetas e ajustar as pontuações de gravidade com base no tipo de conta ou no tipo de recurso ao qual a descoberta está associada.

Diretrizes para mapear descobertas no AWS Security Finding Format (ASFF)

Siga as diretrizes abaixo para mapear suas descobertas para o ASFF. Para obter descrições detalhadas de cada campo e objeto do ASFF, consulte Formato de Descobertas de Segurança da AWS (ASFF) no Guia do usuário do AWS Security Hub .

Informações de identificação

`SchemaVersion` é sempre `2018-10-08`.

`ProductArn`é o ARN que AWS Security Hub atribui a você.

`Id` é o valor que o Security Hub usa para indexar as descobertas. O identificador da descoberta deve ser exclusivo, para garantir que outras descobertas não sejam sobrescritas. Para atualizar uma descoberta, reenvie a descoberta com o mesmo identificador.

`GeneratorId`pode ser o mesmo `Id` ou pode se referir a uma unidade lógica discreta, como um ID de GuardDuty detector da Amazon, ID de AWS Config gravador ou ID do IAM Access Analyzer.

Title and Description

`Title` deve conter algumas informações sobre o recurso afetado. O `Title` é limitado a 256 caracteres, incluindo espaços.

Adicione informações mais detalhadas em `Description`. A `Description` é limitada a 1.024 caracteres, incluindo espaços. Você pode considerar a possibilidade de adicionar truncagem às descrições. Veja um exemplo abaixo:

```
"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.",
```

Tipos de descoberta

Você fornece suas informações sobre o tipo de descoberta em `FindingProviderFields.Types`.

`Types` deve corresponder à taxonomia de tipos para ASFF.

Se necessário, você pode especificar um classificador personalizado (o terceiro namespace).

Timestamps

O formato ASFF inclui alguns carimbos de data e hora diferentes.

`CreatedAt` e **`UpdatedAt`**

Você deve enviar `CreatedAt` e `UpdatedAt` sempre que chamar `BatchImportFindings` para cada descoberta.

Os valores devem corresponder ao formato ISO86 01 no Python 3.8.

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

`FirstObservedAt` e `LastObservedAt`

`FirstObservedAt` e `LastObservedAt` devem coincidir com o momento em que seu sistema observou a descoberta. Se você não registrar essas informações, não precisará enviar esses carimbos de data e hora.

Os valores correspondem ao formato ISO86 01 no Python 3.8.

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

Severity

Você fornece informações de gravidade no objeto `FindingProviderFields.Severity`, que contém os campos a seguir.

`Original`

O valor da gravidade do seu sistema. `Original` pode ser qualquer string, para atender ao sistema que você usa.

`Label`

O indicador necessário do Security Hub da gravidade da descoberta. Os valores permitidos são os apresentados a seguir.

- `INFORMATIONAL`: nenhum problema foi encontrado.
- `LOW`: o problema não requer ação por conta própria.
- `MEDIUM`: o problema deve ser abordado, mas sem caráter urgente.
- `HIGH`: o problema deve ser tratado como uma prioridade.
- `CRITICAL`: o problema deve ser corrigido imediatamente para evitar mais danos.

As descobertas que estão em conformidade devem sempre ter `Label` definido como `INFORMATIONAL`. Exemplos de `INFORMATIONAL` descobertas são descobertas de verificações de segurança aprovadas e AWS Firewall Manager descobertas que foram corrigidas.

Os clientes geralmente classificam as descobertas de acordo com sua gravidade para fornecer às equipes de operações de segurança uma lista de tarefas. Tenha cautela ao definir a severidade da descoberta como `HIGH` ou `CRITICAL`.

Sua documentação de integração deve incluir sua lógica de mapeamento.

Remediation

`Remediation` tem dois elementos. Esses elementos são combinados no console do Security Hub.

`Remediation.Recommendation.Text` aparece na seção Correção dos detalhes da descoberta. Ele tem um hiperlink para o valor de `Remediation.Recommendation.Url`.

Atualmente, somente as descobertas dos padrões do Security Hub, do IAM Access Analyzer e do Firewall Manager exibem hiperlinks para a documentação sobre como corrigir a descoberta.

SourceUrl

Use somente `SourceUrl` se você puder fornecer um URL com link direto ao seu console para essa descoberta específica. Caso contrário, omita-o do mapeamento.

O Security Hub não oferece suporte a hiperlinks desse campo, mas ele está exposto no console do Security Hub.

Malware, Network, Process, ThreatIntelIndicators

Quando aplicável, use `Malware`, `Network`, `Process` ou `ThreatIntelIndicators`. Cada um desses objetos é exposto no console do Security Hub. Use esses objetos no contexto da descoberta que você está enviando.

Por exemplo, se você detectar um malware que faz uma conexão de saída com um nó de comando e controle conhecido, forneça os detalhes da EC2 instância em`Resource.Details.AwsEc2Instance`. Forneça os `ThreatIntelIndicator` objetos relevantes `Malware` e para essa EC2 instância. `Network`

Malware

`Malware` é uma lista que aceita até cinco matrizes de informações de malware. Faça com que as entradas de malware sejam relevantes para o recurso e a descoberta.

Cada entrada tem os campos a seguir.

`Name`

O nome do malware. O valor é uma string com até 64 caracteres.

`Name` deve ser de uma fonte comprovada de inteligência de ameaças ou de um pesquisador.

`Path`

O caminho para o malware. O valor é uma string com até 512 caracteres. `Path` deve ser um caminho de arquivo do sistema Linux ou Windows, exceto nos casos a seguir.

- Se você digitalizar objetos em um bucket do S3 ou em um compartilhamento do EFS de acordo com as regras do YARA, então `Path` é o caminho do objeto S3://ou HTTPS.
- Se você digitalizar arquivos em um repositório Git, então `Path` é o URL do Git ou o caminho do clone.

`State`

O status do malware. Os valores permitidos são `OBSERVED` | `REMOVAL_FAILED` | `REMOVED`.

No título e na descrição da descoberta, forneça o contexto do que aconteceu com o malware.

Por exemplo, se `Malware.State` for `REMOVED`, o título e a descrição da descoberta deverão refletir que seu produto removeu o malware localizado no caminho.

Se `Malware.State` for `OBSERVED`, o título e a descrição da descoberta deverão refletir que seu produto encontrou esse malware localizado no caminho.

`Type`

Indica o tipo de malware. Os valores permitidos são `ADWARE` | `BLENDED_THREAT` | `BOTNET_AGENT` | `COIN_MINER` | `EXPLOIT_KIT` | `KEYLOGGER` | `MACRO` | `POTENTIALLY_UNWANTED` | `SPYWARE` | `RANSOMWARE` | `REMOTE_ACCESS` | `ROOTKIT` | `TROJAN` | `VIRUS` | `WORM`.

Se você precisar de um valor adicional para `Type`, entre em contato com a equipe do Security Hub.

Network

`Network` é um único objeto. Você não pode adicionar vários detalhes relacionados à rede. Ao mapear os campos, use as diretrizes a seguir.

Informações de destino e origem

O destino e a origem são logs de fluxo TCP ou VPC ou logs WAF fáceis de mapear. Eles são mais difíceis de usar quando você descreve informações de rede referentes à descoberta de um ataque.

Normalmente, a fonte é de onde o ataque se originou, mas pode haver outras fontes, conforme listado abaixo. Você deve explicar a fonte em sua documentação e também descrevê-la no título e na descrição da descoberta.

- Para um ataque DDo S em uma EC2 instância, a origem é o atacante, embora um ataque DDo S real possa usar milhões de hosts. O destino é o IPv4 endereço público da EC2 instância. `Direction`está DENTRO.
- Para malwares observados se comunicando de uma EC2 instância para um nó de comando e controle conhecido, a origem é o IPV4 endereço da EC2 instância. O destino é o nó de comando e controle. `Direction` é `OUT`. Você também forneceria `Malware` e `ThreatIntelIndicators`.

`Protocol`

`Protocol` sempre mapeia para um nome registrado da Internet Assigned Numbers Authority (IANA), a menos que você possa fornecer um protocolo específico. Você deve sempre usar isso e fornecer as informações da porta.

`Protocol` é independente das informações de origem e destino. Só forneça quando fizer sentido.

`Direction`

`Direction`é sempre relativo aos limites da AWS rede.

- `IN`significa que está entrando AWS (VPC, serviço).
- `OUT`significa que está saindo dos limites da AWS rede.

Process

`Process` é um único objeto. Não é possível adicionar vários detalhes relacionados ao processo. Ao mapear os campos, use as diretrizes a seguir.

`Name`

`Name` deve corresponder ao nome do executável. Ele aceita até 64 caracteres.

`Path`

`Path` é o caminho do sistema de arquivos para o executável do processo. Ele aceita até 512 caracteres.

`Pid`, **`ParentPid`**

`Pid` e `ParentPid` deve corresponder ao identificador de processo (PID) do Linux ou ao ID de evento do Windows. Para diferenciar, use EC2 Amazon Machine Images (AMI) para fornecer as informações. Os clientes provavelmente conseguem diferenciar entre Windows e Linux.

Carimbos de data e hora (**`LaunchedAt`** e **`TerminatedAt`**)

Se você não conseguir recuperar essas informações de forma confiável e elas não forem precisas em milissegundos, não as forneça.

Se um cliente usa carimbos de data e hora para a investigação forense, não ter nenhum carimbo de data e hora é melhor do que ter o carimbo de data e hora errado.

ThreatIntelIndicators

`ThreatIntelIndicators` aceita uma matriz de até cinco objetos de inteligência de ameaças.

Para cada entrada, `Type` está no contexto da ameaça específica. Os valores permitidos são `DOMAIN` | `EMAIL_ADDRESS` | `HASH_MD5` | `HASH_SHA1` | `HASH_SHA256` | `HASH_SHA512` | `IPV4_ADDRESS` | `IPV6_ADDRESS` | `MUTEX` | `PROCESS` | `URL`.

Veja alguns exemplos de como mapear indicadores de inteligência de ameaças:

- Você encontrou um processo que sabe que está associado ao Cobalt Strike. Você aprendeu FireEye isso no blog.

  Defina `Type` como `PROCESS`. Crie também um objeto `Process` para o processo.
- Seu filtro de e-mail encontrou alguém enviando um pacote com hash conhecido de um domínio mal-intencionado conhecido.

  Crie dois objetos `ThreatIntelIndicator`. Um objeto é para o `DOMAIN`. O outro é para o `HASH_SHA1`.
- Você encontrou malware com uma regra Yara (Loki, Fenrir, Awss3,). VirusScan BinaryAlert

  Crie dois objetos `ThreatIntelIndicator`. Um é para o malware. O outro é para o `HASH_SHA1`.

Resources

Para `Resources`, use nossos tipos de recursos e campos de detalhes fornecidos sempre que possível. O Security Hub está constantemente adicionando novos recursos ao ASFF. Para receber um log mensal das mudanças no ASFF, entre em contato com `<securityhub-partners@amazon.com.>`

Se você não conseguir ajustar as informações nos campos de detalhes de um tipo de recurso modelado, mapeie os detalhes restantes para `Details.Other`.

Para um recurso que não é modelado no ASFF, defina `Type` como `Other`. Para obter informações detalhadas, use `Details.Other`.

Você também pode usar o tipo de `Other` recurso para não AWS descobertas.

ProductFields

Use somente `ProductFields` se você não puder usar outro campo curado para `Resources` ou um objeto descritivo como `ThreatIntelIndicators`, `Network` ou `Malware`.

Se você usar `ProductFields`, deverá fornecer uma justificativa estrita para essa decisão.

Compliance

Use somente `Compliance` se suas descobertas estiverem relacionadas à conformidade.

O Security Hub usa `Compliance` para as descobertas que gera com base nos controles.

O Firewall Manager usa `Compliance` para as respectivas descobertas porque elas estão relacionadas à conformidade.

Campos restritos

Esses campos são destinados para que os clientes acompanhem a investigação de uma descoberta.

Não mapeie para esses campos ou objetos.

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

- `Workflow`

Para esses campos, mapeie os campos que estão no objeto `FindingProviderFields`. Não mapeie para os campos de nível superior.

- `Confidence`: inclua apenas uma pontuação de confiança (0-99) se seu serviço tiver uma funcionalidade semelhante ou se você confirmar 100% de sua descoberta.
- `Criticality`: a pontuação de criticidade (0-99) tem como objetivo expressar a importância do recurso associado à descoberta.
- `RelatedFindings`: forneça descobertas relacionadas somente se você puder acompanhar as descobertas relacionadas ao mesmo recurso ou tipo de descoberta. Para identificar uma descoberta relacionada, você deve consultar o identificador de uma descoberta que já está no Security Hub.

Diretrizes para o uso da API **`BatchImportFindings`**

Ao usar a operação de `BatchImportFindings`API para enviar descobertas para AWS Security Hub, use as diretrizes a seguir.

- Você deve chamar `BatchImportFindings` usando a conta associada às descobertas. O identificador da conta associada é o valor do atributo `AwsAccountId` para a descoberta.
- Envie o maior lote possível. O Security Hub aceita até 100 descobertas por lote, até 240 KB por descoberta e até 6 MB por lote.
- O limite da taxa de aceleração é de 10 TPS por conta por região, com uma explosão de 30 TPS.
- Você deve implementar um mecanismo para manter o estado das descobertas se existirem problemas de controle de utilização ou de rede. Você também precisa do estado de descoberta para poder enviar atualizações de descoberta à medida que uma descoberta entra e sai da conformidade.
- Para obter informações sobre os tamanhos máximos das strings e outras limitações, consulte AWS Security Finding Format (ASFF) no Guia do usuário do AWS Security Hub .

Lista de verificação de preparação do produto

As equipes AWS Security Hub e os parceiros da APN usam essa lista de verificação para validar se a integração está pronta para ser lançada.

Mapeamento do ASFF

Essas perguntas estão relacionadas ao mapeamento de sua descoberta para o AWS Security Finding Format (ASFF).

Todos os dados de descoberta do parceiro estão mapeados no ASFF?

- Mapeie todas as suas descobertas para o ASFF de alguma forma.
- Use campos selecionados, como tipos de recursos modelados, `Network`, `Malware` ou `ThreatIntelIndicators`.
- Mapeie qualquer outra coisa dentro `Resource.Details.Other` ou `ProductFields` conforme apropriado.

O parceiro usa campos **`Resource.Details`**, como **`AwsEc2instance`**, **`AwsS3Bucket`** e **`Container`**? O parceiro usa **`Resource.Details.Other`** para definir detalhes de recursos que não são modelados no ASFF?

- Sempre que possível, use os campos fornecidos para recursos selecionados, como EC2 instâncias, buckets do S3 e grupos de segurança, em suas descobertas.
- Mapeie outras informações relacionadas aos recursos `Resource.Details.Other` somente quando não houver uma correspondência direta.

O parceiro mapeia valores para **`UserDefinedFields`**?

- Não use `UserDefinedFields`.
- Considere usar outro campo selecionado, como `Resource.Details.Other` ou `ProductFields`.

O parceiro mapeia informações **`ProductFields`** que poderiam ser mapeadas em outros campos do ASFF?

- Use somente `ProductFields` para informações específicas do produto, como informações de versionamento, descobertas de gravidade específicas do produto ou outras informações que não possam ser mapeadas em um campo selecionado ou `Resources.Details.Other`.

O parceiro importa seus próprios carimbos de data e hora para **`FirstObservedAt`**?

- O carimbo de data e hora de `FirstObservedAt` tem como objetivo registrar a hora em que uma descoberta foi observada no produto. Mapeie esse campo, se possível.

O parceiro fornece valores exclusivos gerados para cada identificador de descoberta, exceto para descobertas que ele deseja atualizar?

Todas as descobertas no Security Hub são indexadas no identificador (atributo `Id`) da descoberta. Esse valor deve sempre ser exclusivo para garantir que as descobertas não sejam atualizadas acidentalmente.

Você também deve manter o estado do identificador da descoberta com o objetivo de atualizar as descobertas.

O parceiro fornece um valor que mapeia as descobertas para um ID do gerador?

`GeneratorID` não deve ter o mesmo valor que o ID de descoberta.

`GeneratorID` deve ser capaz de vincular logicamente as descobertas pelo que as gerou.

Isso pode ser um subcomponente de um produto (Produto A: vulnerabilidade versus Produto A: EDR) ou algo semelhante.

O parceiro usa os namespaces de tipos de descoberta necessários de uma forma que seja relevante para seu produto? O parceiro usa as categorias ou classificadores de tipos de descoberta recomendados em seus tipos de descoberta?

A taxonomia do tipo de descoberta deve corresponder estreitamente com as descobertas que o produto gera.

Os namespaces de primeiro nível descritos no Formato de descoberta de AWS segurança são obrigatórios.

Você pode usar valores personalizados para os namespaces de segundo e terceiro níveis (categorias ou classificadores).

O parceiro captura informações de fluxo de rede nos campos **`Network`**, se tiver dados de rede?

Se seu produto capturar NetFlow informações, mapeie-as para o `Network` campo.

O parceiro captura as informações do processo (PID) nos campos **`Process`**, se tiver dados do processo?

Se seu produto capturar informações do processo, mapeie-as para o campo `Process`.

O parceiro captura informações de malware nos campos **`Malware`**, se tiver dados de malware?

Se seu produto capturar informações de malware, mapeie-as para o campo `Malware`.

O parceiro captura informações de inteligência contra ameaças nos campos **`ThreatIntelIndicators`**, se tiver dados de inteligência contra ameaças?

Se seu produto capturar informações de inteligência sobre ameaças, mapeie-as para o campo `ThreatIntelIndicators`.

O parceiro fornece uma classificação de confiança para as descobertas? Se o fizerem, é fornecida uma justificativa?

Sempre que você usar esse campo, forneça uma justificativa em sua documentação e manifesto.

O parceiro usa um ID canônico ou ARN para o ID do recurso na descoberta?

Ao identificar AWS recursos, a melhor prática é usar o ARN. Se um ARN não estiver disponível, use o ID do recurso canônico.

Configuração e função de integração

Essas perguntas estão relacionadas à configuração e à day-to-day função da integração.

O parceiro fornece um modelo infrastructure-as-code (IaC) para implantar a integração com o Security Hub, como o Terraform AWS CloudFormation, ou? AWS Cloud Development Kit (AWS CDK)

Para integrações que enviarão descobertas da conta do cliente ou usarão CloudWatch Eventos para consumir descobertas, é necessária alguma forma de modelo de IaC.

AWS CloudFormation é preferível, mas AWS CDK o Terraform também pode ser usado.

O produto do parceiro tem uma configuração de um clique em seu console para sua integração com o Security Hub?

Alguns produtos parceiros usam uma alavanca ou um mecanismo similar em seus produtos para ativar a integração. Isso pode implicar o provisionamento automático de recursos e permissões. Se você enviar descobertas de uma conta de produto, a configuração com um clique é o método preferido.

O parceiro envia apenas descobertas de valor?

Geralmente, você só deve enviar descobertas que tenham valor de segurança para os clientes do Security Hub.

O Security Hub não é uma ferramenta geral de gerenciamento de logs. Você não deve enviar todos os logs possíveis para o Security Hub.

O parceiro forneceu uma estimativa de quantas descobertas eles enviarão por dia por cliente e com que frequência (média e intermitência)?

Números de descobertas exclusivas são usados para calcular a carga no Security Hub. Uma descoberta única é definida como uma descoberta com um mapeamento ASFF diferente de outra descoberta.

Por exemplo, se uma descoberta preencheu somente `ThreatIntelIndicators` e outra preencheu somente `Resources.Details.AWSEc2Instance`, essas são duas descobertas exclusivas.

O parceiro tem uma maneira elegante de lidar com erros 4xx e 5xx, de forma que eles não sejam limitados e que todas as descobertas possam ser enviadas posteriormente?

Atualmente, há uma taxa de intermitência de 30 a 50 TPS na operação de API `BatchImportFindings`. Se os erros 4xx ou 5xx forem retornados, você deverá manter o estado dessas descobertas malsucedidas para poder repeti-las na totalidade mais tarde. Você pode fazer isso por meio de uma fila de letras mortas ou de outros serviços AWS de mensagens, como Amazon SNS ou Amazon SQS.

O parceiro mantém o estado de suas descobertas para que saiba arquivar as descobertas que não estão mais presentes?

Se você planeja atualizar as descobertas substituindo o ID da descoberta original, deve ter um mecanismo para reter o estado para que as informações corretas sejam atualizadas para a descoberta correta.

Se você fornecer descobertas, não use a operação `BatchUpdateFindings` para atualizar as descobertas. Essa operação só deve ser usada pelos clientes. Você só usa `BatchUpdateFindings` quando investiga e utiliza as descobertas.

O parceiro lida com novas tentativas de uma forma que não comprometa as descobertas bem-sucedidas enviadas anteriormente?

Você deve ter um mecanismo para reter a descoberta original IDs em caso de erros, para não duplicar ou sobrescrever as descobertas bem-sucedidas com erro.

O parceiro atualiza as descobertas chamando a operação **`BatchImportFindings`** com o ID de descoberta existente?

Para atualizar uma descoberta, você deve sobrescrever a descoberta existente enviando o mesmo ID da descoberta.

A operação `BatchUpdateFindings` só deve ser usada pelos clientes.

O parceiro atualiza as descobertas usando a API **`BatchUpdateFindings`**?

Se você agir com base nas descobertas, poderá usar a operação `BatchUpdateFindings` para atualizar campos específicos.

O parceiro fornece informações sobre a quantidade de latência entre a criação de uma descoberta e o envio do produto para o Security Hub?

Você deve minimizar a latência para garantir que os clientes vejam as descobertas o mais rápido possível no Security Hub.

Essas informações são obrigatórias no manifesto.

Se a arquitetura do parceiro é enviar descobertas para o Security Hub por meio de uma conta de cliente, isso é feito com êxito? Se a arquitetura do parceiro for enviar descobertas para o Security Hub por meio de sua própria conta, isso é feito com êxito?

Durante o teste, as descobertas devem ser enviadas com sucesso de uma conta de sua propriedade que seja diferente da conta fornecida para o ARN do produto.

Enviar uma descoberta da conta do proprietário do ARN do produto pode ignorar certas exceções de erro das operações de API.

O parceiro fornece uma descoberta rápida ao Security Hub?

Para mostrar que sua integração está funcionando corretamente, você deve enviar uma descoberta de pulsação. A descoberta da pulsação é enviada a cada cinco minutos e usa o tipo de descoberta `Heartbeat`.

Isso é importante se você enviar descobertas de uma conta de produto.

O parceiro se integrou à conta da equipe de produto do Security Hub durante o teste?

Durante a validação da pré-produção, você deve enviar exemplos de descoberta para a AWS conta da equipe de produto do Security Hub. Esses exemplos demonstram que as descobertas são enviadas e mapeadas corretamente.

Documentação

Essas perguntas estão relacionadas à documentação da integração que você fornece.

O parceiro hospeda sua documentação em um site dedicado?

A documentação deve ser hospedada em seu site como uma página da web estática, wiki, Read the Docs ou outro formato dedicado.

A documentação de hospedagem GitHub não satisfaz os requisitos de um site dedicado.

A documentação do parceiro fornece instruções sobre como configurar a integração do Security Hub?

Você pode configurar a integração usando um modelo de IaC ou uma integração de “um clique” baseada em console.

A documentação do parceiro fornece uma descrição de seu caso de uso?

O caso de uso fornecido no manifesto também deve ser descrito na documentação

A documentação do parceiro fornece uma justificativa para as descobertas que eles enviam?

Você deve fornecer a justificativa para os tipos de descobertas que você envia.

Por exemplo, seu produto pode produzir descobertas sobre vulnerabilidades, malware e antivírus, mas você só envia descobertas de vulnerabilidades e malware para o Security Hub. Nesse caso, você deve fornecer uma justificativa para não enviar descobertas de antivírus.

A documentação do parceiro fornece uma justificativa para as descobertas que eles enviam?

Você deve fornecer a justificativa para o mapeamento da descoberta nativa de um produto para o ASFF. Os clientes querem saber onde procurar informações específicas sobre o produto.

A documentação do parceiro fornece orientação sobre como o parceiro atualiza as descobertas, caso as atualize?

Forneça aos clientes informações sobre como você mantém o estado, garante a idempotência e substitui as descobertas por informações. up-to-date

A documentação do parceiro descreve a descoberta da latência?

Minimize a latência para garantir que os clientes vejam as descobertas o mais rápido possível no Security Hub.

Essas informações são obrigatórias no manifesto.

A documentação do parceiro descreve como sua pontuação de gravidade se relaciona com a pontuação de gravidade do ASFF?

Forneça informações sobre como você mapeia `Severity.Original` para o `Severity.Label`.

Por exemplo, se seu valor de severidade for uma nota por letra (A, B, C), você deve fornecer informações sobre como mapear a nota por letra para a etiqueta de severidade.

A documentação do parceiro fornece uma justificativa para os índices de confiança?

Se você fornecer pontuações de confiança, essas pontuações devem ser classificadas.

Se você usar pontuações de confiança preenchidas estaticamente ou mapeamentos derivados da inteligência artificial ou do machine learning, forneça contexto adicional.

A documentação do parceiro indica quais regiões o parceiro oferece ou não suporte?

Anote as regiões que são ou não compatíveis para que os clientes saibam em quais regiões não devem tentar uma integração.

Informações sobre o cartão do produto

Essas perguntas estão relacionadas ao cartão do produto exibido na página Integrações do console do Security Hub.

O ID da AWS conta fornecido é válido e contém 12 dígitos?

Os identificadores da conta têm 12 dígitos. Se o ID da conta contiver menos de 12 dígitos, o ARN do produto não será válido.

A descrição do produto contém 200 caracteres ou menos?

A descrição do produto fornecida no JSON no manifesto não deve ter mais de 200 caracteres, incluindo espaços.

O link de configuração leva à documentação da integração?

O link de configuração deve levar à sua documentação on-line. Não deve levar ao seu site principal ou a páginas de marketing.

O link de compra (se fornecido) leva ao AWS Marketplace anúncio do produto?

Se você fornecer um link de compra, ele deverá ser para uma AWS Marketplace entrada. O Security Hub não aceita links de compra que não sejam hospedados pela AWS.

As categorias de produtos descrevem corretamente o produto?

No manifesto, você pode fornecer até três categorias de produtos. Eles devem corresponder ao JSON e não podem ser personalizados. Você não pode fornecer mais de três categorias de produtos.

Os nomes da empresa e do produto são válidos e corretos?

O nome da empresa deve ter 16 caracteres ou menos.

O nome do produto deve ter 24 caracteres ou menos.

O nome do produto no JSON do cartão do produto deve corresponder ao nome no manifesto.

Informações de marketing

Essas questões estão relacionadas ao marketing para a integração.

A descrição do produto para a página de parceiros do Security Hub tem menos de 700 caracteres, incluindo espaços?

A página de parceiros do Security Hub só aceita até 700 caracteres, incluindo espaços.

A equipe editará descrições mais longas.

O logotipo da página de parceiros do Security Hub não é maior que 600 x 300 px?

Forneça um URL de acesso público com o logotipo da empresa em PNG ou JPG que não seja maior que 600 x 300 pixels.

O hiperlink Saiba mais na página de parceiros do Security Hub leva à página da web dedicada do parceiro sobre a integração?

O link Saiba mais não deve levar ao site principal do parceiro ou às informações da documentação.

Esse link deve sempre ir para uma página da web dedicada com informações de marketing sobre a integração.

O parceiro fornece uma demonstração ou um vídeo instrutivo sobre como usar sua integração?

Um vídeo passo a passo de demonstração ou integração é opcional, porém é recomendado.

Uma postagem no blog da AWS Partner Network está sendo lançada com o parceiro e seu gerente de desenvolvimento de parceiros ou representante de desenvolvimento de parceiros?

AWS As postagens do blog da Partner Network devem ser coordenadas com antecedência com o gerente de desenvolvimento de parceiros ou o representante de desenvolvimento de parceiros.

Essas publicações são distintas de todas as publicações de blog que você cria por conta própria.

Aguarde um prazo de entrega de quatro a seis semanas. Esse esforço deve ser iniciado após a conclusão do teste com o ARN do produto privado.

Um comunicado de imprensa liderado por um parceiro está sendo lançado?

Você pode trabalhar com seu gerente de desenvolvimento de parceiros ou representante de desenvolvimento de parceiros para obter uma cotação do vice-presidente de serviços de segurança externa. Você pode usar essa citação em seu comunicado à imprensa.

Uma publicação de blog liderada por um parceiro está sendo lançada?

Você pode criar suas próprias publicações no blog para mostrar a integração fora do blog da Rede de Parceiros da AWS .

Um webinar conduzido por parceiros está sendo lançado?

Você pode criar seus próprios webinars para mostrar a integração.

Se você precisar de ajuda da equipe do Security Hub, trabalhe com a equipe de produto depois de concluir o teste com o ARN do produto privado.

O parceiro solicitou suporte nas redes sociais de AWS?

Após seu lançamento, você pode trabalhar com o líder de marketing de AWS segurança para usar os canais AWS oficiais de mídia social para compartilhar detalhes sobre seus webinars.

AWS Security Hub Perguntas frequentes sobre parceiros

A seguir estão perguntas comuns sobre como configurar e manter uma integração com o AWS Security Hub.

1. Quais são os benefícios da integração com o Security Hub?
   - Satisfação do cliente: o principal motivo para a integração com o Security Hub é que você tem solicitações de clientes para fazer isso.

     O Security Hub é o centro de segurança e conformidade para AWS os clientes. Ele foi projetado como a primeira parada em que os profissionais de AWS segurança e conformidade vão todos os dias para entender seu estado de segurança e conformidade.

     Ouça seus clientes. Eles dirão se querem ver suas descobertas no Security Hub.
   - Oportunidades de descoberta: promovemos parceiros com integrações certificadas no console do Security Hub, incluindo links para suas listagens do AWS Marketplace . Essa é uma ótima maneira de os clientes descobrirem novos produtos de segurança.
   - Oportunidades de marketing — Fornecedores com integrações aprovadas podem participar de webinars, emitir comunicados à imprensa, criar planilhas simples e demonstrar suas integrações aos clientes. AWS
2. Que tipos de parceiros existem?
   - Parceiro que enviam descobertas ao Security Hub
   - Parceiro que recebe descobertas do Security Hub
   - Parceiros que enviam e recebem descobertas
   - Parceiros de consultoria que ajudam os clientes a configurar, personalizar e usar o Security Hub no ambiente deles
3. Como a integração de um parceiro com o Security Hub funciona de modo geral?

   Você coleta descobertas de uma conta de cliente ou de sua própria AWS conta e transforma o formato das descobertas no Formato de descoberta AWS de segurança (ASFF). Em seguida, você envia essas descobertas para o endpoint regional apropriado do Security Hub.

   Você também pode usar CloudWatch Eventos para receber descobertas do Security Hub.
4. Quais são as etapas básicas para concluir uma integração com o Security Hub?

   a. Enviar as informações do manifesto do seu parceiro.

b. Receba um produto ARNs para usar com o Security Hub, se você estiver enviando descobertas para o Security Hub.

c. Mapear suas descobertas para o ASFF. Consulte the section called “Diretrizes para mapeamento do ASFF”.

d. Definir sua arquitetura para enviar e receber descobertas do Security Hub. Seguir os princípios descritos em the section called “Princípios para criar e atualizar descobertas”.

e. Criar um framework de implantação para os clientes. Por exemplo, AWS CloudFormation scripts podem servir a esse propósito.

f. Documentar sua configuração e fornecer instruções de configuração para os clientes.

g. Definir quaisquer insights personalizados (regras de correlação) que os clientes possam usar com seu produto.

h. Quanto tempo leva para receber as descobertas do Security Hub?

i. Enviar informações de marketing para aprovação (idioma do site, comunicado à imprensa, slide de arquitetura, vídeo, planilha simples).

5. Qual é o processo para enviar o manifesto de parceiro? E para os serviços da AWS enviarem descobertas ao Security Hub?

   Para enviar as informações do manifesto para a equipe do Security Hub, use `<securityhub-partners@amazon.com>`.

   Você recebe o produto ARNs dentro de sete dias corridos.

6. Que tipos de descoberta devo enviar para o Security Hub?

   Os preços do Security Hub baseiam-se parcialmente no número de descobertas ingeridas. Por esse motivo, você deve evitar enviar descobertas que não agreguem valor aos clientes.

   Por exemplo, alguns fornecedores de gerenciamento de vulnerabilidades só enviam descobertas com uma pontuação do Common Vulnerability Scoring System (CVSS) de 3 ou mais em 10 possíveis.

7. Quais são as diferentes abordagens para eu enviar descobertas para o Security Hub?

   Estas são as principais abordagens:

   - Você envia descobertas de sua própria AWS conta designada usando a `BatchImportFindings`operação.

- Você envia descobertas de dentro da conta do cliente usando a operação `BatchImportFindings`. Você pode usar abordagens assume-role, mas essas abordagens não são obrigatórias.

Para obter diretrizes gerais sobre o uso de `BatchImportFindings`, consulte the section called "Diretrizes para o uso da API `BatchImportFindings`".

8. Como faço para reunir minhas descobertas e enviá-las a um endpoint do Security Hub regional?

   Os parceiros usaram abordagens diferentes para isso, pois é altamente dependente da arquitetura da sua solução.

   Por exemplo, alguns parceiros criam um aplicativo em Python que pode ser implantado como um script. AWS CloudFormation O script reúne as descobertas do parceiro no ambiente do cliente, as transforma no ASFF e as envia para o endpoint regional do Security Hub.

   Outros parceiros criam um assistente completo que oferece ao cliente uma experiência com um único clique para enviar as descobertas para o Security Hub.

9. Como posso saber quando começar a enviar descobertas para o Security Hub?

   O Security Hub oferece suporte à autorização parcial em lote para a operação de API `BatchImportFindings`, para que você possa enviar todas as suas descobertas ao Security Hub para todos os seus clientes.

   Se alguns de seus clientes ainda não se inscreveram no Security Hub, o Security Hub não ingere essas descobertas. Ele ingere apenas as descobertas autorizadas que estão no lote.

10. Quais etapas eu preciso concluir para enviar as descobertas para a instância do Security Hub de um cliente?

    a. Garanta que as políticas corretas do IAM estejam em vigor.

    b. Habilite uma assinatura de produto (políticas de recursos) para as contas. Use a operação de API `EnableImportFindingsForProduct` ou a página Integrações. O cliente pode fazer isso ou você pode usar funções entre contas para agir em nome do cliente.

    c. O `ProductArn` da descoberta dever ser o ARN público do seu produto.

    d. O `AwsAccountId` da descoberta deve ser o ID da conta do cliente.

    e. Certifique-se de que suas descobertas não tenham dados malformados de acordo com o AWS Security Finding Format (ASFF). Por exemplo, os campos obrigatórios são preenchidos e não há valores inválidos.

f. Envie descobertas em lotes para o endpoint regional correto.

11. Quais permissões do IAM devem estar em vigor para que eu envie as descobertas?

As políticas do IAM devem ser configuradas para o usuário ou o perfil do IAM que chama `BatchImportFindings` ou para outras chamadas de API.

O teste mais fácil é fazer isso em uma conta de administrador. Você pode restringi-los a `action: 'securityhub:BatchImportFindings'` e `resource: <productArn and/or productSubscriptionArn>`.

Os recursos na mesma conta podem ser configurados com políticas do IAM sem exigir políticas de recursos.

Para descartar problemas de política do IAM do chamador de `BatchImportFindings`, defina a política do IAM para o chamador da seguinte forma:

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

Verifique se não há nenhuma política `Deny` para o chamador. Depois de fazer com que funcione dessa forma, você pode restringir a política ao seguinte:

```
{
    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. O que é uma assinatura de produto?

Para receber descobertas de um produto parceiro específico, o cliente (ou o parceiro com funções em várias contas trabalhando em nome do cliente) deve estabelecer uma assinatura do produto.

Para fazer isso no console, eles usam a página Integrações. Para fazer por meio da API, eles usam a operação de API `EnableImportFindingsForProduct`.

A assinatura do produto cria uma política de recursos que autoriza que as descobertas do parceiro sejam recebidas ou enviadas pelo cliente. Para obter detalhes, consulte Casos de uso e permissões.

O Security Hub tem os seguintes tipos de política de recursos para parceiros:

- `BATCH_IMPORT_FINDINGS_FROM_PRODUCT_ACCOUNT`
- `BATCH_IMPORT_FINDINGS_FROM_CUSTOMER_ACCOUNT`

Durante o processo de integração do parceiro, você pode solicitar um ou os dois tipos de política.

Com `BATCH_IMPORT_FINDINGS_FROM_PRODUCT_ACCOUNT`, você só pode enviar descobertas para o Security Hub por meio da conta listada no ARN do seu produto.

Com `BATCH_IMPORT_FINDINGS_FROM_CUSTOMER_ACCOUNT`, você só pode enviar descobertas da conta do cliente que se inscreveu com você.

13. Suponha que um cliente tenha criado uma conta de administrador e adicionado algumas contas de membros. O cliente precisa inscrever cada conta de membro comigo? Ou o cliente só se inscreve na conta do administrador e eu posso então enviar descobertas com base nos recursos de todas as contas dos membros?

    Essa pergunta questiona se as permissões foram criadas para todas as contas de membros com base no registro da conta de administrador.

    O cliente deve estabelecer uma assinatura de produto para cada conta. Eles podem fazer isso programaticamente por meio da API.

14. Qual é o ARN do meu produto?

    O ARN do seu produto é o identificador exclusivo que o Security Hub gera para você e que você usa para enviar descobertas. Você recebe um ARN de produto para cada produto que você integra ao Security Hub. O ARN correto do produto deve fazer parte de todas as descobertas enviadas ao Security Hub. As descobertas sem o ARN do produto são descartadas. Esse ARN do produto usa o seguinte formato:

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

Exemplo:

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

Você recebe um ARN de produto para cada região em que o Security Hub está implantado. O ID da conta, a empresa e os nomes dos produtos são determinados pelos envios do manifesto de seu parceiro. Você nunca altera nenhuma informação associada ao ARN do seu produto, exceto o código da região. O código da região deve corresponder à região para a qual você envia as descobertas.

Um erro comum é alterar o ID da conta para corresponder à conta na qual você está trabalhando atualmente. O ID da conta não muda. Você envia um ID de conta “inicial” como parte do envio do manifesto. Esse ID da conta está bloqueado no ARN do seu produto.

Quando o Security Hub é lançado em novas regiões, ele usa automaticamente os códigos de região padrão para gerar seu produto ARNs para essas regiões.

Cada conta também é provisionada automaticamente com um ARN de produto privado. Você pode usar esse ARN para testar a importação de descobertas em sua própria conta de desenvolvimento antes de receber o ARN oficial do produto público.

15. Quanto tempo leva para receber descobertas do Security Hub?

As descobertas devem ser fornecidas no Formato AWS de Conclusão de Segurança (ASFF). Para mais detalhes, consulte AWS Security Finding Format (ASFF) no Guia do usuário do AWS Security Hub .

A expectativa é que todas as informações em suas descobertas nativas sejam totalmente refletidas no ASFF. Campos personalizados, como `ProductFields` e `Resource.Details.Other`, permitem mapear dados que não se encaixam perfeitamente nos campos predefinidos.

16. Qual é o endpoint regional correto a ser usado?

Você deve enviar as descobertas para o endpoint regional do Security Hub associado à conta do cliente.

17. Onde posso encontrar a lista de endpoints regionais?

Consulte a lista de endpoints do Security Hub.

18. Posso enviar descobertas entre regiões?

O Security Hub ainda não suporta o envio de descobertas entre regiões para os AWS serviços nativos, como Amazon GuardDuty, Amazon Macie e Amazon Inspector. Se seu cliente permitir, o Security Hub não impede que você envie descobertas de diferentes regiões.

Nesse sentido, você pode chamar um endpoint regional de qualquer lugar, e as informações de recursos do ASFF não precisam corresponder à região do endpoint. No entanto, o `ProductArn` deve corresponder à região do endpoint.

19. Quais são as regras e diretrizes para enviar lotes de descobertas?

Você pode agrupar até 100 descobertas ou 240 KB em uma única chamada de `BatchImportFindings`. Coloque em fila e agrupe o maior número possível de descobertas até esse limite.

Você pode agrupar um conjunto de descobertas de contas diferentes. No entanto, se alguma das contas do lote não estiver inscrita no Security Hub, o lote inteiro falhará. Essa é uma limitação do modelo básico de autorização do API Gateway.

Consulte the section called “Diretrizes para o uso da API `BatchImportFindings`”.

20. Posso enviar atualizações das descobertas que criei?

Sim, se você enviar uma descoberta com o mesmo ARN do produto e o mesmo ID da descoberta, ela substituirá os dados anteriores dessa descoberta. Observe que todos os dados são sobrescritos, então você deve enviar uma descoberta completa.

Os clientes são medidos e cobrados tanto pelas novas descobertas quanto pelas atualizações das descobertas.

21. Posso enviar atualizações das descobertas que criei?

Sim, se o cliente conceder acesso à operação de API `BatchUpdateFindings`, você poderá atualizar determinados campos usando essa operação. Essa operação foi projetada para ser usada por clientes SIEMs, sistemas de tíquetes e plataformas de orquestração, automação e resposta de segurança (SOAR).

22. Como as descobertas se tornam obsoletas?

O Security Hub torna as descobertas obsoletas 90 dias após a data da última atualização. Após esse período, as descobertas obsoletas são removidas do cluster do Security Hub. OpenSearch

Se você atualizar uma descoberta com o mesmo ID de descoberta e ela estiver desatualizada, outra descoberta será criada no Security Hub.

Os clientes podem usar o CloudWatch Events para retirar as descobertas do Security Hub. Isso permite que todas as descobertas sejam enviadas aos alvos escolhidos pelo cliente.

Em geral, o Security Hub recomenda que você crie descobertas a cada 90 dias e não as atualize indefinidamente.

23. Quais aceleradores o Security Hub implementa?

    O Security Hub acelera as chamadas de `GetFindings` API, pois a abordagem recomendada para acessar as descobertas é usar CloudWatch Eventos.

    O Security Hub não implementa nenhum outro controle de utilização em serviços internos, parceiros ou clientes além daquele imposto pelas invocações do API Gateway e do Lambda.

24. Qual é a pontualidade, a latência SLAs ou as expectativas das descobertas enviadas ao Security Hub pelos serviços de origem?

    O objetivo é ser o mais próximo possível em tempo real, tanto para as descobertas iniciais quanto para as atualizações das descobertas. Você deve enviar as descobertas para o Security Hub dentro de cinco minutos após a criação.

25. Como eu recebo todas as descobertas do Security Hub?

    Para receber descobertas, use um dos métodos a seguir.

    - Todas as descobertas são enviadas automaticamente para CloudWatch Eventos. Um cliente pode criar regras de CloudWatch eventos específicas para enviar descobertas para alvos específicos, como um SIEM ou um bucket S3. Esse recurso substituiu a operação herdada da API `GetFindings`.
    - Use CloudWatch Eventos para ações personalizadas. O Security Hub permite que os clientes selecionem descobertas específicas ou grupos de descobertas no console e tomem medidas com base nelas. Por exemplo, eles podem enviar descobertas para um SIEM, sistema de emissão de tíquetes, plataforma de bate-papo ou fluxo de trabalho de correção. Isso faria parte de um fluxo de trabalho de triagem de alertas que um cliente executa no Security Hub. Essas ações são chamadas de ações personalizadas.

      Quando um usuário seleciona uma ação personalizada, um CloudWatch evento é criado para essas descobertas específicas. Você pode aproveitar esse recurso e criar regras e metas de

CloudWatch eventos para um cliente usar como parte de uma ação personalizada. Observe que esse recurso não é usado para enviar automaticamente todas as descobertas de um determinado tipo ou classe para CloudWatch Eventos. Cabe ao usuário agir com base em descobertas específicas.

Você pode usar as operações da API de ação personalizada`CreateActionTarget`, como, para criar automaticamente ações disponíveis para seu produto (como usar AWS CloudFormation modelos). Você também CloudWatch usaria as operações da API de regras de CloudWatch eventos para criar regras de eventos correspondentes associadas à ação personalizada. Usando AWS CloudFormation modelos, você também pode criar regras de CloudWatch eventos para ingerir automaticamente do Security Hub todas as descobertas ou todas as descobertas com determinadas características.

26. Quais são os requisitos para que um provedor de serviços gerenciados de segurança (MSSP) se torne um parceiro do Security Hub?

    Você deve demonstrar como o Security Hub é usado como parte da prestação de serviços aos clientes.

    Você deve ter a documentação do usuário que explique o uso do Security Hub.

    Se o MSSP for um provedor de descoberta, ele deverá demonstrar o envio das descobertas para o Security Hub.

    Se o MSSP receber apenas descobertas do Security Hub, ele deverá, no mínimo, ter um AWS CloudFormation modelo para configurar as regras de CloudWatch eventos apropriadas.

27. Quais são os requisitos para que um parceiro de consultoria da APN que não seja MSSP se torne um parceiro do Security Hub?

    Se você for um parceiro de consultoria da APN, é possível se tornar um parceiro do Security Hub. Você deve enviar dois estudos de caso particulares sobre como você ajudou um cliente específico a:

    - Configurar o Security Hub com as permissões do IAM que o cliente precisa.
    - Conectar soluções de provedores de software independentes (ISV) já integradas ao Security Hub usando as instruções de configuração na página do parceiro no console.
    - Realizar integrações personalizadas de produtos.
    - Criar insights personalizados relevantes para as necessidades e conjuntos de dados do cliente.
    - Criar ações personalizadas.

- Criar manuais de correção.
- Criar guias de início rápido alinhados aos padrões de conformidade do Security Hub. Eles devem ser validados pela equipe do Security Hub.

Os nomes de compilações não precisam ser exclusivos.

28. Quais são os requisitos com relação a como eu implanto minha integração com o Security Hub com meus clientes?

    As arquiteturas de integração entre o Security Hub e os produtos de parceiros variam de parceiro para parceiro em termos de como a solução desse parceiro é operada. Você deve garantir que o processo de configuração da integração não demore mais do que 15 minutos.

    Se você estiver implantando software de integração no AWS ambiente do cliente, deverá utilizar AWS CloudFormation modelos para simplificar a integração. Alguns parceiros criaram uma integração com um clique, o que é altamente recomendável.

29. Quais são meus requisitos de documentação?

    Você deve fornecer um link para a documentação que descreva o processo de integração e configuração entre seu produto e o Security Hub, incluindo o uso de AWS CloudFormation modelos.

    Essa documentação também deve incluir informações sobre o uso do ASFF. Especificamente, isso deve listar os tipos de descoberta do ASFF que você está usando para suas diferentes descobertas. Se você usar as credenciais do, recomendamos que também as mude regularmente.

    Considere incluir outras informações possíveis:

    - Seu caso de uso para integração com o Security Hub
    - Volume médio de descobertas enviadas
    - Sua arquitetura de integração
    - As regiões às quais você atende e não atende
    - Latência entre o momento em que as descobertas são criadas e o momento em que são enviadas ao Security Hub
    - Se você atualiza as descobertas

30. O que são insights personalizados?

É recomendável que você defina insights personalizados para suas descobertas. Os insights são regras de correlação leves que ajudam o cliente a priorizar quais descobertas e recursos mais exigem atenção e ação.

O Security Hub tem uma operação de API `CreateInsight`. Você pode criar insights personalizados dentro de uma conta de cliente como parte do seu AWS CloudFormation modelo. Esses insights aparecem no console do cliente.

31. Posso enviar widgets do painel?

    Não neste momento. Você só pode criar insights gerenciados.

32. Qual é o seu modelo de preços?

    Veja as informações de preço do Security Hub.

33. Como faço para enviar as descobertas para a conta de demonstração do Security Hub como parte do processo final de aprovação da minha integração?

    Envie as descobertas para a conta de demonstração do Security Hub usando o ARN do produto fornecido e `us-west-2` como região. As descobertas devem incluir o número da conta de demonstração no campo `AwsAccountId` do ASFF. Para obter o número da conta demo, entre em contato com a equipe do Security Hub.

    Não nos envie dados confidenciais ou informações de identificação pessoal. Esses dados são usados para demonstrações públicas. Quando você nos envia esses dados, você nos autoriza a usá-los em demonstrações.

34. Quais mensagens de erro ou de sucesso **`BatchImportFindings`** fornece?

    O Security Hub fornece uma resposta para autorização e uma resposta para `BatchImportFindings`. Mais mensagens atualizadas de sucesso, insucesso e erro estão em desenvolvimento.

35. Por qual tratamento de erros o serviço de origem é responsável?

    Os serviços de origem são responsáveis por todo o tratamento de erros. Eles devem lidar com mensagens de erro, novas tentativas, controle de utilização e alarmes. Eles também devem lidar com o feedback ou as mensagens de erro enviadas pelo mecanismo de feedback do Security Hub.

36. Quais são algumas soluções para problemas comuns?

Uma `AuthorizerConfigurationException` é causada por uma malformação de `AwsAccountId` ou `ProductArn`.

Após a refragmentação, observe o seguinte:

- `AwsAccountId` deve ter exatamente 12 dígitos.
- `ProductArn`deve estar no seguinte formato: arn:aws:securityhub: ::product//*<us-west-2 or us-east-1><accountId><company-id><product-id>*

  O ID da conta não muda em relação ao que a equipe do Security Hub incluiu no produto ARNs que eles forneceram a você.

`AccessDeniedException` é causada quando uma descoberta é enviada para ou da conta errada, ou quando a conta não tem uma `ProductSubscription`. A mensagem de erro conterá um ARN com um tipo de recurso de `product` ou `product-subscription`. Esse erro ocorre somente durante chamadas entre contas. Se você chamar `BatchImportFindings` com sua própria conta para a mesma conta em `AwsAccountId` e `ProductArn`, a operação usará políticas do IAM e não tem nada a ver com `ProductSubscriptions`.

Certifique-se de que a conta do cliente e a conta do produto que você usa sejam as contas registradas reais. Alguns parceiros usaram um número de conta do ARN do produto para o produto, mas tentam usar uma conta totalmente diferente para chamar `BatchImportFindings`. Em outros casos, eles criaram `ProductSubscriptions` para outras contas de clientes ou até mesmo para sua própria conta de produto. Eles não criaram `ProductSubscriptions` para a conta do cliente para a qual tentaram importar as descobertas.

37 Para onde envio perguntas, comentários e bugs?

`<securityhub-partners@amazon.com>`

38 Para qual região eu envio descobertas de itens relacionados a serviços da AWS globais? Por exemplo, para onde envio as descobertas relacionadas ao IAM?

Envie as descobertas para a mesma região em que a descoberta foi detectada. Para um serviço como o IAM, sua solução provavelmente encontrará o mesmo problema de IAM em várias regiões. Nesse caso, a descoberta é enviada para todas as regiões em que o problema foi detectado.

Se o cliente executa o Security Hub em três regiões e o mesmo problema de IAM for detectado nas três regiões, envie a descoberta para as três regiões.

Quando um problema for resolvido, envie a atualização da descoberta a todas as regiões para as quais você enviou a descoberta original.

Histórico de documentos do Guia de integração do parceiro

A tabela a seguir descreve as atualizações da documentação do guia.

Alteração	Descrição	Data
Requisitos atualizados para o logotipo do console	As diretrizes do manifesto e do logotipo do parceiro foram atualizadas para indicar que os parceiros devem fornecer uma versão do logotipo no modo claro e no modo escuro para exibição no console do Security Hub. Os logotipos devem estar no formato SVG.	10 de maio de 2021
Os pré-requisitos para novos parceiros de integração foram atualizados	O Security Hub agora também permite parceiros que aderiram ao caminho de parceiros AWS ISV e que usam um produto de integração que concluiu uma revisão técnica AWS básica (FTR). Anteriormente, todos os parceiros de integração precisavam ser parceiros de nível AWS selecionado.	29 de abril de 2021
Novo objeto `FindingProviderFields` no ASFF	Atualizou as informaçõ es sobre o mapeament o de descobertas para o ASFF. Para `Confidence`, `Criticality`, `RelatedFindings`, `Severity` e `Types`, os parceiros mapeiam seus valores para os campos	18 de março de 2021

	em `FindingProviderFields` .	
Novos princípios para criar e atualizar descobertas	Foi adicionado um novo conjunto de diretrizes para criar novas descobertas e atualizar as descobertas existentes no Security Hub.	4 de dezembro de 2020
Versão inicial deste guia	Este Guia de integração de AWS parceiros fornece aos parceiros informações sobre como estabelecer uma integração com AWS Security Hub.	23 de junho de 2020

As traduções são geradas por tradução automática. Em caso de conflito entre o conteúdo da tradução e da versão original em inglês, a versão em inglês prevalecerá.